FLEXera

App Portal / App Broker 2019 R1

Administration Guide

Legal Information

Book Name: App Portal / App Broker 2019 R1 Administration Guide

Part Number: APAB-2019R1-AG00

Product Release Date: March 2019

Copyright Notice

Intellectual Property

Restricted Rights Legend

Contents

1

App Portal / App Broker 2019 R1 Administration Guide

The App Portal / App Broker Administration Guide includes user documentation for both administrators who configure and manage App Portal, and for end users who use the App Portal storefront to request software for their computer or mobile phone.

The App Portal / App Broker 2019 R1 Administration Guide is organized into the following sections:

Table 1-1 • App Portal / App Broker 2019 R1 Administration Guide

Topic	Content
Part 1: App Portal / App Broker System Administration	
Getting Started	Explains what happens the first time you launch the product and are prompted to upload your license file. Also explains how to enter initial deployment technology and integration settings.
Managing Your App Portal Site	Explains how to configure your product website by adjusting the settings on the **Site Management** views.
Managing Your Catalog	Explains how to use the **Catalog Management** views to create and manage catalog items, which are applications/programs that have been published for deployment through the software storefront.
Using App Broker for ServiceNow	Explains how to set up and configure App Broker integration with ServiceNow so that employees can request catalog items—including OS deployment with application migration—from within the ServiceNow user interface.
Using App Broker for BMC	Explains how to integrate App Portal with BMC MyIT so that you can use MyIT as your front end app store, while App Portal performs the behind-the-scenes fulfillment of software requests, including automatically reserving licenses.

Table 1-1 • App Portal / App Broker 2019 R1 Administration Guide (cont.)

Topic	Content
Using Compliance Management Features to Track Software Licensing and Usage	Explains how to use My Apps/Inventory Management and Retire/Upgrade campaigns to track software and computers in use in your company, including license data.
Using Task Sequence Catalog Items to Perform OS and Application Deployment	Explains how to perform OS deployments by offering task sequence catalog items in the App Portal storefront, making your OS deployments self-service instead of administrator-driven.
Using App Survey, Clone/Migrate, and Support Tools to Perform Advanced Deployment Tasks	Explains advanced deployment tasks that you can perform using App Portal that do not involve the checkout of an OSD task sequence catalog item in the App Portal storefront, including using App Survey to migrate applications from a source to target computer, and using Clone/Migrate to migrate applications.
Variables Reference	Lists variables used in App Portal / App Broker.
App Portal API Reference	Describes App Portal's API for web services.
App Broker REST API Reference	Describes App Broker's REST API for web services used to integrate with ServiceNow, BMC MyIT, and other ITSM systems.
Troubleshooting	Lists topics that help you troubleshoot App Portal issues you may encounter.
Part 2: Using the App Portal Enterprise App Store	
Requesting Catalog Items	Explains how to submit requests for catalog items for software or other assets on the **Browse Catalog** tab. After searching the catalog, you can either perform an express checkout of a single item or a standard checkout of multiple items.
Viewing Request Status and Details	Explains how to view information on submitted requests on the **Request Details** view.
Approving or Rejecting Requests on the Approve/Reject Tab	Explains how to approve, reject, reassign, and request additional information regarding submitted catalog item requests.
Using the My Apps Tab to Manage Your Applications and Software Policy Score™	Explains how to use the **My Apps** tab of view a list of applications installed on your computer, view your Software Policy Score™, and respond to unused software and other alerts regarding those applications.

Important • This document does not cover how to use, manage, or install System Center Configuration Manager or Symantec Altiris Client Management Suite or any other deployment technology.

Using Help

When you have questions about App Portal, first consult the App Portal / App Broker user documentation.

Company-Specific User Documentation

To view user documentation specific to your organization's App Portal app store, click the help icon in the navigation bar to open the **Help** tab.
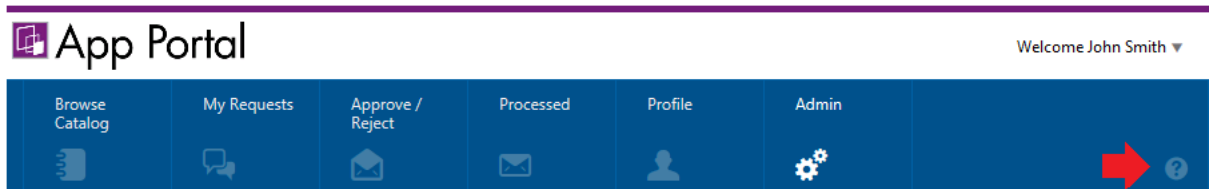
Figure 1-1: Opening User Documentation from the Navigation Menu

The **Help** tab can be customized to provide specialized App Portal / App Broker help for your organization. See Editing the Help Tab Content for instructions.

App Portal / App Broker User Documentation

To view the App Portal / App Broker user documentation, click **App Portal Help** from the login name menu (from any tab).
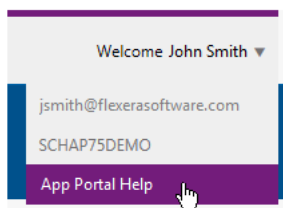
Figure 1-2: Opening User Documentation from the Login Name Menu

When you click on **App Portal Help**, the **App Portal / App Broker User Documentation** page opens:

http://helpnet.flexerasoftware.com/appportal/index.htm

The **App Portal User Documentation** page provides links to open the following documents:

- App Portal / App Broker Administration Guide

- App Portal / App Broker Installation Guide

- App Portal / App Broker Release Notes

These documents are available in both PDF and HTML format.

Contacting Us

Flexera Software is headquartered in Itasca, Illinois, and has offices worldwide. To contact us or to learn more about our products, visit our website at:

http://www.flexerasoftware.com

Part 1

App Portal / App Broker System Administration

The System Administration section of this guide documents relevant information regarding the deployment, configuration, and administration of App Portal / App Broker.

- Getting Started

- Managing Your App Portal Site

- Managing Your Catalog

- Using App Broker for ServiceNow

- Using App Broker for BMC

- Using Compliance Management Features to Track Software Licensing and Usage

- Using Task Sequence Catalog Items to Perform OS and Application Deployment

- Using App Survey, Clone/Migrate, and Support Tools to Perform Advanced Deployment Tasks

- Variables Reference

- App Portal API Reference

- App Broker REST API Reference

- Troubleshooting

2

Getting Started

After you install App Portal / App Broker, as described in the *App Portal / App Broker Installation Guide*, and launch the application for the first time, you will be prompted to specify license and deployment technology information.

You are required to upload the license file before App Portal / App Broker will open for the first time. However, you have the choice of specifying your deployment technology and integration settings upon initial startup or in the App Portal / App Broker administrative user interface under **Site Management > Settings**.

After App Portal is set up, you may also want to periodically view and modify your App Portal user preferences.

- Uploading Your App Portal / App Broker License File

- Specifying Deployment Technology Settings

- Specifying Integration Connection Settings

- About the App Portal Service Account

- Setting User Preferences

Uploading Your App Portal / App Broker License File
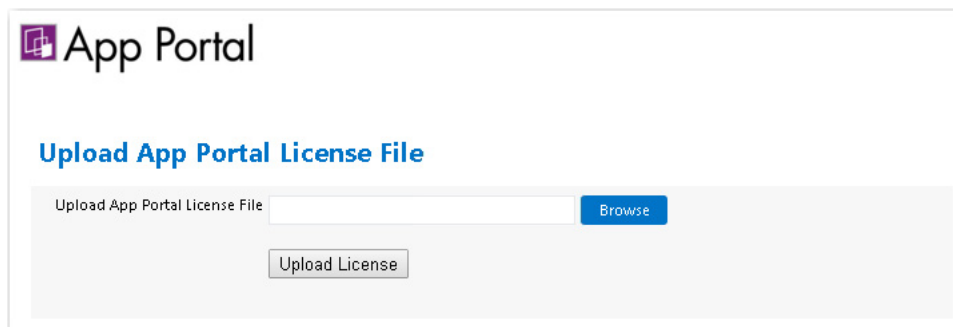
After you install App Portal / App Broker and launch it for the first time, the **Upload App Portal License File** screen opens, prompting you to upload your license file.
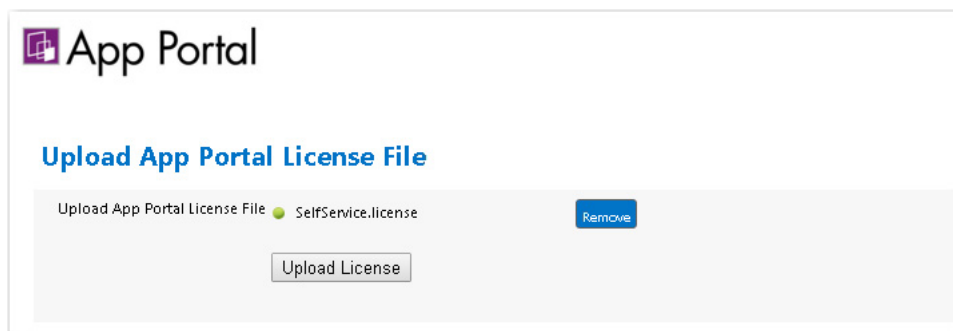
Task   ***To upload an*** App Portal / App Broker ***license file:***

1. If you do not already have an App Portal / App Broker license file, connect to the Flexera Software Product and Licensing Center, download your license file, and store it in a UNC file share that is accessible from the machine where you will be installing App Portal / App Broker.

2. When you launch the application for the first time, the **Upload App Portal License File** page opens.

3.   Click **Browse** and select the license file. The license file name now appears in the text box.
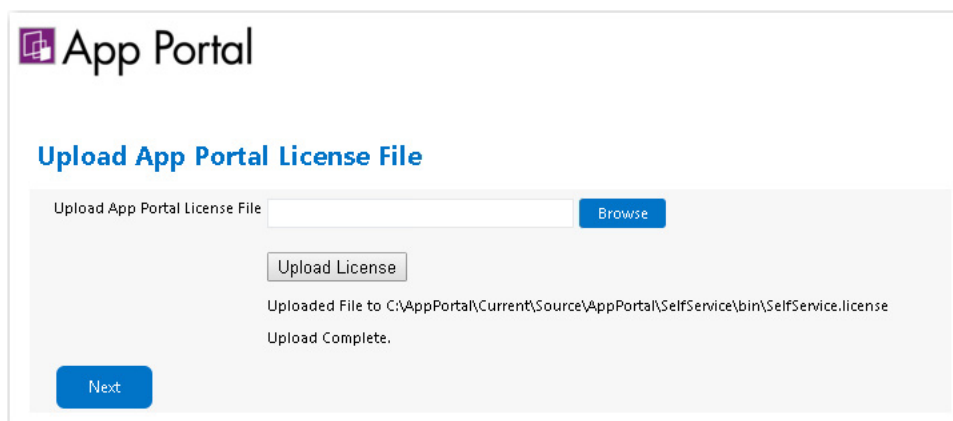
4.   Click **Upload License**. The license file is copied to the following location on the App Portal / App Broker machine:

C:\Program Files (x86)\Flexera Software\App Portal\Web\bin

After the license file has been successfully uploaded, a **Next** button is displayed:

5.   Click **Next** and continue with the steps in Specifying Deployment Technology Settings.

Specifying Deployment Technology Settings

After you have launched App Portal / App Broker for the first time and uploaded the license file, as described in Uploading Your App Portal / App Broker License File, you are then prompted to specify the connection settings for your deployment technology.

You are not required to enter your deployment technology settings at this time. You could skip this step and launch the application, and then specify the deployment settings on the **Site Management > Settings > Deployment** view.

However, if you choose to specify your deployment technology on these initial configuration screens, App Portal / App Broker will be able to automatically set some System Center Configuration Manager settings, including the **Reporting Path** and **Path to inboxes** fields, the System Center Configuration Manager view to use to read the user/computer relationship, and the default success statuses in the **SCCM Status ID Mapping** area.

- Entering System Center Configuration Manager (Current Branch) Settings at Initial Start Up

- Entering System Center 2012 Configuration Manager Settings at Initial Start Up

- Entering Altiris Client Management Suite Settings at Initial Start Up

- Entering AirWatch Settings at Initial Start Up

- Entering Casper Settings at Initial Start Up

- Entering MobileIron Settings at Initial Startup

*Note • You are not required to enter these settings upon initial start up. You can enter or edit these settings at any time by opening the **Deployment** subview of the **Site Management > Settings** view.*

Entering System Center Configuration Manager (Current Branch) Settings at Initial Start Up

To connect App Portal / App Broker to System Center Configuration Manager (Current Branch), you can, optionally, enter settings on the **ConfigMgr** tab of the **Deployment Configuration** screen which opens at initial start up after you have uploaded your license file.

*Note • You can also specify System Center Configuration Manager (Current Branch) deployment settings at any time on the **ConfigMgr** tab of the **Site Management > Settings > Deployment** view.*

To enter System Center Configuration Manager (Current Branch) connection settings upon initial start up of App Portal / App Broker, perform the following steps:

📋

Task   *To enter System Center Configuration Manager (Current Branch) connection settings:*

1. Perform the steps in Uploading Your App Portal / App Broker License File and click **Next**. The **ConfigMgr** tab of the **Deployment Configuration** screen opens.

2. In the **Central Site Server** field, enter the machine name of the System Center Configuration Manager server.

3. In the **Central Site Database Server** field, enter the machine name where the System Center Configuration Manager server database resides.

4. In the **Central Site Database Name** field, enter the database name of the System Center Configuration Manager server database.

5. In the **Central Site Code** field, enter the site code of the System Center Configuration Manager server (in SITE_XXX format).

6. Specify the **User / Computer relationship** that App Portal / App Broker needs to use by selecting one of the following options:

   • **Use SCCM last logon user**—The user to computer relationship will use SMS last logon user.

   • **Use SCCM Primary Console Usage**—Makes use of the System Center Configuration Manager / SMS SP3 feature of tracking login duration to determine primary machine usage

   • **Use AD Computer Managed By**—Uses the AD Computer object "Managed By" attribute to determine the primary user of the computer. This setting requires inventory of the "ManagedBy" AD attribute in System Center Configuration Manager System Discovery.

   • **Use User Affinity**—In System Center 2012 Configuration Manager, you can directly define the users for a computer and the computers for a user. The option could also be referred to as "Use System Center 2012 Configuration Manager user and device assignment".

7. Click **Test** to test the connection settings that are entered.

8. Proceed with setting additional deployment technology settings on the other tabs of the **Deployment Configuration** screen, if desired.

9. Click **Next** to continue. If you have entered connection settings for more than one deployment technology, the **Syncing Configuration** panel opens.

10. From the **Syncing Users** list, select the deployment technology that App Portal / App Broker should use to sync users using built-in sync queries:

   - **Not Defined**

   - **ConfigMgr**

   - **SCCM 2012**

   - **Altiris**

   *Important • If you are going to specify a custom user sync connection string in the **Custom User Sync Settings** area of the **Common** tab of the **Site Management > Settings > Deployment** view, set this field to **Not Defined**.*

11. From the **Syncing Computers** list, select the deployment technology that App Portal / App Broker should use to sync computers using built-in sync queries:

   - **Not Defined**

   - **ConfigMgr**

   - **SCCM 2012**

   - **Altiris**

   *Important • If you are going to specify a custom computer sync connection string in the **Custom Computer Sync Settings** area of the **Common** tab of the **Site Management > Settings > Deployment** view, set this field to **Not Defined**.*

12. Click **Next** to continue.

13. Proceed with the steps in Specifying Integration Connection Settings.

Entering System Center 2012 Configuration Manager Settings at Initial Start Up

To connect App Portal / App Broker to System Center 2012 Configuration Manager, you can, optionally, enter settings on the **SCCM 2012** tab of the **Deployment Configuration** screen which opens at initial start up after you have uploaded your license file.

Note • You can also specify System Center 2012 Configuration Manager deployment settings at any time on the SCCM 2012 tab of the Site Management > Settings > Deployment view.

To enter System Center 2012 Configuration Manager connection settings upon initial start up of App Portal / App Broker, perform the following steps:

Task   *To enter System Center 2012 Configuration Manager connection settings:*

1. Perform the steps in Uploading Your App Portal / App Broker License File and click **Next**. The **SCCM 2012** tab of the **Deployment Configuration** screen opens.

2. In the **Central Site Server** field, enter the machine name of the System Center 2012 Configuration Manager server.

3. In the **Central Site Database Server** field, enter the machine name where the System Center 2012 Configuration Manager server database resides.

4.   In the **Central Site Database Name** field, enter the database name of the System Center 2012 Configuration Manager server database.

5.   In the **Central Site Code** field, enter the site code of the System Center 2012 Configuration Manager server (in SITE_XXX format).

6.   Specify the **User / Computer relationship** that App Portal / App Broker needs to use by selecting one of the following options:

•   **Use SCCM last logon user**—The user to computer relationship will use SMS last logon user.

•   **Use SCCM Primary Console Usage**—Makes use of the System Center Configuration Manager / SMS SP3 feature of tracking login duration to determine primary machine usage

•   **Use AD Computer Managed By**—Uses the AD Computer object "Managed By" attribute to determine the primary user of the computer. This setting requires inventory of the **"ManagedBy"** AD attribute in System Center Configuration Manager System Discovery.

•   **Use User Affinity**—In System Center 2012 Configuration Manager, you can directly define the users for a computer and the computers for a user. The option could also be referred to as "Use System Center 2012 Configuration Manager user and device assignment".

7.   Click **Test** to test the connection settings that are entered.

8.   Proceed with setting additional deployment technology settings on the other tabs of the **Deployment Configuration** screen, if desired.

9.   Click **Next** to continue. If you have entered connection settings for more than one deployment technology, the **Syncing Configuration** panel opens.

10. From the **Syncing Users** list, select the deployment technology that App Portal / App Broker should use to sync users using built-in sync queries:

•   **Not Defined**

•   **ConfigMgr**

•   **SCCM 2012**

- **Altiris**

Important • *If you are going to specify a custom user sync connection string in the* **Custom User Sync Settings** *area of the* **Common** *tab of the* **Site Management > Settings > Deployment** *view, set this field to* **Not Defined**.

11. From the **Syncing Computers** list, select the deployment technology that App Portal / App Broker should use to sync computers using built-in sync queries:

- **Not Defined**

- **ConfigMgr**

- **SCCM 2012**

- **Altiris**

Important • *If you are going to specify a custom computer sync connection string in the* **Custom Computer Sync Settings** *area of the* **Common** *tab of the* **Site Management > Settings > Deployment** *view, set this field to* **Not Defined**.

12. Click **Next** to continue.

13. Proceed with the steps in Specifying Integration Connection Settings.

Entering Altiris Client Management Suite Settings at Initial Start Up

To connect App Portal / App Broker to Altiris Client Management Suite, you can, optionally, enter settings on the **Altiris** tab of the **Deployment Configuration** screen which opens at initial start up after you have uploaded your license file.

Note • *You can also specify Altiris Client Management Suite deployment settings at any time on the* **Altiris** *tab of the* **Site Management > Settings > Deployment** *view.*

To enter Altiris connection settings upon initial start up of App Portal / App Broker, perform the following steps:

Task   **To enter Altiris connection settings:**

1. Perform the steps in Uploading Your App Portal / App Broker License File and click **Next**. The **Deployment Configuration** screen opens.

2. Open the **Altiris** tab.

3. In the **Central Site Server** field, enter the machine name of the Altiris Notification Server.

    Tip • Make sure that ASDK is installed on this machine.

4. In the **Central Site Database Server** field, enter the machine name where the Altiris Notification Server database resides.

5. In the **Central Site Database Name**, enter the database name of the Altiris Notification Server database.

6. Specify the **User / Computer relationship** that App Portal / App Broker needs to use by selecting one of the following options:

    ● **Use last logon user**

    ● **Use User Affinity** (primary device assigned to user)

7. In the **Computer Collection Folder** field, enter the name of the folder to use to create App Portal / App Broker computer filters.

8. In the **User Collection Folder** field, enter the name of the folder to use to create App Portal / App Broker user filters.

9. In the **Advertisement Folder** field, enter the name of the folder to use to create App Portal / App Broker advertisements.

10. Click **Test** to test the connection settings that are entered.

11. Proceed with setting additional deployment technology settings on the other tabs of the **Deployment Configuration** screen, if desired.

12. Click **Next** to continue. If you have entered connection settings for more than one deployment technology, the
Syncing Configuration panel opens.

13. From the **Syncing Users** list, select the deployment technology that App Portal / App Broker should use to sync users
using built-in sync queries:

- **Not Defined**

- **ConfigMgr**

- **SCCM 2012**

- **Altiris**

*Important • If you are going to specify a custom user sync connection string in the **Custom User Sync Settings** area of
the **Deployment > Common** subtab of the **Site Management > Settings** view, set this field to **Not Defined**.*

14. From the **Syncing Computers** list, select the deployment technology that App Portal / App Broker should use to sync
computers using built-in sync queries:

- **Not Defined**

- **ConfigMgr**

- **SCCM 2012**

- **Altiris**

*Important • If you are going to specify a custom computer sync connection string in the **Custom Computer Sync
Settings** area of the **Deployment > Common** subtab of the **Site Management > Settings** view. tab of the set this field to
Not Defined.*

15. Click **Next** to continue.

16. Proceed with the steps in Specifying Integration Connection Settings.

Entering AirWatch Settings at Initial Start Up

To connect App Portal / App Broker to an AirWatch instance, you can, optionally, enter settings on the **AirWatch** tab of the **Deployment Configuration** screen which opens at initial start up after you have uploaded your license file.

*Note • You can also specify AirWatch deployment settings at any time on the **AirWatch** tab of the **Site Management > Settings > Deployment** view.*

To enter AirWatch connection settings upon initial start up of App Portal / App Broker, perform the following steps:

Task   ***To enter AirWatch connection settings:***

1. Perform the steps in Uploading Your App Portal / App Broker License File and click **Next**. The **Deployment Configuration** screen opens.

2. Open the **AirWatch** tab.

3. In the **AirWatch URL** field, enter the URL to your instance of AirWatch.

4. Enter the **User Name** and **Password** to your AirWatch instance.

5. Enter the **API Key** that was provided to you by AirWatch.

6. Click **Test** to test connection settings.

Note • AirWatch users (which are based upon an email address) and are synced to App Portal / App Broker at the same time that the System Center Configuration Manager / Altiris users and are synced. App Portal / App Broker users are matched with System Center Configuration Manager / Altiris users by having the same email address.

7. Proceed with setting additional deployment technology settings on the other tabs of the **Deployment Configuration** screen, if desired.

8. Click **Next** to continue.

9. Proceed with the steps in Specifying Integration Connection Settings.

Entering Casper Settings at Initial Start Up

With App Portal, you can deliver a universal enterprise app store that includes both Windows and OS X desktop applications. You can connect App Portal to a JAMF Casper Suite 9.6.4 server and create catalog items for OS X desktop applications. This gives you license compliance, deployment automation, and control.

To connect App Portal / App Broker to a Casper server, you can, optionally, enter settings on the **Casper** tab of the **Deployment Configuration** screen which opens at initial start up after you have uploaded your license file.

Important • In order for App Portal to be successfully integrated with Casper, your Casper account needs to have a specific set of minimum permissions. For more information, see Required Casper Account Permissions.

Note • You can also specify Casper deployment settings at any time on the Casper tab of the Site Management > Settings > Deployment view.

Note • App Portal and Casper communicate using Casper's JSS API. By default, Casper uses port 8443 for inbound SSL traffic to the JSS. You will need to include the port number in the Casper URL when configuring your settings. If you have modified the inbound SSL port within your JSS configuration, specify your custom port number in the Casper URL.

To enter Casper connection settings upon initial start up of *App Portal / App Broker*, perform the following steps:

Task   **To enter Casper connection settings:**

1. Perform the steps in Uploading Your App Portal / App Broker License File and click **Next**. The **Deployment Configuration** screen opens.

2. Open the **Casper** tab. The **Casper Server Details** are listed.

3. In the **Casper URL** field, enter the URL to your Casper server.

4. Enter the **User Name** and **Password** to your Casper server.

5. In the **App Portal policy folder** field, enter the folder/category in Casper under which the policies created by App Portal / App Broker will reside.

6. In the **Policy template name** field, enter the name of the policy in Casper which can be used as a template.

7. In the **Computer group template name** field, enter the name of the static group in Casper which can be used as a template.

8. Click **Test** to test connection settings.

Note • Casper users (which are based upon an email address) and are synced to App Portal / App Broker at the same time that the System Center Configuration Manager / Altiris users and are synced. App Portal / App Broker users are matched with System Center Configuration Manager / Altiris users by having the same email address.

9. Proceed with setting additional deployment technology settings on the other tabs of the **Deployment Configuration** screen, if desired.

10. Click **Next** to continue.

11. Proceed with the steps in Specifying Integration Connection Settings.

Required Casper Account Permissions

Important • *The Casper account requires full admin access and Administrator privileges in Casper Account settings. If not provided, then the Casper integration with App Portal results in a 401 unauthorized error.*

In order for App Portal to be successfully integrated with Casper, your Casper account needs to have a specific set of minimum permissions. To define permissions on your Casper account, perform the following steps:

Task   *To set required permissions on your Casper account:*

1. Launch Casper and login using your Casper account.
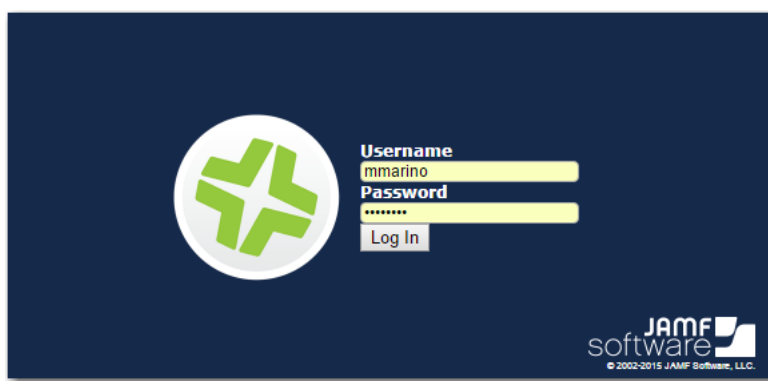
2. On the Casper home page, click the Settings "gear" icon at the top right:

    The **System Settings** tab opens.
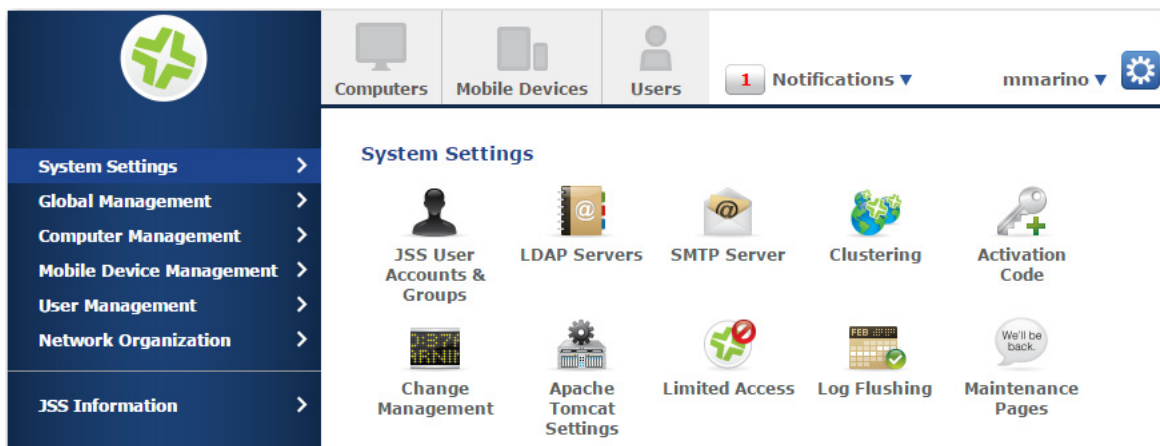
3. Click **JSS User Accounts & Groups**. The **JSS User Accounts & Groups** page opens.
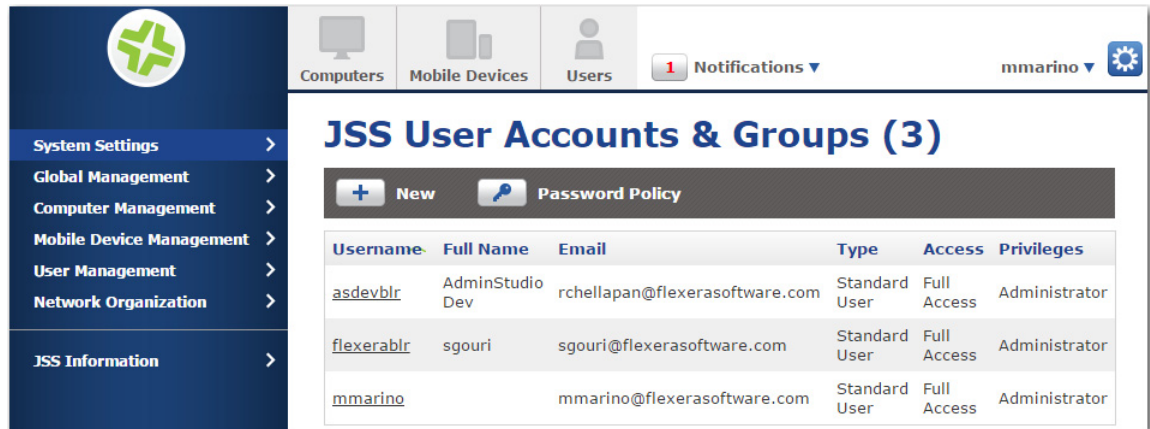
4. Click on the name of your Casper account. The **Account** tab of the account settings page opens.

5. Make sure that **Privilege Set** is set to **Administrator** and that **Access Status** is set to **Enabled**.

*Note • In some versions of Casper, the **Access Status** field may be named **Access Level**. If so, set **Access Level** to **Full Access**.*

> **Important** • *If your Casper system account does not have* **Administrator** *privileges, then App Portal will be unable to integrate with Casper.*

6. Open the **Privileges** tab. The **JSS Objects** subtab of the **Privileges** tab opens.
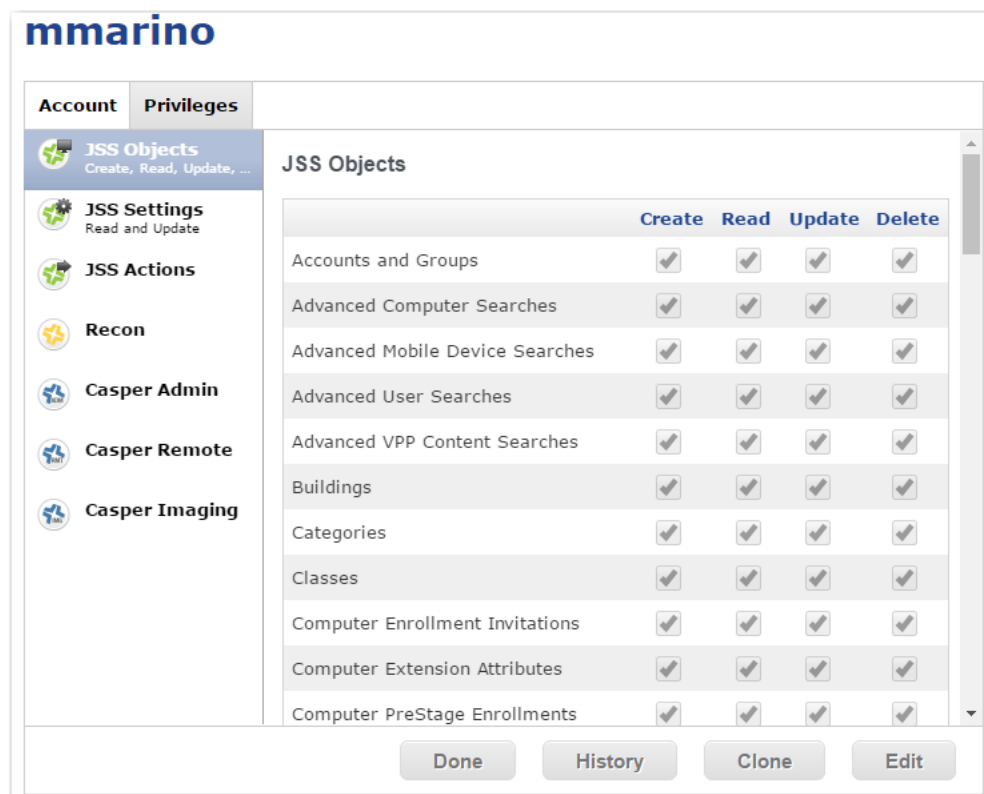
7. On the **JSS Objects** subtab, click **Edit** and make sure that the following permissions are selected:

Object	Permission
Categories	Create
	Read
	Update
Computers	Read
File Share Distribution Points	Read
Packages	Read
Policies	Create
	Read
	Update

Object	Permission
Static Computer Group	Create
	Read
	Update

8. When you are finished selecting permissions, click **Save**.

9. Open the **JSS Settings** subtab.

10. Click **Edit** and make sure that **Read** is selected for **Activation Code**.

11. When you are finished selecting permissions, click **Save**.

API Calls Used by App Portal to Integrate with Casper

Important • *App Portal supports JAMF Casper 9.6.4, On Premises version. Casper on the Cloud is not officially supported. However, you may attempt to integrate with Casper on the Cloud using the API calls described in this section.*

The following is a list of the APIs that App Portal uses to integrate with Casper:

```
<CasperUrl>/JSSResource/computers
<CasperUrl>/JSSResource/computers/subset/basic
<CasperUrl>/JSSResource/users
<CasperUrl>/JSSResource/computergroups
```

```
<CasperUrl>/JSSResource/packages
<CasperUrl>/JSSResource/policies
<CasperUrl>/JSSResource/categories
<CasperUrl>/JSSResource/policies/id/
<CasperUrl>/JSSResource/categories/id/
<CasperUrl>/JSSResource/computergroups/id/0 (POST)
<CasperUrl>/JSSResource/policies/id/0 (POST)
<CasperUrl>/JSSResource/computergroups/id/
<CasperUrl>/JSSResource/categories/name/
<CasperUrl>/JSSResource/categories/id/0 (POST)
<CasperUrl>/JSSResource/computers/name/
<CasperUrl>/JSSResource/packages/id/
<CasperUrl>/JSSResource/distributionpoints
<CasperUrl>/JSSResource/distributionpoints/id/
<CasperUrl>/JSSResource/policies/name/
<CasperUrl>/JSSResource/computergroups/name/
<CasperUrl>/JSSResource/computers/id/{0}/subset/General&Location&Hardware
<CasperUrl>/JSSResource/computers/name/{0}/subset/General&Location
<CasperUrl>/JSSResource/computers/name/{0}/subset/software
```

Note • App Portal does not make any database calls into Casper.

API Descriptions

For details on the purpose of each of the APIs, enter `<CasperUrl>/api`, where `<CasperUrl>` is the URL of your Casper instance.

Entering MobileIron Settings at Initial Startup

You can connect App Portal to a MobileIron server and create catalog items for Apple iOS and Google Android mobile apps. This gives you license compliance, deployment automation, and control.

App Portal imports user information from MobileIron. Once connectivity if configured, and also on a daily basis, App Portal will import users that have managed by MobileIron. App Portal also imports user-to-device relationship for the that are managed by MobileIron.

*Note • You can also specify MobileIron deployment settings at any time on the **MobileIron** tab of the **Site Management > Settings > Deployment** view.*

To enter MobileIron server details, perform the following steps:

Task   ***To enter MobileIron server details at initial startup:***

1. Perform the steps in Uploading Your App Portal / App Broker License File and click **Next**. The **Deployment Configuration** screen opens.

2. Open the **MobileIron** tab. The **MobileIron Server Details** are listed.

3. In the **MobileIron URL** field, enter the URL to your instance of MobileIron.

4. Enter the **User Name** and **Password** to your MobileIron instance.

5. Click **Test** to test connection settings. If successful, the following message is displayed:

```
MobileIron Server settings are valid.
```

Specifying Integration Connection Settings

You can, optionally, enter Flexera Service Gateway, FlexNet Manager Suite, and FlexNet Manager Suite Database Connection settings on the **Integration Settings** screen which opens at initial start up after you have uploaded your license file.

*Note • You can also specify integration connection settings at any time on the **Site Management > Settings > Flexera Integration** view.*

Task   *To enter integration settings upon initial startup:*

1. Perform the steps in Uploading Your App Portal / App Broker License File and click **Next**. The **Deployment Configuration** screen opens.

2. Perform the steps in Specifying Deployment Technology Settings and click **Next**. The **Integration Settings** screen opens.

3. If you have also purchased FlexNet Manager Suite, you can use App Portal / App Broker to manage application licenses. App Portal / App Broker communicates with FlexNet Manager Suite via the Flexera Service Gateway component. To connect App Portal / App Broker to the Flexera Service Gateway, enter the name of your Flexera Service Gateway server in the F**lexera Service Gateway Server Name** field.

4. If you are integrating App Portal / App Broker with FlexNet Manager Suite Cloud, enter the access token that was provided by your system administrator in the **FlexNet Manager Suite Cloud Access Token** field.

5. If you are integrating App Portal / App Broker with FlexNet Manager Suite On Premises, and your App Portal / App Broker system account does not have access to FlexNet Manager Suite On Premises, enter a **Username** (domain\username) and **Password** with appropriate credentials.

6. In order to use the **My Apps** feature, the App Portal system account needs to have read access to the FlexNet Manager Suite database. First, enter the **Database Server Name** and **Database Name** of the FlexNet Manager Suite database in the **FlexNet Manager Suite Database Connection Settings** area. Then, use Microsoft SQL Server Management Studio and give the App Portal system account read access to this database.

7. Click **Test** to test these connection settings.

8. Click **Next**. The **Ready to Save** panel opens, listing a summary of your settings.

9. Click **Save** to save these connection settings. The following message is displayed:

    ```
    Successfully added configuration details
    ```

10. Click **OK**. The **Admin** tab of App Portal / App Broker opens, where you can add additional site settings, as described in Managing Your App Portal Site.

About the App Portal Service Account

Prior to installing App Portal / App Broker, you need to identify and configure an App Portal / App Broker service account. This service account will be used for App Portal / App Broker's interaction with SQL Server and Active Directory.

- App Portal / App Broker Service Account Required Permissions

- Required Updates if the Password of the App Portal Service Account Changes

App Portal / App Broker Service Account Required Permissions

The App Portal / App Broker requires the following permissions:

Table 2-1 • Required Permissions for App Portal / App Broker Service Account

Entity	Required Permissions
SQL Server	System administrator (SysAdmin) permission, including permission to create the App Portal / App Broker database.
System Center Configuration Manager / Altiris Database	Full administrator access, including read (db_datareader) and EXECUTE access on the Microsoft System Center Configuration Manager or Altiris Client Management database in SQL.
App Portal / App Broker Database	DBO permission on the App Portal / App Broker database, including read/write permission.
Client Workstations	Whether or not the App Portal / App Broker service account requires administrative permissions on the client workstations depends upon the deployment technology that you are using. • **System Center 2012 Configuration Manager or System Center Configuration Manager (Current Branch)**—The App Portal / App Broker service account does not require administrative permissions on the client workstations. • **Altiris**—The App Portal / App Broker service account requires full administrative permissions on the client workstations. These permissions are used by App Portal / App Broker to run machine policy evaluation for accelerated software deployments and rerunning advertisements as necessary. They are also used if client-side commands and actions have been created within App Portal / App Broker.

Important • The App Portal / App Broker service account must continue to have these permissions even after the installation is complete.

Required Updates if the Password of the App Portal Service Account Changes

If you change the password of the App Portal service account after you have installed App Portal, you need to also update the password for both the **ESDService** Windows Service and the **SelfService** application pool in IIS.

Table 2-2 • Required Updates if Password of App Portal Service Account Changes

Location	Steps to Take
ESDService Windows Service	You need to update the App Portal service account password on the **ESDService** Windows Service on the App Portal web server. *To update the password on the ESDService Windows Service:* 1. On the App Portal web service, open the Services Microsoft Management Console. 2. Select the **ESDService** in the list and double-click to open the **Properties** dialog box. 3. Open the **Log On** tab and update the password.
SelfService Application Pool in IIS	You need to update the App Portal service account password on the SelfService application pool in IIS on the App Portal server. *To update the password on the SelfService application pool in IIS:* 1. On the App Portal web service, launch Internet Information Services (IIS). 2. In the **Connections** tree, select **Application Pools**. 3. In the **Application Pools** list, select **SelfService** and click **Advanced Settings** in the **Actions** menu. 4. Under **Process Model**, click the browse button in the **Identity** field. The **Application Pool Identity** dialog box opens. 5. Click **Set** next to **Custom account**. The **Set Credentials** dialog box opens. 6. Enter the App Portal service account **User name** and **Password** and click **OK** and click **OK** again to close the **Application Pool Identity** dialog box.
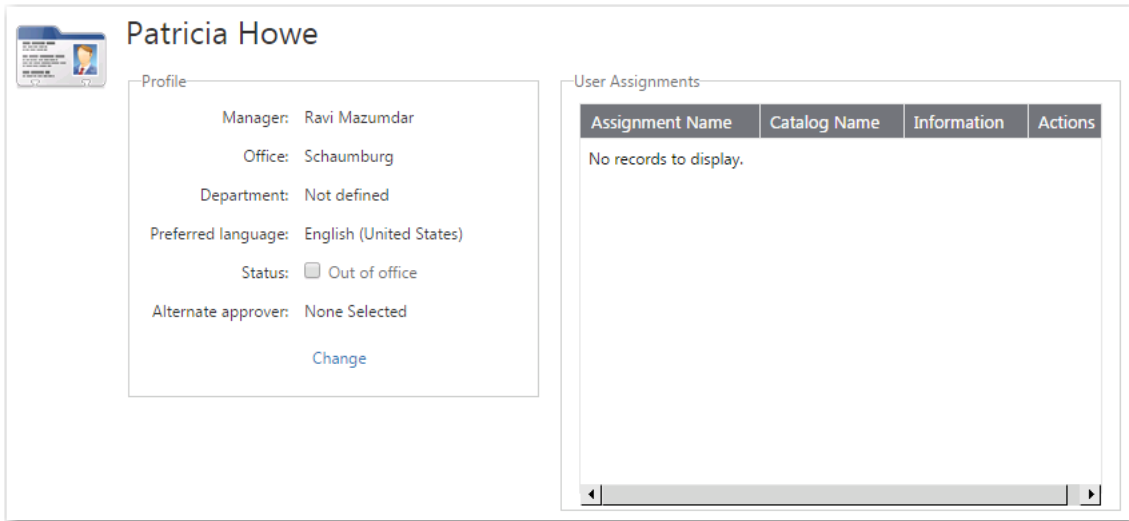
Setting User Preferences

You can view user information and set user preferences on the App Portal **Profile** tab. On the **Profile** tab, you can perform the following tasks:

- Viewing User Information on the User View

- Viewing Categories on the My Categories Tab

- Viewing Readiness Records on the My Readiness Tab

Viewing User Information on the User View

The **Profile > User** tab has two sections: Profile and User Assignments.

Figure 2-1: Profile >User View

Profile

The **Profile** area contains attributes of the user and allows the user to define themselves as **Out of office** as well as specify an **Alternate approver**.

User Assignments

The **User Assignments** area shows catalog items assigned to the user.

- To determine whether an assignment targets a user or a computer depends on the calculation method used in the inventory item.

- Each assignment will display whether it is currently installed and on what systems it is installed on.

- The **Assigned by** value denotes how the assignment was made.

- Assignments can be made as part of an approval process or manually using direct assignments.

Viewing Categories on the My Categories Tab

The **My Categories** view of the **Profile** tab lists all of the catalog categories that you are assigned as the owner of. On the **My Categories** view, category owners can manipulate the applications within their categories.
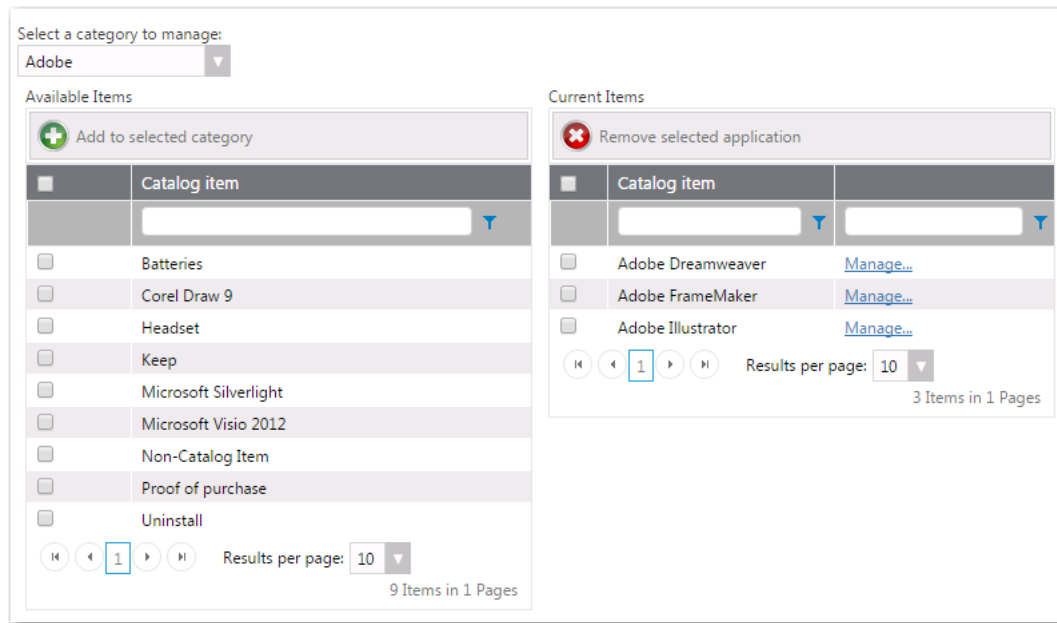
Figure 2-2: Profile > My Categories View

📄

Note • *Category owners are assigned by clicking the **Set Categories Owner** button on the **Categories > Catalog Categories** view under **Site Management** on the **Admin** tab.*

Viewing Readiness Records on the My Readiness Tab

User readiness is used to define records allowing a requester to be defined as "ready" for a catalog item. You use user readiness to inform users using email that they are ready for an item and also restrict the ability to request an item by the presence of a user readiness record.

User readiness records are added to a catalog item that is marked with the **Require User Readiness record?** option in the **Scheduling** options area of the **General > Global** tab of the **Catalog Item Properties** dialog box. User readiness records are added on the **Deployment Management** > **User Readiness** view on the **Admin** tab.

A user's readiness records can be viewed by selecting **My Readiness** on the **Profile** tab.

Figure 2-3: My Readiness View

From this view, you can perform many of the same tasks that can be performed on the **Deployment Management** > **User Readiness** view on the **Admin** tab.

3

Managing Your App Portal Site

This section of the App Portal Administration Guide explains how to configure App Portal's administrative settings, which are accessed from the **Admin** tab.

Table 3-1 • Managing Your Site

Section	Description
Managing Admin and Catalog Permissions	Explains how to specify which users and groups can view and modify administrative settings on the various App Portal views of the **Admin** tab, and which users and groups can view and modify the App Portal catalog.
Setting Language Options	Explains App Portal's localization support for 14 languages. It explains how to activate any of the supported language, and also how to add an additional language by translating supplied text and uploading it to App Portal.
Configuring Your Deployment Technology	Explains how to connect to and configure a connection to System Center Configuration Manager, Altiris Client Management Suite, AirWatch, and Casper.
Configuring ITSM Integration	Explains how to integrate App Portal with ServiceNow, BMC Remedy, or another ITSM system.
Configuring Cloud Application Integration	Explains how to integrate App Portal with Box, Salesforce, and Microsoft Office 365 or other cloud applications so that App Portal can offer a catalog item to request an account in the cloud application.
Configuring Active Directory Settings	Explains how to configure Active Directory settings, including adding global catalogs.
Configuring Corporate Single Sign On	Explains how to enable single sign-on to App Portal / App Broker using SAML 2.0, OAuth 2.0, OpenID, or custom authentication.

Table 3-1 • Managing Your Site

Section	Description
Performing Advanced License Check	Explains how, when performing a license check at checkout, you can instruct App Portal to consider not only available licenses, but also second use rights, upgrade/downgrade rights, and exemption by device role rights (such as an MSDN subscription), all based upon information stored in FlexNet Manager Suite. This feature requires integration with FlexNet Manager Suite.
Managing Notification Email Templates and Messages	Explains how to view and edit system notifications, which are email notifications that are used to communicate with App Portal users. They can be modified to suit your company's language preferences and content.
Branding Your App Portal Site	Explains how to brand your App Portal Site, such as changing the page header logo, customizing the Welcome page, displaying a EULA, and other customizations.
Enabling User Feedback on Your App Portal Site	Explains how to enable a Site Feedback widget so that users of your App Portal site can report feedback or problems.
Viewing Dashboards	Describes the **Dashboards** tab, where you can view helpful reports that demonstrate how much time and money using App Portal is helping you save in your software and operating system deployment projects.
Managing Reports	Reporting allows for the display of App Portal data in a read-only, searchable, and exportable view. This section explains how to create new reports, edit existing reports, and create and edit report categories.
Managing Your App Portal License File	In order for you to access the App Portal website, you need to upload a license file to App Portal. When your license file expires, you will need to upload an updated license file. This section explains how to obtain, upload, and update your license file.
Enabling App Portal Site for Your Enterprise	Explains how to enable your App Portal site so that all directory services users at your enterprise are able to access the site.
Entering Flexera Integration Connection Settings	Explains how to connect App Portal to the Flexera Service Gateway and to Microsoft System Center Orchestrator.
Viewing Error, Email, Request Lifecycle, and Debug Logs	Explains how to troubleshoot App Portal issues by generating and viewing error, email, and debug logs.
Securing HTTP Cookies Created by App Portal	Explains how to make a configuration change so that HTTP cookies will only be transmitted under HTTPS communication. This step is necessary if your App Portal website is running under HTTPS binding (`https://` is visible in the URL).
Site Management Reference	Explains all of the views, tabs, and dialog boxes on the **Site Management** view of the **Admin** tab.

Managing Admin and Catalog Permissions

You manage user access to the views and functionality of the **Admin** tab using the **Admin Security** and **Catalog Security** views under **Site Management**.

- **Admin Security**—When configuring App Portal, you need to specify which users and groups can view and modify administrative settings on the various App Portal views of the **Admin** tab. See Managing Administration Permissions.

- **Catalog Security**—When configuring App Portal, you need to specify which users and groups can view and modify the App Portal catalog. See Managing Catalog Permissions.

Managing Administration Permissions

When configuring App Portal, you will need to specify which users and groups can view and modify settings on the various App Portal views on the **Admin** tab. This secures the App Portal site settings to the listed groups and users.

You configure administrative security on the **Admin Security** view, which is opened by selecting **Admin Security** under **Site Management** on the **Admin** tab.
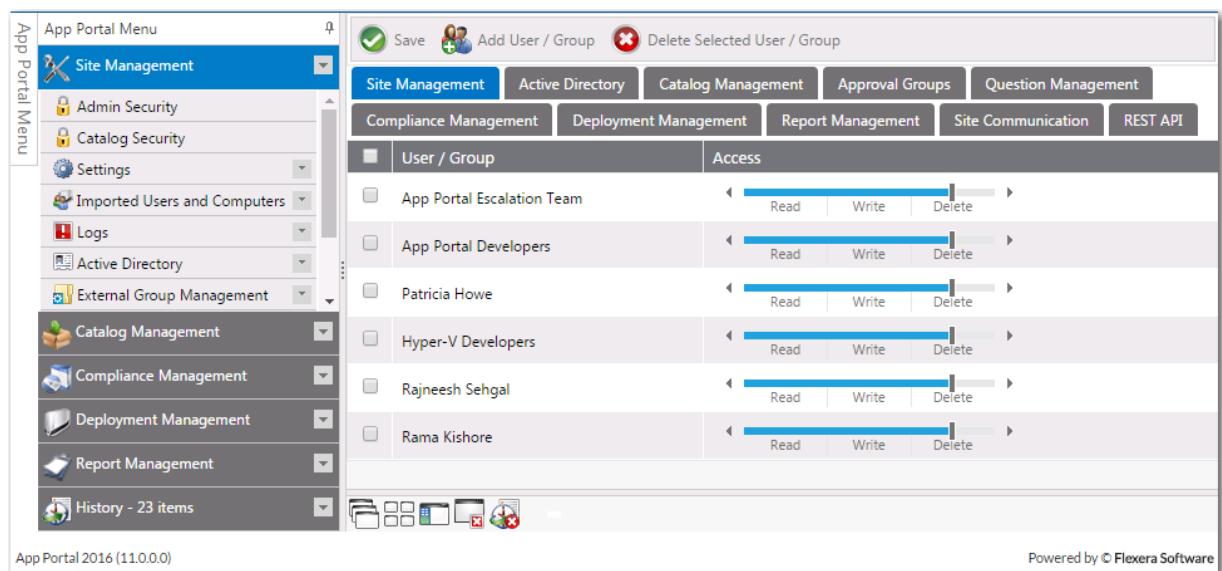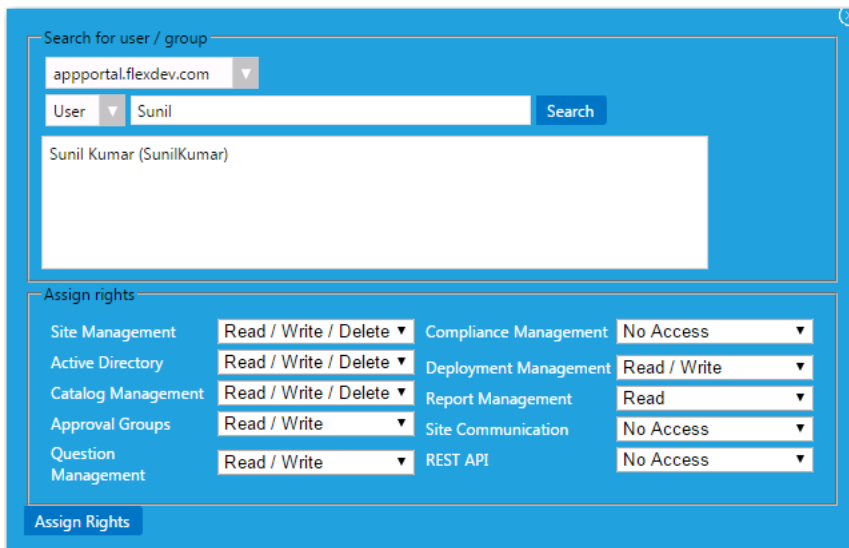
Figure 3-1: Admin Security View

On each of the tabs of the **Admin Security** view, you can view and edit the security settings (**Read**, **Write**, **Delete**) for *existing* users and groups for that particular role.

However, you assign *initial* permissions to a user or group for *all roles* on the pop-up dialog box that opens when you click **Add User/Group** on the **Admin Security View**.

Figure 3-2: Admin Security Add User/Group Dialog Box

Note • *Permissions are the "most restrictive model". For example, if a user is in two groups where one is granted Read permission and the other granted Write permission, the permissions will be Read; they are not cumulative.*

For instructions on how to add and edit user or group's Admin Roles, see the following:

- Adding a User or Group to Admin Roles

- Editing a User or Group's Admin Roles

Adding a User or Group to Admin Roles

To add a user or group to Admin roles, perform the following steps:

Task   ***To add a user or group to Admin roles:***

1. On the **Admin** tab, open the **Site Management > Admin Security** view.

2. Click the **Add User/Group** button. The following dialog box opens:

3. Use the search fields to locate the user or group that you want to add.

4. Select the appropriate permissions from the **Assign rights** fields for each listed role, as described in Admin Security.

5. Click **Assign Rights** to add the user or group. The selected user or group will now have access to the specified roles.

Note • Permissions are the "most restrictive model". For example, if a user is in two groups where one is granted Read permission and the other granted Write permission, the permissions will be Read; they are not cumulative.

Editing a User or Group's Admin Roles

To edit a user or group's Admin roles, perform the following steps:

Task   ***To edit a user or group' Admin roles:***

1. On the **Admin** tab, open the **Site Management > Admin Security** view.

   Users and groups with assigned roles are listed. On each of the tabs of the **Admin Security** view, you can view and edit the security settings (**Read**, **Write**, **Delete**) for the listed users and groups for that particular role (**Site Management**, **Active Directory**, **Catalog Management**, etc.).
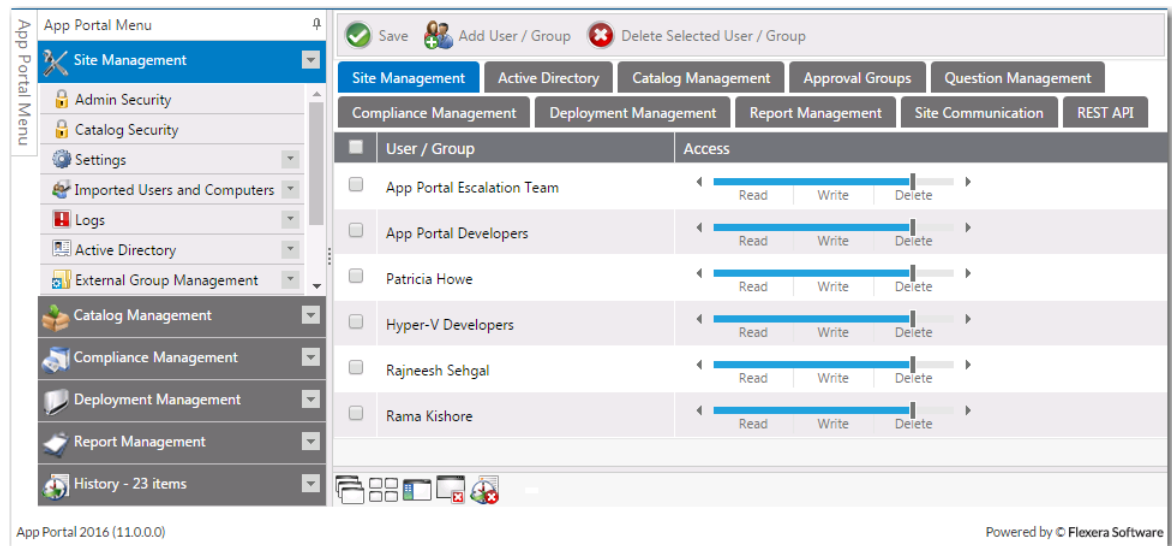
2. On each of the tabs of the **Admin Security** view, adjust the user or group's assigned rights for that role by sliding the indicator to select the desired rights, as shown in the following example:
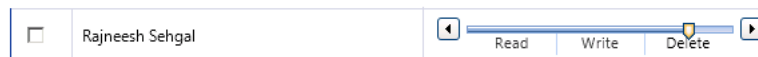
For information on each of these roles, see Admin Security.

3. To remove the user or group's **Admin** rights, select the checkbox next to the user or group name and then click **Delete Selected User / Group**.

4. Repeat for each of the tabs of the **Admin Security** view.

5. Click **Save**.

Note • Note that permissions are the "most restrictive model". For example, if a user is in two groups where one is granted Read permission and the other granted Write permission, the permissions will be Read; they are not cumulative.

Managing Catalog Permissions

When configuring App Portal, you will need to specify which users and groups can view and modify the App Portal catalog. This secures the App Portal site catalogs to the listed groups and users.

You configure catalog security on the **Catalog Security** view, which is opened by selecting **Catalog Security** under **Site Management** on the **Admin** tab.
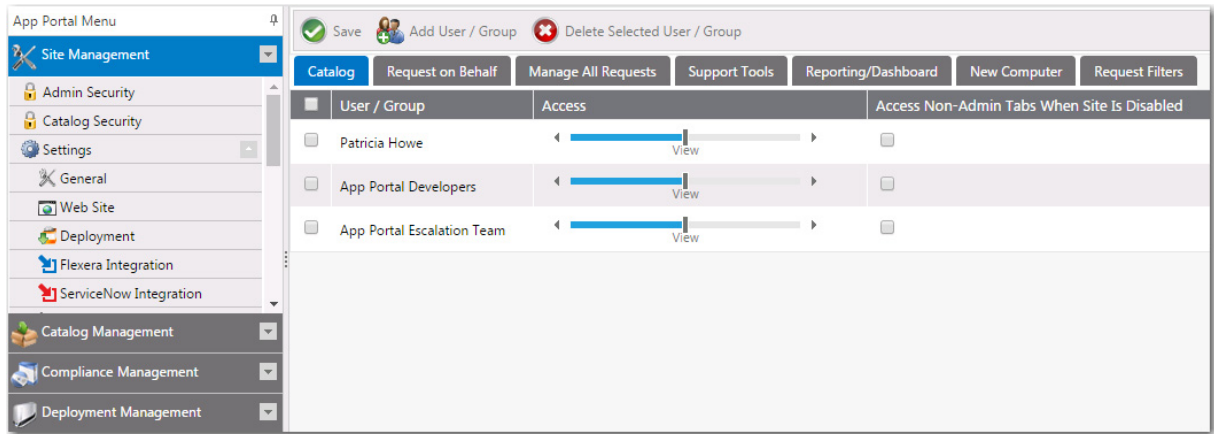
Figure 3-3: Catalog Security View

On each of the tabs of the **Catalog Security View**, you can view and edit the security settings for *existing* users and groups for that particular role.

However, you assign *initial* permissions to a user or group for all roles on the pop-up dialog box that opens when you click **Add User/Group** on the **Catalog Security View**.
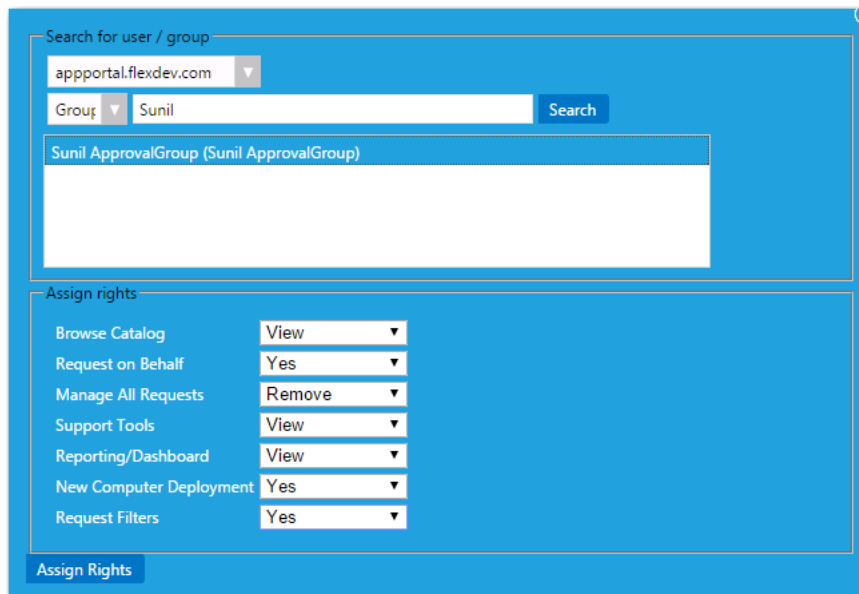
Figure 3-4: Catalog Security Add User/Group Dialog Box

Note • Permissions are the "most restrictive model". For example, if a user is in two groups where one is granted View permission and the other granted Modify permission, the permissions will be View; they are not cumulative.

For additional managing catalog permissions, see the following:

● Adding a User or Group to Catalog Roles

● Editing a User or Group's Catalog Roles

●   Providing Access to Non-Admin Tabs When App Portal Site is Disabled

Adding a User or Group to Catalog Roles

To enable permissions to see and manage the App Portal catalog, perform the following steps:

Task   ***To assign catalog permissions:***

1.   On the **Admin** tab, open the **Site Management > Catalog Security** view.

2.   To add a user or group, click the **Add User/Group** button. The following dialog box opens:

3.   Use the search fields to locate the user or group that you want to add.

4.   Select the appropriate permissions from the **Assign rights** fields for each listed role, as described in Catalog Security.

5.   Click **Assign Rights** to add the user or group.

Editing a User or Group's Catalog Roles

To edit a user or group's Catalog roles, perform the following steps:

Task   ***To edit a user or group' Admin roles:***

1.   On the **Admin** tab, open the **Site Management > Catalog Security** view.

Users and groups with assigned roles are listed. On each of the tabs of the **Catalog Security** view, you can view and edit the security settings (**View**, **Modify**, **Remove**, **Yes**) for the listed users and groups for that particular role (**Catalog, Request on Behalf, Manage All Requests**, etc.).
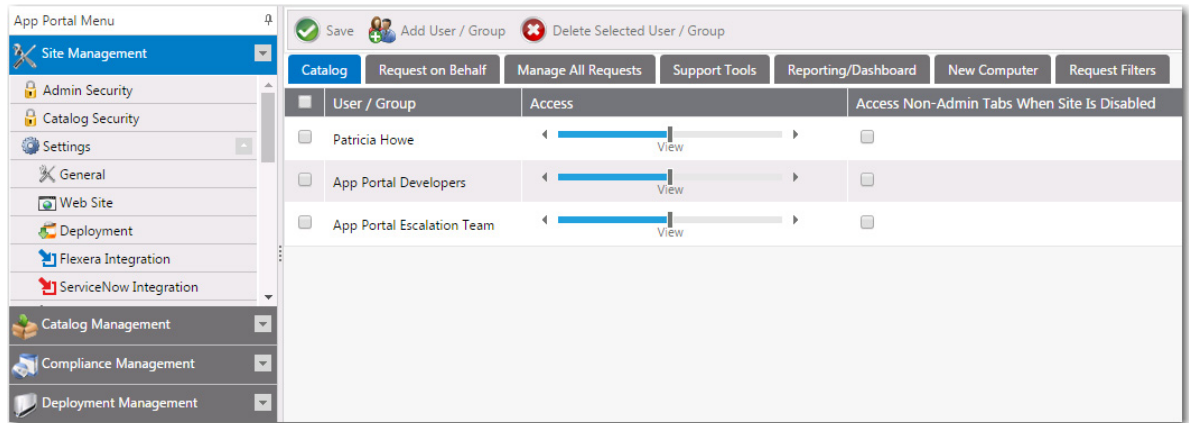
2. On each of the tabs of the **Catalog Security** view, adjust the user or group's assigned rights for that role by sliding the indicator to select the desired rights, as shown in the following example:
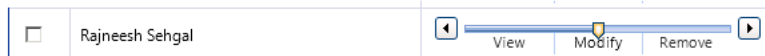
For information on each of these roles, see Catalog Security.

3. To remove the user or group's **Catalog** rights, select the checkbox next to the user or group name and then click **Delete Selected User / Group**.

4. Repeat for each of the tabs of the **Catalog Security** view.

5. Click **Save**.

Note • Note that permissions are the "most restrictive model". For example, if a user is in two groups where one is granted View permission and the other granted Modify permission, the permissions will be View; they are not cumulative.

Providing Access to Non-Admin Tabs When App Portal Site is Disabled

When managing catalog items for App Broker, some administrators might want to view and test catalog items in the App Portal end user interface: the **Browse Catalog** and the other end-user facing tabs. However, because in this scenario the App Portal site is not enabled (because all end users are using the ServiceNow interface), only those App Portal users with full administrative rights are able to view the App Portal end user interface.

To address this, you can select the **Access Non-Admin Tabs When Site Is Disabled** option on the **Site Management > Catalog Security** view. If this option is selected, the user will be permitted to view the end user facing App Portal interface even though the App Portal site is not enabled (because the **Enable site?** option on the **Site Management > Settings > General** view is not selected).

Figure 3-5: Access Non-Admin Tabs When Site Is Disabled Option

Setting Language Options

App Portal provides out-of-the-box localization support for its customer user interface, providing a choice of the following 14 languages:

- Chinese (Simplified)

- Dutch

- English

- French

- German

- Italian

- Japanese

- Korean

- Portuguese

- Portuguese (Brazil)

- Russian

- Spanish

- Spanish (Mexico)

- Thai

App Portal's localization support includes the following features:

- **End user screens and email notifications**—The localization support applies to the end user screens and the notifications/email messages.

- **Ability to localize questions and answers**—App Portal also provides you with an interface to localize the questions and answers that you associate with a catalog item request. The out-of-the-box questions and answers that are shipping with the product are already translated.

- **Language auto-detected by browser**—App Portal will automatically detect the language of the requesting browser from the user's culture settings and display that language. It will not be necessary for the end user to make a selection to change the displayed language.

- **Ability to add support for additional languages**—If you want to display App Portal's end user interface in a language other than those 14 that are supported, App Portal provides you with an interface to upload translated text in additional languages.

Information about App Portal's language support is presented in the following topics:

- Activating Languages

- Uploading Additional Languages

- Localizing Questions and Answers

- Editing Text Strings in the Language Text View

Activating Languages

App Portal provides out-of-the-box localization support for its customer user interface, providing a choice of the following 14 languages (end user screens only).

- Chinese (Simplified)
- Dutch
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese
- Portuguese (Brazil)
- Russian
- Spanish
- Spanish (Mexico)
- Thai

By default, only English is activated. To activate additional languages, perform the following steps.

Task   ***To activate additional languages:***

1. Under **Site Management**, select **Communication > Languages**. The **Languages** view opens.

2. To activate an additional language, click the drop down list under **Available Languages**, select one or more additional languages, and then click **Add**.

3. The language that App Portal uses is determined by the browser culture settings of the user. However, some notifications are sent outside of the browser's session, such as a successful installation email. The site does not know what the language of the target user is.

You can create collections to help identify the proper language to use in these cases. Collections starting with the prefix `ESD_Language_<LanguageName>` will show in the list. Select the collection that matches the selected language from the **Select Collection** list.

Uploading Additional Languages

App Portal provides out-of-the-box localization support for its customer user interface, providing a choice of 14 languages (end user screens, notification messages, and email).

However, if you want to provide support for displaying App Portal's end user interface in a language other than those 14 that are supported, you can easily upload translated text in additional languages. The text strings for the App Portal user interface are in one file, while the text strings for notification and email text is in a different set of files, one for each language.

- Adding a New Language for App Portal's User Interface

- Adding a New Language for App Portal's Notifications / Email

- Uploading Edited Language Files

- Loading Translated Text for Out-of-the Box Questions and Answers

Adding a New Language for App Portal's User Interface

App Portal's localized text strings for the user interface is contained in an Excel file, which is installed in the following location in the App Portal installation directory:

`\App Portal\Web\App_Data\AppPortal_OOB_Localization_Strings.xlsx`

Each column of the Excel spreadsheet contains the text strings for a supported language:

	A	B	C	D	E	F	G	H
1	ResourceId	English	German	German (Switzerland)	German (Liechtenstein)	French	French (Canada)	Japanese
2	Accept	Accept	Annehmen	Annehmen	Annehmen	Accepter	Accepter	決定
3	Accepted	Accepted	Angenommen	Angenommen	Angenommen	Accepté	Accepté	受諾
4	Accepted - No Further Status	Accepted - No Further Status	Angenommen - kein weiterer Status	Angenommen - kein weiterer Status	Angenommen - kein weiterer Status	Accepté - Pas d'autre état	Accepté - Pas d'autre état	受諾 - これ以上ステータスなし
5	AcceptedBy	Accepted By	Angenommen von	Angenommen von	Angenommen von	Accepté par	Accepté par	承諾者
6	AcceptedRequest	Accepted the following request id(s):	Die folgenden Anfrage-IDs wurden angenommen:	Die folgenden Anfrage-IDs wurden angenommen:	Die folgenden Anfrage-IDs wurden angenommen:	Les identifiants de demande suivants ont été acceptés :	Les identifiants de demande suivants ont été acceptés :	次の要求 ID を承認:
7	AcceptedRequest_ RequestDetails	Accepted Request	Anfrage angenommen	Anfrage angenommen	Anfrage angenommen	Demande acceptée	Demande acceptée	承認済みの要求
						Les	Les	

Figure 3-6: App Portal Text Strings in Excel Spreadsheet

To add an additional language to App Portal's user interface language file, perform the following steps:

Task **To add a language to App Portal's user interface language file:**

1. Make a copy of the `AppPortal_OOB_Localization_Strings.xlsx` file.

2. Copy the **English** column into a new column, and enter the name of the new language in the heading row.

3. Have the text strings in the new column translated and enter the translated strings into the Excel file.

Adding a New Language for App Portal's Notifications / Email

App Portal's localized text strings for notifications and email are found in a set of Excel files, one for each language, which are installed in the following location in the App Portal installation directory:

`\App Portal\Web\App_Data\Notifications`

Each Excel file contains the text strings for a supported language. For example, the `AppPortal_OOB_Notification_Strings_French.xls` file contains the French text strings.

Figure 3-7: App Portal Text Strings in Excel Spreadsheet

To add an additional language for App Portal's notifications and email, perform the following steps:

Task   ***To add a language for App Portal's notifications and email:***

1. Make a copy of the following Excel file on the App Portal server:

    `\App Portal\Web\App_Data\Notifications\AppPortal_OOB_Notification_Strings_English.xls`

2. Rename the copy to include the name of the new language, such as:

    `AppPortal_OOB_Notification_Strings_Hindi.xls`

3. Have the text strings in that Excel file translated.

Uploading Edited Language Files

After you have translated both the user interface and notification / email text for the new language, perform the following steps to upload the translated strings.

Task   ***To upload edited language files:***

1. On the App Portal server, open the following page in a browser:

    `http://APPPORTALSERVER/esd/ImportLanguageStrings.aspx`

    The **App Portal Language Importer Tool** page opens:

App Portal Language Importer Tool

Enter Full Localization Excel Path On Server

`C:\Program Files (x86)\Flexera Software\App Portal\Web\App_Data\AppPorta`

Sheet Name

`Sheet1`

[Load Languages]

Note • The Microsoft Access Database Engine x64 is required to be installed to use this tool. You can download it from the following website:

http://www.microsoft.com/en-us/download/details.aspx?id=13255

2. In the **Enter Full Localization Excel Path On Server** field, enter the path to the edited Excel file containing the user interface translated strings.

3. If the language file has all of the strings on the first sheet, leave the **Sheet Name** set to `Sheet1`.

4. Click **Load Languages**. The new language for the user interface will now be available in App Portal.

5. On the App Portal server, open the following page in a browser:

    `http://APPPORTALSERVER/esd/ImportNotificationStrings.aspx`

    The **App Portal Notification Importer Tool** page opens:

App Portal Notification Importer Tool

Enter Full Notification Excel Path On Server

`C:\Program Files (x86)\Flexera Software\App Portal\Web\App_Data\Notificat`

Sheet Name

`Sheet1`

[Load Notifications]

Note • If your server does not have the Access Database Engine x64, you will be prompted to download it.

6. In the **Enter Full Localization Excel Path On Server** field, enter the path to the edited Excel file containing the translated notification strings.

7. If the language file has all of the strings on the first sheet, leave the **Sheet Name** set to Sheet1.

8. Click **Load Notifications**. The new language for the notifications / email will now be available in App Portal.

9. Proceed with the steps in Activating Languages.

Note • When you upload the Excel file containing the translated strings, the strings are copied into the App Portal database; App Portal reads the strings from the database, not from the Excel files. Therefore, if you choose to edit the Excel files to make some changes, you will need to upload the edited files. As an alternative, you can make changes directly on the **Communication > Language Text** *view, as described in Editing Text Strings in the Language Text View.*

Loading Translated Text for Out-of-the Box Questions and Answers

Earlier versions of App Portal did not support the translation of question and answer text. Starting with App Portal 2015, you can translate question and answer text in the **Question Localization** and **Answer Localization** views.

App Portal also provides translations (in the 14 supported languages) of the out-of-the-box questions and answers that come with the product (such as KeepQuestion1 and MobileCatalogQuestion, etc.). In some instances, this translated text may not be loaded during installation or upgrade. If this is the case, run the following SQL file on the App Portal database to upload the translations of the out-of-the-box questions and answers:

```
[INSTALLDIR]\Web\DefaultSchema\Question_Anwer_OOB_Translations.sql
```

Localizing Questions and Answers

In addition to localizing the App Portal user interface and notification / email text, you can also localize the questions and answers that you associate with catalog item requests. This localization can be done on the **Question Localization** and **Answer Localization** views under **Site Management > Questions**.

Task   *To localize questions and answers:*

1. Under **Site Management > Questions**, select **Question Localization**. The **Question Localization** view opens.

2. From the **Select Language** list, select the activated language that you want to translate the questions for. The existing questions (and each question's pop-up description) are listed.

3. Enter the translated text for the selected language in the **Translation** columns.

4. Click **Save**.

5. Under **Site Management > Questions**, select **Answer Localization**. The **Answer Localization** view opens.

6. From the **Select Language** list, select the activated language that you want to translate the answers for. The existing answers for each question are listed.

7. In the **Translation** column, enter the translated text for each answer.

Editing Text Strings in the Language Text View

As described in Uploading Additional Languages, you can add new languages by adding translated text to existing Excel files and then uploading the files to App Portal. You can also edit existing text strings by editing those Excel files and re-uploading them.

However, an easier way of editing user interface text strings may be to use the **Communication > Language Text** view. On the **Language Text** view, you can display the user interface text strings for any of the activated languages, and modify the text strings for that language. The edits that you make will be immediately saved in the App Portal database.

Once you are satisfied with the changes and have saved them, click **Publish Translation** to make the changes appear in the portal.

To edit user interface text strings on the Language Text view, perform the following steps.

Task   ***To edit user interface text strings on the Language Text view:***

1. Open the **Site Management > Communication > Language Text** view.

2. From the **Select a language** list, select the language of the text strings that you would like to edit.

3. Edit the text strings in the **Translation** column.

4. Click **Show Untranslated Items** to only display text strings that have not been translated. Click the button again to go back to viewing the entire list.

5. Click **Save Translation** to save your edits.

6. Click **Publish Translation** to publish your edits to the App Portal database.

Note • *If, after editing text strings on the* **Language Text** *view, you want to go back to the default translations, you just need to re-upload the original Excel files, as described in* Uploading Additional Languages.

Configuring Your Deployment Technology

App Portal supports Microsoft System Center Configuration Manager (current branch), Microsoft System Center 2012 Configuration Manager, Altiris Client Management Suite 7.1 or later, AirWatch and MobileIron (for mobile applications), and JAMF Casper Suite 9.6.4 (for Macintosh desktop applications).

You connect App Portal to a deployment technology and enter configuration settings on the tabs of the **Site Management > Settings > Deployment** view.

- **About deployment technologies**—For detailed information about connecting to more than one deployment technology, see About the Supported Deployment Technologies.

- **Common**—To select the deployment technology that App Portal should use to perform specific tasks, make selections on the **Common** tab. See Entering Common Deployment Technology Settings.

- **System Center Configuration Manager (current branch)**—To connect App Portal to System Center Configuration Manager (current branch), enter server connection settings on the **ConfigMgr** tab. See Entering System Center Configuration Manager (Current Branch) Deployment Technology Settings.

- **System Center 2012 Configuration Manager**—To connect App Portal to System Center 2012 Configuration Manager, enter server connection settings on the **SCCM 2012** tab. See Entering System Center 2012 Configuration Manager Deployment Technology Settings.

- **Altiris**—To connect App Portal to Altiris Client Management Suite, enter server connection settings on the **Altiris** tab. See Entering Altiris Client Management Suite Settings.

- **AirWatch**—To connect App Portal to AirWatch, enter server connection settings on the **AirWatch** tab. See Entering AirWatch Settings.

- **Casper**—To connect App Portal to Casper, enter server connection settings on the **Casper** tab. See Entering Casper Settings.

- **MobileIron**—To connect App Portal to MobileIron, enter server connection settings on the **MobileIron** tab. See Entering MobileIron Settings.

Important • *Starting with App Portal 2013, your deployment technology is no longer specified during App Portal installation. Instead, you specify your deployment technology connection settings on the configuration screens displayed upon initial startup (as described in the Getting Started section under* Specifying Deployment Technology Settings*) or on the* **Site Management > Settings > Deployment** *view.*

About the Supported Deployment Technologies

App Portal supports the following deployment technologies for software distribution:

- Microsoft System Center 2012 Configuration Manager

- Altiris Client Management Suite 7.1 or later

- JAMF Casper Suite 9.6.4.

- AirWatch (for mobile applications)

- MobileIron (for mobile applications)

The purpose of App Portal's support for multiple deployment technologies is to enable you to:

- Present a single App Portal instance to your users even if your organization uses both System Center Configuration Manager and Altiris deployment technologies across your enterprise.

- Present a universal catalog to your users that includes both desktop and mobile applications, and includes both Windows and OS X applications.

- Enable you to provide a universal catalog containing:

  - Both desktop and mobile applications

  - Both Windows and OS X desktop applications

  - Google Android, iOS, and Windows Phone mobile applications

You enter the deployment technology connection settings by opening the **Deployment** subview of the **Site Management > Settings** view, and then entering the settings on the **ConfigMgr**, **SCCM 2012**, **Altiris**, **AirWatch**, **Casper**, or **MobileIron** tabs.

Figure 3-8: SCCM 2012 Tab of the Site Management > Settings > Deployment View

App Portal can only be connected to multiple servers of the same type if they are set up in a hierarchical relationship, with only the "main" site's connection information entered on tabs of the **Site Management > Settings > Deployment** view. The following table describes the acceptable hierarchical relationships for the deployment technologies:

Table 3-2 • Acceptable Hierarchical Relationships for Deployment Technologies

Technology	Description
System Center 2012 Configuration Manager **System Center Configuration Manager (Current Branch)**	**Single Primary Site OR Central Administration Site > Child Primary Sites** For System Center 2012 Configuration Manager, App Portal only communicates with one site: either a Single Primary Site or a Central Administration Site (which in turn replicates data to all Child Primary Sites).
Altiris Client Management Suite 7.1 or later	**Single Primary Site OR Central Site > Child Primary Sites** For Altiris. App Portal only communicates with **one** site: either a Single Primary Site or a Central Site (which in turn replicates data to all Child Primary Sites).

Important • App Portal does not support connecting to multiple, disconnected deployment servers that are using the same deployment technology and version.

Note • When using System Center Configuration Manager, Microsoft .NET Framework 4.5.1 is required to be installed on the IIS server in order to run the App Portal service and web site. This is not required when using Altiris Client Management Suite.

Entering Common Deployment Technology Settings

On the **Common** tab of the **Deployment** view, you need to select the deployment technology that App Portal should use to perform user syncing, computer syncing, evaluating collection membership, and other tasks.

You can connect App Portal to multiple deployment technologies: System Center 2012 Configuration Manager, Symantec Altiris, AirWatch (mobile applications), and Casper (Macintosh desktop applications). You can also specify custom a custom connection string to another third-party deployment technology. You are permitted to set up App Portal to perform some tasks with one deployment technology and other tasks with a different deployment technology.

*Note • Until you perform these steps on the **Deployment > Common** tab to sync user and computer data with the selected deployment technology, App Portal will not recognize the logged in user.*

To enter common deployment technology settings, perform the following tasks:

📋

Task   **To enter common deployment technology settings:**

1. On the **Admin** tab, open the **Site Management > Settings > Deployment** view.

2. Open the **Common** tab.

3. If you are using more than one deployment technology, in the **Define order for detecting client deployment technology list**, specify the order in which App Portal will check them to determine which deployment technology the end user's computer is a client of.

4. From the **Syncing Users** list, select the deployment technology you want App Portal to use to sync users using built-in sync queries.

📄

Note • *If you are going to specify a custom computer sync connection string in the Custom Computer Sync Settings and Custom User Computer Map Sync Settings areas below, set this field to **Not Defined**.*

5. From the **Syncing Computers** list, select the deployment technology you want App Portal to use to sync computers using built-in queries.

📄

Note • *If you are going to specify a custom computer sync connection string in the Custom Computer Sync Settings and Custom User Computer Map Sync Settings areas below, set this field to **Not Defined**.*

6. From the **Evaluating collection membership** list, select the deployment technology that you want App Portal to use to evaluate collection membership for standard conditions.

7. From the **Inventory/OS Deployment** list, select the deployment technology that you want App Portal to use to perform OS deployments and to read inventory data.

> *Note •* *Not supported for Altiris unless also using FlexNet Manager Suite.*

8. In the **Sync Page Size** field, enter the batch size to process users and computers. The default value is **100**.

9. Click **Save**, and then click the **Sync Data Now** button to sync App Portal using the current selections.

> *Note •* *By default, the sync also happens at 2:00 a.m. each morning. To configure the time, open the **Settings > Timers** view and edit the **Time of day to sync users and computers** field.*

10. If you want App Portal to use custom user sync queries, enter those queries in the following text boxes:

- **Custom User ID Sync SQL Query**—Query to obtain user IDs so that App Portal can process them in batch. See example in Custom User ID Sync SQL Query.

- **Custom User Sync SQL Query**—Query to obtain all user columns. Some of the columns and their names are mandatory, as described in the provided query sample. See example in Custom User Sync SQL Query.

- **Custom User Sync Connection String**—If you do not specify a custom connection string, App Portal will default to the connection string of the technology selected for **Syncing Users**. See example in Custom User Sync Connection String.

    Click the **Test User Sync Settings** button to test the entered queries.

11. If you want App Portal to use custom computer sync queries, enter those queries in the following text boxes:

- **Custom Computer ID Sync SQL Query**—Query to obtain computer IDs so that App Portal can process them in batch. See example in Custom Computer ID Sync SQL Query.

- **Custom Computer Sync SQL Query**—Query to obtain all computer columns. Some of the columns and their names are mandatory, as described in the provided query sample. See example in Custom Computer Sync SQL Query.

- **Custom Computer Sync Connection String**—If you do not specify a custom connection string, App Portal will default to the connection string of the technology selected for **Syncing Users**. See example in Custom Computer Sync SQL Query.

    Click the **Test Computer Sync Settings** button to test the entered queries.

12. If you want App Portal to use custom user computer map sync settings, enter those queries in the following text boxes:

- **Custom User Computer Map ID Sync SQL Query**—Query to obtain user IDs and computer IDs so that App Portal can process them in batch. See example in Custom User Computer Map ID Sync SQL Query.

- **Custom User Computer Map Sync SQL Query**—Query to obtain all user and computer columns. Some of the columns and their names are mandatory, as described in the provided query sample. See example in Custom User Computer Map Sync SQL Query.

- **Custom User Computer Map Sync Connection String**—If you do not specify a custom connection string, App Portal will default to the connection string of the technology selected for **Syncing Users**. See example in Custom User Computer Map Sync Connection String.

    Click the **Test User Computer Map Sync Settings** button to test the entered queries.

13. Click **Save** to save your settings.

Entering System Center Configuration Manager (Current Branch) Deployment Technology Settings

To connect App Portal to System Center Configuration Manager Branch (current branch), you need to enter settings on the **ConfigMgr** tab of the **Site Management > Settings >Deployment** view.

Note • System Center Configuration Manager (current branch) is the latest product release of Configuration Manager from Microsoft. The phrase "current branch" indicates this is a version of System Center Configuration Manager that supports incremental updates to the product. Starting with this release in December 2015, System Center Configuration Manager:

- *Does not use a year or product identifier in the product name, as seen with past versions like System Center 2012 Configuration Manager.*
- *Supports incremental in-product updates, also called update versions.*

To enter System Center Configuration Manager (current branch) connection settings, perform the following steps.

Task   *To enter System Center Configuration Manager (current branch) connection settings:*

1. On the **Admin** tab, open the **Site Management > Settings > Deployment** view.

2. Open the **ConfigMgr** tab.

3. In the **Central Site Server** field, enter the machine name of the System Center Configuration Manager (current branch) server.

4. In the **Central Site Database Server** field, enter the machine name where the System Center Configuration Manager (current branch) server database resides.

5. In the **Central Site Database Name** field, enter the database name of the System Center Configuration Manager (current branch) server database.

📄

Note • Make sure that you enter just the name of your actual System Center Configuration Manager database instance, not server_name\instance.

6. In the **Central Site Code** field, enter the site code of the System Center Configuration Manager (current branch) server (in SITE_XXX format).

7. By default, when creating a collection for a catalog item, App Portal uses "All System" as the limiting collection for device-based deployments. If you instead want to specify which limiting collection to use, enter a collection name in the **Limiting Collection for Device** field to set as the limiting collection ID for all device-based collections created by App Portal for device-based deployments.

8. By default, when creating a collection for a catalog item, App Portal uses "All Users as the limiting collection for user-based deployments. If you instead want to specify which limiting collection to use, enter a collection name in the **Limiting Collection for User** field to set as the limiting collection ID for all user-based collections created by App Portal for user-based deployments.

9. Click **Test** to test the connection settings that are entered.

10. Set the **Enable workstation verification?** field to one of the following options to enable/disable the actions in the **Select verification level** list.

- **Select verification level**—Tells App Portal how to handle users who visit from machines that were not originally registered with App Portal. Select one of the following options:

  - **Warning**—Users will be prompted with a notification that they are not using the discovered machine.

  - **Disallowed**—Users will not be able to visit the App Portal Storefront from other machines.

> *Note • Users matching one of the specified attributes will not be required to accept the EULA.*

> *Note • This field is disabled when the **User / Computer relationship** field is set to **Use SCCM last logon user**.*

11. Specify the **User / Computer relationship** that App Portal needs to use by selecting one of the following options:

- **Use SCCM last logon user**—The user to computer relationship will use SMS last logon user.

- **Use SCCM Primary Console Usage**—Makes use of the System Center Configuration Manager / SMS SP3 feature of tracking login duration to determine primary machine usage

- **Use AD Computer Managed By**—Uses the AD Computer object "Managed By" attribute to determine the primary user of the computer. This setting requires inventory of the `"ManagedBy"` AD attribute in System Center Configuration Manager System Discovery.

- **Use User Affinity**—In System Center Configuration Manager (current branch), you can directly define the users for a computer and the computers for a user. The option could also be referred to as "Use System Center Configuration Manager (current branch) user and device assignment".

12. Specify all other System Center Configuration Manager (current branch) options, as described in ConfigMgr Tab.

13. Click **Save**.

Entering System Center 2012 Configuration Manager Deployment Technology Settings

To connect App Portal to System Center 2012 Configuration Manager, you need to enter settings on the **SCCM 2012** tab of the **Site Management > Settings >Deployment** view.

To enter System Center 2012 Configuration Manager connection settings, perform the following steps:

Task ***To enter System Center 2012 Configuration Manager connection settings:***

1. On the **Admin** tab, open the **Site Management > Settings > Deployment** view.

2. Open the **SCCM 2012** tab.

3. In the **Central Site Server** field, enter the machine name of the System Center 2012 Configuration Manager Server.

4. In the **Central Site Database Server** field, enter the machine name where the System Center 2012 Configuration Manager Server database resides.

5. In the **Central Site Database Name** field, enter the database name of the System Center 2012 Configuration Manager Server database.

Note • Make sure that you enter just the name of your actual System Center Configuration Manager database instance, not `server_name\instance`.

6. In the **Central Site Code** field, enter the site code of the System Center 2012 Configuration Manager Server (in `SITE_XXX` format).

7. By default, when creating a collection for a catalog item, App Portal uses "All System" as the limiting collection for device-based deployments. If you instead want to specify which limiting collection to use, enter a collection name in the **Limiting Collection for Device** field to set as the limiting collection ID for all device-based collections created by App Portal for device-based deployments.

8. By default, when creating a collection for a catalog item, App Portal uses "All Users as the limiting collection for user-based deployments. If you instead want to specify which limiting collection to use, enter a collection name in the **Limiting Collection for User** field to set as the limiting collection ID for all user-based collections created by App Portal for user-based deployments.

9. Click **Test** to test the connection settings that are entered.

10. Set the **Enable workstation verification?** field to one of the following options to enable/disable the actions in the **Select verification level** list.

- **Select verification level**—Tells App Portal how to handle users who visit from machines that were not originally registered with App Portal. Select one of the following options:

  - **Warning**—Users will be prompted with a notification that they are not using the discovered machine.

  - **Disallowed**—Users will not be able to visit the App Portal Storefront from other machines.

  📄

  Note • Users matching one of the specified attributes will not be required to accept the EULA.

  📄

  *Note • This field is disabled when the **User / Computer relationship** field is set to **Use SCCM last logon user**.*

11. Specify the **User / Computer relationship** that App Portal needs to use by selecting one of the following options:

- **Use SCCM last logon user**—The user to computer relationship will use SMS last logon user.

- **Use SCCM Primary Console Usage**—Makes use of the System Center Configuration Manager / SMS SP3 feature of tracking login duration to determine primary machine usage

- **Use AD Computer Managed By**—Uses the AD Computer object "Managed By" attribute to determine the primary user of the computer. This setting requires inventory of the `ManagedBy` AD attribute in System Center Configuration Manager System Discovery.

- **Use User Affinity**—In System Center 2012 Configuration Manager, you can directly define the users for a computer and the computers for a user. The option could also be referred to as "Use System Center 2012 Configuration Manager user and device assignment".

12. Specify all other System Center 2012 Configuration Manager options, as described in SCCM 2012 Tab.

13. Click **Save**.

Entering Altiris Client Management Suite Settings

To connect App Portal to Altiris Client Management Suite, you need to enter settings on the **Deployment > Altiris** subtab of the **Settings View**, which is opened by selecting **Settings** under **Site Management** on the **Admin** tab.

To enter Altiris connection settings, perform the following steps:

Task **To enter Altiris connection settings:**

1. On the **Admin** tab, open the **Site Management > Settings > Deployment** view.

2. Open the **Altiris** tab.

3. In the **Central Site Server** field, enter the machine name of the Altiris Notification Server.

Tip • *Make sure that ASDK is installed on this machine.*

4. In the **Central Site Database Server** field, enter the machine name where the Altiris Notification Server database resides.

5. In the **Central Site Database Name**, enter the database name of the Altiris Notification Server database.

Note • *Make sure that you enter just the name of your actual Altiris database instance, not* `server_name\instance`*.*

6. Click **Test** to test the connection settings that are entered.

7. Specify the **User / Computer relationship** that App Portal needs to use by selecting one of the following options:

- **Use last logon user**

- **Use User Affinity** (primary device assigned to user)

8. In the **Computer Collection Folder** field, enter the name of the folder to use to create App Portal computer filters.

9. In the **User Collection Folder** field, enter the name of the folder to use to create App Portal user filters.

10. In the **Advertisement Folder** field, enter the name of the folder to use to create App Portal advertisements.

11. After adding the user/computer to a filter for deployment, App Portal can update the policy on the Altiris Management Agent on the client to receive the deployment. However, in order to do this, the App Portal system account needs remote WMI access on all the machines. If the remote WMI permissions are granted, select the **Update Machine Policy On Altiris Management Agent** option to allow App Portal to remotely update client policy.

12. Specify all other Altiris options, as described in Altiris Tab.

13. Click **Save**.

> 📄
>
> **Note •** The **Use Central Site for All Deployments** option is always selected, because App Portal only communicates with the central site.

Entering AirWatch Settings

With App Portal, you can deliver a universal enterprise app store: both desktop and mobile applications together. You can connect App Portal to an AirWatch server and create catalog items for Apple iOS and Google Android mobile apps, both internal and public store. This gives you license compliance, deployment automation, and control.

To connect App Portal to an AirWatch server, you need to enter settings on the **AirWatch** tab of the **Site Management > Settings > Deployment** view.

- Entering AirWatch Server Details

- Entering AirWatch Status Mapping Settings

Entering AirWatch Server Details

To enter AirWatch server details, perform the following steps:

📋

Task   ***To enter AirWatch server details:***

1. On the **Admin** tab, open the **Site Management > Settings > Deployment** view.

2. Open the **AirWatch** tab. The **AirWatch Server Details** are listed.

3. In the **AirWatch URL** field, enter the URL to your instance of AirWatch.

4. Enter the **User Name** and **Password** to your AirWatch instance.

5. Enter the **API Key** that was provided to you by AirWatch.

6. Click **Test** to test connection settings. If successful, the following message is displayed:

```
AirWatch Server settings are valid.
```


Note • *AirWatch users (which are based upon an email address) and are synced to AppPortal at the same time that the System Center Configuration Manager / Altiris users and are synced. App Portal users are matched with System Center Configuration Manager / Altiris users by having the same email address.*

Entering AirWatch Status Mapping Settings

When App Portal publishes a request to AirWatch, AirWatch returns a status message to indicate success or failure of the deployment:

- **Success**—AirWatch returns `Installed` or `Managed`.

- **Failure**—AirWatch returns `NotInstalled`.
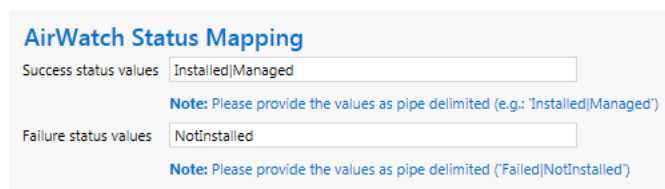
If, at some future time, AirWatch changes their status messages to something different, you can update these values by performing the following steps.

Task **To enter AirWatch status mapping settings:**

1. On the **Admin** tab, open the **Site Management > Settings > Deployment** view.

2. Open the **AirWatch** tab. The **AirWatch Status Mapping** settings are listed.

3. In the **Success status values** field, enter the new "success" status values.

4. In the **Failure status values** field, enter the new "failure" status values.

Entering Casper Settings

With App Portal, you can deliver a universal enterprise app store that includes both Windows and OS X desktop applications. You can connect App Portal to a JAMF Casper Suite 9.6.4 server and create catalog items for OS X desktop applications. This gives you license compliance, deployment automation, and control.

Note • *To deploy Apple iOS mobile apps, you need to connect to an AirWatch server, as described in Entering AirWatch Settings.*

Important • *App Portal supports JAMF Casper 9.6.4, On Premises version. Casper on the Cloud is not officially supported. However, you may attempt to integrate with Casper on the Cloud using API calls. For more information, see API Calls Used by App Portal to Integrate with Casper.*

Note • *In order for App Portal to be successfully integrated with Casper, your Casper account needs to have a specific set of minimum permissions. For more information, see Required Casper Account Permissions.*

Note • *For information on the API calls used by App Portal when integrating with Casper, see API Calls Used by App Portal to Integrate with Casper.*

To connect App Portal to a Casper server, you need to enter settings on the **Casper** tab of the **Site Management > Settings > Deployment** view.

- Entering Casper Server Details

- Entering Casper XPath Mapping Settings

- Entering Casper Machine Name Configuration Additional Properties

Entering Casper Server Details

In addition to entering the Casper server connection details, you also need to enter Casper policy information. Casper policies allow you to remotely perform common management tasks on managed computers. For example, you can run scripts, manage accounts, and distribute software using a policy. For App Portal to create a policy and a static group, it needs a template for each of these.

To enter Casper server details, perform the following steps:

Task   ***To enter Casper server details:***

1. Open the **Site Management** > **Settings > Deployment** view.

2. Open the **Casper** tab. The **Casper Server Details** are listed.

3. In the **Casper URL** field, enter the URL to your Casper server.

    📄

    Note • App Portal and Casper communicate using Casper's JSS API. By default, Casper uses port 8443 for inbound SSL traffic to the JSS. You will need to include the port number in the Casper URL when configuring your settings. If you have modified the inbound SSL port within your JSS configuration, specify your custom port number in the Casper URL.

4. Enter the **User Name** and **Password** to your Casper server.

5. In the **App Portal Policy folder** field, enter the folder/category in Casper under which the policies created by App Portal will reside.

6. In the **Policy template name** field, enter the name of the policy in Casper which can be used as a template.

7. In the **Computer group template name** filed, enter the name of the static group in Casper which can be used as a template.

8. Click **Test** to test connection settings. If successful, the following message is displayed:

    ```
    Casper Server settings are valid.
    ```

    📄

    Note • Casper users (which are based upon an email address) and are synced to App Portal at the same time that the System Center Configuration Manager / Altiris users and are synced. App Portal users are matched with System Center Configuration Manager / Altiris users by having the same email address.

Entering Casper XPath Mapping Settings

The **Casper XPath Mapping** area of the **Casper** tab provides a means for you to adapt to changes to the Casper APIs that may occur in future releases of Casper.

App Portal uses these XPaths to access values from the API results sent from Casper. If any of these change in the Casper API in the future, you can make the corresponding necessary changes here.

There is no need to modify these XPath mapping settings. But, If, at some future time Casper changes their XPath mapping settings to something different, you can update these values by performing the following steps.

Task   **To enter Casper XPath status mapping settings:**

1.   Open the **Site Management > Settings > Deployment** view.

2.   Open the **Casper** tab. The **Casper XPath Mapping** settings are listed.

Casper XPath Mapping

Computer group name xpath	/computer_group/name
Policy name xpath	/policy/general/name
Policy package id xpath	/policy/package_configuration/packages/package/i
Policy packages xpath	/policy/package_configuration/packages
Policy groups xpath	/policy/scope/computer_groups
Category id xpath	/policy/general/category/id
Category name xpath	/policy/general/category/name
Policy frequency xpath	/policy/general/frequency
Policy check-in trigger xpath	/policy/general/trigger_checkin
Policy distribution point xpath	/policy/general/target_drive
Policy ID xpath	/policy/general/id
Update inventory for policy	/policy/maintenance/recon

3.   Make any edits, as required.

4.   Click **Save**.

Entering Casper Machine Name Configuration Additional Properties

The **Casper Machine Name Configuration** area of the **Casper** tab provides a means for you to change user computer mappings that App Portal utilizes for Casper. By default, App Portal maps to Casper using email addresses. Changing the mapping lets you map to Casper with **UserName** Or **FullName** Or **DisplayName**. In some environments, the user name has a unique ID which helps uniquely identify each user. If you enter additional properties in the **Casper Machine Name Configuration** section and a sync is performed, the Macintosh machine name will get appended with the additional properties and the entire string will be treated as a machine name. For example:

●   If the Macinstoch machine name is **MacABC** and you have configured an additional property as **mac_address** then the machine name will be the entire string: **MacABC; 0C:4D:E9:CD:EC:C4**.

●   If you have configured the additional property as **serial_number,udid** then the machine name will look similar to the following:
MacABC; C07NG0W4DWYL; AEB468FF-904B-5D76-8167-392761E942CD.

Task   ***To enter additional properties for Casper machine name configuration:***

1. Open the **Site Management** > **Settings > Deployment** view.

2. Open the **Casper** tab. The **Casper Machine Name Configuration** are listed.

3. In the **Additional properties for device sync** field, enter information in the following format:

    ```
    serial_number,mac_address,udid
    ```

    When the above details are configured and a sync is performed, then the Macintosh machine name will get appended
    with the additional properties and the entire string will be treated as a machine name.

> **Note** • *When checking out Casper catalog items, the mapping to Casper must be considered when specifying the
> machine name. Consider the following steps:*

  a. Select the **Enable request to manual list?** option for a Casper catalog item.

  b. On the resulting **Choose Target** panel of the **Checkout** view (available for requesters who have been assigned
      the Request to Manual list), select the **Add machine names or user IDs manually** option.

  c. On the **Checkout** screen where you **Enter Target /Users**, enter the Macintosh name in the format that
      corresponds to the currently configured mapping to Casper. When additional properties are specified in the
      Additional properties for device sync field of the **Casper Machine Name Configuration** section (in the **Casper**
      tab of the **Site Management > Settings > Deployment** view), then the machine name must be entered as the
      entire string in a format such as **MacABC; 0C:4D:E9:CD:EC:C4** or **MacABC; C07NG0W4DWYL; AEB468FF-904B-
      5D76-8167-392761E942CD** depending on the additional properties you specified.

Entering MobileIron Settings

You can connect App Portal to a MobileIron server and create catalog items for Apple iOS and Google Android mobile apps.
This gives you license compliance, deployment automation, and control.

App Portal imports user information from MobileIron. Once connectivity if configured, and also on a daily basis, App Portal
will import users that have managed by MobileIron. App Portal also imports user-to-device relationship for the that are
managed by MobileIron.

To connect App Portal to a MobileIron server, you need to enter settings on the **MobileIron** tab of the **Site Management >
Settings > Deployment** view.

Task **To enter MobileIron server details:**

1. On the **Admin** tab, open the **Site Management > Settings > Deployment** view.

2. Open the **MobileIron** tab. The **MobileIron Server Details** are listed.

3. In the **MobileIron URL** field, enter the URL to your instance of MobileIron.

4. Enter the **User Name** and **Password** to your MobileIron instance.

5. Click **Test** to test connection settings. If successful, the following message is displayed:

    MobileIron Server settings are valid.

Configuring ITSM Integration

App Portal includes out-of-the-box integration, via web services, with both ServiceNow and BMC Remedy IT Service Management (ITSM) systems. You can also use App Portal's built-in reusable framework to integrate with other ITSM systems.

When integration is set up, whenever specified actions occur in App Portal (such as when a request is submitted), tickets in the attached ITSM system can be automatically opened or closed, or the status of a ticket can be reported on.

Information about ITSM integration is organized in the following topics:

- About ITSM Integration

- Connecting to ServiceNow or BMC Remedy and Creating Default Operations

- Editing ITSM Services

- Configuring Operations

- Setting ITSM Actions on Catalog Items

- Deploying via API to Enable App Portal Approvals in an External ITSM System

- Integrating With the ServiceNow User Interface

- Integrating With Another ITSM System

- Accessing Custom Attributes Obtained from a Custom SQL Sync Query in an ITSM System

Note • You can also use App Broker to integrate App Portal's app store features with the ServiceNow service catalog interface. Like App Portal, App Broker is a universal enterprise app store for desktop, mobile, and cloud applications that enables IT to maintain license compliance while providing automated software delivery. But, instead of using the App Portal end user interface, employees request software directly in the ServiceNow self-service portal. For more information, see Using App Broker for ServiceNow.

Note • You can also use App Broker for ServiceNow or App Broker for BMC to integrate App Portal's app store features with the ServiceNow or BMC MyIT service catalog interfaces. When you integrate ServiceNow or BMC MyIT with App Broker, instead of using the App Portal end user interface, employees request software directly in the ITSM system's self-service portal. For more information, see Using App Broker for ServiceNow and Using App Broker for BMC.

About ITSM Integration

App Portal includes out-of-the-box integration, via web services, with both ServiceNow and BMC Remedy IT Service Management (ITSM) systems. You can also use App Portal's built-in reusable framework to integrate with other ITSM systems.

When integration is set up, whenever specified actions occur in App Portal (such as when a request is submitted), tickets in the attached ITSM system can be automatically opened or closed, or the status of a ticket can be reported on. Notations of these actions are recorded in both App Portal and the ITSM system.

By integrating App Portal with your ITSM system, you are unifying your app store with your service desk. This enables you to leverage your established ITSM approval workflows and procedures. It also enables you to present to your employees a common portal for all service requests, a single place to request both applications and IT services. This encourages easier adoption and eliminates the need for additional training.

You can also embed the App Portal interface within the ServiceNow interface, giving your users an even more integrated experience.

Integrating with ServiceNow or Remedy involves the following steps:

Table 3-3 • Steps to Integrate with ServiceNow or Remedy

Task	Description
Connecting to ServiceNow or BMC Remedy and Creating Default Operations	You first enter the connection information to your ServiceNow or Remedy instance on the **Site Management > Settings > ServiceNow Integration** or **3rd-Party Integration** view.
	After you enter connection information to ServiceNow or Remedy, click the **Create Default Operations** button to instruct App Portal to connect to the ITSM system and obtain all of the ITSM system's exposed web services.

Table 3-3 • Steps to Integrate with ServiceNow or Remedy

Task	Description
Configuring Operations	App Portal only interacts with a portion of the parameters of each operation: parameters that relate to create, read, update, or delete tasks. Therefore, App Portal automatically defines the parameters associated with those tasks.
	However, if desired, you can edit those parameters or define new parameters on the **Configure Operation** view, which lists all of the parameters associated with the selected operation.
Adding and Configuring New Operations	When App Portal creates default operations for ServiceNow or Remedy, it creates all operations necessary for a typical integration with an ITSM system.
	However, if desired, you can add and configure additional operations.
Setting ITSM Actions on Catalog Items	In order for a catalog item request to trigger an event in an ITSM system, you need to define ITSM-specific actions on that catalog item. This is done on the **Actions** tab of the **Catalog Item Properties** dialog box.

You can also integrate with another ITSM system and manually add and configure default operations, as described in Integrating With Another ITSM System.

Connecting to ServiceNow or BMC Remedy and Creating Default Operations

To integrate App Portal with Service Now or BMC Remedy, you first need to open the **Site Management > Settings > ServiceNow Integration** or **3rd-Party Integration** view and provide the URLs to the relevant web services along with the credentials required to create both incidents and requests on these systems.

Important • *In order to use ServiceNow ITSM actions in App Portal, the* eLementFormDefault *value setting in ServiceNow needs to be unselected. If it is selected, App Portal gets a null response for the ServiceNow ID. For more information, see:*

http://wiki.servicenow.com/index.php?title=Microsoft_.NET_Web_Services_Client_Examples#gsc.tab=0

Connecting to ServiceNow

To connect App Portal to ServiceNow, perform the following steps.

Task   ***To connect to ServiceNow:***

1. On the **Admin** tab, open the **Site Management > Settings > ServiceNow Integration** view.

2. In the **ServiceNow Instance URL** field, enter the URL to your instance of ServiceNow.

   Important • *Do not use any special characters in the URL fields. The only special character that is permitted is _ (underscore). Dashes (-) and other special characters are not permitted.*

3. Enter the **User Name** and **Password** to ServiceNow system.

   Important • *The account used to connect to ServiceNow must have access to invoke web methods in ServiceNow. This account also needs to have been granted the following ServiceNow permissions: `Itil`, `soap_create`, `soap_query_update`, and `soap_script`.*

4. Click **Test** to test the connection to the ServiceNow.

5. Under **ServiceNow Integration**, click **Create Default ITSM Operations** to create the ITSM operations in App Portal for the Incident Management and Request Management features in ServiceNow. This prompts App Portal to connect to the default incident management APIs, extract web methods and their parameters, and create the default web service operations. When App Portal is complete, the following message appears:

   ```
   Default ServiceNow Operations created successfully. Please click ITSM Integration node to view the
       list of systems and operations.
   ```

   The following ServiceNow web services are created:

Service	Operations
ServiceNow - Create Incident Management Service	• Create ServiceNow Incident • Delete Existing ServiceNow Incident • Get Existing ServiceNow Incident Status • Update Existing ServiceNow Incident

Service	Operations
ServiceNow - Create Request Management Service	• Create ServiceNow Request • Create ServiceNow Request for Cloud • Get Existing ServiceNow Request Status • Update ServiceNow Request

Note • Additional web services are created when using App Broker. See App Portal / App Broker ServiceNow Web Services.

*Note • When you click **Create Default ITSM Operations**, App Portal imports all web services. If you then modify one of the web services (as described in Configuring Operations) and click **Create Default Operations** again, App Portal will not overwrite the already-imported (and edited) web service. It will only import new web services or web services that were deleted.*

6. Click **Save** to save your entries.

*Note • With App Broker, you can manage your application catalog in App Portal, but users can request software catalog items directly in the ServiceNow self-service portal. You can also use the App Portal Employee App Provision Request wizard (from within the ServiceNow user interface) to request OSD task sequence catalog items. Using these features would require you to configure additional settings on the **ServiceNow Integration** view. For more information, see Using App Broker for ServiceNow and ServiceNow Integration.*

Connecting to BMC Remedy

To connect App Portal to BMC Remedy, perform the following steps.

Task   ***To connect to BMC Remedy:***

1. On the **Admin** tab, open the **Site Management > Settings > 3rd-Party Integration** view.

2. In the **Remedy Instance URL**, enter the URL to your instance of the Remedy web service.

Important • *Do not use any special characters in the URL fields. The only special character that is permitted is _ (underscore). Dashes (-) and other special characters are not permitted.*

3. Enter the **User Name** and **Password** to BMC Remedy system. The account used to connect must have access to invoke web methods in BMC Remedy.

4. Click **Test** to test the connection to BMC Remedy.

5. Next, click the **Create Default Operations** button for BMC Remedy. This prompts App Portal to connect to the default incident management APIs, extract web methods and their parameters, and create the default web service operations. When App Portal is complete, the following message appears:

    ```
    Default Remedy Operations created successfully. Please click ITSM Integration node to view the list
        of systems and operations.
    ```

    The following web methods are created:

Service	Operations
Create Incident Management Service	● Create Remedy Incident
Create Request Management Service	● Create Remedy Service Request
	● Create Remedy Service Request for Cloud

Service	Operations
Incident Status Management Service Wrapper	● Get Existing Remedy Incident Status
Query Incident Management Service	● Update Existing Remedy Incident
Service Request Status Management Service Wrapper	● Get Existing Remedy Service Request Status

Note • *When you click* **Create Default Operations**, *App Portal imports all web services. If you then modify one of the web services (as described in* Configuring Operations*) and click* **Create Default Operations** *again, App Portal will not overwrite the already-imported (and edited) web service. It will only import new web services or web services that were deleted.*

6. Click **Save** to save your entries.

At this point, ITSM integration is complete. However, you may choose to customize/configure these operations for your organization, as described in Configuring Operations.

Editing ITSM Services

If you want to edit the properties of an existing ITSM web service, perform the following steps.

Task   *To edit an existing ITSM web service:*

1. Open the **Site Management > ITSM Integration** view.

2. Click on the **Configuration** link of the web service you want to edit. The **Configure Service** view opens.

3. Edit the following properties:

Property	Description
Provide System name	Edit the name that identifies this ITSM system.
Provide descriptive name	Edit the brief description of this ITSM system. This description is listed in the **System Description** column of the **ITSM Integration** view.
Choose provider	Select the provider of this ITSM service: **ServiceNow**, **Remedy**, or **Others**.
Provide WSDL URL	Edit the URL to your instance of the ITSM system. *Important* • *Do not use any special characters in the URL field. The only special character that is permitted is _ (underscore). Dashes (-) and other special characters are not permitted.*
Choose authentication type	Select either **Provided Credentials** or **Integrated** to indicate the authentication type. If you chose **Provided Credentials**, you also need to enter a **User name** and **Password**.
Email Address for Alerts	Enter email addresses, one entry per line, to be notified when alerts are generated in relation to this service.

4. Click **Test** to test the settings.

5. Click **Save** to save your edits.

Configuring Operations

For ServiceNow and BMC integration, default operations are created and configured automatically when you click the **Create Default Operations** button on the **Site Management > Settings > ServiceNow** or **3rd-Party Integration** views. However, you may choose to customize/configure these operations for your organization.

Note • *Before you can configure the* `Request_Submit_Service` *operation for a BMC Remedy service request, you are required to first obtain a SRD (Service Request Definition) Template from BMC. For instructions, see* Obtaining a SRD (Service Request Definition) Template for a BMC Remedy Service Request.
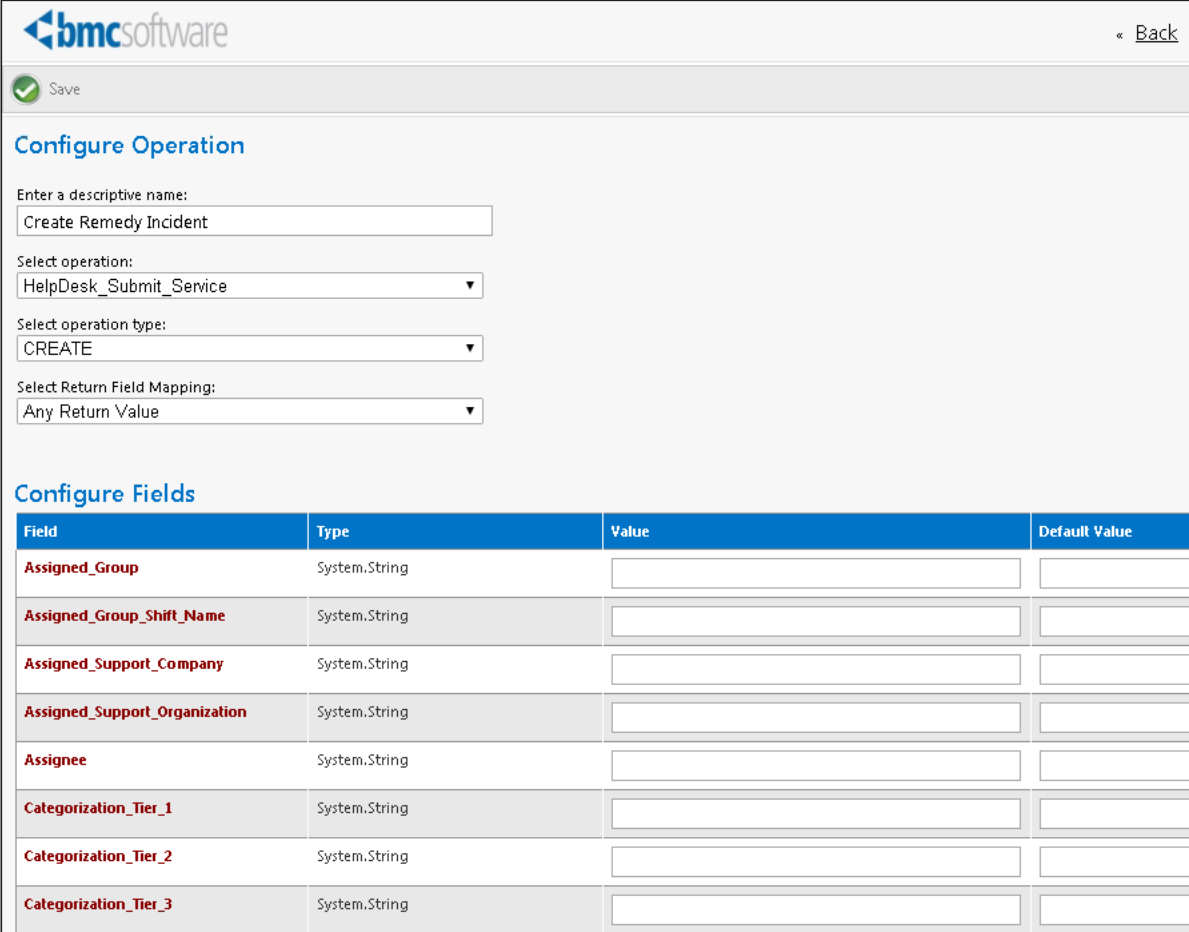
If you are integrating with an ITSM system other than ServiceNow or Remedy, you will need to manually create the required operations.

You perform both of these tasks on the **Configure Operation** view.

- About the Configure Operation View

- Editing an Existing Operation

- Obtaining a SRD (Service Request Definition) Template for a BMC Remedy Service Request

- Viewing ITSM Notations in App Portal and ITSM System

About the Configure Operation View

You open the **Configure Operation** view by clicking on an operation name in the ServiceNow, Remedy, or other ITSM system operation list. For example, the following is the Configure Operation view for the Create Remedy Incident operation:

Figure 3-9: Configure Operation View for Create Remedy Incident Operation

 The **Configure Operation** view has two sections: the operation settings and the parameter settings.

- About the Operation Settings

- About the Parameter Settings

About the Operation Settings

The operation settings, which are listed at the top of the **Configure Operation** view, identify the operation's name, associate an operation and operation type that exists in the ITSM system, and specifies the expected value that will be returned to App Portal when this operation is executed.

Table 3-4 • Operation Settings on the Configure Operation View

Property	Description
Enter a descriptive name	Name of the operation assigned by App Portal.
Select operation	Identifies the operation in the ServiceNow or Remedy system.
	For example, ServiceNow uses the `insert` operation to create incidents.
Select operation type	Identifies the type of operation in the ServiceNow or Remedy system.
	For example, the ServiceNow `insert` operation has a operation type of `CREATE`.
Select Return Field Mapping	Identifies the return value for this operation.
	When an ITSM incident is created, App Portal expects an incident ID to be returned. In the case of the **Create ServiceNow Incident** operation, the return value is a *strongly typed* object, which means that it consists of several primitive types: `sys_id` and `number`. Because `sys_id` represents the incident number, you would select `sys_id` from this list. App Portal will store the returned `sys_id` as a variable: Record ID.
	If the return value is a *primitive type* object, which means that it only consists of one parameter, select **Any Return Value** from this list.

About the Parameter Settings

For each parameter in the **Configure Fields** table, the following information is listed::

Table 3-5 • Properties in the Configure Fields Table

Property	Description
Field	Name of the parameter in the ITSM system. There are two types of parameters:
	• **Strongly typed object**—Parameter (or class) consisting of multiple primitive types or subparameters. For example, a parameter named `FullName` could consist of two subparameters: `FirstName` and `LastName`. A strongly typed object is displayed with a gray background, and each of its subparameters has a white background.
	• **Primitive object**—Parameter that has only one value, such as an integer (10), a decimal (10.0), or a string (text).
Type	Identifies the data type of the parameter, such as `System_String`, or `System_Boolean`.
Value	If a value is entered in this field, that value is sent to the ITSM system. If the field is blank, the ITSM will assign this parameter its default value.

Table 3-5 • Properties in the Configure Fields Table

Property	Description
Default Value	Used to provide a value to send to the ITSM system if no valid value was returned by App Portal. For example, supposed that the parameter is department and the valid values are IT, Engineering, Administration, or QA. If the catalog item triggering the ServiceNow incident did not have a department specified, then App Portal would send to ServiceNow the default value (such as None).
Valid Values	For some parameters, valid values are listed in this column. For example, the Reported_Source parameter for the **Create Remedy Incident** operation lists the following valid values listed below. Because the valid values are listed here, it makes it easy for you to select one and copy it to the **Default Value** column. ● DirectInput ● Email ● ExternalEscalation ● Fax ● SelfService ● etc.

The **Configure Fields** table lists all of the parameters associated with the selected ITSM system operation. However, App Portal only interacts with a portion of these parameters: those that relate to create, read, update, or delete tasks.

● **App Portal automatically defines mandatory parameters**—App Portal automatically defines parameters that are either mandatory for performing the operation or are descriptive. For each of these defined parameters, App Portal will gather data and pass it on to the ITSM system. App Portal variables will be replaced with incident-specific values at run time.

● **App Portal does not define optional parameters**—App Portal does not automatically define optional parameters. For those parameters that are not configured in App Portal, it is assumed that the ITSM system will insert its default value into that field when the incident is created.

● **Variables are used in strings**—Note that App Portal variables are used in parameters with a type of "string", and those variables will be replaced with incident-specific values at run time. The variables are used customize these notations to refer to a specific App Portal catalog item request. These notations will be displayed in both App Portal and in the ITSM system.

● **All incidents will use the same parameters**—Every incident that is created in the ITSM system will use the same data values, with the exception of the fact that variables are resolved at run time.

For example, for the Create ServiceNow Incident operation, App Portal defined the following parameters:

Table 3-6 • Defined Parameters for the Create ServiceNow Incident Operation

Field	Value
category	inquiry

Table 3-6 • Defined Parameters for the Create ServiceNow Incident Operation

Field	Value
comments_and_work_notes	New incident created by App Portal
description	Request for Catalog Item ##PackageTitle## was submitted in App Portal by ##FullName## for Device ##MachineName##
escalation	0
impact	2
incident_state	1
severity	3
short_description	Request for ##PackageTitle## was submitted in App Portal.
state	1
urgency	2

Configuring Additional Parameters

You may choose to define additional parameters in the **Configure Fields** table. If you want to pass a value for one of the initially undefined parameters to the ITSM system, you need to determine what the valid values are for that parameter in the ITSM system, and then enter the value that you would like to pass into the **Value** column for that parameter on the **Configure Operation** view.

Editing an Existing Operation

To edit an existing operation, perform the following steps:

Task   **To edit an existing operation:**

1. On the **Admin** tab, select **Site Management > ITSM Integration**. The **ITSM Integration** view opens, listing the available services of the connected systems.

If you are connected to Service Now, the following services could be listed:

- **ServiceNow - Catalog Import Set Management Service**

- **ServiceNow - Create Incident Management Service**

- **ServiceNow - Create Request Management Service**

- **ServiceNow - Update Task Sequence Request Management Service**

If you are connected to Remedy, five services are listed:

- **Remedy - Create Incident Management Service**

- **Remedy - Create Request Management Service**

- **Remedy - Incident Status Management Service Wrapper**

- **Remedy - Query Incident Management Service**

- **Remedy - Service Request Status Management Service Wrapper**

If you have added a connection to another ITSM system, it will be listed here.

2. Click on one of the services. A list of the operations included in the selected service opens:

3. Click on an operation. The **Configure Operation** view for that operation opens.

4. In the top part of this screen, review and edit the operation settings, as described in About the Operation Settings.

5. In the **Configure Fields** table, edit the parameters, as described in About the Parameter Settings.

Note • When configuring the `Request_Submit_Service` operation for a BMC Remedy service request, you need to enter a value in the `TitleInstanceID` field that identifies a BMC Service Request Definition template. For information on obtaining this value, see *Obtaining a SRD (Service Request Definition) Template for a BMC Remedy Service Request*.

6.   Click **Save** to save your edits.

Obtaining a SRD (Service Request Definition) Template for a BMC Remedy Service Request

When configuring the Request_Submit_Service operation of the **Create Remedy Service Request** or **Create Remedy Service Request for Cloud** service (on the **Configure Operation** view), you are required to enter the ID of a BMC SRD (Service Request Definition) Template in the **TitleInstanceID** field.

For instructions on how to create an SRD (Service Request Definition) Template from BMC Remedy and obtain this ID, review and follow the instructions in the following videos:

● **BMC Remedy ITSM: Configuring Service Request Management**
https://www.youtube.com/watch?v=-sUdcQiRjPQ

● **BMC Service Request Management: SRD Creation**
https://www.youtube.com/watch?v=sGl0nIC_fd0

Once you have created the Service Request Definition template, you can obtain the TitleInstanceID by using the following URL:

http://*YourInstanceName:PortNumber*/arsys/forms/YourInstanceName/SRD:ServiceRequestDefinition_Base

The BMC **Service Request Definition ID+** page opens.

Figure 3-10: InstanceID of a BMC Service Request Definition

Then, open the **Create Remedy Service Request** or **Create Remedy Service Request for Cloud** operation (in the **Remedy - Create Request Management Service** system), and paste the **InstanceID** you copied from the SRD into the **TitleInstanceID** field of the **Configure Fields** table.

Viewing ITSM Notations in App Portal and ITSM System

When App Portal is integrated with an ITSM system, notations are made in both App Portal and the ITSM system to track the progress of an incident. In the following example, a notation of the creation of an ITSM incident, with its ticket number, appears on the **Notes** tab of the **Request Details** dialog box.
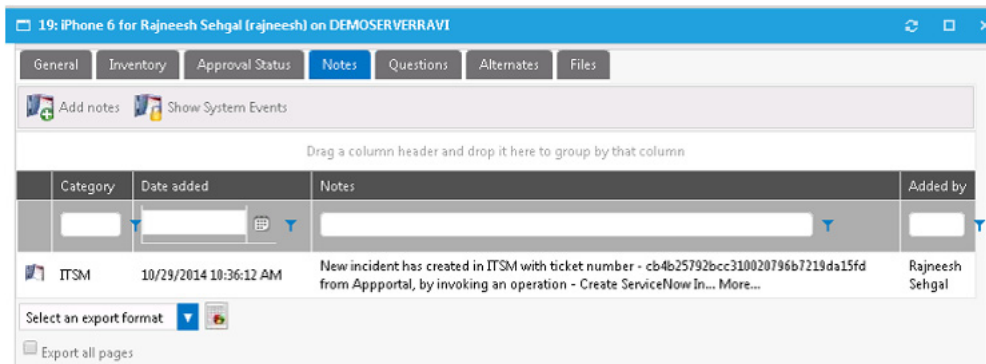
Figure 3-11: Notation from ITSM System Displayed on the Notes Tab of Request Details Dialog Box

Below is an example of a notation that is made in the ITSM system when App Portal created an incident. Note that the text that is displayed was defined in the **Value** field for the **short_description** parameter.
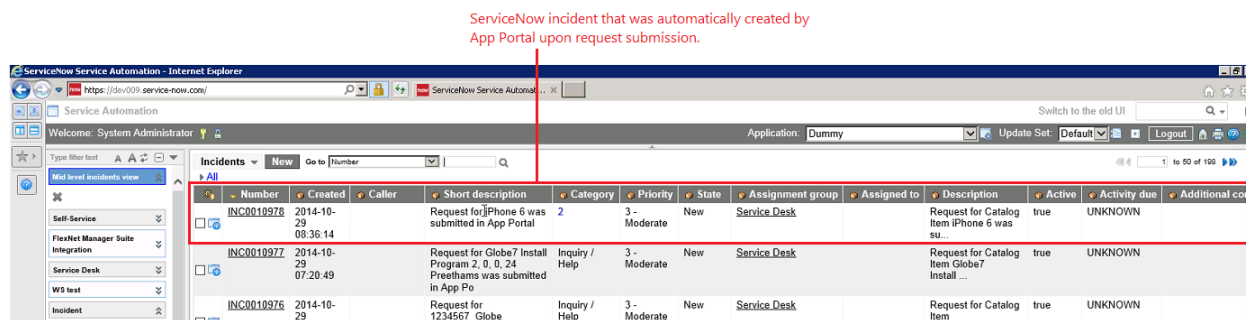
Figure 3-12: Notation Identifying ITSM Incident Created by App Portal

Setting ITSM Actions on Catalog Items

In order for a catalog item request to trigger an event in an ITSM system, you need to define ITSM-specific actions. These ITSM actions can be specified both on a global level or on a specific catalog item:

● **Global level**—Open the **Site Management > Commands & Actions > Request Commands** view and add the ITSM action to an event. If the ITSM action is defined here, it will apply to all catalog items.

● **Catalog item level**—Open the Actions tab of the Catalog Item Properties dialog box and add the ITSM action to an event. **If the ITSM action is defined here, it will apply to only this specific catalog item.**

You can select any of the actions in the **Current Events and Actions** column and then associate an ITSM action to it. In the following example, an ITSM-related action has been associated with the **On Submit**, **On Cancel,** and **On Check Status** events. Upon the submission of a request containing this catalog item, a **Create ServiceNow Incident** action will be triggered:
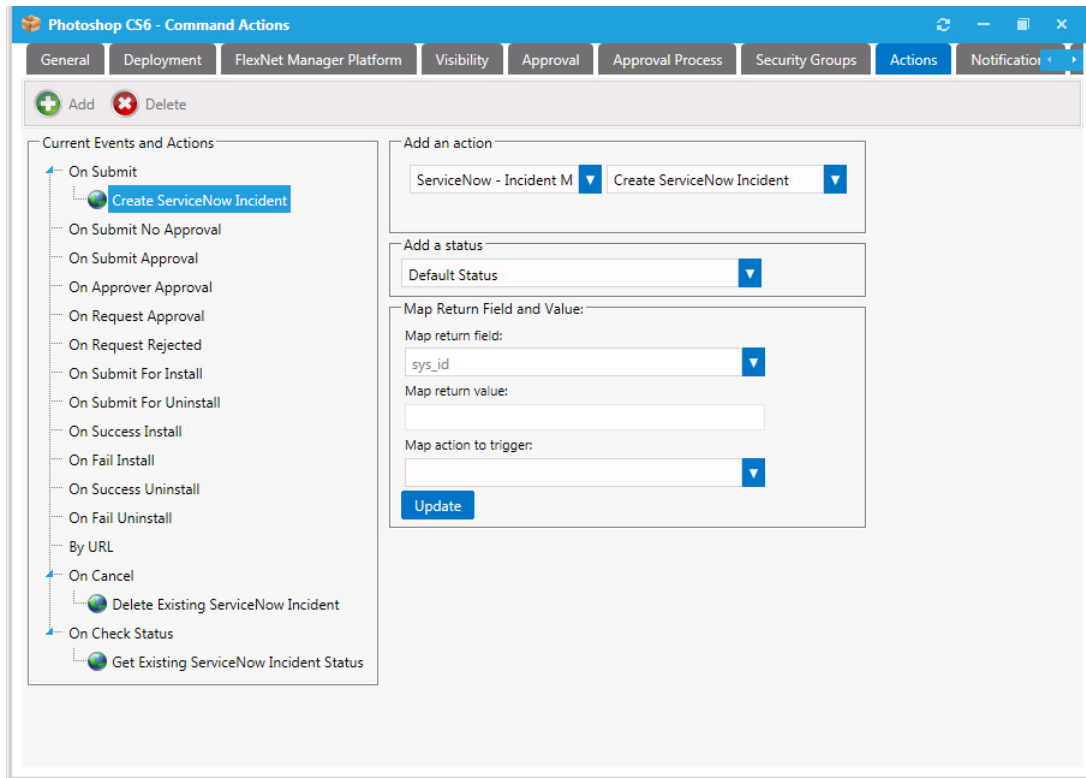
Figure 3-13: ITSM-Related Actions on a Catalog Item

To add an ITSM action, perform the following steps.

Task   ***To add an ITSM action to a catalog item:***

1.   Do one of the following:

     ● Open the **Actions** tab of the catalog item's **Catalog Item Properties** dialog box.

     ● Open the **Site Management > Commands and Actions > Request Commands** view.

     The Actions view opens.

2. In the **Current Events an Actions** tree, select the event that you want to add an action to.

   For example, if you want to trigger the creation of an incident in the ITSM system when catalog items are submitted in a request, select **On Submit**.

3. From the **Select a service** list, select the name of the ITSM operation that you want to trigger. For example, you could select **Create ServiceNow Incident.**

4. [If applicable] From the **Add a status** list, select one of the following statuses to indicate the status that the request will be assigned after this action is performed:

   ● Default Status

   ● Completed

   ● In Progress

   ● Warning

5. The **Map return field** list will be pre-selected based upon the action and operation that you picked.

6. [If applicable] In the **Map return value** field, enter the value that you want to match, such as when you are adding an action to an **On Check Status** event. In this instance, you would want to take some action depending upon what value is returned from the ITSM system. For example, if the **Map return value** is set to **True**, then you want App Portal to trigger the action you select.

7. [If applicable] From the **Map action to trigger** list, select one of the following three actions that you want App Portal to trigger if the return value from the ITSM system matches the value entered in the **Map return value** field:

   ● Execute Operation

   ● Initiate Deployment

   ● Cancel App Portal Request

> *Note • The* ***Initiate Deployment*** *action could be used if you want to perform the approval process in the external ITSM system, not in App Portal. As soon as App Portal received notification of the approval in ITSM, deployment could be triggered. For more information on setting this up, see* Deploying via API to Enable App Portal Approvals in an External ITSM System*.*

8. Click **Add** to add the action.

About the On Check Status Event

The **On Check Status** event exists specifically for use in ITSM integration. If this event is associated with an action, App Portal will periodically monitor the ITSM system for a particular status. The moment that App Portal detects that the selected status has been reached, an additional action can be taken. For example, if a status of **Approved** is reached in a ServiceNow incident, App Portal could then trigger the deployment of the software.

Deploying via API to Enable App Portal Approvals in an External ITSM System

When a request is submitted, if a catalog item does not require an approval, App Portal automatically triggers deployment of that catalog item. However, if you have integrated App Portal with an ITSM system and you want to perform approvals using that system, you would not want the catalog item to be deployed until the external approval was performed.

In this situation, you would need to select the **Start deployment using API?** option on a catalog item's **Deployment > Global** tab of the **Catalog Item Properties** dialog box to delay deployment until a response from the ITSM system would trigger the deployment via App Portal's API.

In any other scenario, this option can also be used to have more control over deployment, post-request submission.

Integrating With the ServiceNow User Interface

To display App Portal within the ServiceNow user interface, and to make it available as a selection on the ServiceNow application menu, perform the following steps.

Task   ***To add App Portal to the ServiceNow user interface:***

1. Launch your instance of ServiceNow.

2. Locate the **Self Service** menu, which is located along the left side of the interface.
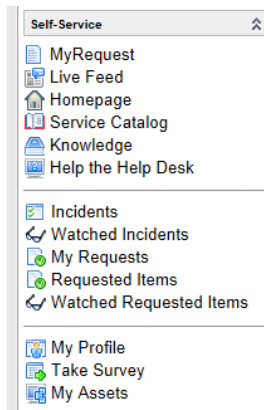
3. Click on **Self-Service** and select **Edit Application Menu** from the context menu. The **Application Menu** view opens.

4. Click **New**. The New Module view opens.

5. Enter the following information:

Property	Value
Title	Flexera Software App Portal
Link type	URL (from Arguments)
Application menu	Self-Service
Arguments	`http://APPPORTALSERVERNAME/esd/DefaultForUIEmbedding.aspx`

6. Click **Submit**. Now **Flexera Software App Portal** should be listed on the **Self-Service** menu.

7. In the **Self-Service** menu, click **Flexera Software App Portal**. App Portal will open in the right pane of the ServiceNow interface.
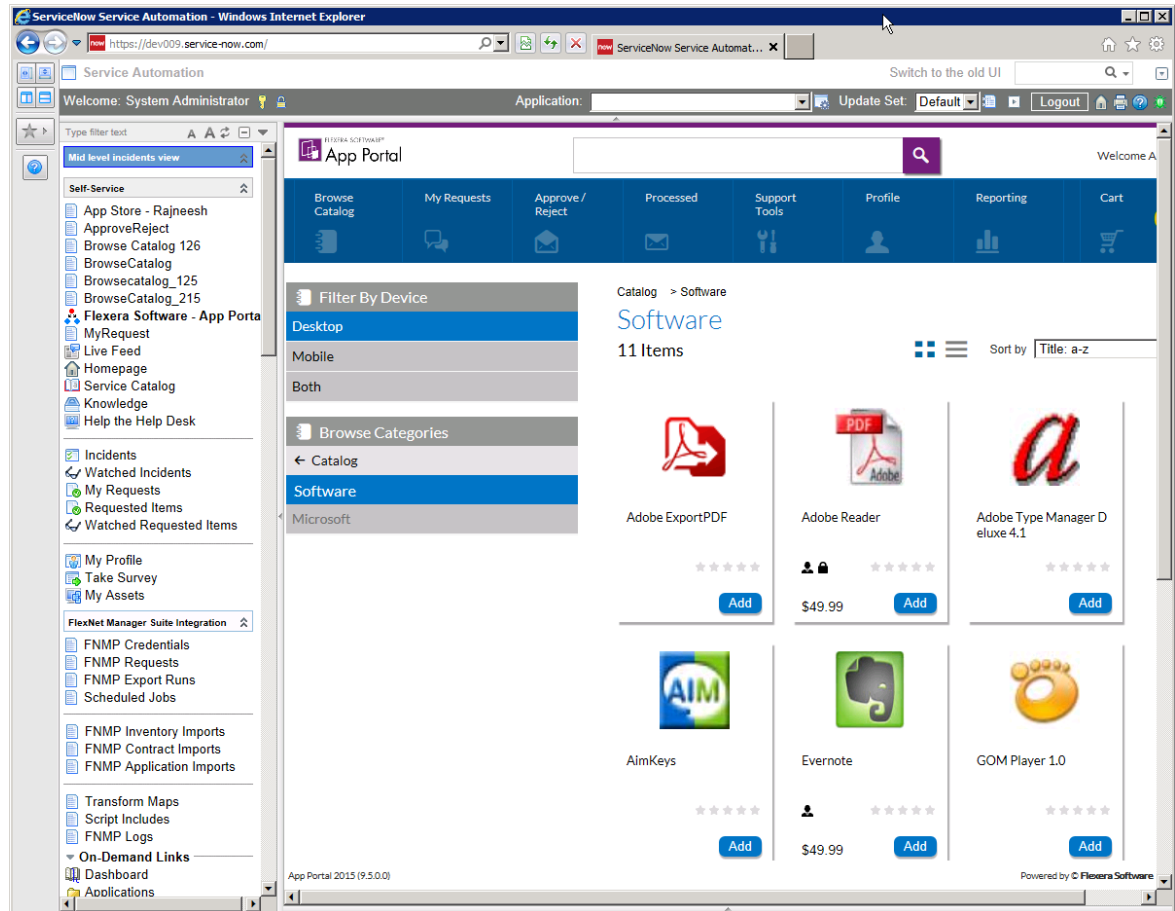
Integrating With Another ITSM System

If you want to integrate with an ITSM system other than ServiceNow or Remedy, you can use App Portal's framework to perform the integration.

- Adding a New ITSM System

- Adding and Configuring New Operations

- Configure Catalog Items

Adding a New ITSM System
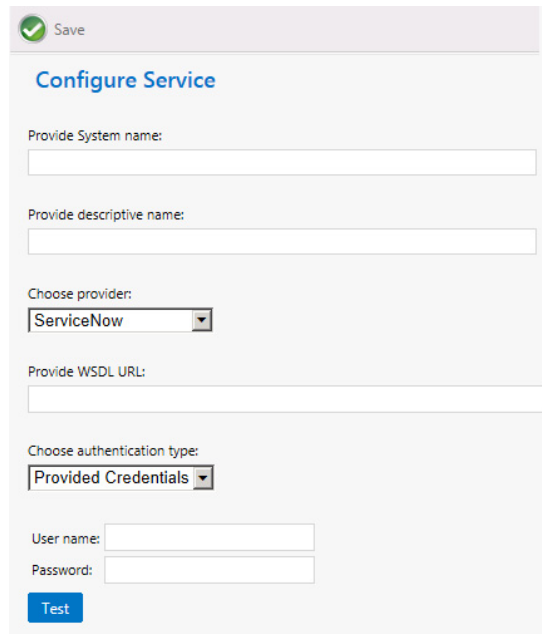
To integrate with an ITSM system other than ServiceNow or Remedy, click **Add System** on the **Site Management > ITSM Integration** view and enter the connection information on the **Configure Service** view.

Task   **To add a new ITSM system:**

1. Open the **Site Management > ITSM Integration** view.

2. Click **Add System**. The **Configure Service** view opens.

3. In the **Provide System name** field, enter a brief name to identify this ITSM system.

4. In the **Provide descriptive name** field, enter a brief description of this ITSM system. This description will be listed in the **System Description** column of the **ITSM Integration** view.

5. From the **Choose provider** list, select **Others**.

6. In the **Provide WSDL URL**, enter the URL to your instance of the ITSM system.

Important • Do not use any special characters in the URL field. The only special character that is permitted is _ (underscore). Dashes (-) and other special characters are not permitted.

7. From the **Choose authentication type** list, select either **Provided Credentials** or **Integrated** to indicate the authentication type. If you chose **Provided Credentials**, you also need to enter a **User name** and **Password**.

8. Click **Test** to test the connection to the ITSM system.

9. Click **Save** to save these settings. The new ITSM system is now listed on the **ITSM Integration** view.

Adding and Configuring New Operations

If you connect to an ITSM system other than ServiceNow or Remedy, you will have to create all of the required operations manually. To create an new operation, perform the following steps:

Task **To create a new operation:**

1. On the **Admin** tab, select **Site Management > ITSM Integration**. The **ITSM Integration** view opens, listing the available services of the connected systems.

If you have added a connection to another ITSM system, it will be listed here.

2. Click on the **System Name** of the connection to your new ITSM system. A list of the operations defined for the selected service opens, if any.

3. Click **Add Operation**. The **Configure Operation** view opens.

4. In the top part of this screen, define the following properties:

Property	Description
Enter a descriptive name	Enter a name to identify this new operation.
Select operation	From this list, select the operation that the ITSM system uses to perform the desired operation.
Select operation type	From this list, select the operation type of the operation selected in the **Select operation** list.
Select Return Field Mapping	Select the return value for this operation. - If the return value is a *strongly typed* object, which means that it consists of several primitive types, select the primitive type that would identify this record in App Portal. - If the return value is a *primitive type* object, which means that it only consists of one parameter, select **Any Return Value** from this list.

5. In the **Configure Fields** table, add and configure all of the parameters required for this operation (defined in the ITSM system documentation), as described in About the Parameter Settings.

6. Click **Save** to save to create the operation.

Configure Catalog Items

In order for a catalog item request to trigger an event in an ITSM system, you need to define ITSM-specific actions on that catalog item. This is done on the **Actions** tab of the **Catalog Item Properties** dialog box.

Because you have already added the ITSM system to App Portal (as described in Adding a New ITSM System) and added the required operations (as described in Adding and Configuring New Operations) , you will now be able to select the ITSM system and the operation from the lists in the **Add an action** section of the **Actions** tab of the **Catalog Item Properties** dialog box. You will be able to select any of the actions in the **Current Events and Actions** column and then associate an ITSM action to it.

For instructions on how to add actions to catalog items for this new ITSM system, see Setting ITSM Actions on Catalog Items.

Accessing Custom Attributes Obtained from a Custom SQL Sync Query in an ITSM System

After you perform a custom SQL sync query, you can access the additional Active Directory attributes that you obtained during the sync by creating custom variables, either globally or per catalog item. Custom variables are available for use in custom script commands, external web actions, and ITSM calls.

To pass the value of an Active Directory attribute obtained during a custom SQL sync query into an ITSM call, perform the following steps.

Task   ***To pass the value of Active Directory attribute obtained during a custom SQL sync query into an ITSM call:***

1. On the **Admin** tab, open the **Catalog Management** > **Catalog** > **Custom Variables** view.

   *Note • You also have the option of adding custom variables to an individual catalog item on the **Custom Variables** tab of the **Catalog Item Properties** dialog box.*

2. Click **Add New Variable**. A dialog box opens prompting you to define the variable.

   Variable Name
   Custom_

   Value

   Description

   Add Variable

3. Enter the following information to define the custom variable:

   - **Variable Name**—Enter any user-defined name.

   - **Value**—Enter the value of an Active Directory attribute that you have synced as part of a custom SQL sync query.

   - **Description**—Enter a description of the variable and its value.

   For example:

   Variable Name
   Custom_   SkypeUserName

   Value
   ##SkypeUserName##

   Description
   User name required to logon to a Skype video conference.

   Add Variable

   *Note • A prefix of **Custom_** is automatically added to the **Variable Name**.*

4. Click **Add Variable** to save the variable.

5. Open the **Site Management > ITSM Integration** view.

6. Click on a name in the **System Name** column. The list of operations for that system opens. The following is a list of operations associated with the **ServiceNow - Create Incident Management Service**.

7. Click on an operation name in the list, such as **Create ServiceNow Incident** or **Create Remedy Incident**. The **Configure Operation** view opens.

8. In the **Value** and/or **Default Value** column of the field where you want to use the custom variable, enter text containing the custom variable enclosed in ##, such as:

When this field is resolved in the ITSM system, the value of this custom variable will be displayed.

9. Click **Save**.

Configuring Cloud Application Integration

If you integrate App Portal with a cloud application, App Portal will be able to include a catalog item that, when checked out on the Browse Catalog tab, will create an account in that cloud application for the requester. The requester will then receive an email that includes account login details.

By integrating App Portal with cloud applications, it enables you to provision cloud applications with the same level of automation and control as desktop and mobile applications. Your users would be able to request cloud applications from the same store they get mobile and desktop applications.

- Integrating With Box, Salesforce and Office 365

- Integrating With Other Cloud Applications

Integrating With Box, Salesforce and Office 365

App Portal provides out-of-the-box support for three cloud applications—Box, Salesforce, and Microsoft Office 365—and automatically creates a catalog item for each. However, before you can make one of these catalog items available in your catalog, you need to connect to Box, Salesforce, and/or Office 365 and enter your company's account information.

- Connecting to Box, Salesforce, and Office 365

- Using Out-of-the-Box Catalog Items for Box, Office 365, Salesforce

- Creating Cloud Catalog Items to Request Box, Office 365, and Salesforce Access Using ITSM System

Connecting to Box, Salesforce, and Office 365

App Portal can be integrated with cloud applications so that App Portal can offer a catalog item that will either automatically create an account for the requester in that cloud application, or submit a request in an ITSM system to create an account for the requester in that cloud application.

App Portal provides out-of-the-box support for three cloud applications—Box, Salesforce, and Microsoft Office 365—and automatically creates these three catalog items.
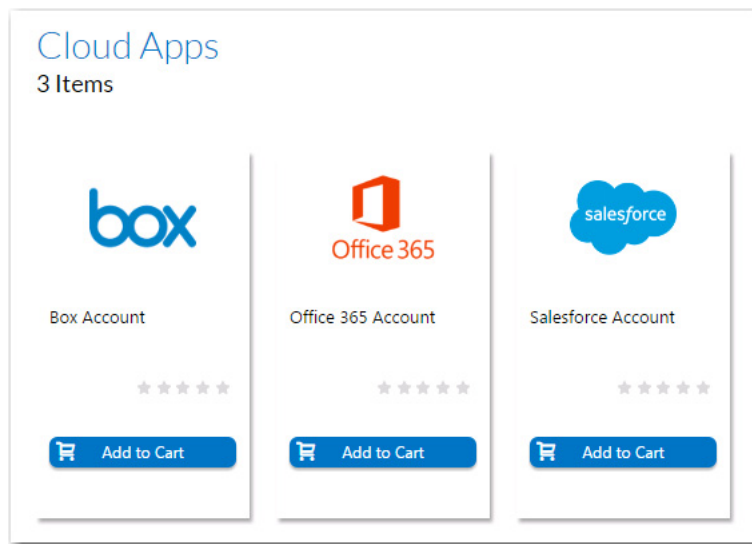
Figure 3-14: Out-of-the-Box Cloud Catalog Items

To enable this feature, you need to connect App Portal to these cloud applications by performing the following steps.

Important • *Because some of the settings need to be stored locally, when you enter cloud application connection settings, you must be on the machine where App Portal is installed.*

Task   **To connect App Portal to a cloud application:**

1. Log on to the vendor web site and create a custom cloud application for your organization. You will obtain the credentials and end points required to integrate App Portal with that cloud application. For information, see the following sites:

Cloud Application Vendor	Help Topic
Box.com	https://box-content.readme.io/docs/box-platform
Salesforce	http://www.salesforce.com/platform/getting-started/
Microsoft Office 365	http://dev.office.com/

2. On the App Portal **Admin** tab, open the **Site Management > Settings > Cloud Apps** view.

3. Open the **Box**, **Salesforce**, or **Office 365** tab.

Note • *All three of the tabs on the* **Cloud Apps** *view have the same fields and buttons.*

4.   Enter the following credentials and end points, which were obtained when your corporate account with the cloud application vendor was created:

Property	Description
Client ID	Enter the client ID that was provided to you by the cloud application vendor.
Client Secret	Enter the client secret code that was provided to you by the cloud application vendor.
Redirect URL	Enter the redirect URL that was provided to you by the cloud application vendor. The redirect endpoint is the endpoint in the client application where the resource owner is redirected to, after having granted authorization at the authorization endpoint. **Important** • *This URL must be on the local machine (the machine where App Portal is installed).*
Authorization end point	Enter the endpoint on the authorization server where the resource owner logs in, and grants authorization to the client application.
Token end point	Enter the endpoint on the authorization server where the client application exchanges the authorization code, client ID and client secret, for an access token.
API URL	Enter the API URL for the cloud application vendor.

5. Click **Save and Generate Access Token**. A message box opens stating that the cloud application vendor credentials were saved successfully, and prompting you to perform additional tasks to generate a token.
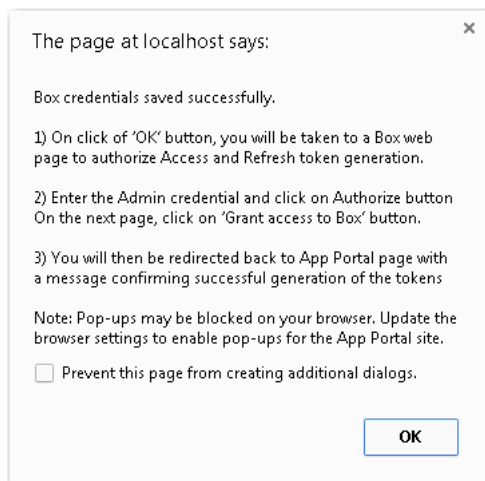
6. Click **OK** on the dialog box. A web page opens where you will be prompted to grant access to the cloud application.
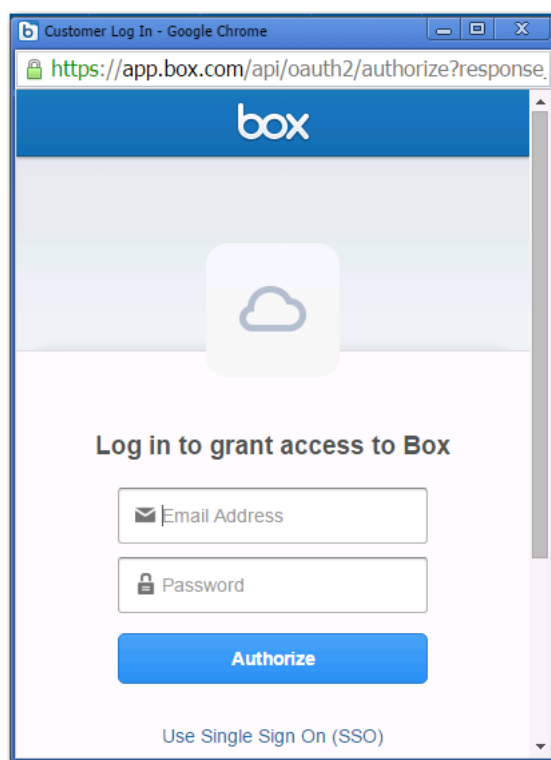
7. Enter your user ID and password to the cloud application. You are then prompted to grant access to the cloud application.
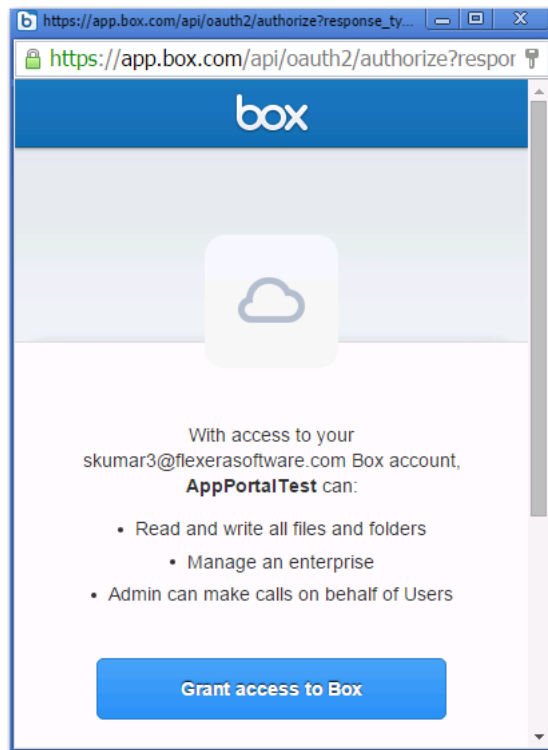
8. Click the **Grant access** button. A message appears in App Portal confirming successful creation of the access token.
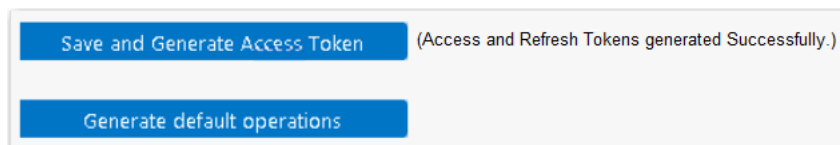
The access token is saved in the App Portal database. Whenever an account is requested, App Portal will use this token to authenticate the user.

9. Click the **Generate default operations** button. A message opens stating that the operations were created successfully.
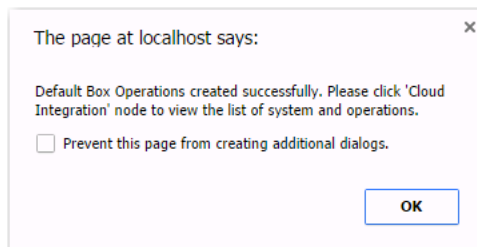
10. Click **OK**.

11. Open the **Site Management > Cloud Integration** view, and then click on the name of the connected cloud application. A **Create user account** operation will be listed for each of the connected cloud applications.

Using Out-of-the-Box Catalog Items for Box, Office 365, Salesforce

App Portal provides out-of-the-box support for three cloud applications: Box, Salesforce, and Microsoft Office 365. App Portal automatically creates these three catalog items.
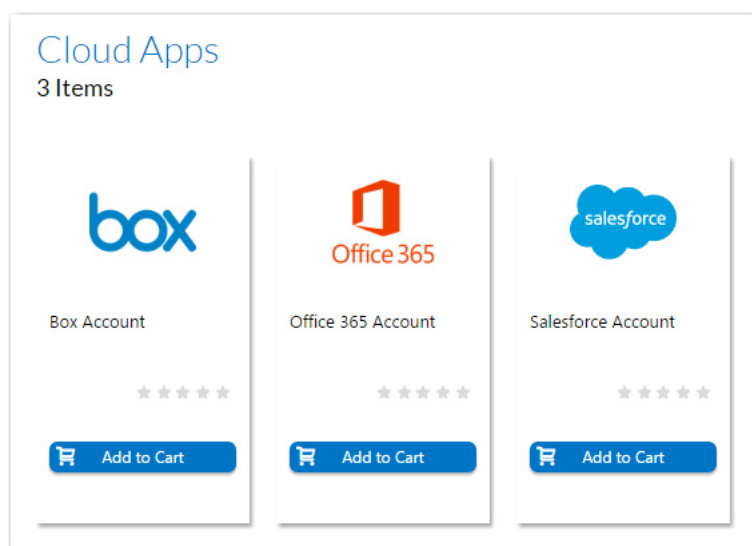
Figure 3-15: Out-of-the-Box Catalog Items for Box, Office 365, and Salesforce

Once you have created a custom cloud application for your organization on the Box, Office 365, or Salesforce website, and have then performed the steps in Connecting to Box, Salesforce, and Office 365, you can make these catalog items available in your App Portal storefront.

To make these catalog items available in your App Portal storefront, perform the following steps.

Task   *To enable out-of-the-box cloud catalog items:*

1. On the **Admin** tab, select **Catalog Management > Current Catalog** Items.

2. Open the **Catalog Item Properties** dialog box for the Box, Salesforce, or Office 365 catalog item that you want to enable.

3. On the **General > Global** tab, select the **Is enabled?** option under **Global Options**.
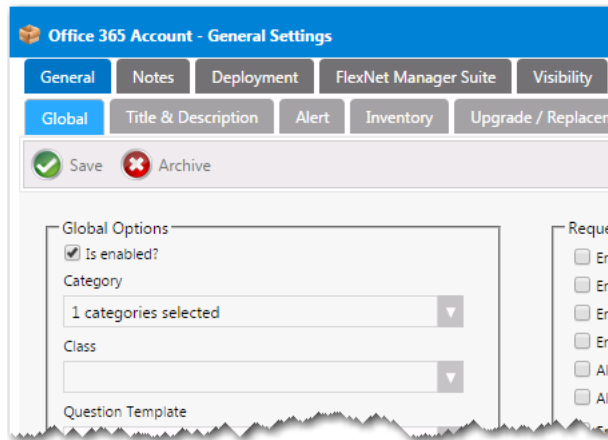
4.   Click **Save**.

Creating Cloud Catalog Items to Request Box, Office 365, and Salesforce Access Using ITSM System

Rather than using the out-of-the-box catalog items to directly request a Box, Office 365, or Salesforce account from the vendor, you can set up a cloud catalog item to generate a request in an ITSM system for account creation in Box, Office 365, or Salesforce.

Task   ***To create a cloud catalog item to request Box, Office 365, or Salesforce access using an ITSM system:***

1.   Create a new cloud catalog item, as described in Creating a Cloud Catalog Item. Select **Others** on the **Cloud Account Type** panel of the New Catalog Item Wizard.

2.   Open the **Actions** tab of the cloud catalog item's **Catalog Item Properties** dialog box.

3.   Select the **On Submit** node in the **Current Events and Actions** tree.

4.   From the **Select a service** and **Select a method or command** lists, select one of the following sets of options:

ITSM System	Select a service	Select a method or command
BMC Remedy	Remedy - Create Request Management Service	Create Remedy Service Request for Cloud
ServiceNow	ServiceNow - Create Request Management Service	Create ServiceNow Request for Cloud

5.   Click **Save**.

Passing Cloud Variables to the ITSM System

When you use an ITSM system to request account creation in a cloud application, App Portal uses the ##Cloud_Variables## variable to pass all the attached cloud variables with the catalog item to the ITSM system.

ServiceNow

For ServiceNow, cloud variables get resolved in the description field of the **insert** suboperation of the **Create ServiceNow Request for Cloud** operation.

description	System.String	##Cloud_Variables##

Figure 3-16: ServiceNow: "description" Field of the "insert" Suboperation

Remedy

For Remedy, cloud variables get resolved in the Details field of the **Request_Submit_Service** suboperation of the **Create Remedy Service Request for Cloud** operation.

Details	System.String	##Cloud_Variables##

Figure 3-17: BMC Remedy: "Details" Field of the "Request_Submit_Service" Suboperation

Integrating With Other Cloud Applications

App Portal can be integrated with cloud applications so that App Portal can offer a catalog item that will automatically create an account for the requester in that cloud application. App Portal provides out-of-the-box support for Box, Salesforce, and Microsoft Office 365, and automatically creates these three catalog items.

However, you can also manually create a connection to another cloud application system (such as DropBox, WebEx, GotoMeeting, Concur, etc.) so that you can create catalog items for that system.

- Adding Web Services for a New Cloud Application

- Adding a New Cloud Application System

- Adding Operations for Cloud Applications

- Setting Cloud Application Actions on Catalog Items

- Adding Custom Variables to Cloud Catalog Items

Adding Web Services for a New Cloud Application

To add a new cloud application to App Portal, you need to write web services for that application. App Portal provides sample web methods that you can copy and modify per the new cloud application's API requirements.

Task **To add web services for the new cloud application:**

1. Make a copy of the following file:

   ```
   C:\Program Files (x86)\Flexera Software\App Portal\Web\WS\SaasIntegration.asmx
   ```

2. Locate a [WebMethod] section in this file:

```
[WebMethod]
public string CreateUserInOffice365(string Cloud_Variable)
{
    string result = string.Empty;
    try
    {
        var input = GetVariables(Cloud_Variable);

        string accountEnabled, disabledPlans, skuId, city, country, department, dirSyncEnabled, display
        string mail, mailNickName, mobile, otherMails, passwordPolicies, password, forceChangePasswordN
        string state, streetAddress, surname, telephoneNumber, usageLocation, userPrincipalName, userTy

        accountEnabled = disabledPlans = skuId = city = country = department = dirSyncEnabled = display
        mail = mailNickName = mobile = otherMails = passwordPolicies = password = forceChangePasswordNe
        state = streetAddress = surname = telephoneNumber = usageLocation = userPrincipalName = userTyp

        var list = input.Keys.ToList();

        if (list.Contains("accountenabled", StringComparer.OrdinalIgnoreCase)) { accountEnabled = input
        if (list.Contains("disabledplans", StringComparer.OrdinalIgnoreCase)) { disabledPlans = input[l
        if (list.Contains("skuid", StringComparer.OrdinalIgnoreCase)) { skuId = input[list.First(x => x
        if (list.Contains("city", StringComparer.OrdinalIgnoreCase)) { city = input[list.First(x => x.1
        if (list.Contains("country", StringComparer.OrdinalIgnoreCase)) { country = input[list.First(x
        if (list.Contains("department", String      rer.Ordin                        rtment = inp
```

3. Modify the [WebMethod] section per the new cloud application's API requirement.

4. Copy the new .asmx file to the same location as SaasIntegration.asmx.

Adding a New Cloud Application System

To add a new cloud application system, perform the following steps.

Task   **To edit an existing cloud application system:**

1. First, perform the steps in Adding Web Services for a New Cloud Application.

2. In App Portal, open the **Site Management > Cloud Integration** view.

3. Click **Add System**. The **Configure Service** view opens.

4. Enter the following properties:

Property	Description
Provide System name	Enter a name that to identify this cloud application system.
Provide descriptive name	Enter a brief description of this cloud application system. This description is listed in the **System Description** column of the **Cloud Integration** view.
Choose provider	Select **Others**.
Provide WSDL URL	Enter the URL to `.asmx` file you created in Adding Web Services for a New Cloud Application, followed by `?wsdl`: `http://localhost/esd/WS/MyCloudAppIntegration.asmx?wsdl` **Important** • *Do not use any special characters in the URL field. The only special character that is permitted is _ (underscore). Dashes (-) and other special characters are not permitted.*
Choose authentication type	Select either **Provided Credentials** or **Integrated** to indicate the authentication type. If you chose **Provided Credentials**, you also need to enter a **User name** and **Password**.

Property	Description
Test	Click to test the service settings
Email Address for Alerts	Enter email addresses, one entry per line, to be notified when alerts are generated in relation to this service.

5. Click **Save** to save your edits.

Adding Operations for Cloud Applications

When integrating with Box, Salesforce, or Office 365 cloud applications (which are supported out-of-the-box), the default operations are created and configured automatically when you click the **Generate default operations** button on one of the tabs of the **Site Management > Settings > Cloud Apps** view.

However, if you connect to a cloud application other than Box, Salesforce, or Office 365 (as described in Adding a New Cloud Application System), you will have to create all of the required operations manually.

Also, you may choose to customize/configure existing out-of-the-box operations for your organization.

This section explains how to add and configure operations on the **Configure Operation** view.

- About the Configure Operation View for Cloud Applications

- Adding a New Operation for a Cloud Application

About the Configure Operation View for Cloud Applications

You open the **Configure Operation** view by clicking on an operation name in the Box, Office 365, Salesforce, or other cloud application system operation list. For example, the following is the **Configure Operation** view for the Box **Create User Account** operation:

Figure 3-18: Configure Operation View for Box Create User Account Operation

The **Configure Operation** view has two sections: the operation settings and the parameter settings.

- About the Operation Settings

- About the Parameter Settings

About the Operation Settings

The operation settings, which are listed at the top of the **Configure Operation** view, identify the operation's name, associate an operation and operation type that exists in the cloud application, and specifies the expected value that will be returned to App Portal when this operation is executed.

Table 3-7 • Operation Settings on the Configure Operation View

Property	Description
Enter a descriptive name	Name of the operation assigned by App Portal.
Select operation	Identifies the operation in the cloud application. For example, Box uses the `CreateUserInBox` operation to create a user account. *Note • When configuring an operation for a new cloud application, you need to first add web services to the App Portal `saasintegration.asmx` file in order to populate this list, as described in Adding Web Services for a New Cloud Application.*
Select operation type	Identifies the type of operation in the cloud application. For example, the Box `CreateUserInBox` operation has a operation type of `CREATE`.
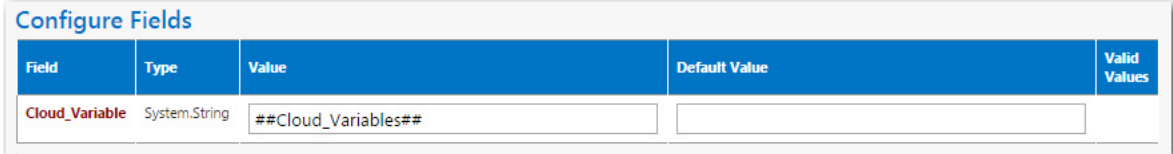
Table 3-7 • Operation Settings on the Configure Operation View

Property	Description
Select Return Field Mapping	Identifies the return value for this operation. When a cloud account is created, App Portal expects a value to be returned. Because the return value is a *primitive type* object, which means that it only consists of one parameter, select **Any Return Value** from this list.

About the Parameter Settings

For a Cloud Application operation, only one field needs to be listed in the Configure Fields table, **Cloud_Variable**, with a value of ##Cloud_Variables##.

You can add variables to a cloud application on the **Cloud Apps** tab of the **Catalog Item Properties** dialog box for this cloud application's catalog item, as described in Defining Custom Variables for Cloud Catalog Items.

Figure 3-19: Cloud_Variable for Cloud Application Operation

Adding a New Operation for a Cloud Application
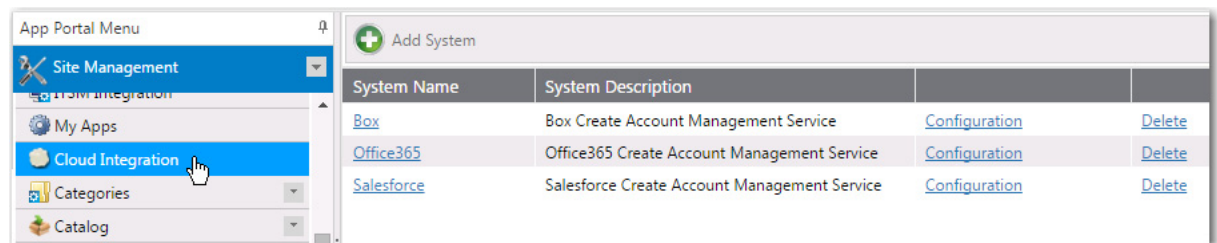
If you connect to a cloud application other than Box, Salesforce, or Office 365, you will have to create all of the required operations manually. To create an new operation, perform the following steps:

Task   **To create a new operation for a cloud application:**

1. On the **Admin** tab, select **Site Management > Cloud Integration**. The **Cloud Integration** view opens, listing the available services of the connected cloud applications.

    If you have added a connection to another cloud application, it will be listed here.

2. Click on the **System Name** of the cloud application to which you want to add an operation. A list of the operations defined for the selected service opens, if any.

3. Click **Add Operation**. The **Configure Operation** view opens.

4. In the top part of this screen, define the following properties:

Property	Description
Enter a descriptive name	Enter a name to identify this new operation.
Select operation	From this list, select the operation that the cloud application uses to perform the desired operation. **Important •** *In order for an operation to be listed in this drop down list for a new cloud application, you need to have performed the steps in* Adding Web Services for a New Cloud Application.
Select operation type	From this list, select the operation type of the operation selected in the **Select operation** list: **CREATE**, **DELETE**, or **INVOKE**.
Select Return Field Mapping	Select the return value for this operation. ● If the return value is a *strongly typed* object, which means that it consists of several primitive types, select the primitive type that would identify this record in App Portal. ● If the return value is a *primitive type* object, which means that it only consists of one parameter, select **Any Return Value** from this list.

5. In the **Configure Fields** table, enter the following value for the **Cloud_Variable** field: `##Cloud_Variables##`.

Important • *Do not add any additional fields to the Configure Fields table. Instead, you can add variables to the **Cloud Apps** tab of the **Catalog Item Properties** dialog box for this cloud application's catalog item, as described in* Defining Custom Variables for Cloud Catalog Items.

6. Click **Save** to save to add the operation.

7. Proceed with the steps described in Setting Cloud Application Actions on Catalog Items and Adding Custom Variables to Cloud Catalog Items.

Setting Cloud Application Actions on Catalog Items

In order for a catalog item request to trigger an event in a cloud application, you need to define cloud application-specific actions on that catalog item. This is done on the **Actions** tab of the **Catalog Item Properties** dialog box. These cloud application actions can be specified on a specific catalog item, but only those that have a type of **Cloud Catalog Item**.

Note • Before you can set a cloud application action on a catalog item for a new cloud application, you need to have already added the cloud application to App Portal (as described in Adding a New Cloud Application System) and added the required operations (as described in Adding Operations for Cloud Applications).

You can select any of the actions in the **Current Events and Actions** column and then associate a cloud application action to it. In the following example, a cloud application-related action has been associated with the **On Submit** event. Upon the submission of a request containing this catalog item, a **Create user account** action will be triggered:
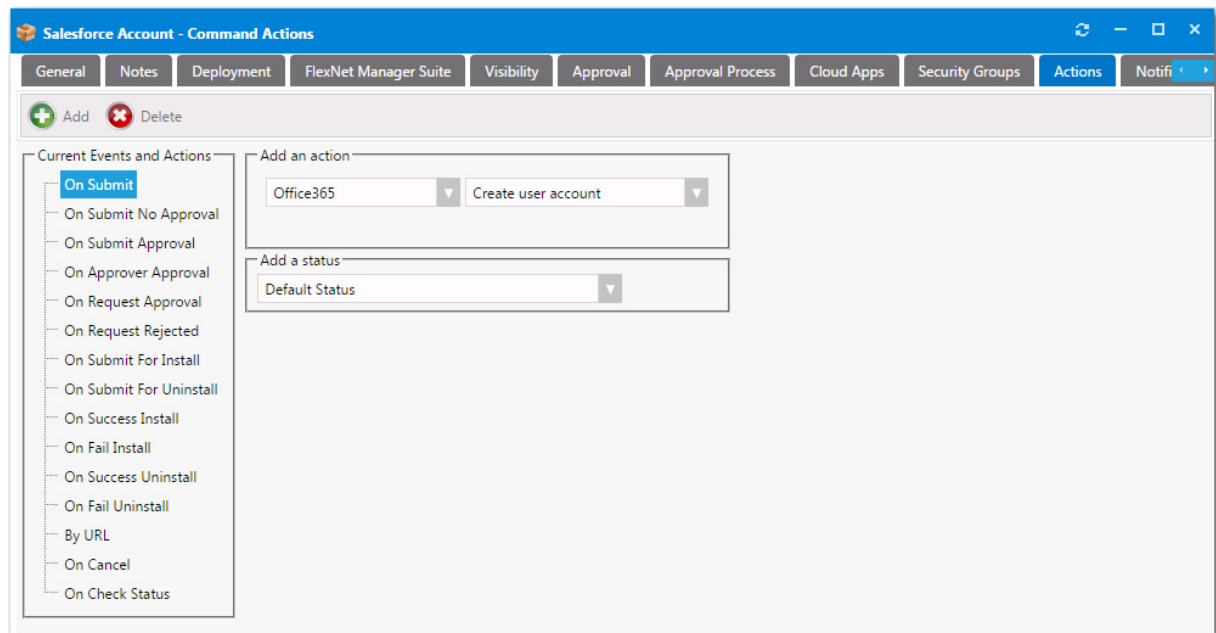
Figure 3-20: Cloud Application-Related Actions on a Catalog Item

To add an action to a cloud catalog item, perform the following steps.

Task **To add an action to a cloud catalog item:**

1. Open the **Actions** tab of the catalog item's **Catalog Item Properties** dialog box.

2. In the **Current Events an Actions** tree, select the event that you want to add an action to.

For example, if you want to trigger the creation of a user account in the cloud application when catalog items are submitted in a request, select **On Submit**.

3.   From the **Select a service** list, select the name of the cloud application operation that you want to trigger. For example, you could select **Create user account.**

4.   [If applicable] From the **Add a status** list, select one of the following statuses to indicate the status that the request will be assigned after this action is performed:

- **Default Status**

- **Completed**

- **Failed**

- **In Progress**

- **Succeeded**

- **Warning**

5.   Click **Add** to add the action.

Adding Custom Variables to Cloud Catalog Items

For the out-of-the-box cloud catalog items or Salesforce, Box, and Office 365, the necessary variables are automatically created and displayed on the **Cloud Apps** tab of the **Catalog Item Properties** dialog box.
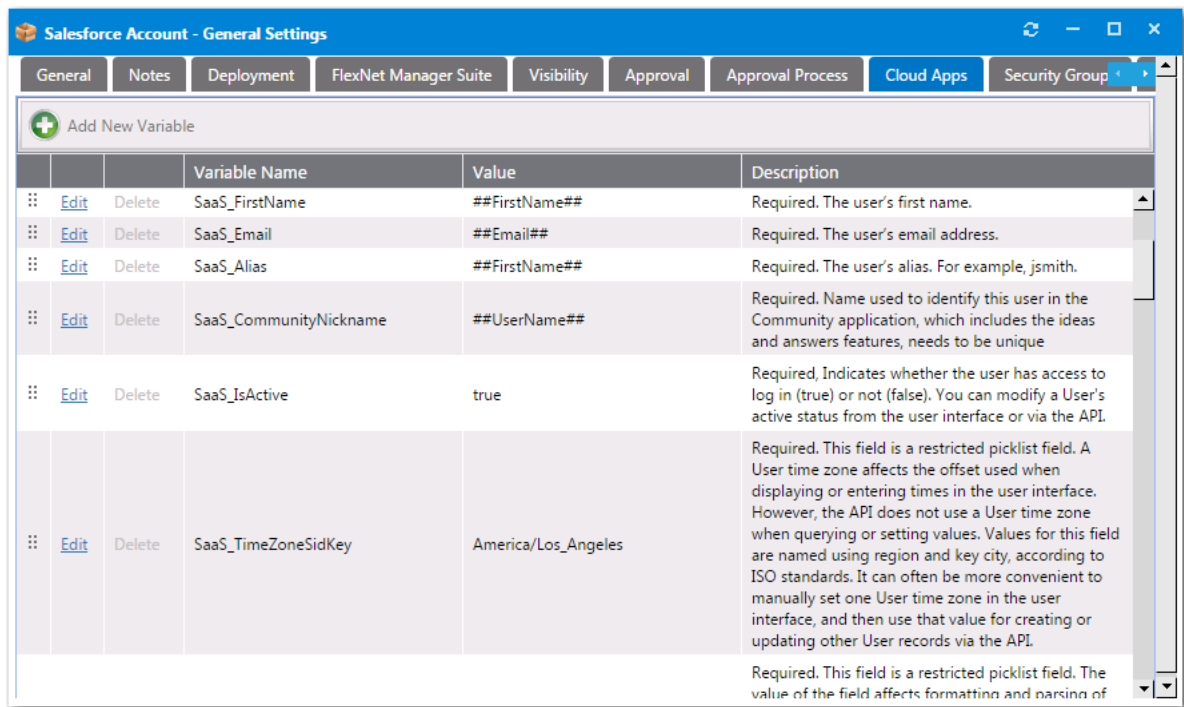
Figure 3-21: Cloud Apps Tabs

However, when you are creating a catalog time for another cloud application, you are required to determine what variables are required by the cloud application vendor and then add those variables to the **Cloud Apps** tab of that cloud catalog item.

For instructions on how to add custom variables to the **Cloud Apps** tab, see Defining Custom Variables for Cloud Catalog Items.

Configuring Active Directory Settings

You can perform Active Directory configuration activities using the **Site Management > Active Directory** portion of the App Portal interface.

- Adding an Active Directory Forest

- Performing Active Directory Property Mapping

- Configuring Virtual Properties

- Creating User Impersonation Accounts

Important • *The system account credentials entered on the* **Site Management > Active Directory > Integration** *view are used to search for users and groups but* **are not** *used to add to an Active Directory group. Instead, the App Portal service account credentials, which are specified during installation,* **are** *used to add to an Active Directory group.*

Note • *In previous App Portal releases, you specified Active Directory settings on the* **Active Directory** *tab of the* **Site Management > Settings** *view, where you identified the server name or LDAP path to provide Global Catalog access for locating user objects for a single root forest. This functionality has been moved to the* **Site Management > Active Directory > Integration** *view.*

Adding an Active Directory Forest

A "forest" is a single instance of Active Directory. Forests contain domains (which contain users, computers, , resources, etc.). In an enterprise, multiple forests can share Active Directory responsibilities by creating trust relationships between the forests. In this way, each forest can be connected with every other forest to form a collaborative directory service solution.

In previous App Portal releases, App Portal could only communicate with domains within a single root forest, the root forest where App Portal and its deployment system (System Center Configuration Manager and/or Symantec Altiris) were installed. Starting with App Portal 2015, App Portal supports multiple Active Directory forests that have different root forests. This enables users from those forests to have access to App Portal, and enables App Portal to search users/groups from domains in those forests.

Important • *The system account credentials entered on the* **Site Management > Active Directory > Integration** *view are used to search for users and groups but* **are not** *used to add to an Active Directory group. Instead, the App Portal service account credentials, which are specified during installation,* **are** *used to add to an Active Directory group.*

You manage Active Directory forests on the **Site Management > Active Directory > Integration** view.
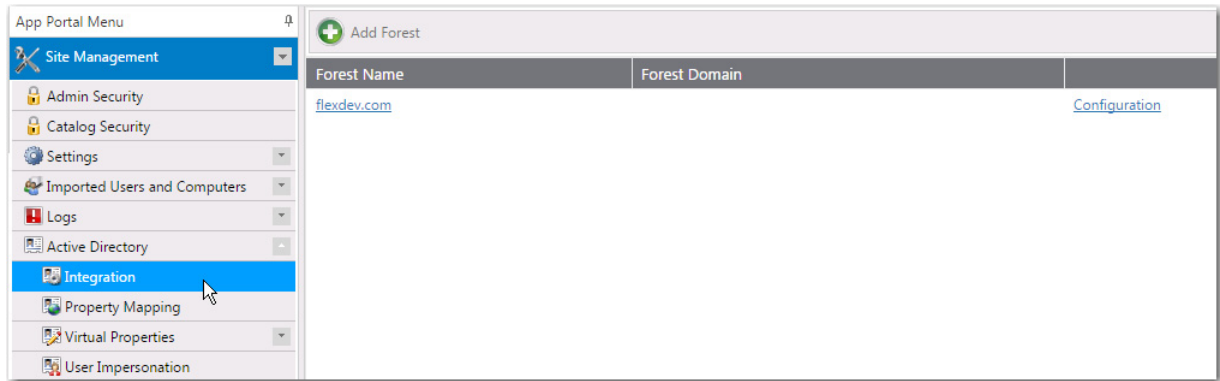
Figure 3-22: Integration View Under Site Management > Active Directory

To enable App Portal to communicate with an additional Active Directory forest, you need to add it by clicking **Add Forest**.

Task   ***To add an Active Directory forest:***

1.   On the **Site Management > Active Directory > Integration** view, click **Add Forest**. The Configure Forest view opens.

2.   In the **Root Domain Forest Server / Path** field, enter the path to the root domain Active Directory forest path that you are adding.

3.   From the **Choose authentication type** list, select **Provided Credentials** or **Integrated**.

4.   If you chose Provided Credentials from the Choose authentication type list, enter the appropriate User name and Password.

5.   Click **Test** to test the connection.

6.   Click **Save** to save the Active Directory forest. It will now be listed on the **Active Directory > Integration** view.

7.   Click on the name of the forest that you just added. A list of the domains within that forest is listed.

8. If you do not want one of the listed domains in the Active Directory forest that you just added to have access to App Portal, click **Delete** to delete that specific domain.

9. To add a new domain to this Active Directory forest, click **Add Domain**. To modify one of the existing domains, click on its name to open the **Configure Domain** view.

10. Make any desired modifications and then click **Save** to save your edits.

Performing Active Directory Property Mapping

The **Property Mapping** subview of the **Site Management > Active Directory** view includes the **Allow Inventory Allocation** and **Allow Deployment** options.

Figure 3-23: Property Mapping Toolbar

Properties determine the attributes that you want to utilize in App Portal approval, deployment, and provisioning processes. App Portal includes the most common properties.

Allow Inventory Allocation

When an attribute is specified for Inventory Allocation, the attribute will be displayed in the dropdown list for inventory allocation. You should only identify attributes for inventory allocation that represent groups of users. Suitable properties include office and department. Attributes not suitable for inventory allocation include last name, manager, etc. as they typically do not represent groups of users.

Allow Deployment

By enabling a property for deployment you can select this property to view all users that match this property when using the Request on Behalf feature. Rather than searching by user or computer selecting a property will show all users and their associated computers for selection.

Configuring Virtual Properties

Virtual Properties allow you to group similar properties together as a single logical name. Virtual properties are used primarily for inventory allocation.

The **Active Directory > Virtual Properties** view includes two subviews: **New Virtual Property** and **View Virtual Properties**.

- Creating a New Virtual Property

- Viewing Virtual Properties

Creating a New Virtual Property

To create a new virtual property, perform the following steps.

Task   ***To create a new virtual property:***

1. On the **Admin** tab, open the **Site Management > Active Directory > Virtual Properties > New Virtual Property** view.
    s

2. In the **Virtual Property Name** field, enter a logical name that will represent the properties specified in the current property list.

3. Under **Property Source**, select one of the following options to identify the Active Directory property from where to extract its values:

    -   **Active Directory User Property**—Select this option to extract values from an Active Directory user property. If you select this option, you are prompted to select properties by using the arrow keys to move them from the **Available** to the **Current** list.

    -   **User Organizational Unit**—Select this option to extract values from a User Organizational Unit. When you select this option, a tree view of Organizational Units will be displayed in the **Available** area. Click and drag to move properties from the tree to the **Current** list.

- **Computer Organizational Unit**—Select this option to extract values from a Computer Organizational Unit. When you select this option, a tree view of **Organizational Unit**s will be displayed in the **Available** area. Click and drag to move properties from the tree to the **Current** list.

4.   Click **Save**.

Viewing Virtual Properties

All virtual properties are listed on the **View Virtual Properties** subview of the **Site Management > Active Directory > Virtual Properties** view.
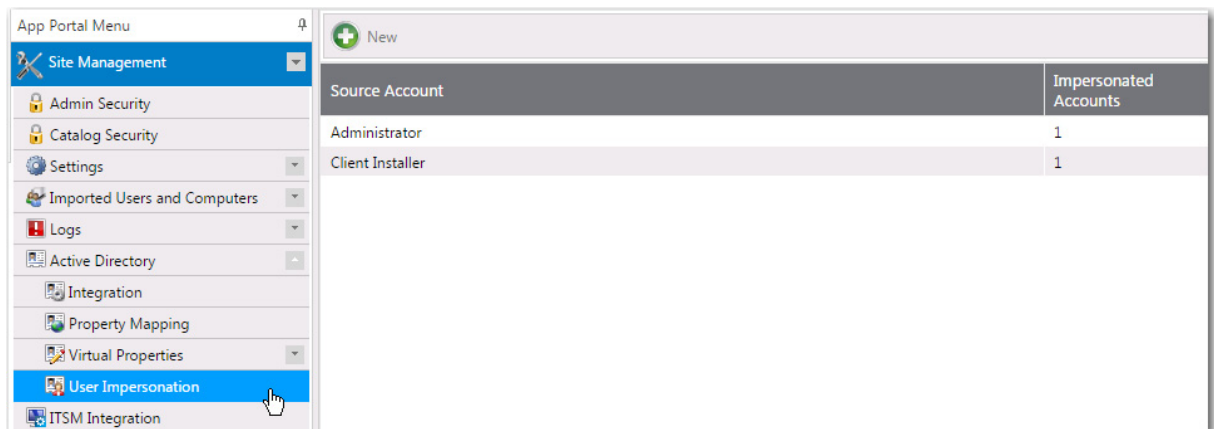
Figure 3-24: View Virtual Properties Subview

To edit an existing virtual property, click on it. A view similar to the New Virtual Property view opens, where you perform edits.

Creating User Impersonation Accounts

On the **User Impersonation** view, which is opened by selecting **Settings > User Impersonation** under **Site Management**, you can create user impersonation accounts.

Figure 3-25: User Impersonation View

Click **New** or double-click on an existing impersonated account to open the User Impersonation Properties Dialog Box.

User Impersonation Properties Dialog Box

The **User Impersonation Properties** dialog box is opened by clicking **New** or double-clicking on an existing impersonated account on the **Site Management > User Impersonation** view.
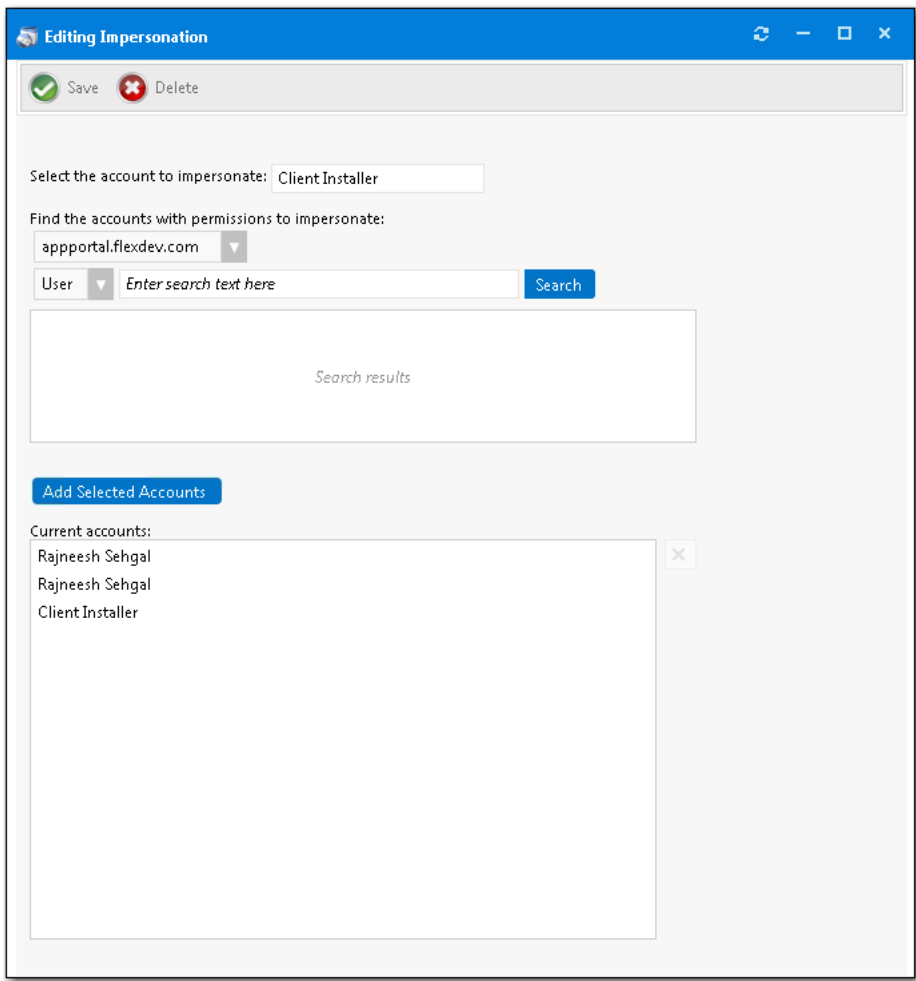
Figure 3-26: User Impersonation Properties Dialog Box

The **User Impersonation Properties** dialog box includes the following properties:

Table 3-8 • User Impersonation Properties Dialog Box

Property	Description
Select the account to impersonate	Enter the name of the account you want to impersonate.
Search box	Use the search box to find the accounts that have the permissions that you want to impersonate.
Add Selected Accounts	Select a user in the Search results area and click **Add Selected Accounts** to add the user to the **Current accounts** list.

Table 3-8 • User Impersonation Properties Dialog Box

Property	Description
Current accounts	List of selected users.

Configuring Corporate Single Sign On

In previous releases, access to the App Portal app store was limited to domain-authenticated users only. Starting with App Portal 2016, you can configure single sign-on authentication for your users using your corporate single sign-on system, enabling them to access the App Portal app store on-the-go from locations outside the corporate network or VPN.

Single sign-on authentication is supported when using the both the standard App Portal user interface and the mobile interface.

Single sign-on is configured on the **Site Management > Settings > Single Sign On** view, where you can separately specify settings for both the **Standard User Interface** and the **Mobile User Interface** (SAML 2.0 only).

Figure 3-27: Site Management > Settings > Single Sign-On View

App Portal provides support for the following single sign-on authentication types:

Table 3-9 • Supported Single Sign-On Types

Type	Description
SAML 2.0	SAML (Security Assertion Markup Language) 2.0 is an XML-based, open-standard data format for enabling web browser single sign-on. See Configuring SAML 2.0 Authentication. *Note • SAML 2.0 is the only type of single sign-on authentication type supported by the App Portal mobile interface.*
OAuth 2.0	OAuth is an open standard for authorization, commonly used as a way for users to log in to third party websites using their Google, Facebook, Microsoft, Twitter, etc. accounts without exposing their password. See Configuring OAuth 2.0 Authentication. *Note • Not supported by the App Portal mobile interface.*
OpenID Connect	OpenID is an open standard and decentralized authentication protocol which allows users to be authenticated by co-operating sites (known as relying parties) using a third-party service. See Configuring OpenID Connect Authentication. *Note • Not supported by the App Portal mobile interface.*
Custom	To implement a custom single sign-on authentication type, you would need to write a custom SSL page (`.aspx`) to redirect to. App Portal is installed with a boilerplate custom SSL page named `CustomSignon.aspx`, which your services team can customize for your organization. See Configuring Custom Authentication. *Note • Not supported by the App Portal mobile interface.*

Important • When using single sign-on, App Portal needs to be configured to run with anonymous authentication in IIS. By default, Windows Authentication is selected.

Configuring SAML 2.0 Authentication

SAML (Security Assertion Markup Language) 2.0 is an XML-based, open-standard data format for enabling web browser single sign-on.

The following instructions explain how to configure SAML 2.0 authentication for your App Portal site when using both Okta and PING Identity identity management systems.

- Configuring SAML 2.0 Authentication Using Okta

- Configuring SAML 2.0 Authentication Using Ping Identity

Configuring SAML 2.0 Authentication Using Okta

To configure SAML 2.0 authentication for your App Portal site using Okta, perform the following steps:

Task   ***To configure SAML 2.0 authentication using Okta:***

1. Logon to your identity provider platform's web site and open the page containing your account's SAML settings. The following are the **SAML Settings** in Okta:

SAML Settings		Edit
GENERAL		
Single Sign On URL	http://10.20.153.191/esd/SamlSignOn.aspx	
Recipient URL	http://10.20.153.191/esd/SamlSignOn.aspx	
Destination URL	http://10.20.153.191/esd/SamlSignOn.aspx	
Audience Restriction	http://10.20.153.191/esd	
Default Relay State	3	
Name ID Format	EmailAddress	
Response	Signed	
Assertion Signature	Signed	
Signature Algorithm	RSA_SHA1	
Digest Algorithm	SHA256	
Assertion Encryption	Unencrypted	
SAML Single Logout	Disabled	
authnContextClassRef	PasswordProtectedTransport	
Honor Force Authentication	Yes	
SAML Issuer ID	http://www.okta.com/${org.externalKey}	

2. In your identity provider platform, provide this URL for redirecting to App Portal after sign in:

   `http://`*`YOURAPPPORTALSERVER`*`/esd/SamlSignOn.aspx`

   *Note • This URL would be entered in the **Single Sign On URL**, **Recipient URL**, and **Destination URL** fields in the Okta sample settings, shown above.*

3. In your identity provider platform, make sure that the **Name ID Format** is set to **Email Address**. After you do this, whenever SAML 2.0 authentication occurs, your identity provider platform will send the email address that is registered with their system into App Portal as part of SAML association.

4. Download an authentication certificate from the identity provider platform.

5. Launch App Portal and open the **Site Management > Settings > Single Sign-On** view.

6. From the **Single sign-on type** list, select **SAML 2.0**. The SAML 2.0 settings are listed.

7. Click **Browse** next to **Identity provider certificate** and select the authentication certificate that you obtained from your identity provider platform.

8. In the **Single sign-on URL** field, enter the single sign-on URL from your identity provider platform.

    Important • App Portal assumes IdP-initiated single sign-on (identity provider-initiated single sign-on). App Portal does not prompt for login credentials; instead it redirects the user to the specified identity provider, and the identity provider prompts the user to authenticate using their preferred method, such as user name/password, smart card, token, multi-factor authentication, etc.

9. In the **Signature node XPath** field, the default setting is `//ds:Signature`. Adjust this signature node XPath as needed, per your identity provider platform.

10. In the **Attribute node XPath** field, the default setting is below. Adjust this attribute node XPath as needed, per your identity provider platform.

    `/saml2p:Response/saml2:Assertion/saml2:Subject/saml2:NameID`

    *Tip • When configuring the **Attribute node XPath** field, you may want to consider using a Mozilla Firefox plug-in named **SAML Tracer**, a tool for viewing SAML messages sent through the browser during single sign-on. You can use the SAML Tracer plug-in to capture the network communications between App Portal and the identity provider when a user is authenticating, identify the SAML packets, and display them in a readable format. You can then look at the XML structure of that SAML data to determine the correct XPath to enter in the **Attribute node XPath** field.*

11. Optionally, edit the value in the **Redirect Url Parameter** field. The **Redirect Url Parameter** declaration, which is set by default to `RelayState`, is optional extra information that may be sent along with a SAML message. This parameter may specify a URL the service provider should redirect to once single sign-on completes.

12. Click **Save**.

13. To configure IIS to use anonymous authentication instead of Windows authentication, perform the following steps.

    a. Open IIS Manager and select the **ESD** virtual directory under **Sites** in the tree.
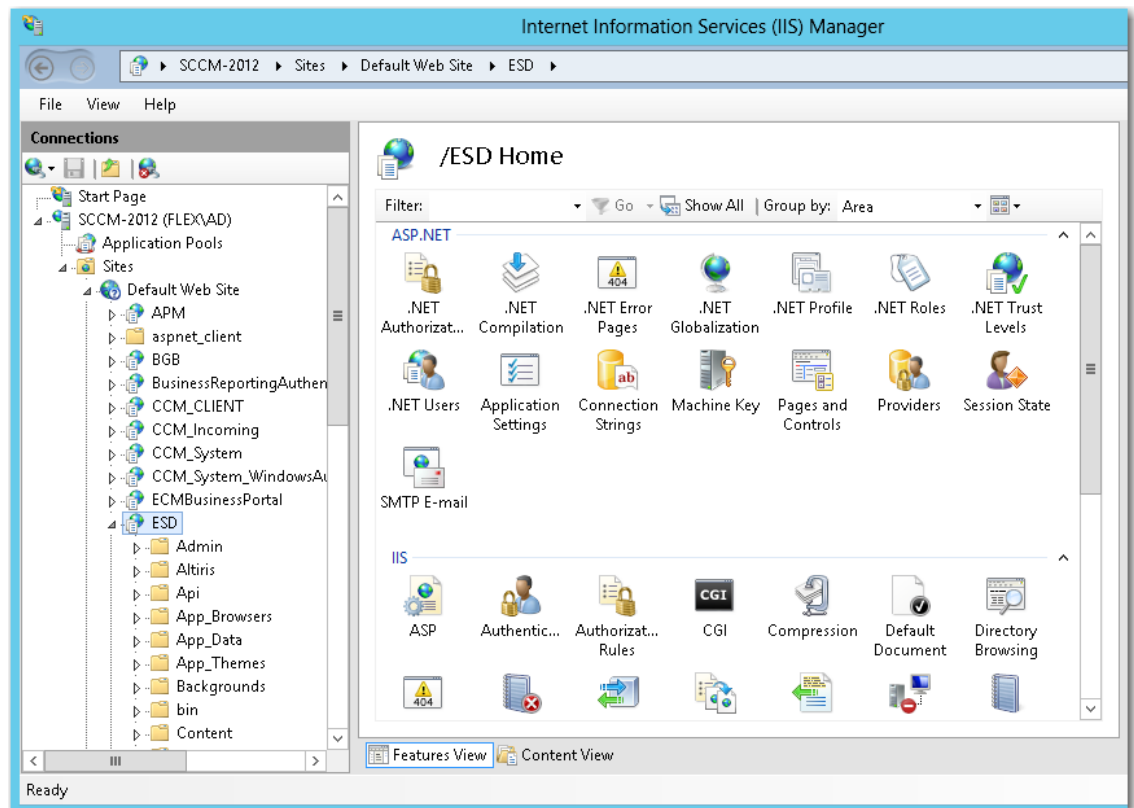
    b. Double-click on **Authentication** to open the **Authentication** view.
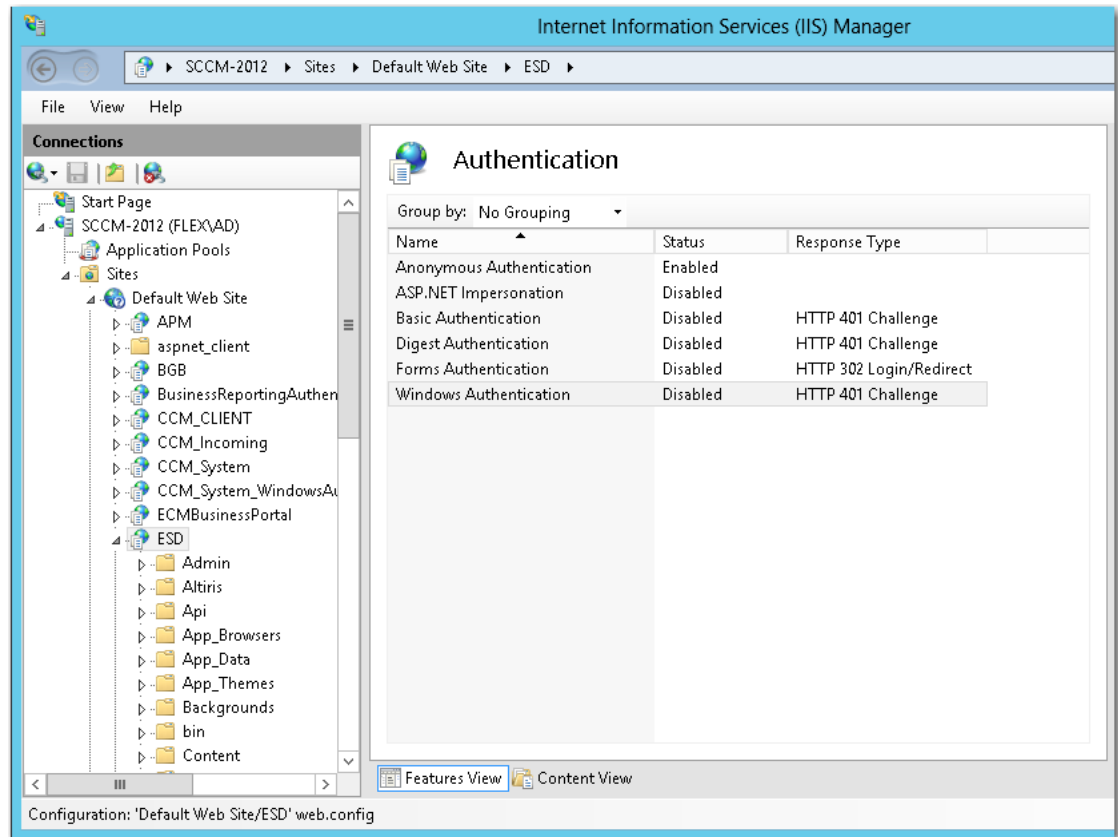
c.   Set **Anonymous Authentication** to **Enabled**, and set **Windows Authentication** to **Disabled**.

Configuring SAML 2.0 Authentication Using Ping Identity

To configure SAML 2.0 authentication for your App Portal site using Ping Identity, perform the following tasks:

● Configure App Portal as a New Application in Ping Identity

● Configure Users in Ping Identity

● Configure Single Sign On Settings in App Portal

● Configure IIS to use Anonymous Authentication instead of Windows Authentication

Configure App Portal as a New Application in Ping Identity

To configure App Portal as a new application in Ping Identity, perform the following steps.

Task   ***To configure App Portal as a new application in Ping Identity:***

1.   Log into Ping Identity as an admin and open the **My Applications** tab on the **Applications** menu.

2.   Click **Add Application** and select **New SAML Application.**
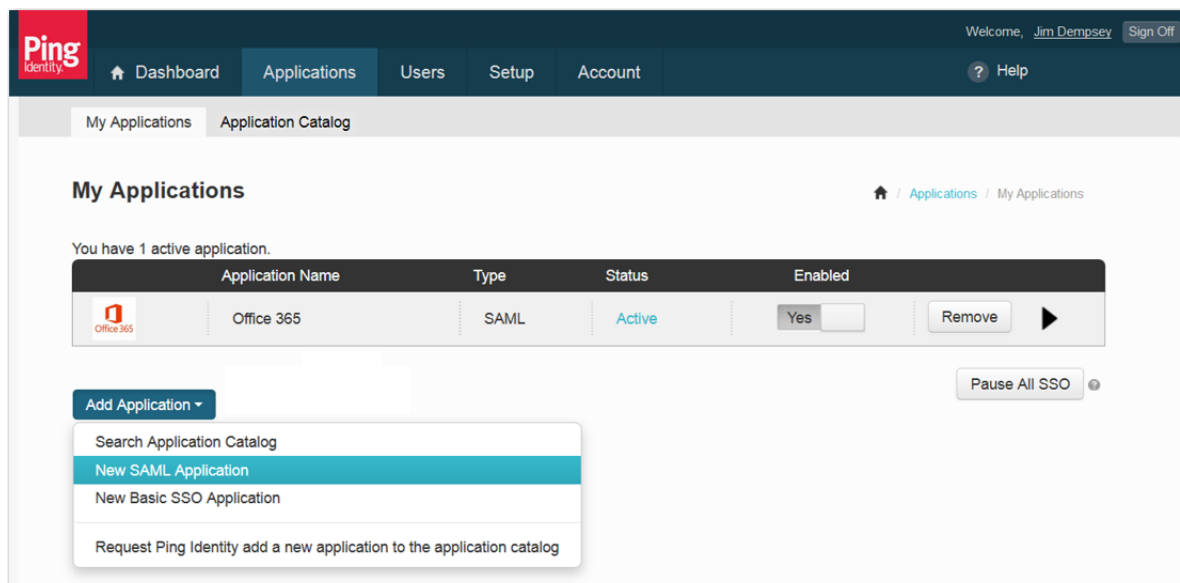
The **1. Application Details** view opens.

3. Enter the **Application Name** as you want it to appear to your SSO users.

4. Enter an **Application Description**.

5. Select a **Category**.

6. Click **Change** and upload an **Application Icon**, which will be displayed in the SSO dock.

7. Click **Continue to Next Step**. The **2. Application Configuration** view opens.

8. Select the **I have the SAML configuration** tab

9. For the **Protocol Version**, select **SAML v2.0**.

10. In the **Assertion Consumer Service (ACS)** field, enter the URL to your App Portal server followed by `/esd/SamlSignOn.aspx`.

11. In the **Entity ID** field, enter the URL to your App Portal instance (ending in `/esd`).

12. In the **Signing Algorithm** list, select **RSA_SHA1**.

13. Click **Continue to Next Step**. The **3. SSO Attribute Mapping** view opens.

14. Click **Add new attribute**. An empty row is listed.

15. Enter `FirstName` in the **Application Attribute** column, select **First Name** in the **Identity Bridge Attribute or Literal Value** column, and select the check the box in the **Required** column.

16. Repeat these steps to add rows for `LastName` and `Email`.

17. Click **Save & Publish**. **The 4. Review Setup view opens.**

18. Review your settings and click **Finish**. App Portal should now appear in your list of active applications.
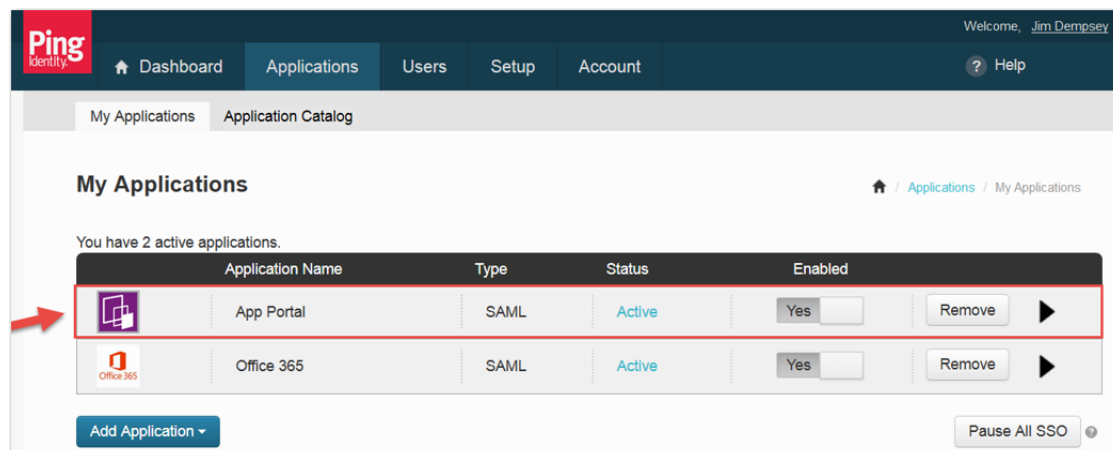
Configure Users in Ping Identity

The next step is to configure users in Ping Identity, if they are not already configured.

Task   ***To configure users in Ping Identity:***

1. Log into Ping Identity as an admin and open the **User Directory > Users** tab on the **Users** menu. The **Users** view opens.
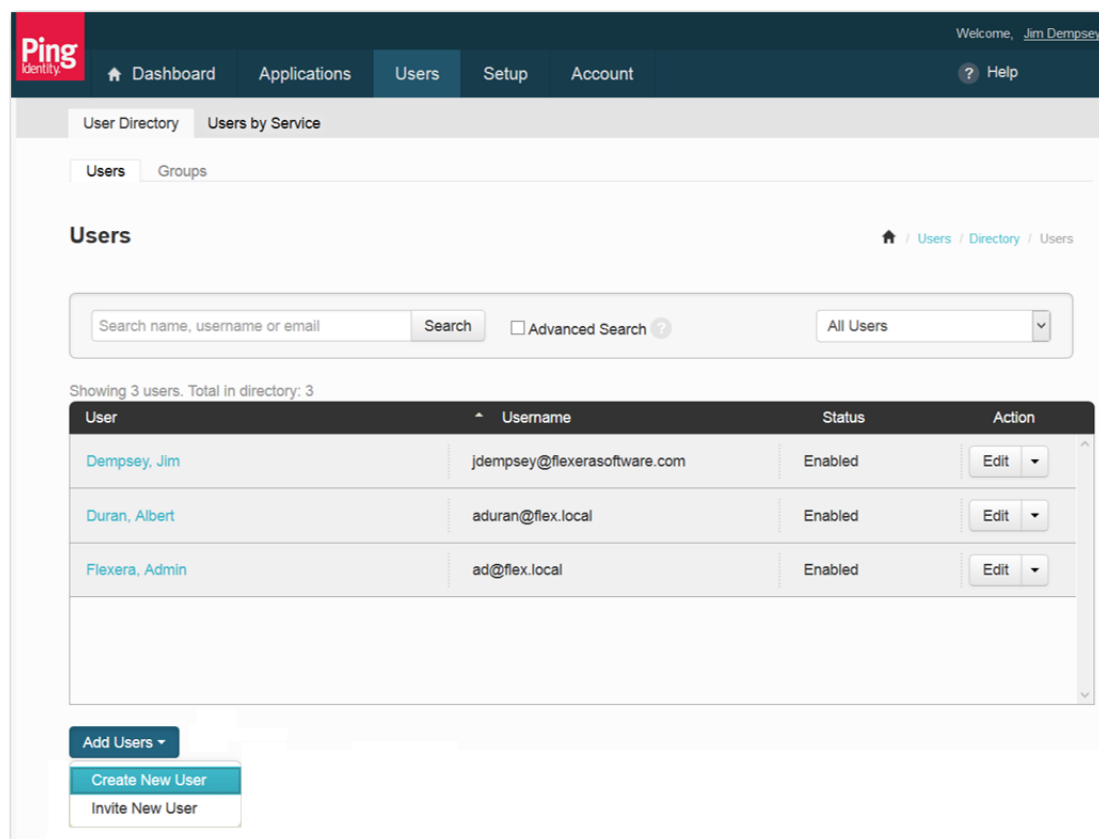
2. Click on **Add Users** and select **Create New User**. The Create New User dialog box opens.

3. Enter values for **New Password** and **Confirm New Password**.

4. Enter a **Username**. This is often the email address of the user, but could be anything you want your users to sign in with, such as Active Directory user name.

5. Enter a **First Name**, **Middle Name** (optional), and **Last Name**.

6. In the **Formatted Name** field, the name as it will appear in the SSO solution is listed.

7. In the **Email (Work)** field, enter the user's email address, which must match the user's email address in Active Directory. This is how the SSO user name is mapped to an Active Directory user account.

8. Click **Save.** The details of the new user are listed.

9. Review the details of your newly created user.

10. Repeat this procedure to create additional users.

Configure Single Sign On Settings in App Portal

To configure single sign-on settings in App Portal, perform the following steps.

Task   ***To configure single sign-on settings in App Portal:***

1. Log into Ping Identity as an admin and open the **My Applications** tab on the **Applications** menu.

2. Click on **App Portal** to view the details of the App Portal application.

3. Copy the **Initiate Single Sign-On (SSO) URL** to the clipboard

4. Next to **Signing Certificate**, click the **Download** link. You are prompted to save the **idp-signing.crt** file.
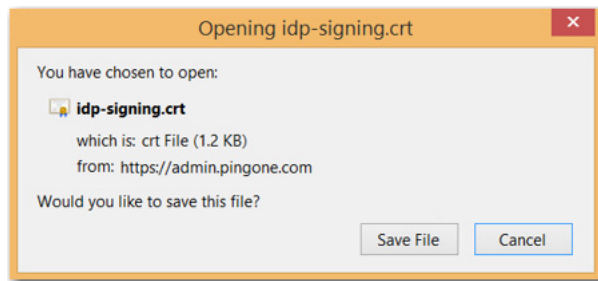
5. Click **Save File** and save the file to a safe place that is accessible from your App Portal server.

6. Log into App Portal as an admin and open the **Site Management > Settings > Single Sign-On** view.

7. Under **Standard User Interface** and/or **Mobile User Interface**, select **SAML 2.0** from the **Single sign-on type** list.
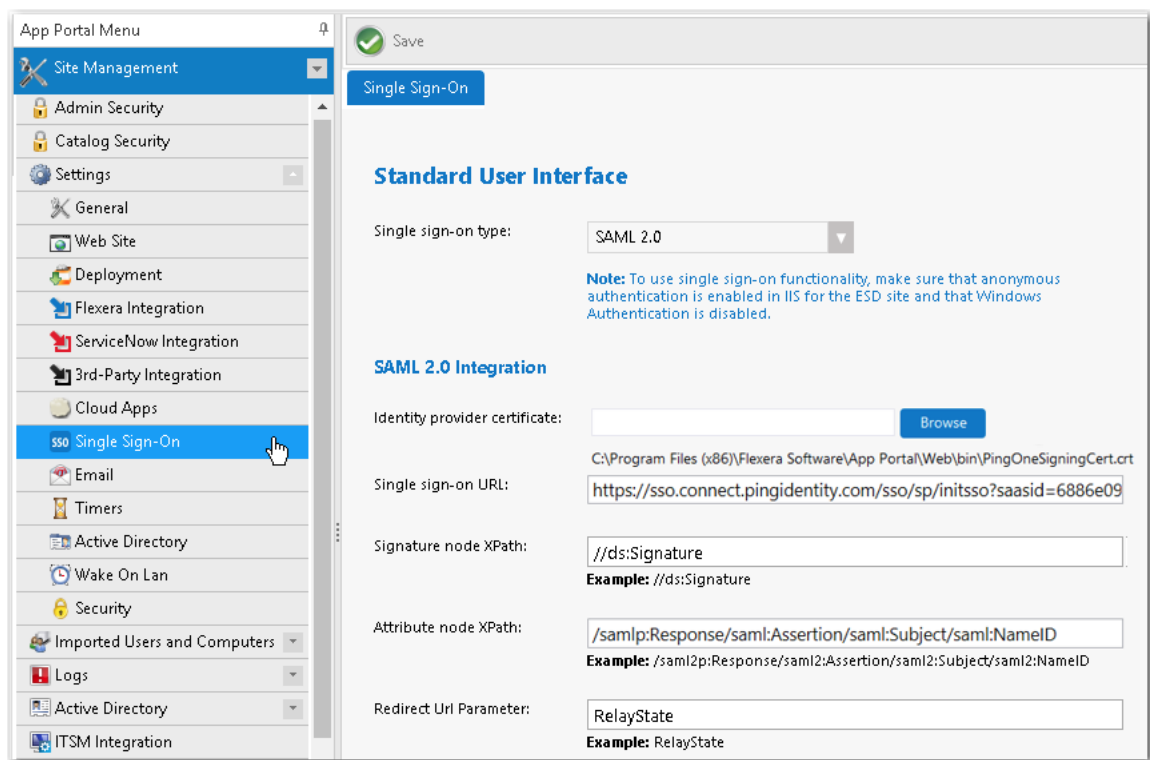
8. Click the **Browse** button and select the `idp-signing.crt` file you downloaded earlier.

9. Paste the Ping Identity **Single sign-on URL** from the clipboard.

10. Set the **Attribute node XPath** value to `/samlp:Response/saml:Assertion/saml:Subject/saml:NameID`.

11. Click **Save**.

Configure IIS to use Anonymous Authentication instead of Windows Authentication

To configure IIS to use anonymous authentication instead of Windows authentication, perform the following steps.

Task   ***To configure IIS to use anonymous authentication:***

1.   Open IIS Manager and select the **ESD** virtual directory under **Sites** in the tree.
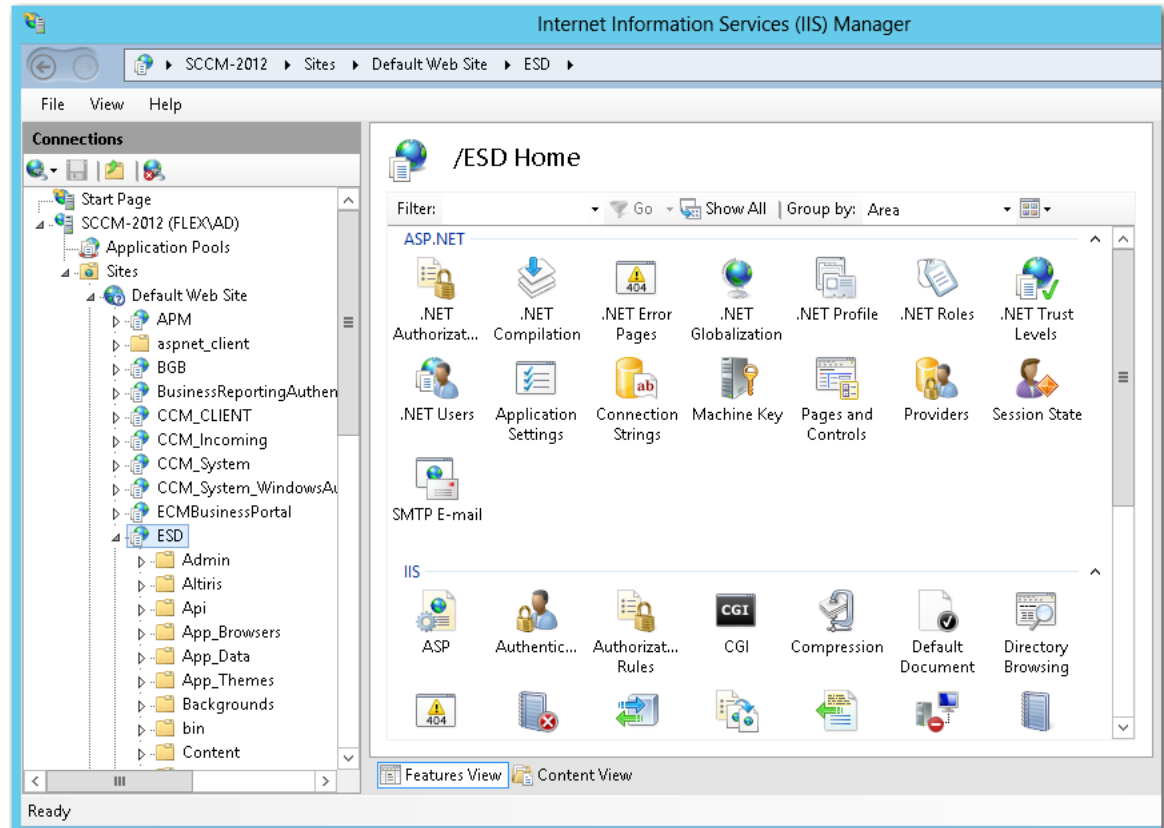
2.   Double-click on **Authentication** to open the **Authentication** view.
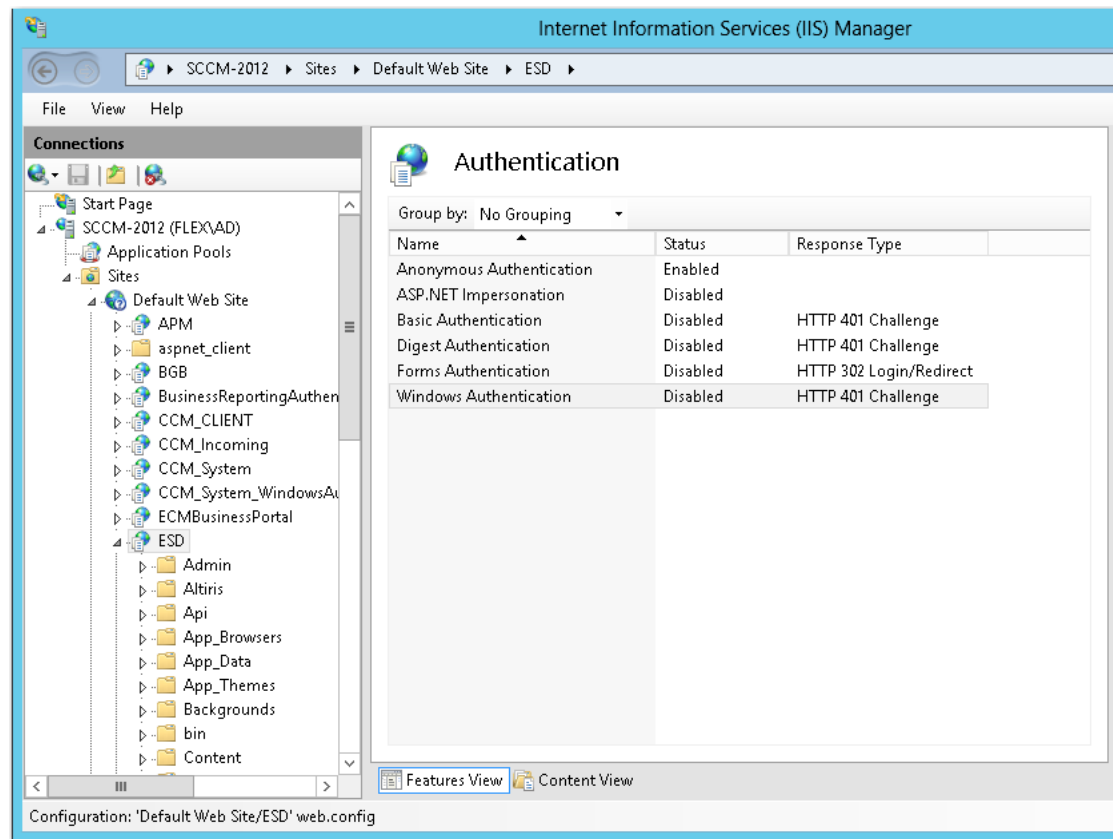
3.   Set **Anonymous Authentication** to **Enabled**, and set **Windows Authentication** to **Disabled**.

You are now ready to test SAML SSO with App Portal. The next time you open the App Portal website, and you should be redirected to sign in through your SSO solution. Upon successful authentication, you should be redirected back to the App Portal website and signed in.

Configuring OAuth 2.0 Authentication

OAuth is an open standard for authentication, commonly used as a way for users to log in to third party websites using their Google, Facebook, Microsoft, Twitter, etc. accounts without exposing their password. One vendor that provides OAuth authentication is Google. For example, when linked to Google for authentication, users are prompted to login to Google instead of App Portal.

To configure OAuth 2.0 authentication for your App Portal site, perform the following steps:

Task   **To configure OAuth 2.0 authentication:**

1.   Logon to your identity provider platform's web site and open the page containing your account settings.

2.   In your identity provider platform, provide this URL for redirecting to App Portal after sign in:

`http://YOURAPPPORTALSERVER/esd/oauth2SignOn.aspx?MethodToInvoke=CallBack`

3.   Obtain the following from your identity provider platform:

- **Client ID**

- **Client Secret**

4. Launch App Portal and open the **Site Management > Settings > Single Sign-On** view.

5. From the **Single sign-on type** list, select **OAuth 2.0**. The **OAuth 2.0** settings are listed.

6. In the **Client Id** and **Client Secret** fields, enter the information obtained from your identity provider platform.

7. In the **Call Back Url** field, enter the following:

   `http://YOURAPPPORTALSERVER.YourDomainName/esd/oauth2SignOn.aspx?MethodToInvoke=CallBack`

8. Enter information provided by your identity provider platform into the in the following fields:

   - Authorization end point

   - Scope

   - Profile end point

   - Token end point

9. Click **Save**.

10. To configure IIS to use anonymous authentication instead of Windows authentication, perform the following steps.

   a. Open IIS Manager and select the **ESD** virtual directory under **Sites** in the tree.
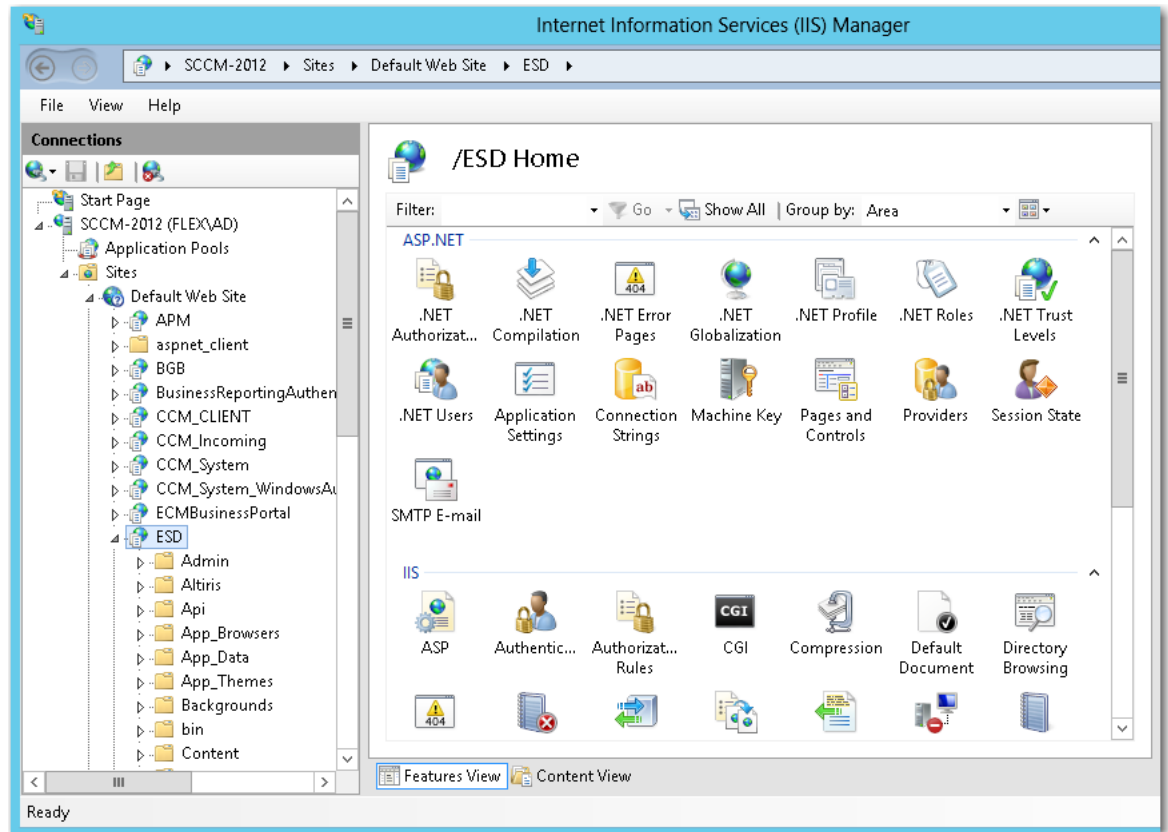
b. Double-click on **Authentication** to open the **Authentication** view.
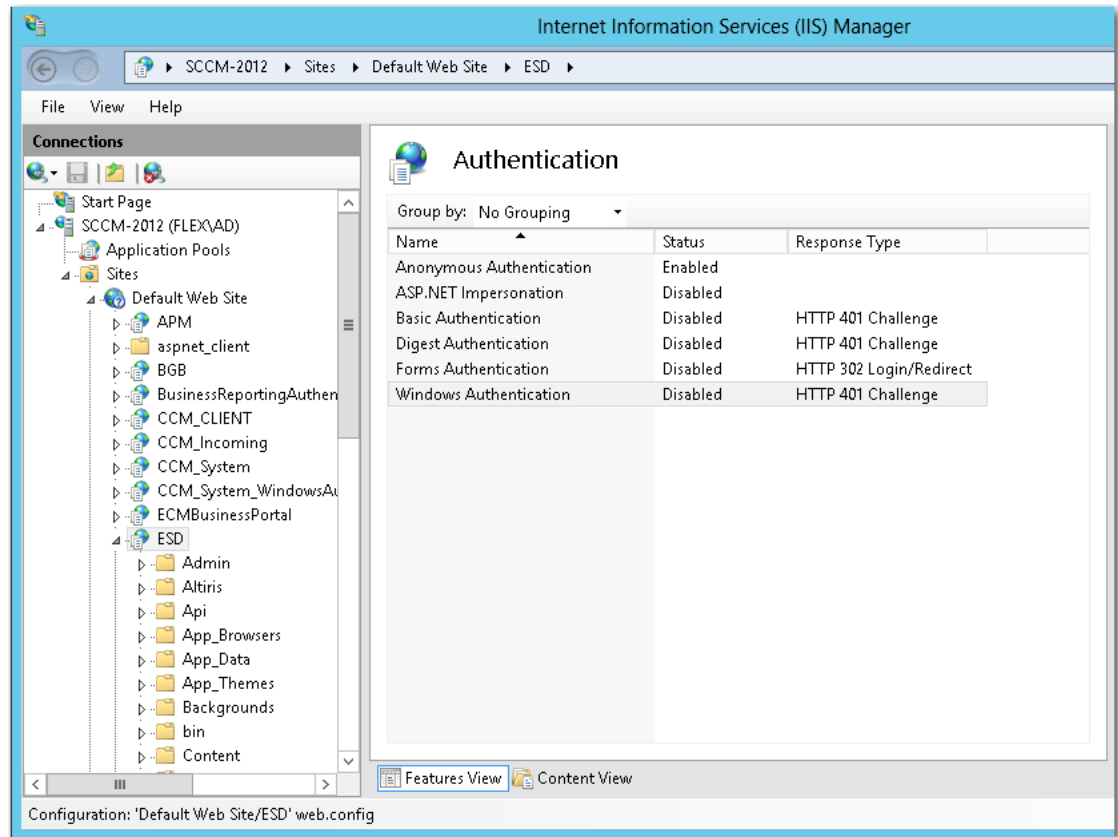
c.   Set **Anonymous Authentication** to **Enabled**, and set **Windows Authentication** to **Disabled**.

Configuring OpenID Connect Authentication

OpenID is an open standard and decentralized authentication protocol which allows users to be authenticated by co-operating sites (known as relying parties) using a third-party service.

To configure OpenID Connect authentication for your App Portal site, perform the following steps:

Task   ***To configure OpenID Connect authentication:***

1.   In your identity provider platform, provide this URL for redirecting to App Portal after sign in.

      `http://`*YOURAPPPORTALSERVER*`/esd/OpenIdSignOn.aspx`

2.   Obtain the **Single sign-on URL**, **Authentication request end point**, and **Client ID** from your identify provider.

3.   Launch App Portal and open the **Site Management > Settings > Single Sign-On** view.

4.   From the **Single sign-on type** list, select **OpenID Connect**. The **OpenID Connect** settings are listed.

5. Enter the **Single sign-on URL**, **Authentication request end point**, and **Client ID** that you obtained from your identity provider platform.

6. In the **Redirect URL** field, enter:

   `http://YOURAPPPORTALSERVER/esd/OpenIdSignOn.aspx`

7. In the **State** field, enter any value that will passed back to App Portal by the identity provider platform post login for validation. The **State** value helps to validate that the correct ID Token is received. Also, this value comes as a Key in the Form element.

8. In the **Nonce** field, enter any value that will passed back to App Portal by the identity provider platform post login for validation. The **Nonce** value helps to validate that the correct ID Token is received. Also, it is used to mitigate replay attacks.

9. When the client application receives the ID Token from the identity provider platform, it is the responsibility of the client to validate the ID Token. This validation process involves a number of steps which would get performed when the **Bypass token validation** option is not selected. If you want to bypass token validation, select the **Bypass token validation** option.

10. Click **Generate 'Initiate Login URL'**. Using the information provided, login URL is generated.

11. Click **Save** to save the OpenID Connect details.

12. Copy the generated URL.

13. Return to the account settings page of your identity provider platform and paste the generated URL into the **Initiate login URL** field.

14. To configure IIS to use anonymous authentication instead of Windows authentication, perform the following steps.

    a. Open IIS Manager and select the **ESD** virtual directory under **Sites** in the tree.
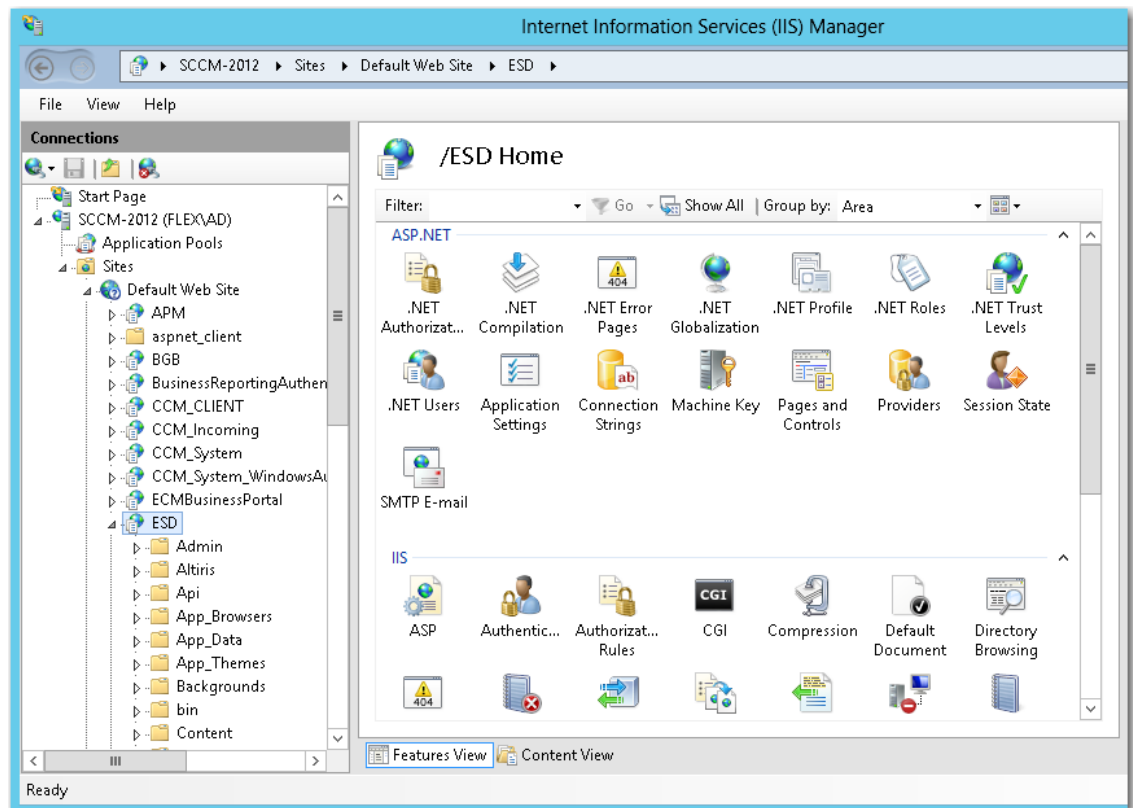
    b. Double-click on **Authentication** to open the **Authentication** view.
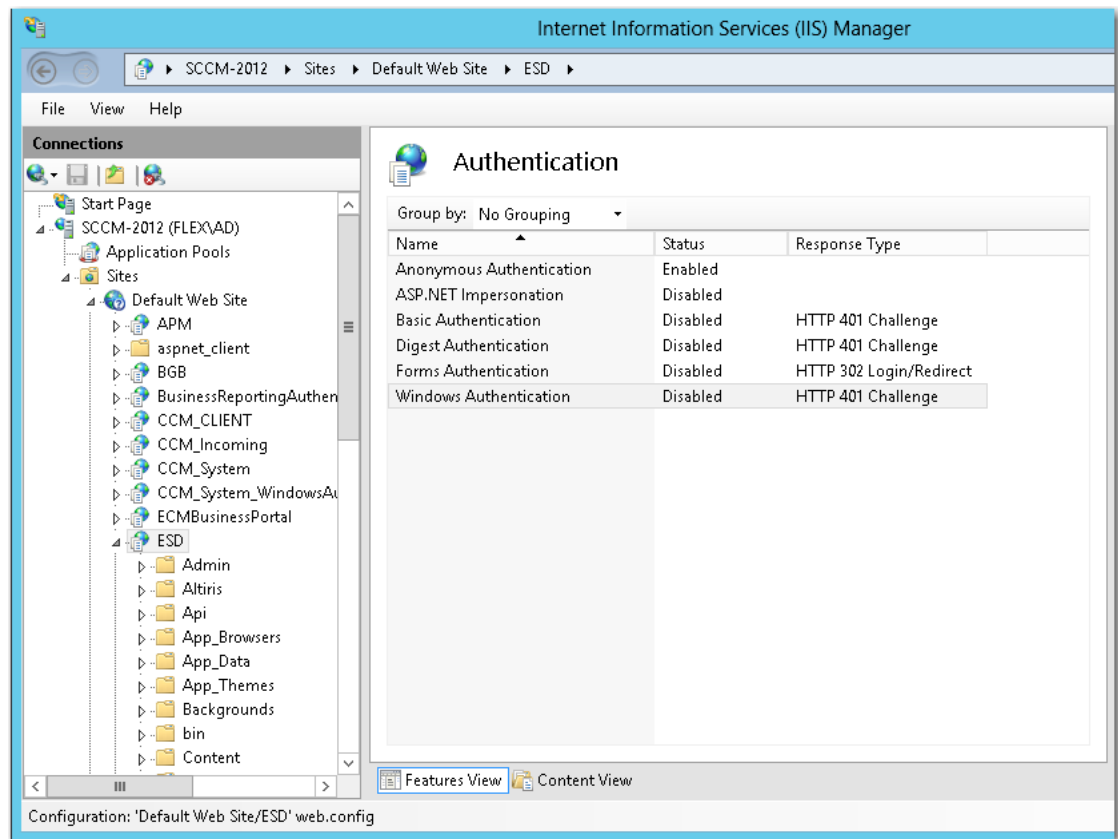
    c.   Set **Anonymous Authentication** to **Enabled**, and set **Windows Authentication** to **Disabled**.

Configuring Custom Authentication

To implement a custom single sign-on authentication type, you would need to write a custom page (`.aspx`) to redirect to. App Portal is installed with a boilerplate custom page named `CustomSignon.aspx`, which your services team can customize for your organization. This file can be found in the following location:

```
C:\Program Files (x86)\Flexera Software\App Portal\Web\CustomSignon.aspx
```

To configure custom authentication, perform the following steps.

Task   *To configure custom authentication:*

1. Obtain the boilerplate custom page installed with App Portal:

   ```
   C:\Program Files (x86)\Flexera Software\App Portal\Web\CustomSignon.aspx
   ```

2. Customize the SSL page for your organization.

3. Launch App Portal and open the **Site Management > Settings > Single Sign-On** view.

4. From the **Single sign-on type** list, select **Custom**.

5. To configure IIS to use anonymous authentication instead of Windows authentication, perform the following steps.

     a.   Open IIS Manager and select the **ESD** virtual directory under **Sites** in the tree.
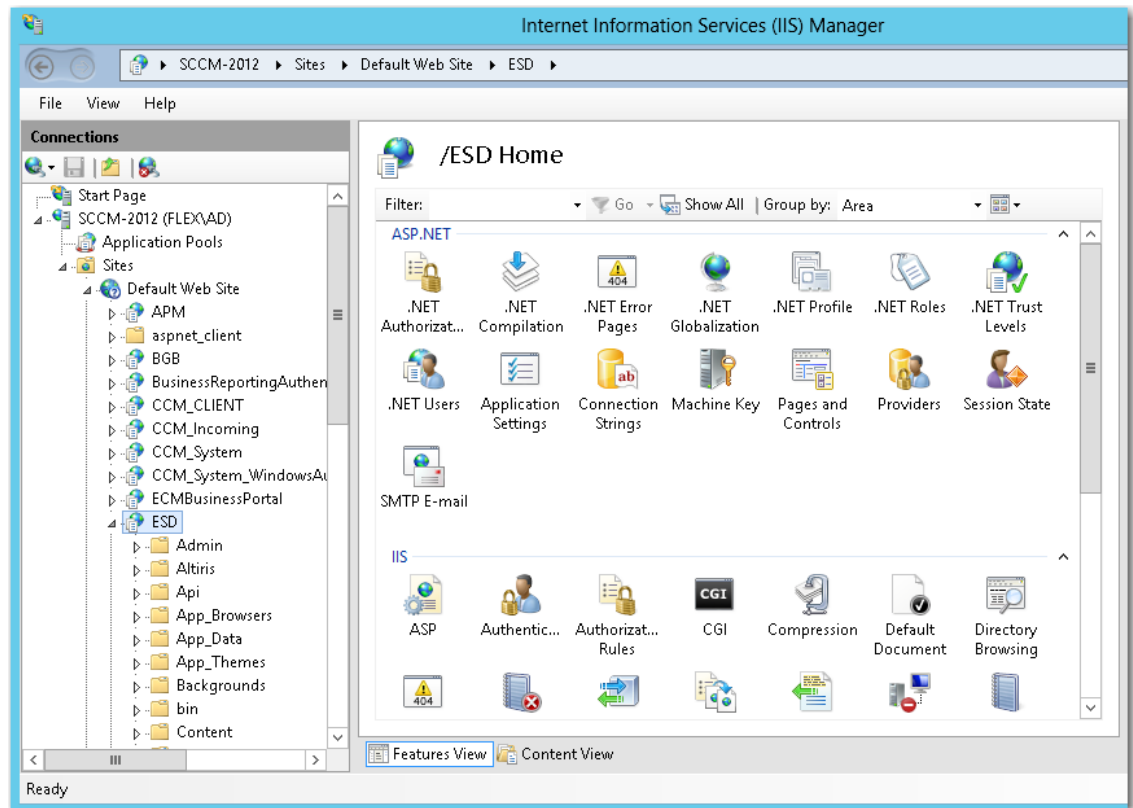
     b.   Double-click on **Authentication** to open the **Authentication** view.
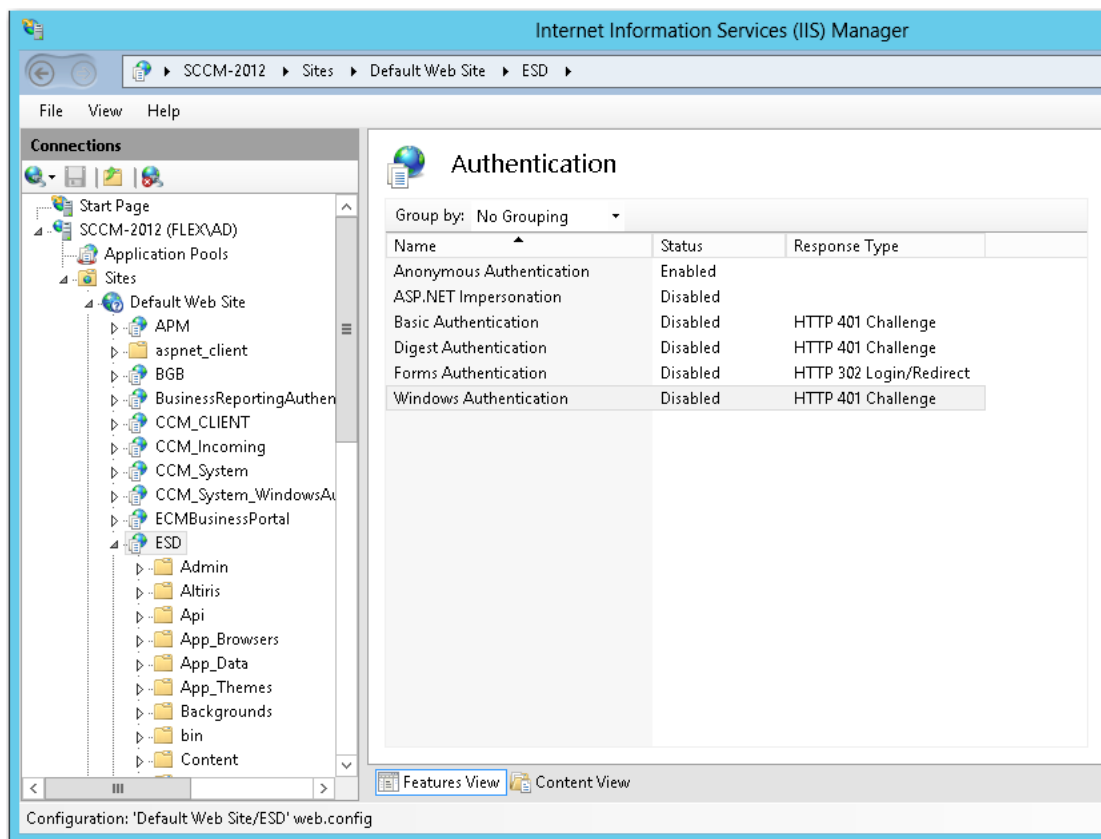
c. Set **Anonymous Authentication** to **Enabled**, and set **Windows Authentication** to **Disabled**.

Performing Advanced License Check

📑

Edition • *This feature requires the additional purchase of FlexNet Manager Suite.*

📄
❗

Important • *To use this feature, you must install the FlexNet Manager Suite 2015 R2 SP5-02 Hotfix, available in the Flexera Software Product and License Center.*

Starting with App Portal 2016, license entitlement evaluation has been enhanced to consider not only available licenses, but also second use rights, upgrade/downgrade rights, and exemption by device role rights (such as an MSDN subscription), all based upon information stored in FlexNet Manager Suite.

App Portal gives users the ability, at a more advanced level, to check if a license reservation is needed for a catalog item by evaluating the following during checkout:

● **Right of second use (also known as portable use)**—The right to use the software on both a desktop and a laptop with the same owner and only consume one license.

● **Upgrade rights**—The right to use the latest version of the software as soon as it becomes available.

● **Downgrade rights**—The right to use an older version of the software than the version purchased.

- **Exemption by device role rights**—The right to install software based upon a subscription role, such as an MSDN subscription.

These additional license rights are evaluated at checkout before a license is reserved. This solution helps ensure that your organization evaluates all key entitlement rights and does not mistakenly purchase more license entitlements that you actually require.

Enabling Advanced License Check

By default, advanced license check is not enabled. To enable it globally, select the **Enable Advanced License Check with FlexNet Manager Suite** option on the **Site Management > Settings >Flexera Integration** view.

You can also control the advanced license check feature on a catalog item basis by selecting the **Check for available license during checkout** option on the **FlexNet Manager Suite** tab of the **Catalog Item Properties** dialog box.
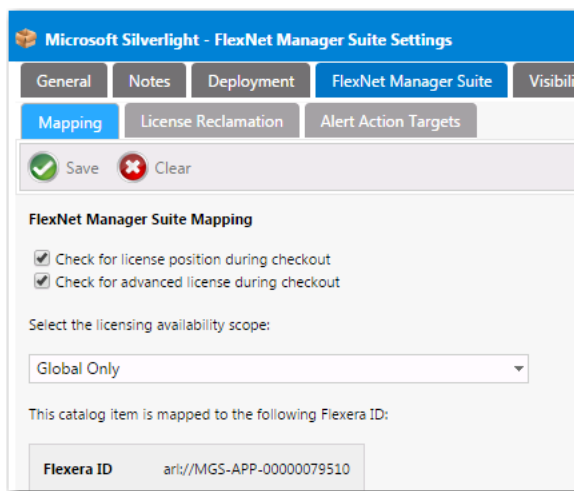
Figure 3-28: Check for Advanced License During Checkout Option

About Product Use Rights

Enabling the "advanced license check" process will improve the entitlement estimate during the reservation process, but it may run the risk of a few exceptions. For instance, the following may occur:

- Changes between the pre- and post-approval process may occur.

- Changes between the request process and the deployment / inventory may occur.

- Reassignment of license through the license reconcile process may produce unexpected results.

There are known limitations in the license optimization performed when using the advanced license check. For instance, only the user/device relevant to the request is considered. In the scenario described in the following table, no new license is required if you consider both User 1 and User 2: you just need to exchange the current licenses between User 1 and User 2. However, because only User 2 is considered at the time of the request, the system wrongly detects that a new license is needed. These are corner case scenarios but they may exist.
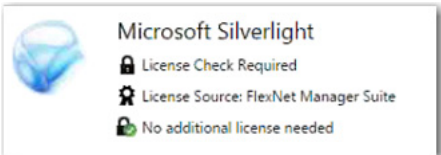
Table 3-10 •

Users	License	Request	What should happen	What will happen
User 1	Has a license with **right of second use**	—	**User 1** and **User 2** should switch licenses so that **User 2** has a right of second use.	An additional license will be purchased for **User 2**.
User 2	Has a license with **no right of second use**	**User 2** requests a license for a second device		

Advanced License Check User Experience

When this feature is enabled, catalog items on the Browse Catalog tab that require a license will display the text "License Check is Required" rather than "License Required". An advanced license check will be performed using the data from FlexNet Manager Suite to determine whether the right of second use, upgrade/downgrade rights, or exemptions by device role apply.

Table 3-11 •

Without Advanced License Check	With Advanced License Check
Items requiring a license identified by the phrase **License Required**.	Items requiring a license are identified by the phrase **License Check Required**.
License availability is identified as either **License available** or **License not available**.	If an item requires a license and, after an advanced license check is performed, it is determined that the user already has rights to a license for that item (possibly due to second use, upgrade, downgrade, or role rights), the phrase **No additional license needed** is listed.

Managing Notification Email Templates and Messages

System notifications are emails and messages that are used to communicate status and events to App Portal users. They can be modified to suit your company's language preferences and content.

You view and edit notifications on the **Site Management > Communication > Notifications** view.

- About Notifications

- Editing Notification Email Templates and Messages

About Notifications

You can edit and customize notification email templates and messages on the **Site Management > Communication > Notifications** view on the **Admin** tab.

- Enabling HTML Formatting of Email Communication

- Specifying Notification Language

- Types of Notifications

Enabling HTML Formatting of Email Communication

To enable HTML formatting of email communication, select the **HTML Email Format** option on the **Email** tab under **Site Management > Settings**.

Figure 3-29: Enabling HTML Formatting of Email

Specifying Notification Language

App Portal provides a number of notification messages, in both email and web form, to communicate status and events within the software. These notification messages are customizable in content and language. A number of variables are provided that can be placed in most notifications to offer a wealth of information.

The notifications can be language specific. By default English is the primary language. You can add additional languages to App Portal from the **Communication > Languages** node.

The current language being edited is selected in the **Select a language** list:

Figure 3-30: Selecting a Language

Types of Notifications

On the **Site Management > Communication > Notifications** view, notification email templates and messages are listed on four tabs, each listing alerts and notifications for different areas of the App Portal site.

You can customize these default App Portal notifications for your organization by editing text, changing font family or color, adding graphics, etc.

To edit a notification, select the notification in the list and double-click. The notification will open in an editor dialog box.

For a complete list of default notifications, see List of Notification Email Templates and Messages.

Editing Notification Email Templates and Messages

You view and edit notification email templates and messages on the **Communication > Notifications** view under **Site Management** on the **Admin** tab.

---

*Note • Before beginning to edit your default email notifications, make sure that the **HTML Email Format** option on the **Email** tab of the **Site Management > Settings** view is selected.*

Task   ***To edit a default notification email:***

1. Open the **Admin** tab.

2. Under **Site Management**, select **Communication > Notifications**. The default email notifications are listed on the following tabs: **Global**, **Software**, **General**, and **License Reclamation**.

3. Locate the notification that you want to edit and double-click on it. The email opens in an editor.
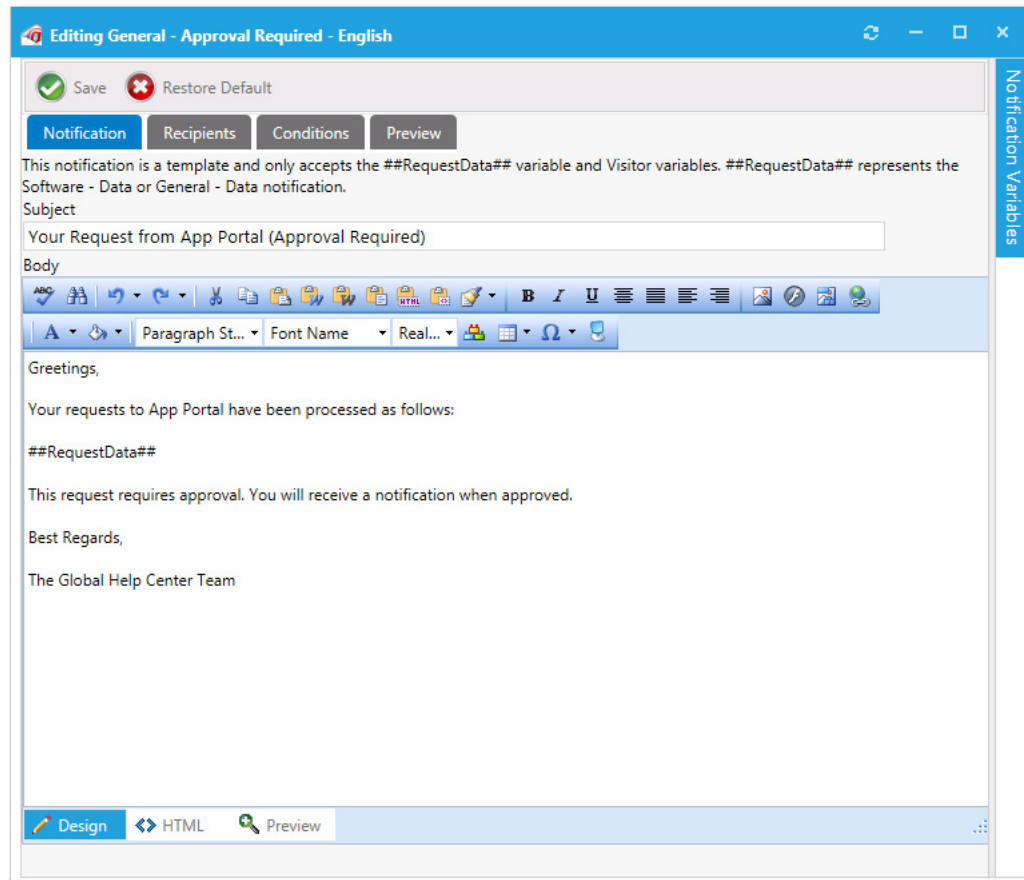
4. On the **Notification** tab, edit and format the email using the tools on the tool bar.

    If you prefer to directly edit the HTML code of the email, click **HTML** at the bottom of the editor.

    The HTML code will be displayed:
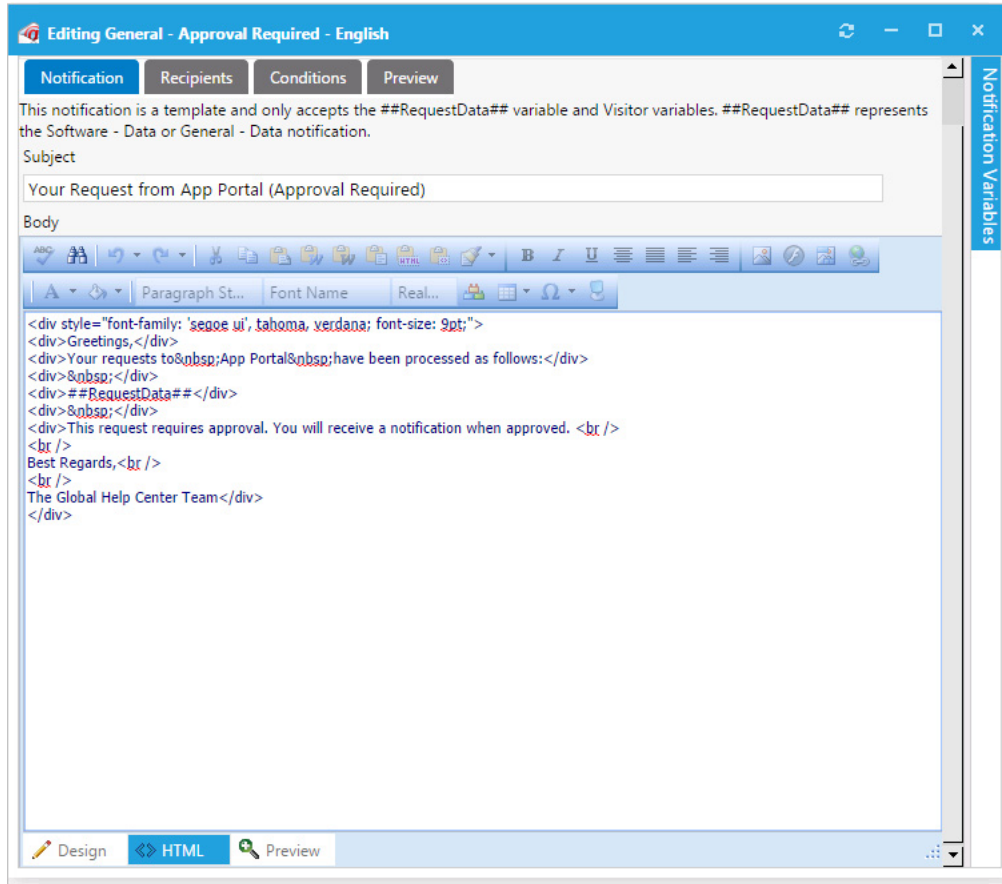
When editing notifications, you can customize them to match your company brand by including company fonts, colors, and logos.

5. To insert a variable into the email, click on the **Notification Variables** button on the right side of the dialog box to open the **Notification Variables** dialog box, select a variable from the list, and click **Add**.

6. To add additional recipients to these emails, as CC or BCC notifications, open the **Recipients** tab and enter email addresses, one per line.

7. You can specify conditions on a notification on the **Conditions** tab.

For most email notifications, you can filter the recipient against membership rules to determine whether the recipient should receive the notification. You add these conditions on the **Conditions** tab.

If a match is found against one of the conditions, then the notification is not sent to the recipient. Recipients include both the requester and target user of the request.

In the above example if the target user or the requester is in the **Admin User New** Security Group, the notification will not be sent.

8. After you have finished editing the notification email, click **Save**.

Tip • In addition to listing email notification files, the **Global** *subtab of the* **Communication > Notifications** *view also lists HTML files that can be edited to brand various portions of the App Portal site. See* Branding Your App Portal Site.

Branding Your App Portal Site

There are several tasks you can perform to brand your App Portal Site. Most of these tasks are performed under **Site Management > Settings** on the **Admin** tab. In addition to adding company fonts, colors, and logos to the default email notifications that are sent out by App Portal, as described in Editing Notification Email Templates and Messages, you can also perform the following tasks:

●   Changing the Page Header Logo

●   Customizing the Welcome Page

●   Customizing the App Portal User Interface Colors

●   Displaying a EULA to New Users

●   Editing the Help Tab Content

●   Adding Announcements to the Page Header

- Specifying a Company Support Home Page URL

- Updating the Site Name in Browser Title Bar

Changing the Page Header Logo

By default, the Flexera Software App Portal logo is displayed in the page header:
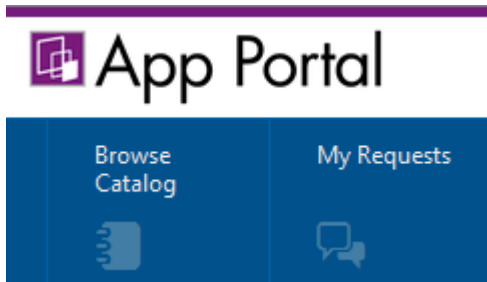
Figure 3-31: App Portal Logo in Page Header

To display a different image in the page header, perform the following steps:

Task   **To change the page header logo:**

1. Open the **Admin** tab.

2. Under **Site Management**, select **Settings > Web Site > Catalog Appearance**. The **Web Site > Catalog Appearance** view opens.

3. Scroll down to the **Visual Styling** properties and locate the **Company Logo URL** property.

This field lists the location of the company logo that appears at the top left of all App Portal screens. By default, the location of the App Portal logo is listed in this field.

4. In the **Company Logo URL** field, enter the location of the image you want to appear in the page header. You can specify either a local file or a URL to a file at a remote location.

Tip • *The image should be a maximum of 40 pixels in height. The default App Portal logo is displayed at 40px H by 176px W, but a replacement image can be wider; it just cannot be more than 40 pixels in height. If the specified image is more than 40 pixels in height, it will be automatically reduced in size and displayed at a height of 40 pixels.*

5. Click **Save**. The new image now appears in the Page Header of your site.

Tip • *To see the new logo, you may need to close your App Portal browser and then reopen it or refresh the browser window.*

Customizing the Welcome Page

By default, a generic message is listed on the Welcome Page, which is displayed when the **Browse Catalog** tab is selected and a catalog item is not selected.
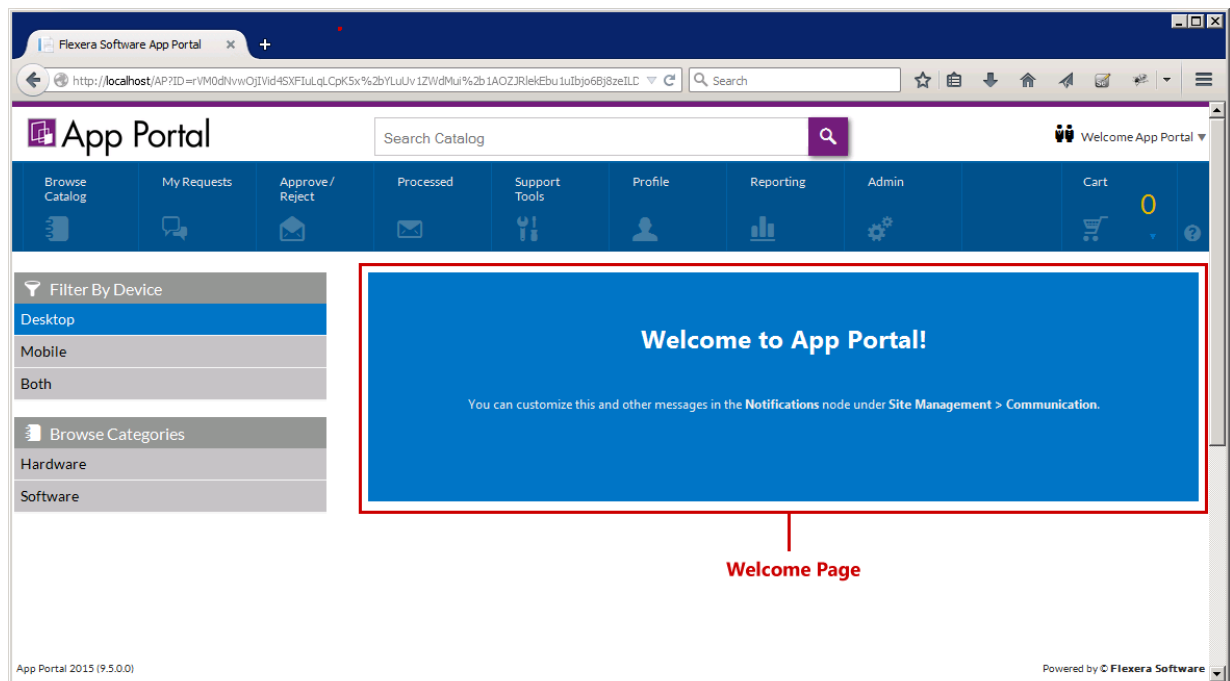
Figure 3-32: Welcome Page

To customize your Welcome Page, perform the following steps:

Task   ***To customize the Welcome Page:***

1. Open the **Admin** tab.

2. Under **Site Management**, select **Communication > Notifications**. The **Notifications View** opens.

3. On the **Global** tab, double-click on **Welcome**. The **Welcome** file opens in an HTML Editor.
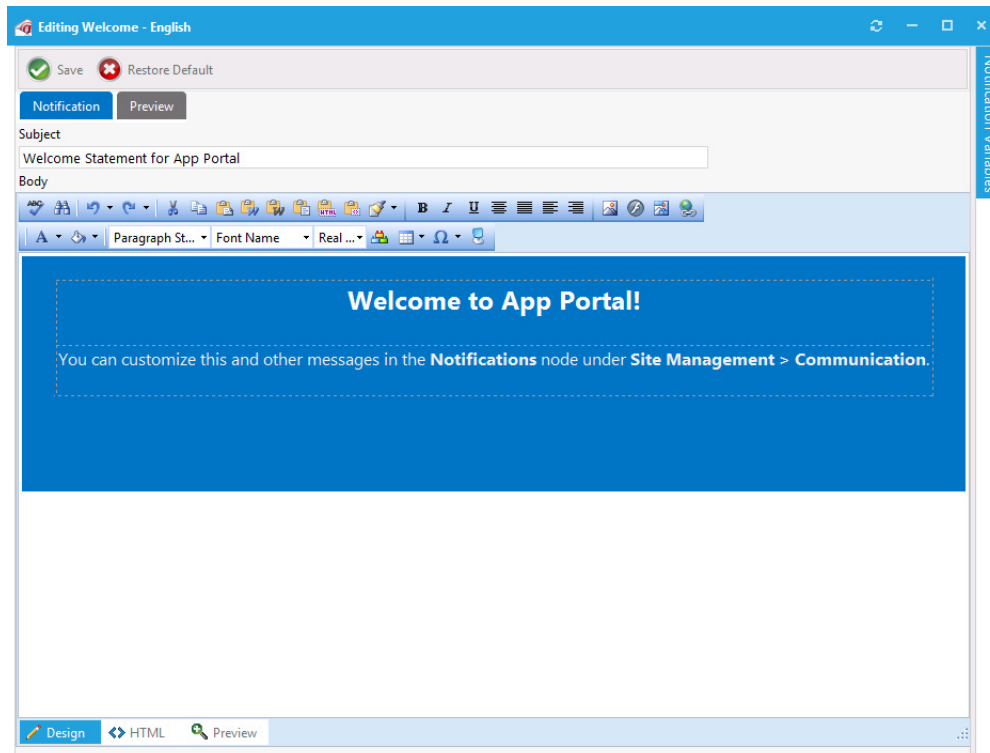
4. Edit the text, using the functions on the toolbar to customize it.

5. To add images, click the **Image Manager** button ( ), and use the **Image Manager** to upload and select an image to insert.

6. Make any other necessary edits in the Editor window. Or, if you prefer to directly edit the HTML code, click **HTML** at the bottom of the editor.

7. Click **Save**. The edited Welcome page is now displayed.

Tip • To see the edited Welcome Page, you may need to close your App Portal browser and then reopen it.

Customizing the App Portal User Interface Colors

By default, App Portal's user interface is branded with a color theme that mostly consists of various shades of blue and gray. However, you can change the color theme on the **Corporate Branding** tab of the **Site Management > Settings > Web Site** view.

Figure 3-33: Corporate UI Branding Tab

There are two methods for changing the App Portal color theme to match your corporate colors:

- Changing the Base Color and Automatically Generating Other Colors

- Changing the Individual Component Colors

Important • If you have modified the CSS files shipped with previous releases of App Portal to customize the colors of the site, those changes will not be retained when you upgrade to App Portal 2015 R2. You will need to perform the steps listed here to customize the colors of your App Portal user interface.

Changing the Base Color and Automatically Generating Other Colors

The easiest way to change the App Portal color theme is to simply change the color listed in the **Select base color** field. App Portal will then automatically generate color codes of various shades of that color that will be used throughout the site.

Task　**To change the color theme by selecting a new base color:**

1. Identify the HEX value of your desired corporate color. For example, if your company had a green logo, the color could be #006600:

#006600

2. On the **Admin** tab, open the **Site Management > Settings > Web Site** view.

3. Open the **Corporate Branding** tab.

4. In the **Select base color** box, enter **#006600** and click **Apply**. The colors in the **Your custom color column** are automatically changed based upon the base color that you entered.

5. If you are satisfied with the colors listed in the **Your custom color**, click **Save**. The browser window will be refreshed and the new color theme will be displayed.

6. To return to the default Flexera Software colors, click the **Reset to default** button at the bottom of the **Corporate UI Branding** tab.

Changing the Individual Component Colors

You have the option of setting the color individually for each of the listed components of the App Portal application. This is a more difficult option because you have to specify slight variations in your corporate color to serve as hover colors and the background colors for drop down menus, etc.

Task   **To change the color theme by specifying colors for App Portal components:**

1. Specify the colors that you want to use for the following App Portal components:

Component	Sub Components	Your Custom Color
Nav bar	Background	
	Icons (unselected)	
	Hover	
Browse categories menu	Menu header background	
	Categories background	
	Category (hover)	
Buttons	Primary	
	Primary (hover)	
	Secondary	
	Secondary (hover)	
Grid/Table	Header row background	
	Row (hover) background	
	Row (alternate) background	
View and dialog box tabs	Tabs (selected)	
	Background	
Highlight color	Search box button, Top border, Progress wheel	
Pop up dialog box	Background	
Others	View titles/subtitles	
	Hyperlink	
	Background of summary box on Checkout page (in progress)	
	Welcome menu hover	
	Dropdown menu hover	
	Admin tab navigation menu hover	
	Image button hover	

2. On the **Admin** tab, open the **Site Management > Settings > Web Site** view.

3. Open the **Corporate Branding** tab.

4. In the **Your custom color** column, enter the colors you have selected.

5. Click **Save**. The browser window will be refreshed and the new colors you specified will be displayed.

6. To return to the default Flexera Software colors, click the **Reset to default** button at the bottom of the **Corporate UI Branding** tab.

Displaying a EULA to New Users

You can choose to display an End User License Agreement the first time an end user opens App Portal. After that user accepts the EULA, it will no longer be displayed.

To enable the display of a EULA to new users, perform the following steps:

Task   ***To enable the display of a EULA to new users:***

1. On the **Admin** tab under **Site Management**, select **Settings**.

2. On the **General** tab, select the **Require EULA?** option and click **Save**.

3. Under **Site Management**, select **Communication > Notifications**. The **Notifications View** opens.

4. On the **Global** tab, double-click on **EULA**. The default **EULA** file opens in an HTML Editor.
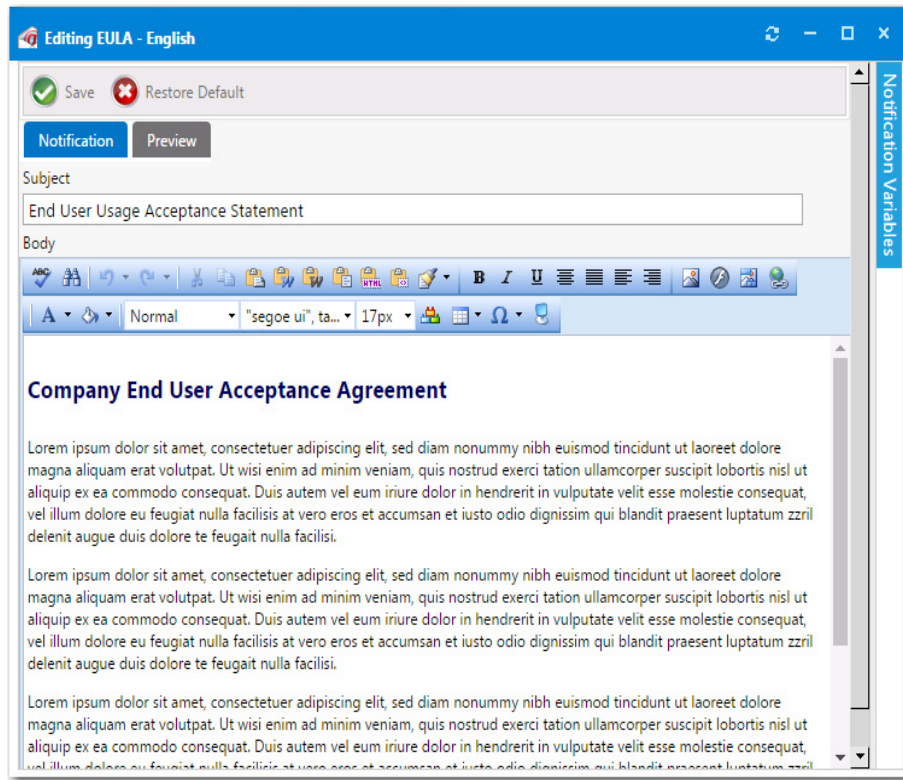
5. Insert the text of your organization's EULA, and format it using the functions on the toolbar.

If you prefer to directly edit the HTML code, click **HTML** at the bottom of the editor.

6. Click **Save**. The next time a new user opens App Portal for the first time, they will be prompted to accept the EULA.
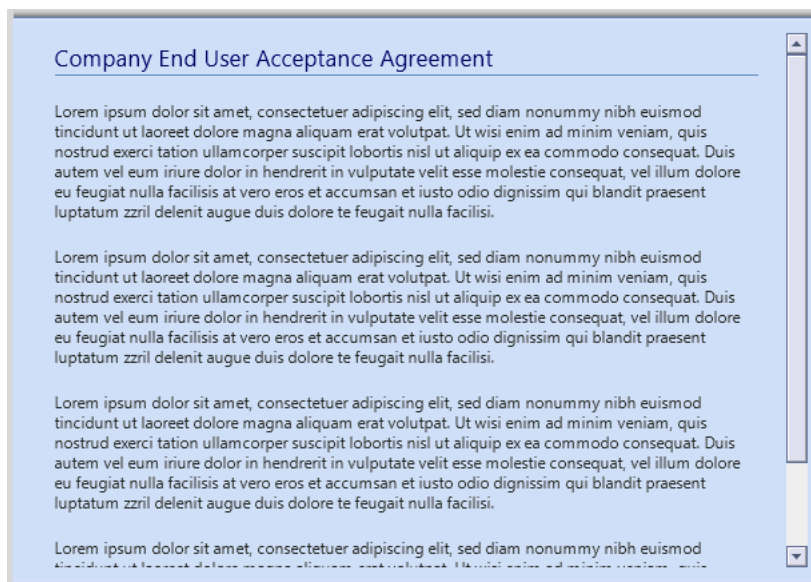
Editing the Help Tab Content

You can customize the **Help** tab to display any content you feel would be most helpful to users at your enterprise.

To customize the content of the **Help** tab, perform the following steps:

Task   ***To customize the content of the Help tab:***

1.   Open the **Admin** tab.

2.   Under **Site Management**, select **Communication > Notifications**. The **Notifications View** opens.

3.   On the **Global** tab, double-click on **Help Page**. The **Help Page** file opens in an HTML Editor.

4.   Edit the text, using the functions on the toolbar to customize it.

     If you prefer to directly edit the HTML code, click **HTML** at the bottom of the editor.

5.   To add images, click the **Image Manager** button ( ), and use the **Image Manager** to upload and select an image to insert.

     *Note • You cannot use Image Manager when you are in **HTML** mode. You must be in **Design** mode.*

6.   Make any other necessary edits, and then click **Save**. The new content will now be displayed on the **Help** tab.

Adding Announcements to the Page Header

You use the **Communication > Announcements** view to add announcements to the App Portal site. Announcements are displayed on the top right corner of the browser window.
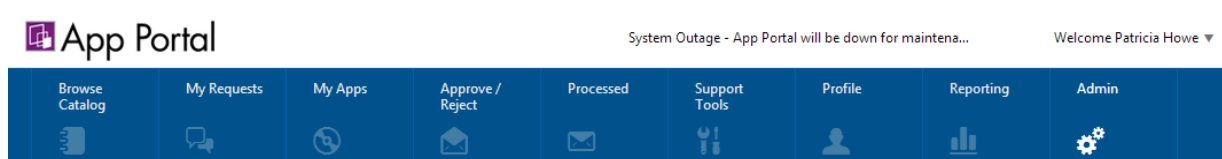
Figure 3-34: Announcement Displayed on the App Portal Site

Task   ***To add announcements to the App Portal page header:***

1.   Open the **Admin** tab.

2.   Under **Site Management**, select **Communication > Announcements**. The **Announcements View** opens.

3.   Click **New**. The **New Announcement** dialog box opens.

4. In the **Announcement title** field, enter a brief title for this new announcement.

5. In the **Expire date** field, enter the date and time after which you no longer want this announcement displayed. If you do not enter an **Expire date**, the announcement will not expire.

6. In the **Announcement** text editor, enter the text of the announcement.

7. Click **Save announcement**. The next time the browser window is refreshed, the **Announcement title**, along with the beginning text of the announcement will be displayed. If a user clicks on the announcement title, a browser window opens displaying the full text of the message.
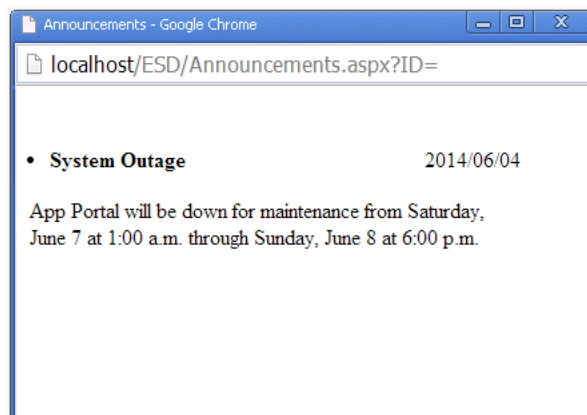
Specifying a Company Support Home Page URL

If you specify a URL for a company Support site, a support icon will be displayed at the top of each App Portal page, which will be linked to that site:
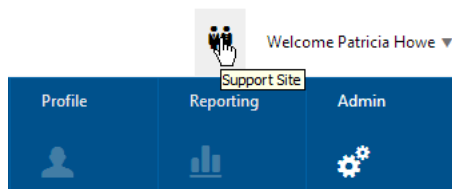
Figure 3-35: Displaying Link to Company Support Page

To specify a company Support home page, perform the following steps:

Task   ***To specify a company Support home page:***

1. On the **Admin** tab under **Site Management**, select **Settings > Web Site**.

2. Open the **Catalog Appearance** tab.

3. Under **Visual Styling**, enter a URL in the **URL for company support home page** field.

4. Click **Save**. The next time the App Portal browser window is opened, the Support icon will be displayed, and it will be linked to the Support site URL you entered.

Updating the Site Name in Browser Title Bar

You can customize the name that is displayed in the title bar of the App Portal browser window. By default, `Flexera Software App Portal` is displayed.

Task   ***To update the site name in the browser title bar:***

1. On the **Admin** tab under **Site Management**, select **Settings > Web Site**.

2. Open the **General** tab.

3. Under **Site Settings**, edit the title in the **Site Title** field.

4. Click **Save**. The next time the App Portal browser window is opened, the new site title will be displayed.

Enabling User Feedback on Your App Portal Site

You can enable a Site Feedback widget for your App Portal site so that users can report feedback or problems. Users are able to select whether they have feedback or are experiencing a problem, and can also specify which site feature (module) that their feedback pertains to. They have the option of uploading files to associate with their feedback.

If the site feedback has been enabled for your App Portal site, as described in Enabling Site Feedback, the Site Feedback widget appears in the lower right corner of all non-Admin pages of the App Portal site.
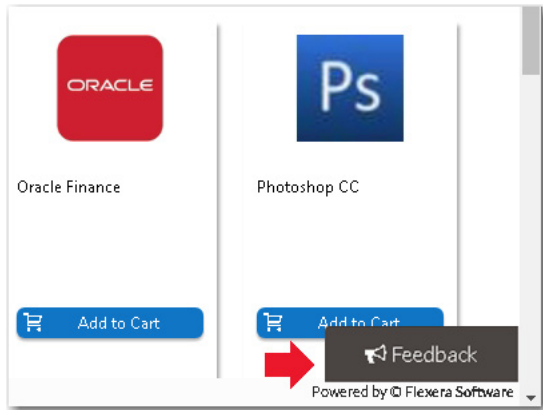
Figure 3-36: Site Feedback Widget

When a user clicks the **Feedback** button, a Feedback window opens, prompting them to describe their issue and also giving them the option to upload files.
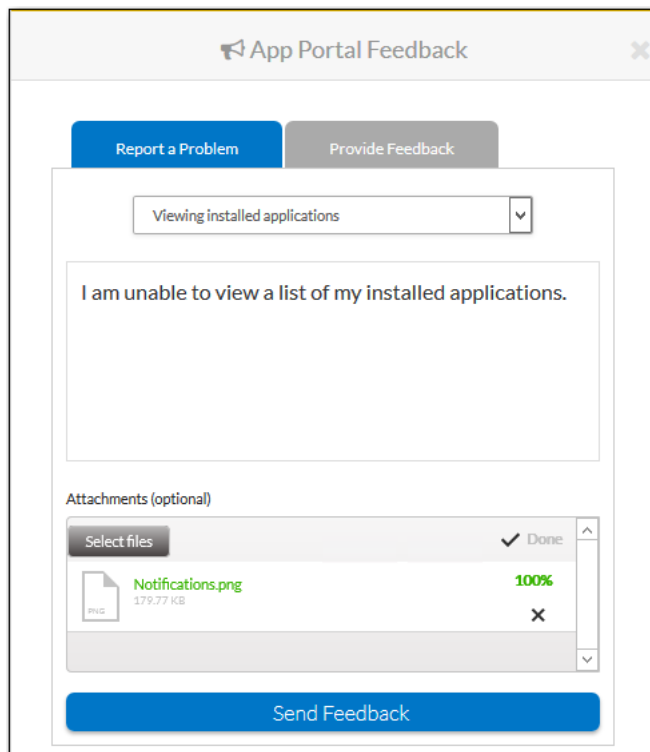
Figure 3-37: Feedback Window

Administrators can view submitted feedback and respond.

Information about enabling the Site Feedback widget is presented in the following sections:

- Enabling Site Feedback

- Submitting Site Feedback

- Viewing and Site Feedback and Setting Status

- Customizing the List of Feedback Modules

Enabling Site Feedback

To turn on the display of the Site Feedback widget on the non-admin pages of your App Portal site, perform the following steps.

Task   ***To enable site feedback:***

1. On the **Admin** tab, select **Site Management > Communication > Site Feedback**. The **Site Feedback** view opens, and displays a note stating that site feedback is currently turned off.
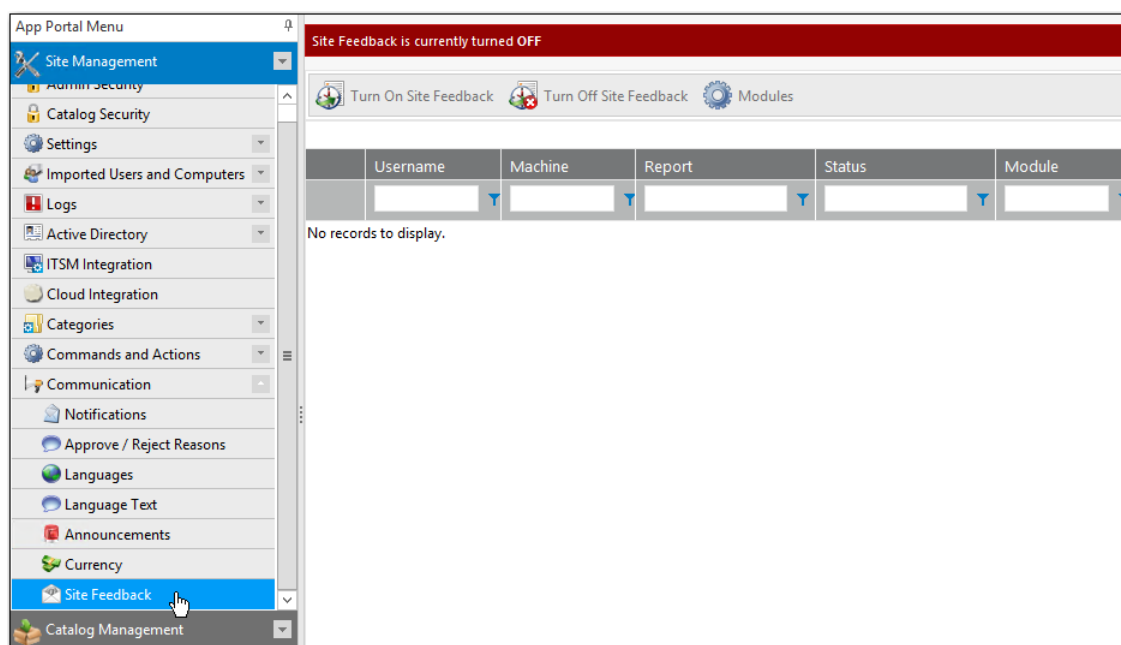
2. Click **Turn On Site Feedback**. A message appears stating that site feedback is currently turned on.
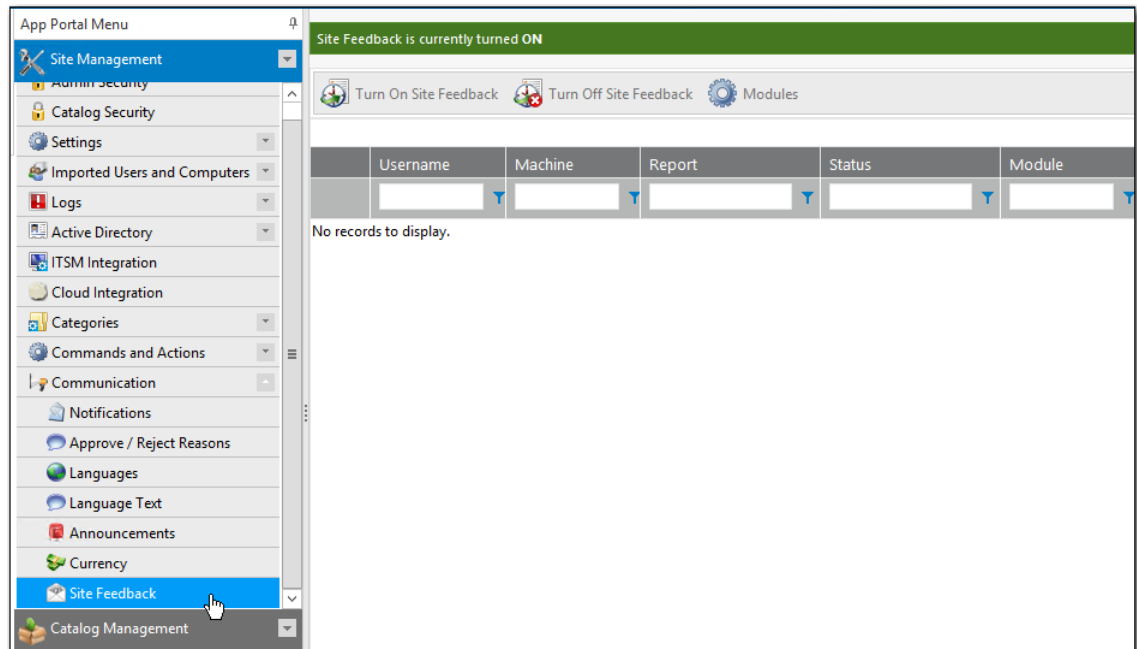
3. Open any non-admin page of App Portal, such as the **Browse Catalog** tab. The Site Feedback widget is now displayed in the bottom right corner.
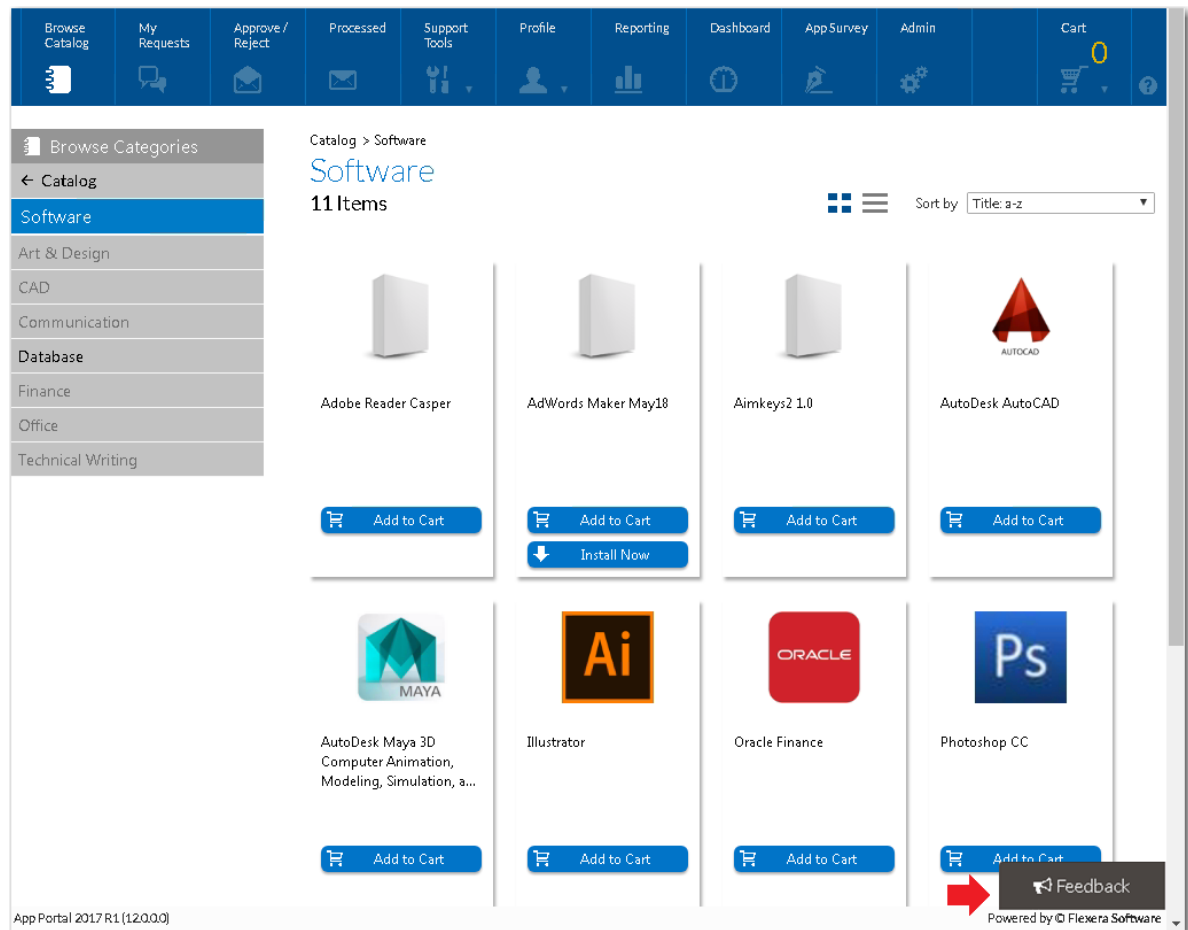
Submitting Site Feedback

If the site feedback has been enabled for your App Portal site, as described in Enabling Site Feedback, the Site Feedback widget appears in the lower right corner of all non-admin pages of the App Portal site.
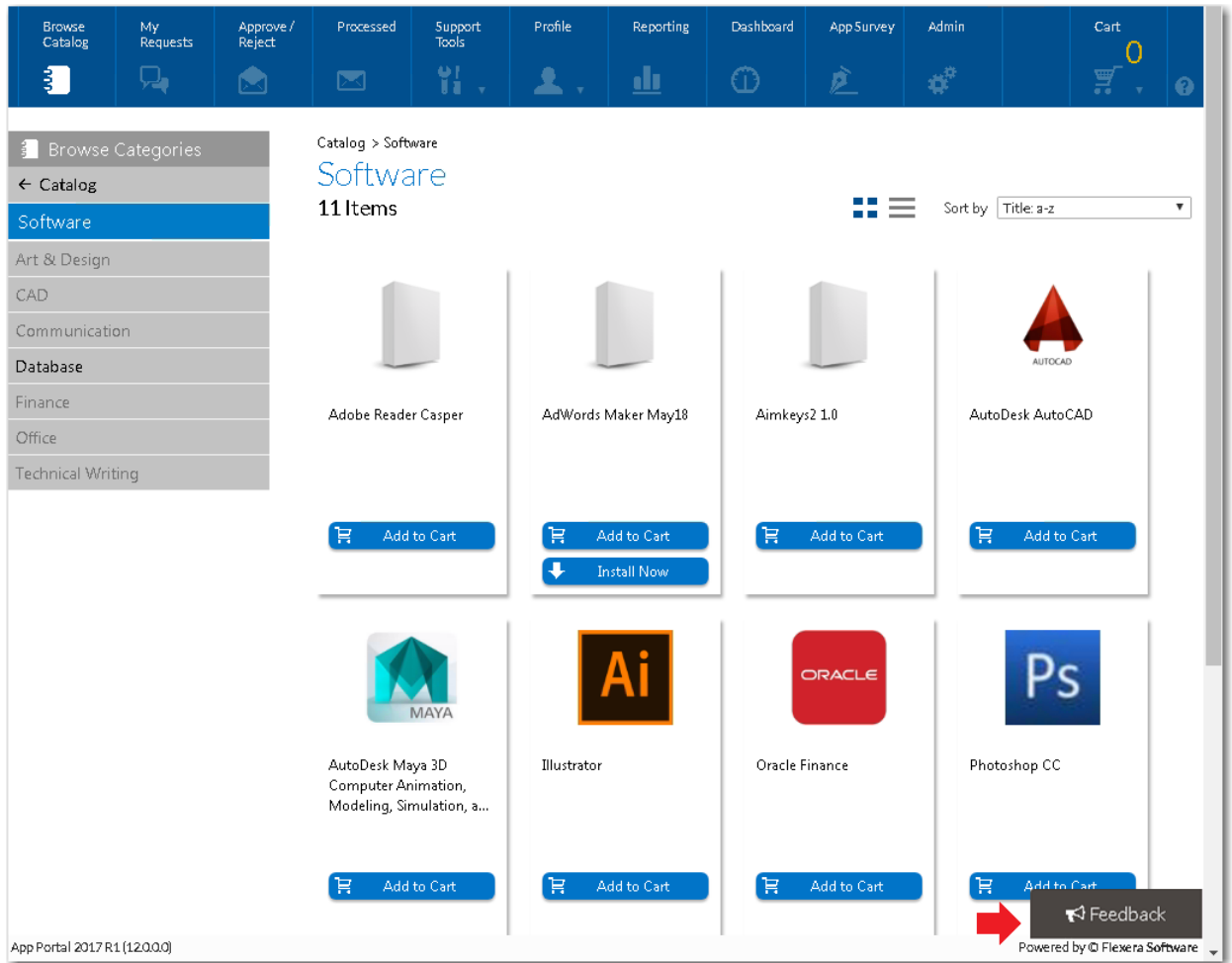
Figure 3-38: Site Feedback Widget

To submit feedback on the App Portal site, perform the following steps:

Task   **To submit feedback on the App Portal site:**

1.   In the lower right-corner of an App Portal (non-admin) view, click **Feedback**. The Feedback window opens.

2.   Select one of the following options:

- **Report a Problem**—Select this option to report a problem that you encountered when using the App Portal website, such as an error message, or unexpected behavior.

- **Provide Feedback**—Select this option to express an opinion on App Portal features and capabilities, or to request enhancements.

3.   Click in the **Select an App Portal features** list and select the App Portal feature that your feedback relates to.

4.   In the **Provide a description of your issue or feedback...** box, describe the issue that you have encountered or the enhancement that you want to request.

5.   If desired, click **Select files** and attach files to this feedback submission.

6. When you have completed entering feedback, click **Send Feedback** to submit the feedback. A message confirming that your feedback has been submitted is displayed for about 5 seconds.

Viewing and Site Feedback and Setting Status

On the **Site Feedback** view, App Portal administrators can review the feedback submissions sent by users, and update the status of feedback issues.

Task   **To view site feedback:**

1. On the **Admin** tab, select **Site Management > Communication > Site Feedback**. The **Site Feedback** view opens, listing all submitted feedback.

2. To view the details of a feedback submission, click **Select** next to the feedback issue you want to view. The Feedback Details view opens, displaying both the text of the submitted feedback issue and a list of the files that were uploaded with the feedback issue.

The following information is displayed:

Property	Description
Unique Name	User name of person who submitted the issue.
Machine Name	Machine name from which the issue was submitted.
Created (UTC)	Date and time that the issue was submitted.
Report Type	Identifies this issue as either a **Problem** or **Feedback**.
Module	App Portal module selected when the issue was submitted.
Uploads	Number of files uploaded with this feedback issue.

3. To download an uploaded file, click the **Download** link next to the file name.

4. After addressing the feedback issue, you can change its response status to one of the following:

- New

- Open

- Review

- Reject

- Needs Clarification

- Hold

- Backlog

- Close

Customizing the List of Feedback Modules

When a user submits a feedback issue, they are prompted to select an App Portal feature from the **Which site module?** list to categorize the issue they are submitting:
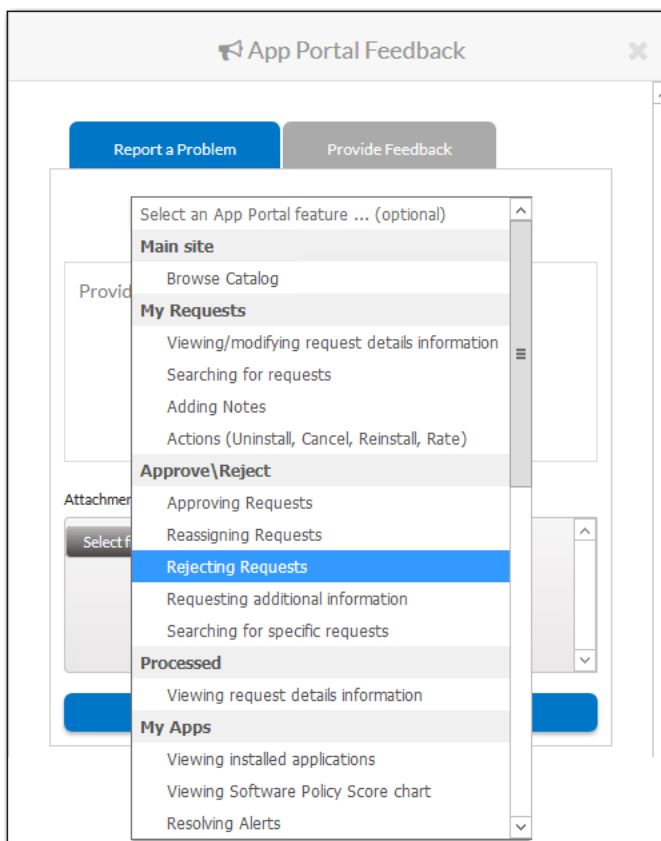
Figure 3-39: Which site module? list

By default, the following modules are listed:

Table 3-12 • App Portal Feedback Modules

Category	Subcategory	Sub-Subcategory
Main site	Browse Catalog	
	My Requests	Viewing/modifying request details information
		Searching for requests
		Adding notes
		Actions (Uninstall, Cancel, Reinstall, Rate)
	Approve\Reject	Approving requests
		Reassigning requests
		Rejecting requests
		Requesting additional info
	Processed	Viewing request details information
	My Apps	Viewing installed applications
		Viewing Software Policy Score chart
		Resolving alerts
		Uninstalling installed application
	Profile	Viewing user information
		Viewing User Readiness records
	Reporting	Viewing reports
		Saving reports
	Dashboard	Viewing ROI reports
		Exporting reports
	App Survey	Selecting applications
		Answering questions
		Reviewing selections

Table 3-12 • App Portal Feedback Modules

Category	Subcategory	Sub-Subcategory
Mobile Site	Searching for catalog items	
	Requesting catalog items	
	Viewing categories	
	Viewing catalog item descriptions	
	Other	
Notifications	Clicking a link within notifications	

Important • *Only site modules that do not have child modules are selectable by end users.*

You can customize this list of feedback modules to hide items, show previously hidden items, and add new items.

Task

To customize the App Portal feedback module list:

1. On the **Admin** tab, select **Site Management > Communication > Site Feedback**. The **Site Feedback** view opens, listing all submitted feedback.

2. Click the **Modules** button. The **Site Feedback Modules** view opens.

3. Expand the tree in the **Preview Site Module Tree Structure** to view the currently displayed modules.

4. To hide a module, select the module name from the **Hide Site Module Selection** list and then click **Hide**.

Important • *If you hide a parent module group, all of its child modules will also be hidden from the* **Select an App Portal**
feature *list on the Feedback form.*

5. To show a previously hidden module, select the module name from the **Show Site Module Selection** list and then
click **Show**.

6. To add a new module to the list, perform the following steps in the **Add Site Module Selection** area:

a. Enter a name for the module in the **Enter module name** text box.

b. From the **Select a parent group**, select one of the listed items.

Note • *You cannot create a new root-level parent group, which are* **Main site**, **Mobile site**, *and* **Notifications**.

c. Click **Show**.

Viewing Dashboards

On the **Dashboard** tab, you can view helpful reports that demonstrate how much time and money using App Portal is
helping you save in your software and operating system deployment projects. The following dashboards of reports are
available:

- Software Reclamation Dashboard

- Software and OS Deployment ROI Dashboards

- SLA Dashboard

For related information refer to the following sections:

- Setting Global Dashboard Options (which includes information about setting thresholds for successful, pending, and
  failed reclamations)

- Assigning Permissions to View Dashboards

Software Reclamation Dashboard

App Portal's **Software Reclamation** dashboard is now the Home page of App Portal if you have permissions to view it. App
Portal's **Software Reclamation** dashboard provides tiles and graphs to give you an overview of the progress and status of
your software reclamation policies. The tiles at the top of the dashboard display the total reclamation savings over a
specified time frame, and also displays the percentage of successful, pending, and failed reclamations in that same time
frame. Six graphs are also provided on the dashboard that give granular reclamation details. With all of this information
readily available, you will be able to more closely monitor your software reclamation efforts, helping to drive continual
software license reclamation and optimization.
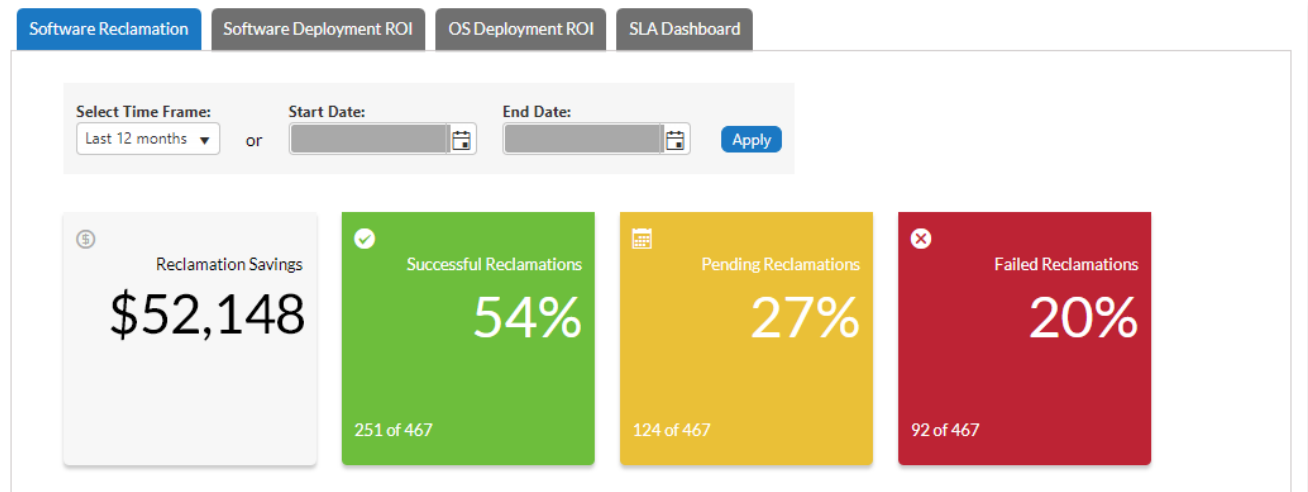
Figure 3-40: Software Reclamation Dashboard Tiles

The following graphs are also provided on the Software Reclamation dashboard below the overview tiles.

- Software Reclamation Savings

- Top Software Titles by Reclamation Savings

- Top Software Titles Reclaimed

- Top Software Titles by Reclamation Status

- Software Reclamation Status

- Reclamation Response Breakdown for Top Software Titles

For related information, refer to:

- Viewing the Software Reclamation Dashboard

- Choosing Time Frame for Graph Data

- Selecting Graph Export, Annotate, and Print Options

- Clicking Interactive Graph Legends

- Setting Global Dashboard Options

- Assigning Permissions to View Dashboards

Software Reclamation Savings

The **Software Reclamation Savings** dashboard displays reclamation savings over a specified time frame. To change the time frame, use the **Select Time Frame** drop-down list or the **Start Date** and **End date** fields and click **Apply** as described in Choosing Time Frame for Graph Data.
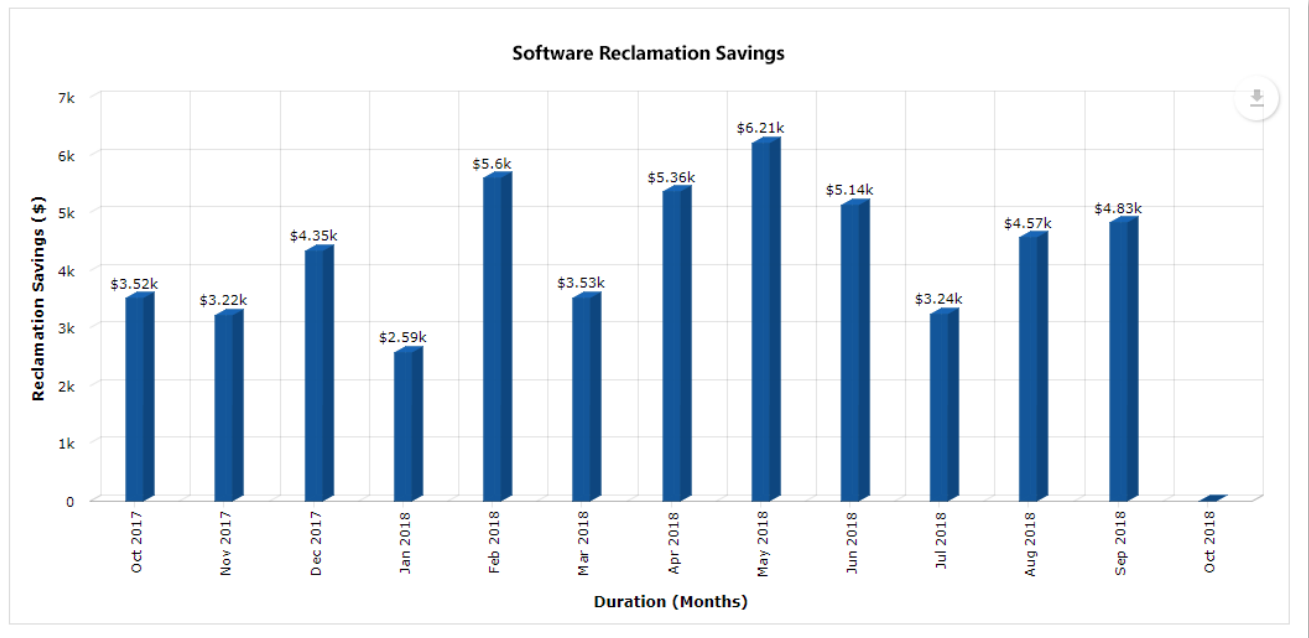
Figure 3-41: Software Reclamation Savings

Each bar represents the total savings earned for that time frame, with the total cost displayed on the top of each bar. Hovering over any bar provides an enhanced view of the reclamation savings for the specified time frame.

Export, annotation and printing options: At the top right of the graph, there is a down arrow that provides options for exporting and printing, and includes an annotate option that lets you add notes to the graph. For more information, refer to Selecting Graph Export, Annotate, and Print Options.

Top Software Titles by Reclamation Savings

This graph displays the software titles that have generated the most reclamation savings over a specified time frame. To change the time frame, use the **Select Time Frame** drop-down list or the **Start Date** and **End date** fields as described in Choosing Time Frame for Graph Data.

The number of titles displayed in the graph is based upon the number selected in the **Software Titles** drop-down. Selectable values are 5, 10, 25, 50, 100. The default is 5.
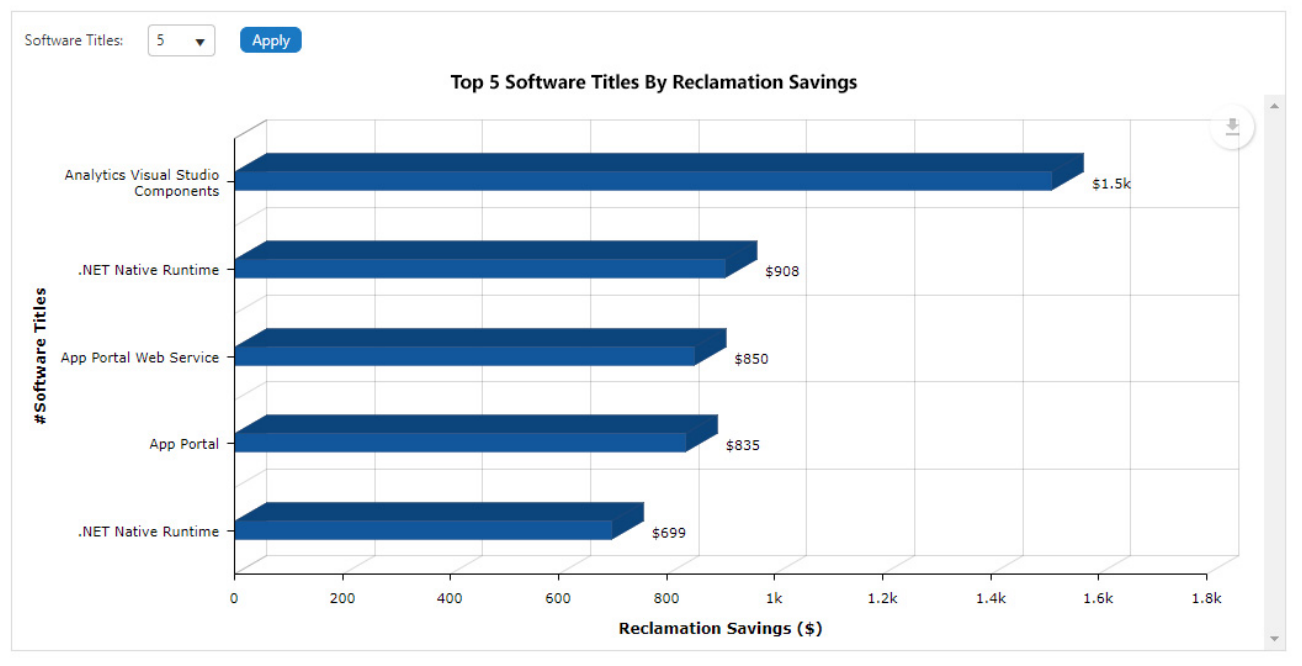
Figure 3-42: Top Software Titles by Reclamation Savings

Each bar represents the total number of savings earned for that time slot, with the total cost displayed at the far right of each horizontal bar. Hovering over the bar also displays the reclamation savings and application details.

Export, annotation and printing options: At the top right of the graph, there is a down arrow that provides options for exporting and printing, and includes an annotate option that lets you add notes to the graph. For more information, refer to Selecting Graph Export, Annotate, and Print Options.

Top Software Titles Reclaimed

This graph displays the software titles that have been reclaimed over the specified time frame. To change the time frame, use the **Select Time Frame** drop-down list or the **Start Date** and **End date** fields and click **Apply** as described in Choosing Time Frame for Graph Data.

Each bar represents the total number of successfully reclaimed software for that time slot, with the total number displayed on the top of each bar. Each bar is divided by colors with each color representing individual software titles. When hovering over a color, the name of the software title is displayed along with the version and the reclaimed count for that duration.

The number of titles displayed in the graph is based upon the number selected in the **Software Titles** drop-down. Selectable values are 5, 10, 25, 50, 100. The default is 5.
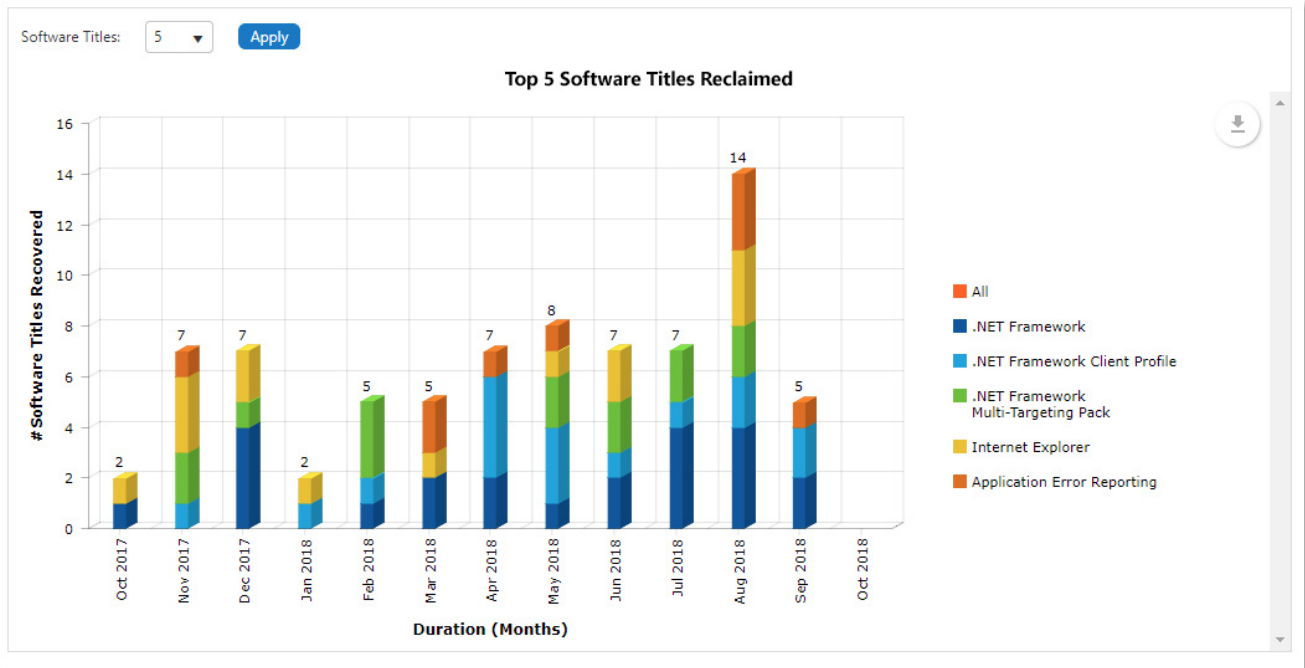
Figure 3-43: Top Software Titles Reclaimed

Clickable interactive legend: On the right side of the graph, the status legend is displayed, and you can click to deselect and remove any status from the graph. Clicking that status legend again adds it back to the graph. For more information, refer to Clicking Interactive Graph Legends.

Export, annotation and printing options: At the top right of the graph, there is a down arrow that provides options for exporting and printing, and includes an annotate option that lets you add notes to the graph. For more information, refer to Selecting Graph Export, Annotate, and Print Options.

Top Software Titles by Reclamation Status

This graph displays the top software titles that have been processed for reclamation over the specified time frame. To change the time frame, use the **Select Time Frame** drop-down list or the **Start Date** and **End date** fields and click **Apply** as described in Choosing Time Frame for Graph Data.

The number of titles displayed in the graph is based upon the number selected in the **Software Titles** drop-down. Selectable values are 5, 10, 25, 50, 100. The default is 5.
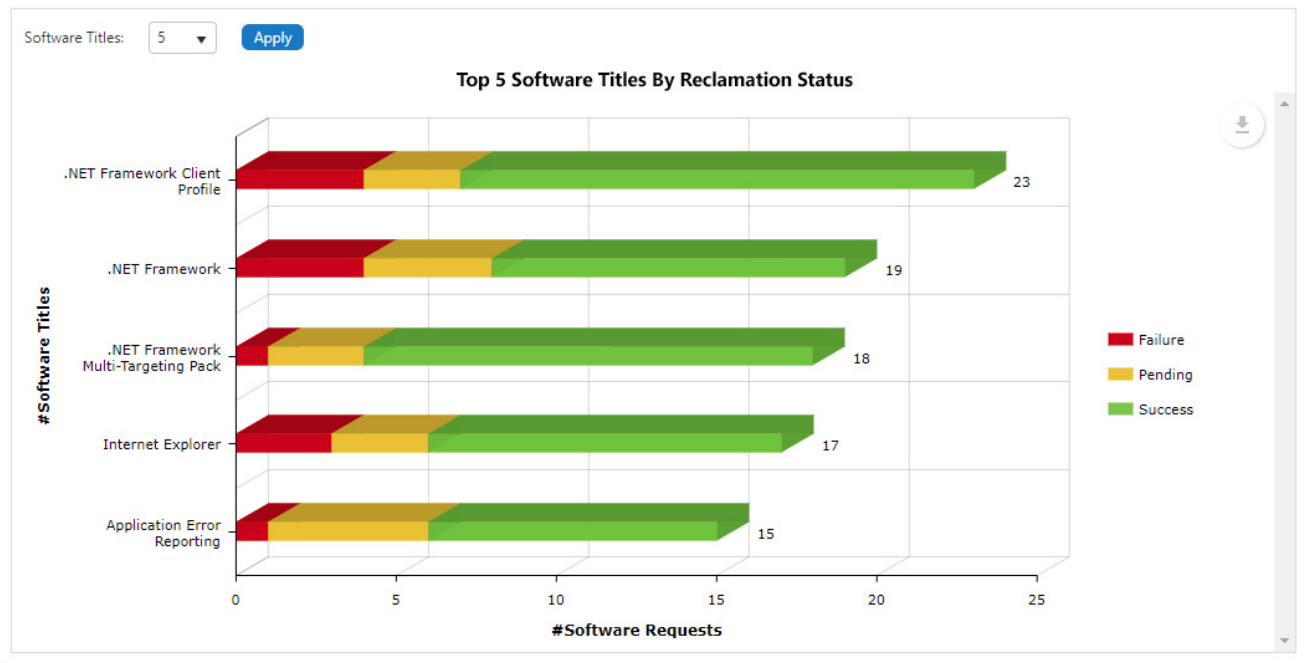
Figure 3-44: Top Software Titles by Reclamation Status

Each bar is divided into statuses: **Failure** in red, **Pending** in yellow and **Success** in green. Hovering over the color provides the name and version of the software title and the **Failure**/**Pending**/**Success** status count in that duration. At the end of the horizontal bar, the total number of requests placed for the software title is displayed.

Clickable interactive legend: On the right side of the graph, the status legend is displayed, and you can click to deselect and remove any status from the graph. Clicking that status legend again adds it back to the graph. For more information, refer to Clicking Interactive Graph Legends.

Export, annotation and printing options: At the top right of the graph, there is a down arrow that provides options for exporting and printing, and includes an annotate option that lets you add notes to the graph. For more information, refer to Selecting Graph Export, Annotate, and Print Options.

Software Reclamation Status

This graph displays the total software reclamation requests that have been placed over the specified time frame, and then groups them by **Failed**/**Pending**/**Success** status. To change the time frame, use the **Select Time Frame** drop-down list or the **Start Date** and **End date** fields and click **Apply** as described in Choosing Time Frame for Graph Data. The bottom of the graph is categorized by years, months, weeks, or in days depending on the selected time frame.

The number of titles displayed in the graph is based upon the number selected in the **Software Titles** drop-down. Selectable values are 5, 10, 25, 50, 100. The default is 5. If you change the number selected in the **Software Titles** drop-down and click **Apply**, the graph will render that number of bars with a scroll bar added as needed so you can scroll to see all software title bars.
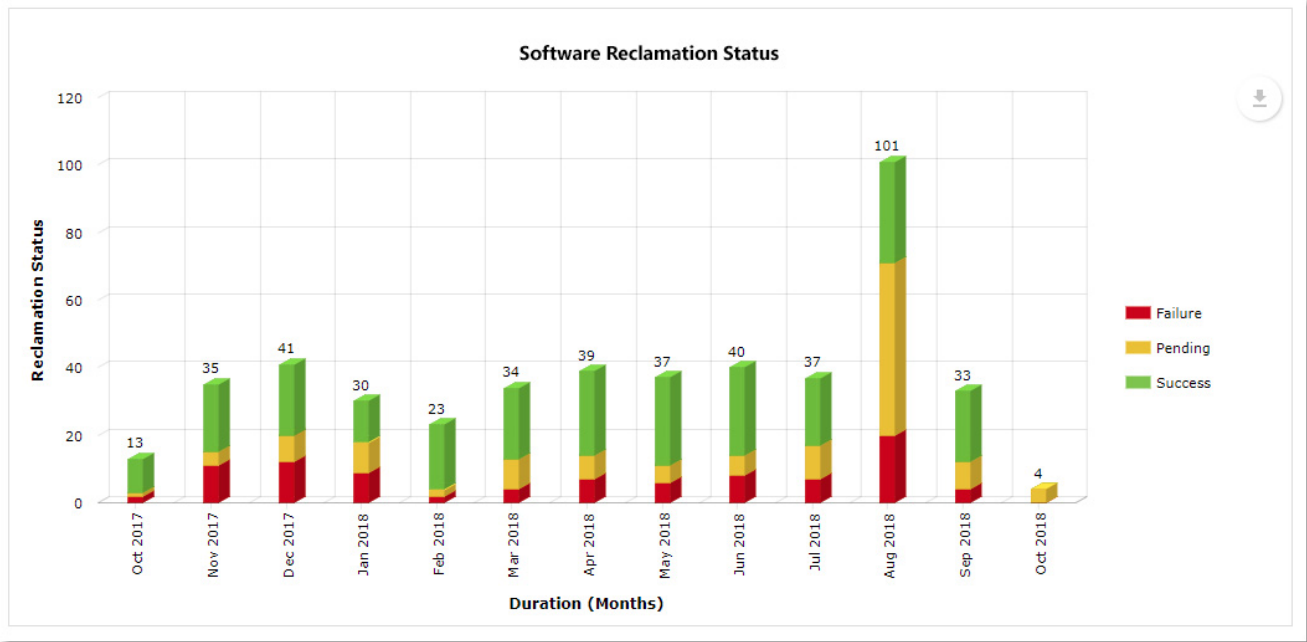
Figure 3-45: Software Reclamation Status

Each bar on the graph represents the total number of software requests placed over the time frame shown, with the total number of requests displayed on the top of each bar. Each bar is divided by colors according to the status of the software request. Hovering overing over a color on a bar displays the number of reclamation requests for that status and time frame.

Clickable interactive legend: On the right side of the graph, the status legend is displayed, and you can click to deselect and remove any status from the graph. Clicking that status legend again adds it back to the graph. For more information, refer to Clicking Interactive Graph Legends.

Export, annotation and printing options: At the top right of the graph, there is a down arrow that provides options for exporting and printing, and includes an annotate option that lets you add notes to the graph. For more information, refer to Selecting Graph Export, Annotate, and Print Options.

Reclamation Response Breakdown for Top Software Titles

This graph displays the software titles that have been reclaimed over a specified time frame and groups the results by reclamation response (**Keep**, **Not Responded**, **User Uninstall**, and **System Uninstall**). To change the time frame, use the **Select Time Frame** drop-down list or the **Start Date** and **End date** fields and click **Apply** as described in Choosing Time Frame for Graph Data. The bottom of the graph is categorized by years, months, weeks, or in days depending on the selected time frame.

The number of titles displayed in the graph is based upon the number selected in the **Software Titles** drop-down. Selectable values are 5, 10, 25, 50, 100. The default is 5.
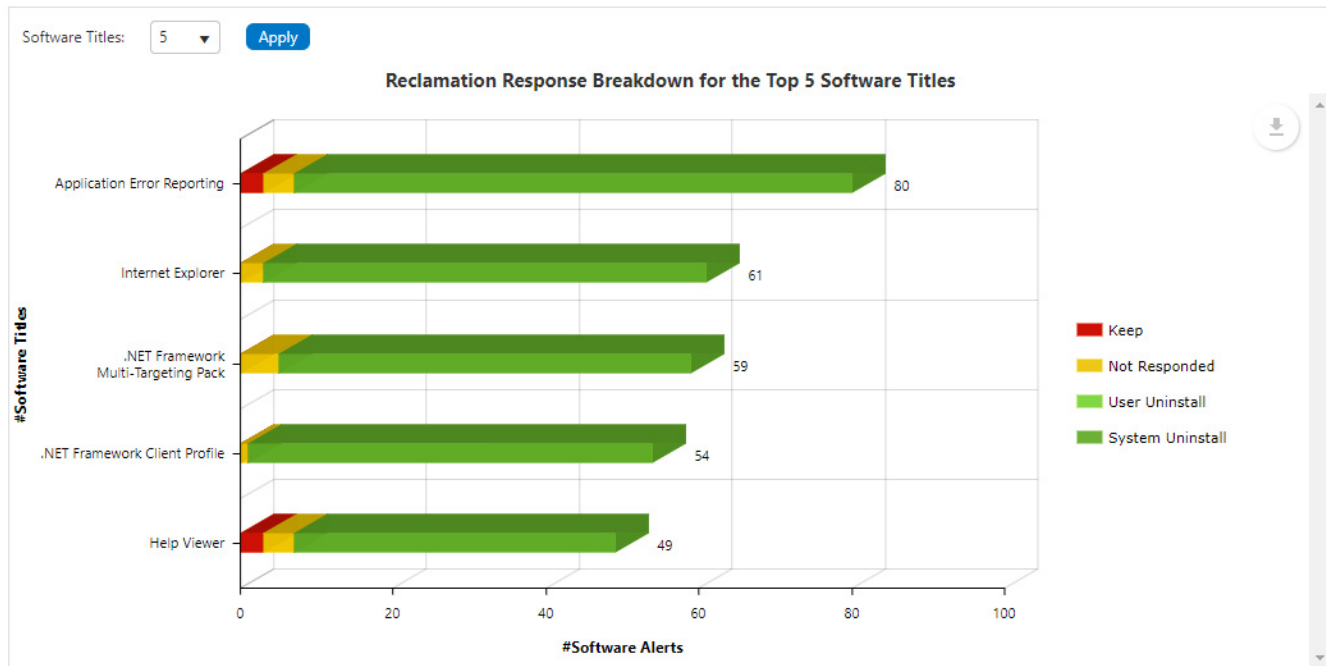
Figure 3-46: Reclamation Response Breakdown for Top Software Titles

Each bar represents individual software titles sorted by maximum alerts generated. Each color represents the different responses (**Keep**, **Not Responded**, **User Uninstall**, and **System Uninstall)** taken by a user or system administrator. Hovering over the color displays the name and version of the software along with number of the type of actions taken for the selected time frame. At the end of the horizontal bar, the total number of alerts generated for the respective software is displayed.

Clickable interactive legend: On the right side of the graph, the status legend is displayed, and you can click to deselect and remove any status from the graph. Clicking that status legend again adds it back to the graph. For more information, refer to Clicking Interactive Graph Legends.

Export, annotation and printing options: At the top right of the graph, there is a down arrow that provides options for exporting and printing, and includes an annotate option that lets you add notes to the graph. For more information, refer to Selecting Graph Export, Annotate, and Print Options.

Viewing the Software Reclamation Dashboard

To view the **Software Reclamation** dashboard, perform the following steps.

Task   ***To view the Software Reclamation dashboard:***

1. Set desired dashboard options as described in Setting Global Dashboard Options.

2. To access the dashboard, click the **Dashboard** tab.

    The dashboard opens the **Software Reclamation** tab, which is the default tab.

📄

*Note • Any user who has View permission for the Reporting/Dashboard (provided under **Admin-> Catalog Security -> Reporting/ Dashboard**) sees the **Software Reclamation** dashboard when logging in to App Portal. For users who don't have permission to view the **Reporting/ Dashboard**, their default landing page is the **Browse Catalog** page, Users with permission can also access the **Software Reclamation** dashboard from anywhere in App Portal by clicking the **Dashboard** tab.*

3.   To set the thresholds for successful, pending, and failed reclamations, refer to Setting Global Dashboard Options.

4.   Set the desired data interval by doing *either* of the following:

   •   Choose a time frame from the **Select Time Frame** drop down (last 12, 9, 6, or 3 months) and click **Apply**.

   •   Select the **Start Date** and **End Date** lists, and click **Apply**.

5.   To remove any legend value and color from a graph (for any graph that include a legend on the right of the graph), click the value in the legend that you want removed. For more information, refer to Clicking Interactive Graph Legends.

6.   To export, print, or annotate a graph, click the down arrow at the top right of the graph and select an option. For more information, refer to Selecting Graph Export, Annotate, and Print Options.

The following graphs that are provided on the Software Reclamation dashboard.

   •   Software Reclamation Savings

   •   Top Software Titles by Reclamation Savings

   •   Top Software Titles Reclaimed

   •   Top Software Titles by Reclamation Status

   •   Software Reclamation Status

   •   Reclamation Response Breakdown for Top Software Titles
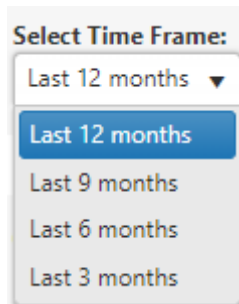
For information about dashboard global options, refer to:

   •   Choosing Time Frame for Graph Data

   •   Selecting Graph Export, Annotate, and Print Options

   •   Clicking Interactive Graph Legends

   •   Setting Global Dashboard Options

   •   Assigning Permissions to View Dashboards
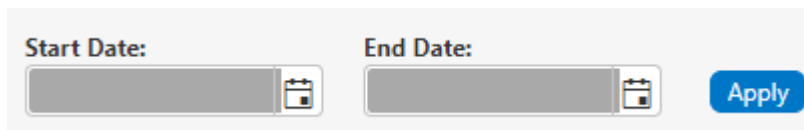
Choosing Time Frame for Graph Data

The default date selected in the **Select Time Frame** drop-down list is **Last 12 months**. The time frame that is selected or specified is used for **all** graphs on the **Software Reclamation** dashboard. There are two ways you can specify a different time frame.

   •   Choose a time frame from the **Select Time Frame** drop-down list and click **Apply**.
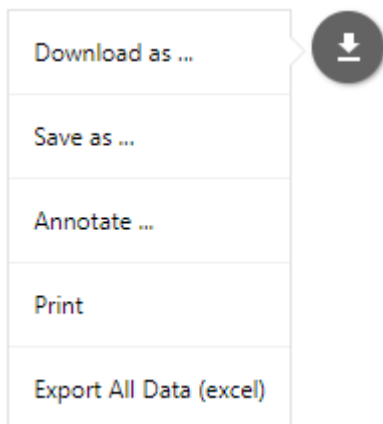
- Specify a custom time frame in the **Start Date** and **End date** fields and click **Apply**.

Note • The last selected date control will be stored in browser storage. When you log in again, all Software Reclamation dashboard graphs will be rendered based on those stored dates.

Selecting Graph Export, Annotate, and Print Options

Each of three graphs on the **Software Reclamation** dashboard contain additional options. Click the down arrow at the top right of any graph to choose a graph option.

The following options are provided:

- **Download**—Downloads the graph as PNG, JPG, SVG, or PDF.

- **Save as**—Saves the graph data as CSV, XSLX, or JSON.

- **Annotate**—Lets you add notes to the graph. After you click **Annotate** and add notes to the graph, the drop-down list of options adds a **Cancel** option that gives you a way to erase annotations.

- **Print**—Prints the graph.

● **Export All Data (Excel)**—Exports data for all the software titles for the selected time frame (i.e., not only data for the of titles shown in the graph but data for all titles).

*Note • The **Export All Data (Excel)** option is provided for the following graphs only: **Top Software Titles by Reclamation Savings**, **Top Software Titles by Reclamation Status**, **Reclamation Response Breakdown for Top Software Titles.***

Clicking Interactive Graph Legends

Many graphs on the **Software Reclamation** dashboard contain legends at the right of the graph that provide a key for the colors used in the graph. These legends are interactive. You can click any legend value to remove it from the graph. Clicking a deselected legend value adds it back to the graph.

For example, the following shows the Software Reclamation Status graph with all legend values included.
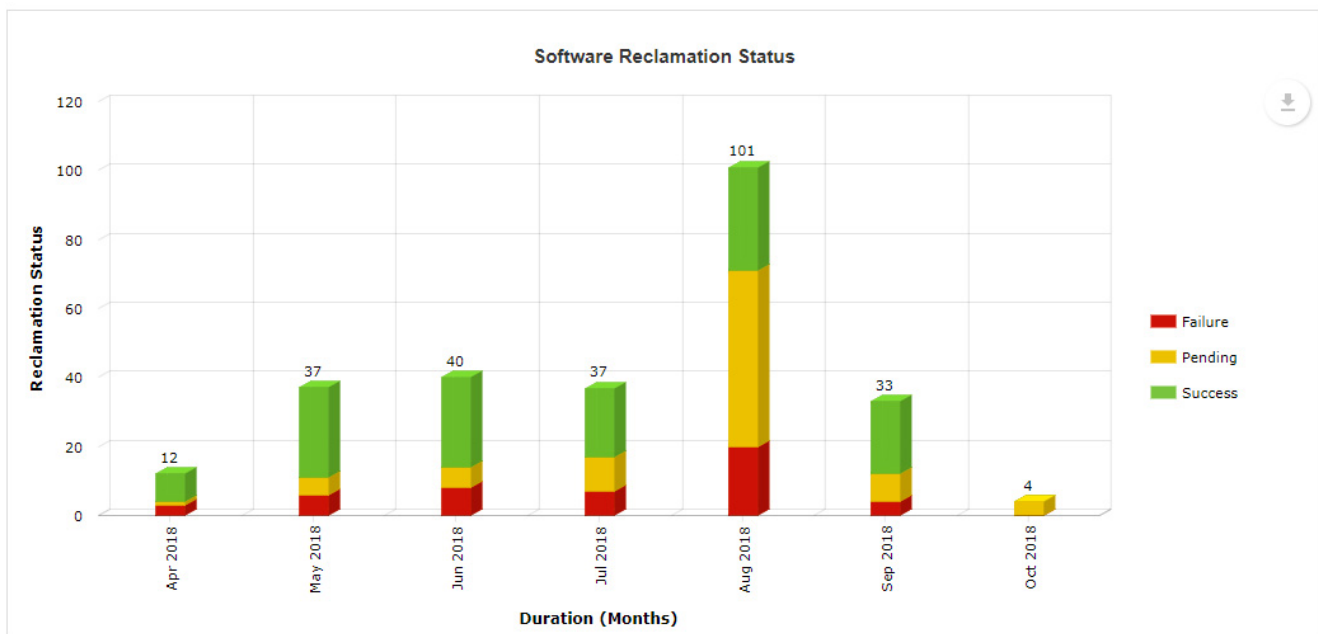
Figure 3-47: All legend values included in graph

Clicking the red **Failure** legend status grays out that status in the legend and removes all red sections of the bars in the graph.
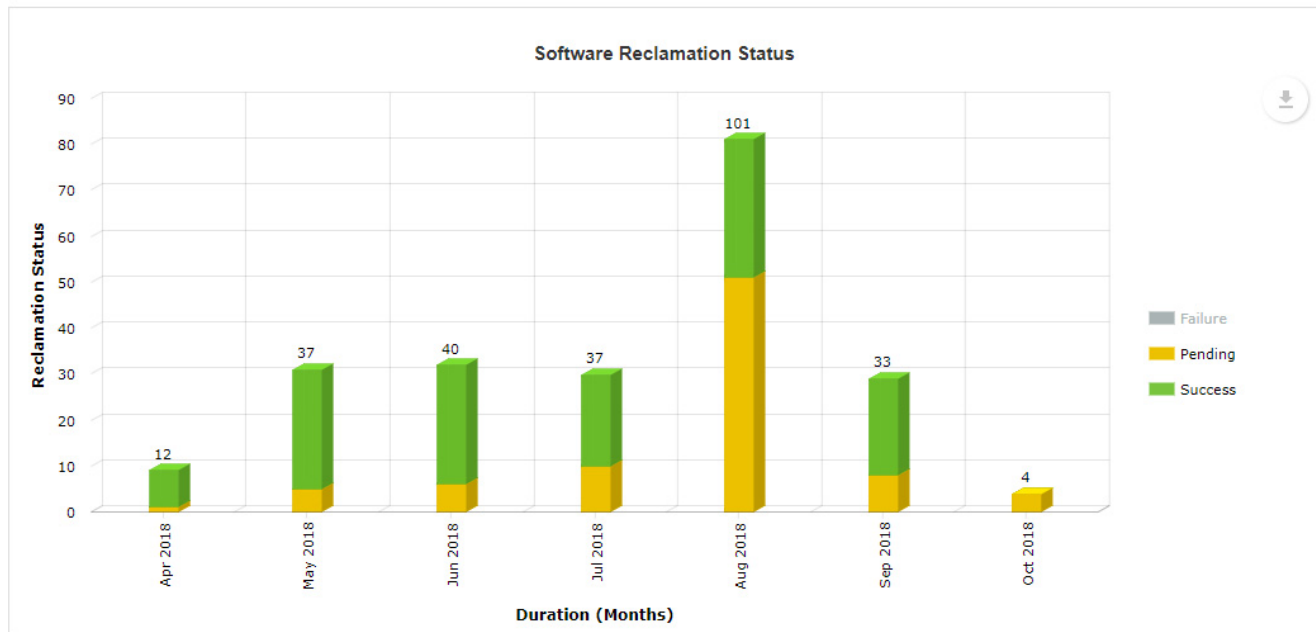
Figure 3-48: Failure status deselected in the legend and removed from graph

Software and OS Deployment ROI Dashboards

App Portal's **Software Deployment ROI** and **OS Deployment ROI** dashboard reports provide administrators with time and cost savings associated with implementing IT automation by using App Portal for application and OS requests.
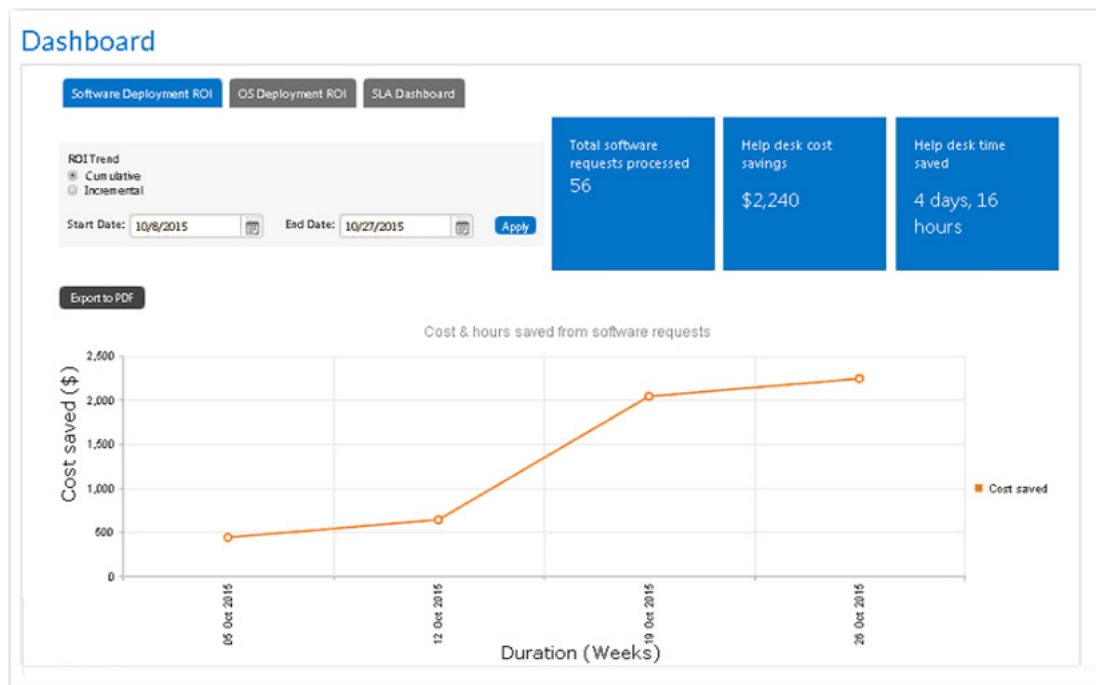
Figure 3-49: Software Deployment ROI Dashboard

To view the **Software Deployment ROI** and **OS Deployment ROI** dashboard reports, perform the following steps:

Task   ***To view the Software Deployment ROI and OS Deployment ROI dashboard reports:***

1.   Set your desired dashboard options, as described in Setting Global Dashboard Options.

2.   Open the **Dashboard** tab and select **Software Deployment ROI** or **OS Deployment ROI**.

3.   Choose the **ROI Trend** you would like to view by selecting either **Cumulative** (shows the data growing over time) or **Incremental** (only includes the data measured during the specified interval).

4.   Set the desired data interval that you would like to review by making selections from the **Start Date** and **End Date** lists, and then click **Apply**.

5.   Click on the dots in the line chart to view additional information.

Note the following about these ROI dashboards:

- **Software deployment only**—The **Software Deployment ROI** dashboard only includes software requests; it does not include data from general or task sequence requests.

- **OSD deployment only**—The **OS Deployment ROI** dashboard only includes OSD requests.

- **Duration increment**—The duration increment of the line chart (days, weeks, months, quarters, or years) is dependent upon the length of the date range:

Duration Increment	Length of Date Range
Days	0 to 15 days
Weeks	15 to 105 days
Months	105 days to 15 months
Quarters	15 months to 45 months
Years	Over 45 months

SLA Dashboard

The **SLA Dashboard** lists statistics on both deployment progress and catalog items awaiting action.
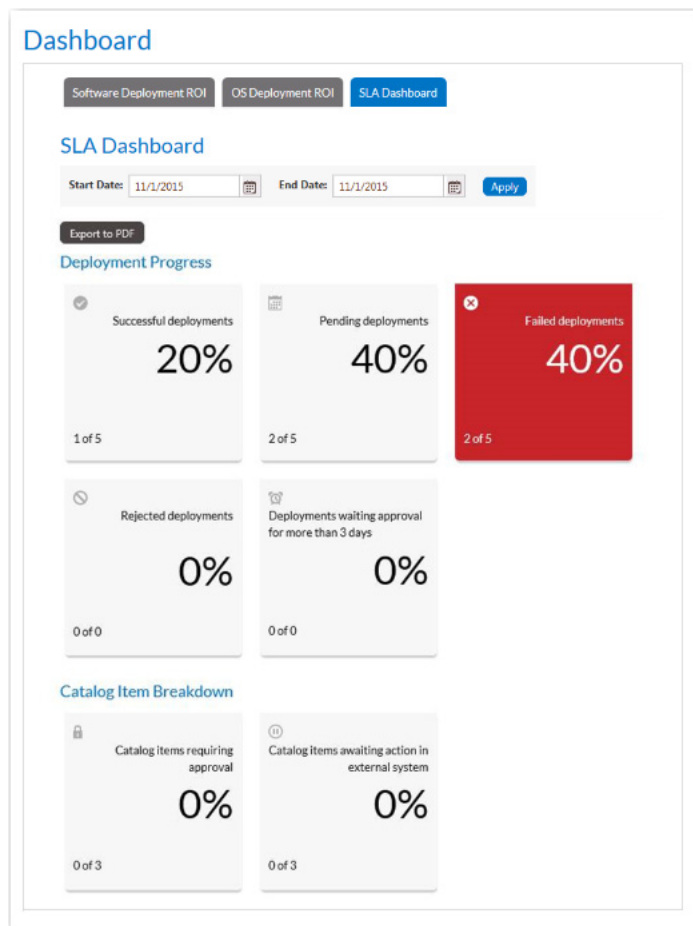
Figure 3-50: SLA Dashboard

Deployment Progress Area

The **SLA Dashboard** lists statistics on deployment progress in the following categories:

- Successful deployments

- Pending deployments

- Failed deployments

- Rejected deployments

- Deployments waiting approval for more than n days

Catalog Breakdown Area

The **Catalog Breakdown** area lists the percentage of catalog items that are awaiting outside action:

- Requiring approval

- Awaiting action in external system

You can click on any of the cards to view a list of the requests that fall into that category.

Viewing the SLA Dashboard

To view the **SLA Dashboard**, perform the following steps.

Task   ***To view the SLA Dashboard:***

1. Set your desired dashboard options, as described in Setting Global Dashboard Options.

2. Open the **Dashboard** tab and select **SLA Dashboard**.

3. Choose time frame you would like to view statistics for by making selections from the **Start Date** and **End Date** lists, and then click **Apply**.

4. Click on any of the cards to view a list of the requests that fall into that category.

Setting Global Dashboard Options

You set dashboard reporting options on the **Dashboard** tab of the **Site Management > Settings > Web Site** view.

Task   **To set dashboard options:**

1. On the **Admin** tab, open the **Site Management > Settings > Web Site** view and click the **Dashboard** tab.

2. Under **Threshold settings** (under the **Software Reclamation - Dashboard Settings** section), enter the percentage of the total number of reclamations that need to be reached in the following categories before that category's card changes color in the **Software Reclamation** dashboard:

   - **Successful reclamations**—Displays in green if threshold is met; otherwise displays in yellow.

   - **Pending reclamations**—Displays in yellow if threshold is met; otherwise displays in gray.

   - **Failed reclamations**—Displays in red if threshold is met; otherwise displays in gray.

3. Under **Provide adjustable variables for Software Requests**, enter the number of **Hours per request** and **Cost per hour** of a typical software request.

4. Under **Provide adjustable variables for OSD Requests**, enter the number of **Hours per request** and **Cost per hour** of a typical OSD request.

5. In the **No. of days the requests are waiting for approval**, enter the threshold number of days that a request needs to be waiting before it is listed in the **Deployment waiting approval for more than n days** card on the **SLA Dashboard**.

6. Under **Threshold settings**, enter the percentage of the total number of requests that need to be in one of the following categories before that category's card would be displayed in red (instead of gray) in the **SLA Dashboard** report:

    ● Failed deployments

    ● Rejected requests

    ● Approval pending

7. Click **Save**.

Assigning Permissions to View Dashboards

For a user to be able to view the dashboard reports, you first need to give them permission to view the **Dashboard** tab in the navigation bar, and then you need to give them permission to view each of the three report subtabs.

● Assigning Permission to View the Dashboard Tab

● Assigning Permission to View the Report Subtabs on the Dashboard Tab

Assigning Permission to View the Dashboard Tab

To assign a user permission to view the Dashboard tab in the navigation bar, perform the following steps.

Task   ***To assign permission to view the Dashboard tab:***

1. On the **Admin** tab, select **Site Management > Catalog Security**. The **Catalog Security** view opens.
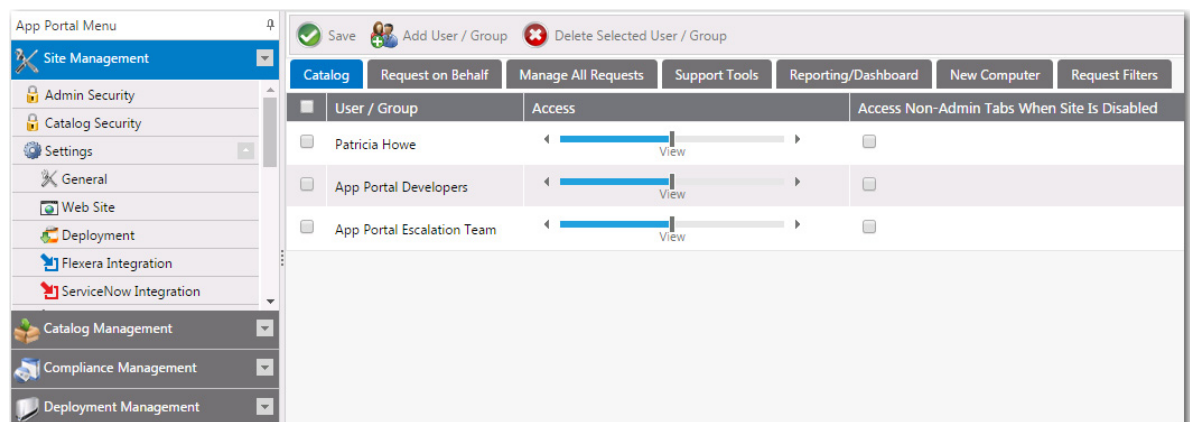
2. Click Add User / Group.

3. Use the **Search** functionality to locate the user that you want to give dashboard permission to, or locate a group that the user belongs to.

4. From the **Reporting/Dashboard** list, select **View**.

5. Click **Assign Rights**.

Assigning Permission to View the Report Subtabs on the Dashboard Tab

To assign a user permission to view the **Software Deployment ROI**, **OS Deployment ROI**, and **SLA Dashboard** subtabs on the **Dashboard** tab, perform the following steps.

Task   *To assign permission to view the report subtabs on the Dashboard tab:*

1. On the **Admin** tab, select **Report Management > Dashboard Categories**. The **Dashboard Categories** view opens.
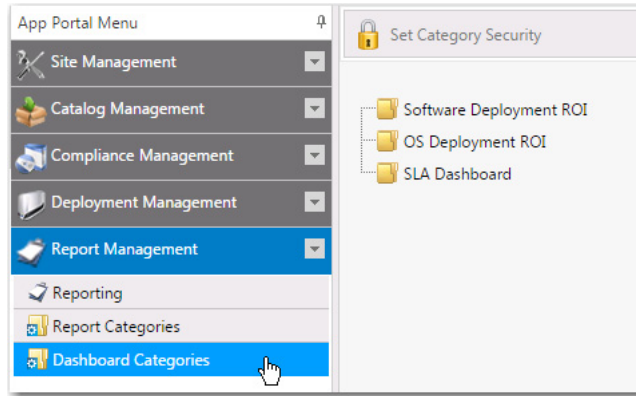
2. Select the name of the report that you want to assign permission to and then click **Set Catalog Security**. The **Category Security** dialog box opens.
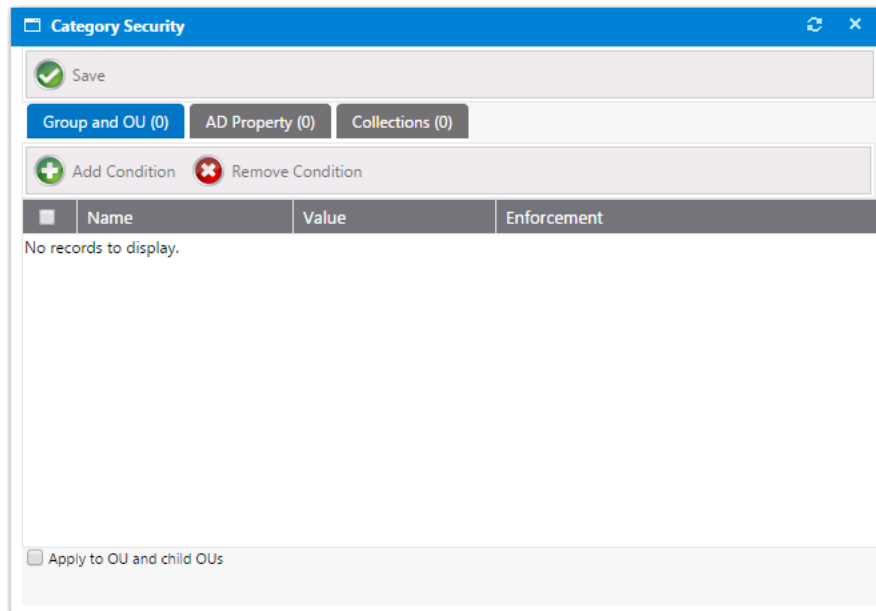
3. Select the **Group and OU**, **AD Property**, or **Collections** tab.

4. Click **Add Condition**. The **Add Condition** dialog box opens.

5. Use the search box to search for the group, OU, AD, or collection that you want to assign permission to, and select the checkbox next to the item in the search results list.
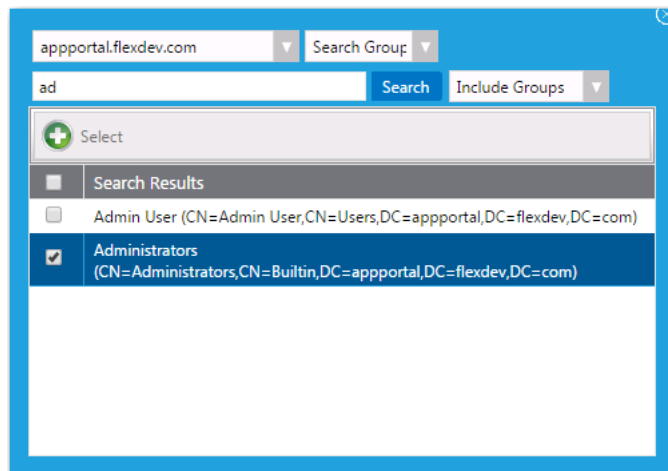
6. Click the **Select** button to add the condition. After you add a condition to any of the three subtabs (**Group and OU**, **AD Property**, or **Collections**), that condition is listed on that subtab.

7. After the condition is added, specify the enforcement option you want to take effect by making a selection in the **Enforcement** column: **Include** or **Exclude**.
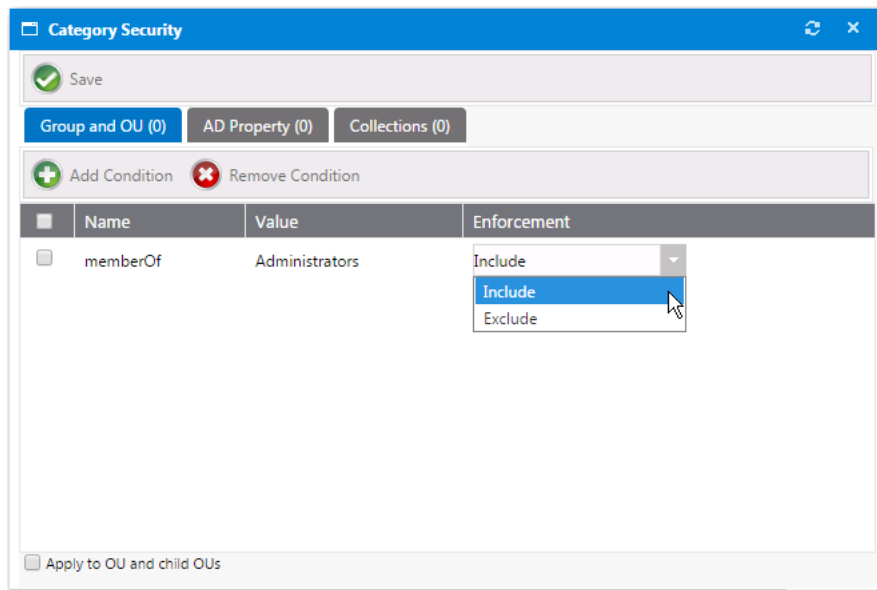
8. Click **Save**.

9. Repeat for the other report subtabs in on the **Dashboard** tab.

Managing Reports

Reporting allows for the display of App Portal data in a read-only, searchable, and exportable view. You can create new reports, edit existing reports, and create and edit report categories.

App Portal can display the following types of reports:

- **Standard reports**—Starting with App Portal 7.5, App Portal includes support for reports generated using Microsoft SQL Reporting Services. Over 40 standard reports are shipped with App Portal, and you have the ability to create your own custom reports, as described in Creating a New Standard RDLC-Based Report.

- **Legacy reports**—Legacy reports are derived from SQL views and stored procedures. These report views and procedures begin with v_Rep for report views and sp_Rep for stored procedures. Prior to App Portal 7.5, this was the only type of report that was available in App Portal.

This section explains how to view reports, and how to create new reports.

- Viewing Reports

- Creating Report Categories

- Creating a New Standard RDLC-Based Report

- Creating a New Legacy Report

- Adding a Standard Report to the Reporting Tab

- Removing a Report from the Reporting Tab

Note • *You can create and secure categories in the* **Report Categories** *node under* **Report Management > Report Categories**. *Each category can have its own security provision for it so that the reports within that category can only be viewed by those users with access. See*

Viewing Reports

All of the reports that are listed on the **Site Management >Reporting** view of the **Admin** tab will be available to view on the **Reporting** tab. To view an App Portal report, perform the following steps.

Task   *To view a report:*

1. Open the **Reporting** tab of App Portal. The Reporting view opens and available reports are listed in the left pane, grouped into categories.

2. Select the report that you want to view. The report opens in the right pane.
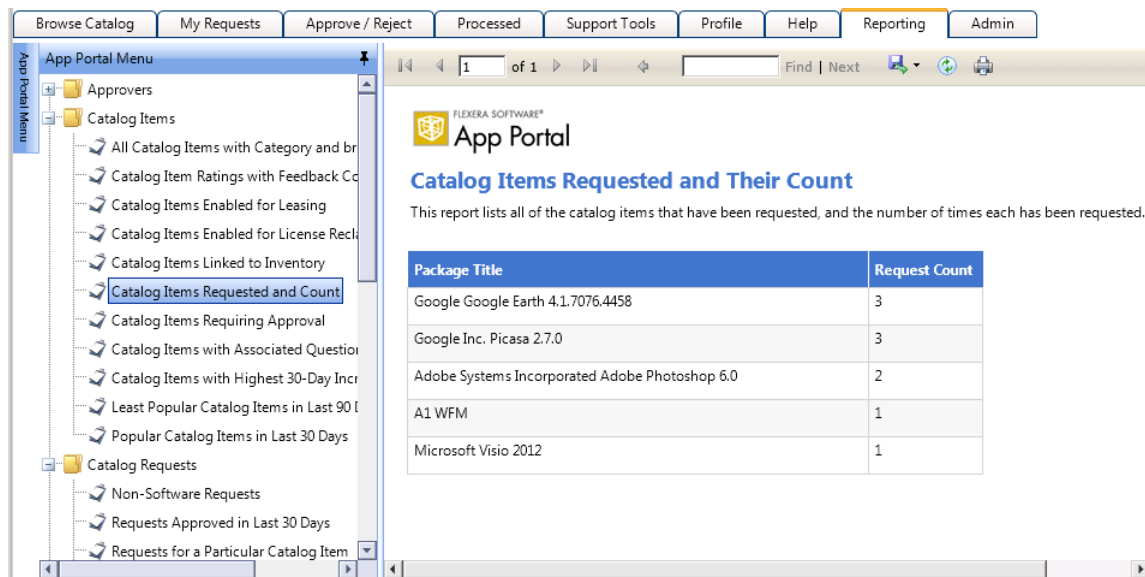
Creating Report Categories

Reports are organized using categories. Categories, which are listed in the left pane of the **Reporting** tab, are visible to end users when they are viewing reports. Each category can have its own security provision for it so that the reports within that category can only be viewed by those users with access.
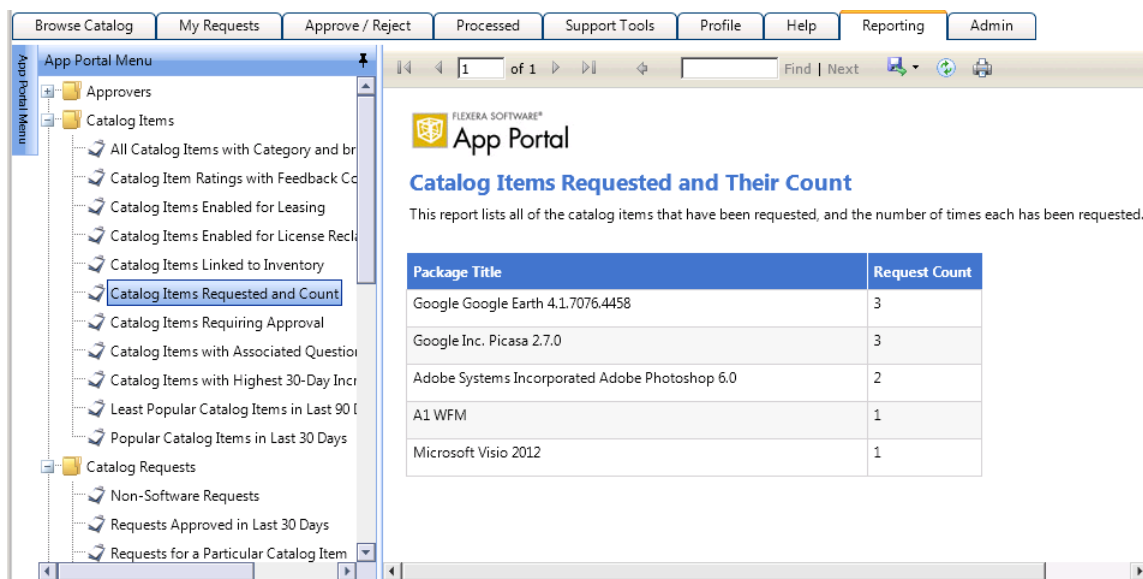
Figure 3-51: Report Categories on the Reporting Tab

To create a report category, perform the following steps.

Task   ***To create a catalog category:***

1. Open the **Admin** tab.

2. Under **Report Management**, select **Report Categories**. Existing categories are listed in the right pane.
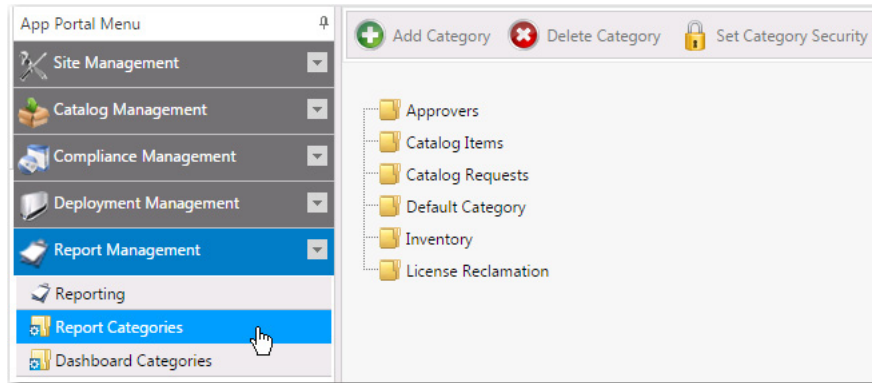
3. In the category tree, select the category that you would like to add a subcategory to (or to create a category at the root level, do not select a category), and then click **Add Category**. You are prompted to enter a **New Category Name**.
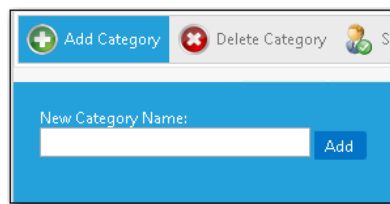
4. Enter a name to identify the category and click **Add**. The new category is now listed in the tree.

5. Select the new category in the list and click **Set Category Security**. The **Category Security** dialog box opens.
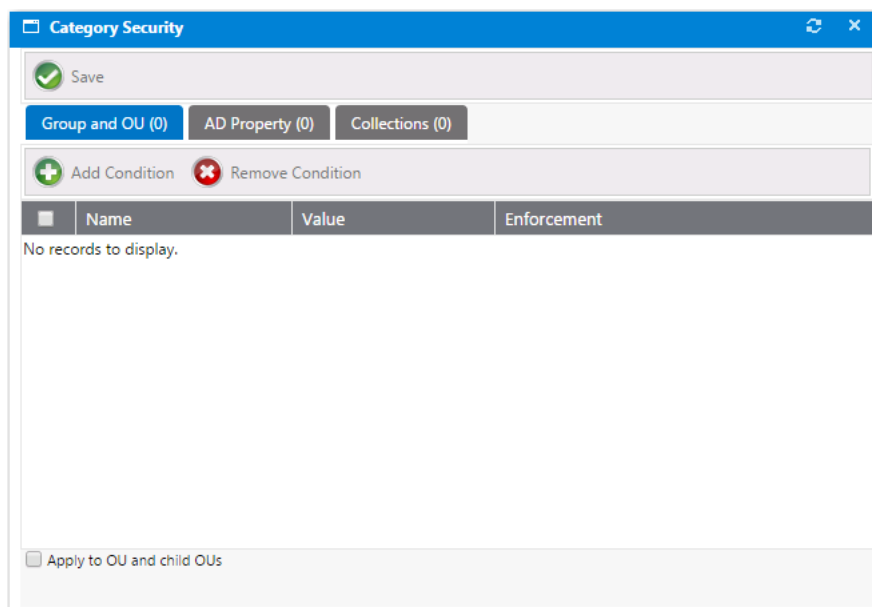
6. Use the **Add Condition** button to open the Add Condition Dialog Box and add conditions to control access to the reports in this category.

7. Click **Save**.

Creating a New Standard RDLC-Based Report

You can create your own custom reports that are generated using Microsoft SQL Reporting Services.

To create a custom report, you need to first create an `.rdlc` file (using either Microsoft SQL Server Business Intelligence Development Studio or Visual Studio 2010), copy that file to the App Portal installation directory, and then edit the App Portal Report Definition file (`AdminStudio.Reports.xml`) to add a reference to your custom report.

Task   ***To create a custom Microsoft SQL Reporting Services report:***

1. Create an `.rdlc` file.

2. Copy that file to the following directory on the machine where App Portal is installed:

   `[App Portal Installation Directory]\Web\ReportDefinition\RDLC`

3. Open the `AdminStudio.Reports.xml` file, found in the following location, in a text editor:

   `[App Portal Installation Directory]\Web\ReportDefinition`

4. In the `AdminStudio.Reports.xml` file, copy an existing `<Report>` element under the `<Reports>` element. Below is the `<Report>` element for the **Catalog Items Requested and Their Count** report:

```
<Report Name="Catalog Items Requested and Count" RdlcPathType="Relative"
    RdlcPath="RDLC\CatalogItemsRequestedAndCount.rdlc" >
    <DataSources>
        <DataSource DataSourceName="CatalogItemsRequestedAndCount" SqlCommandType="SQL"
            SqlCommandString="Select wp.PackageTitle,Count(wp.PackageTitle) as [RequestCount]
            from WD_PackageRequests as pr INNER JOIN Wd_webpackages  as wp
            on pr.PackageID_FK = wp.PackageID Group by wp.PackageTitle order by
            RequestCount desc">
                <SqlParameters>
                    <SqlParameter/>
                </SqlParameters>
        </DataSource>
    </DataSources>
</Report>
```

5. Replace the highlighted text above with the correct information for your new custom report: the data source and the parameters that are required for any drill through reports that you include.

   In this XML file, note the following parameter values:

Parameter	Values
`RdlcPathType`	Valid values are `Relative` or `Absolute`.
`SqlCommandType`	Valid values are `StoredProcedure` or `SQL`.
`SqlCommandString`	Enter the stored procedure name or an SQL string.

6.   To view your custom report in App Portal, you need to add the report to the **Reporting** tab, as described in Adding a Standard Report to the Reporting Tab.

Creating a New Legacy Report

Note • This feature is available for System Center Configuration Manager deployment technology only.

You can create a new legacy report that derives data from an available stored SQL view or procedure. You can link columns to external reports from System Center Configuration Manager by passing the correct query string values.

To create a new legacy report, perform the following steps.

Task   ***To create a new report:***

1.   On the **Report Management > Reporting** view, click **New Legacy Report**. The **New Legacy Report** dialog box opens.

2.   Enter a report name in the **Report Name** field.

3.   Under **Report Category**, select a category to associate the report to.

*Note • You can create and secure categories in the **Report Categories** node under **Site Management > Categories**. Each category can have its own security provision for it so that the reports within that category can only be viewed by those users with access.*

4.   From the **Report View** list, select the SQL view or procedure to derive the report data from and click **Save**. The report is saved and additional fields are displayed.

In this image, the v_rep_RequestCount report has a column, Machine, that is linked to an System Center Configuration Manager report with a report ID of 10. Report ID 10 requires a variable called Machine which contains a machine name. When the user selects a machine from the machine column they will be directed to System Center Configuration Manager report ID 10.

5. Click **Save**.

Adding a Standard Report to the Reporting Tab

App Portal is shipped with over 40 standard RDLC-based reports (reports that are generated using Microsoft SQL Reporting Services). By default, all of these reports are listed on the **Report Management > Reporting** view, which makes them available to view on the **Reporting** tab.

However, if you have removed a standard report from this list (as described in Removing a Report from the Reporting Tab) or have created a new standard report that you want to make available on the **Reporting** tab (as described in Creating a New Standard RDLC-Based Report), you will need to add the report to the **Report Management > Reporting** view.

Task   ***To add a standard report to the Reporting tab:***

1. Open the **Report Management > Reporting** view.

2. Click **New Standard Report**. If you have previously deleted a standard report or have created a new standard report (as described in Creating a New Standard RDLC-Based Report), there should be a report listed in the **Report** list.

3. Select a report from the **Report** list.

4. Under **Report Category**, select a category to associate the report with.

5. Click **Save**. The report is now listed on the **Reporting** view and can be viewed on the **Reporting** tab.

Removing a Report from the Reporting Tab

All of the reports listed on the **Report Management > Reporting** view are available to view on the **Reporting** tab to users who have permission to view them.

To delete a report from the **Reporting** tab, perform the following steps:

Task   ***To remove a report from the Reporting tab:***

1. Open the **Report Management > Reporting** view.

2. Double-click the report that you want to remove. The **Report Properties** dialog box opens.

3. Click **Delete**. You are prompted to confirm the deletion.

4. Click **OK**. The report is deleted from the list on the **Reporting** view and is no longer available on the **Reporting** tab.

Important • When you remove a standard report from the **Reporting** *view, you are not deleting the actual* .RDLC *file; you are just removing it from the list. To re-add the report, click the* **New Standard Report** *button and select the report from the* **Report** *list.*

Managing Your App Portal License File

In order for you to access the App Portal website, you need to upload a license file to App Portal. When your license file expires, you will need to upload an updated license file. License files can be downloaded from the Flexera Software Product and License Center.

You upload license files on the **General** tab of the **Site Management > Settings** view on the **Admin** tab.

- Obtaining a New or Updated App Portal License File

- Uploading a License File Immediately After Installation

- Uploading a New License File

- Uploading an New License File After Expiration

Obtaining a New or Updated App Portal License File

To obtain your App Portal license file, perform the following steps:

Task   ***Obtaining an App Portal license file:***

1. Log on to the **Flexera Software Product and License Center**:

   `https://flexerasoftware.flexnetoperations.com`

2. In the left navigation, under **Entitlements**, click **Product List**.

   - If you have access to multiple products, the **Product List** page opens and lists all of the product lines to which your account is entitled. Click the **App Portal** link to proceed to the **Product Information** page.

- If you do not have access to multiple products, clicking the **Product List** link opens the **Product Information** page directly.

3. In the **Product and File Downloads** column, click the App Portal link for the version that you want to download a license file for. The **Product Download** page opens.

4. Click the download button next to the license file.

Uploading a License File Immediately After Installation

After installation, the first time that you open App Portal, you are prompted to upload a license file. Until you upload the license file, you will be unable to open the App Portal website. For more information, see Uploading Your App Portal / App Broker License File.

Uploading a New License File

When your license file is nearing its expiration date, you will need to upload an new license file.

Task   ***To upload an updated license file:***

1. On the **Admin** tab, select **Settings > General** under **Site Management**. The **General** view opens.

2. Click **Add/Update license key** (which is located to the right of the registered user's name). You are then prompted to browse to the license file.

3. Click **Browse**, select the updated license file, and click **Upload License**.

Uploading an New License File After Expiration

When your license file expires, you will be warned and will be prompted to upload an new license file.

Task   ***To upload a new license file after expiration:***

1. When you launch App Portal, the following screen will appear informing you that your license has expired:
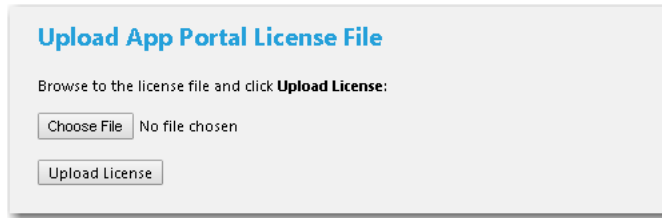
2. Click **Add/Update license file**. You are then prompted to upload a new license file.

3. Click **Choose File** and browse to your new license file.

4. After you have selected the new license file, click **Upload License**.

Enabling App Portal Site for Your Enterprise
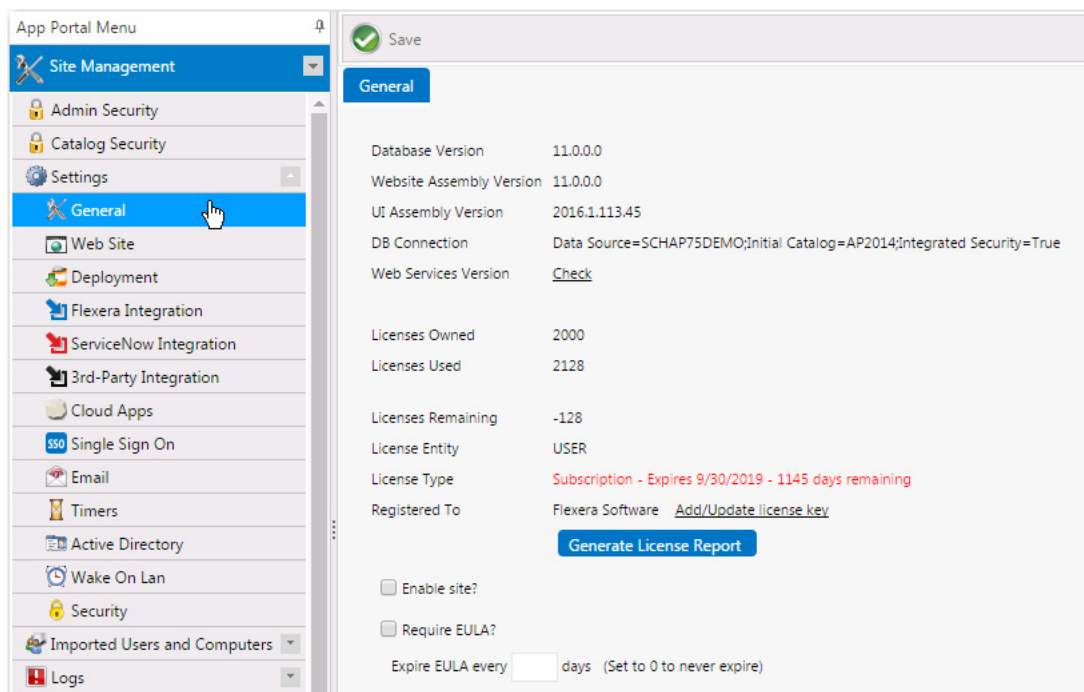
When the App Portal site is enabled, all directory services users at your enterprise are able to access the site and perform activities such as using the **Browse Catalog** and **My Requests** tabs to submit a request and the **Approve / Reject** tab to approve or reject a request.

However, while setting up App Portal's security settings, creating the default templates, and adding catalog items, you would not want these users to be able to access the site (unless they have explicitly been given permission). Therefore, there is "switch" setting which you need to select before App Portal is available to all of the users and groups in your enterprise.

Task   ***To enable App Portal for your enterprise:***

1. Open the **Admin** tab.

2. Under **Site Management**, select **Settings**. The **General** tab of the **Settings View** opens.

3. Select the **Enable site?** option.

4. Click **Save**. App Portal will now be visible in all users and groups in your enterprise.

📄

Note • *A user needs to have been assigned specific permissions in order to access the views on the* **Admin** *tab, as described in* Managing Administration Permissions.

Entering Flexera Integration Connection Settings

If you connect App Portal to the Flexera Service Gateway, App Portal will be able to communicate with FlexNet Manager Suite and manage application licenses. You can also integrate App Portal with Microsoft System Center Orchestrator, a workflow management solution for the data center that lets you automate the creation, monitoring, and deployment of resources in your environment.

- Connecting to the Flexera Service Gateway

- Entering FlexNet Manager Suite Settings

- Connecting to Microsoft System Center Orchestrator

Connecting to the Flexera Service Gateway

If you have also purchased FlexNet Manager Suite, you can use App Portal to manage application licenses.

App Portal communicates with FlexNet Manager Suite, as well as AdminStudio and Workflow Manager, via the Flexera Service Gateway component. To connect App Portal to the Flexera Service Gateway, perform the following steps.

📋

Task   **To connect to the Flexera Service Gateway:**

1. Select **Site Management > Settings** > **Flexera Integration**. The **Flexera Integration** view opens.

2. In the **Flexera Service Gateway Server Name** field, enter the name of your Flexera Service Gateway server.

3. Click **Save**.

📄

Note • *To integrate with FlexNet Manager Suite, you may also have to enter appropriate credentials, as described in* Entering FlexNet Manager Suite Settings.

📄

Note • *For more information on using the FlexNet Manager Suite to manage application licenses, see* Setting FlexNet Manager Suite Licensing Options.

Entering FlexNet Manager Suite Settings

App Portal can integrate with both the On Premises and Cloud versions of FlexNet Manager Suite. To connect to FlexNet Manager Suite, perform the following steps.

Note • To integrate with FlexNet Manager Suite, you also have to connect to the Flexera Service Gateway, as described in Connecting to the Flexera Service Gateway.

Task   **To enter FlexNet Manager Suite settings:**

1.   Select **Site Management > Settings > Flexera Integration**. The **Flexera Integration** view opens.

2.   If using a multi-tenant instance of FlexNet Manager Suite, enter the **FlexNet Manager Suite UID**, a value that uniquely identifies a tenant in a multi-tenant instance of FlexNet Manager Suite.

3.   Do one of the following:

   • **To connect to FlexNet Manager Suite Cloud,** enter your access token in the **FlexNet Manager Suite Cloud Access Token** field.

   • **To connect to FlexNet Manager Suite On Premises**, enter a **Username** (in `domain\username` format) and **Password**. However, if your App Portal system account has access to FlexNet Manager Suite, this step may not be necessary.

4.   In order to use the **My Apps** feature, the App Portal system account needs to have read access to the FlexNet Manager Suite database. If you want to use the My Apps feature, enter the **Database Server Name** and **Database Name** of the FlexNet Manager Suite database.

   Important • You also need to use Microsoft SQL Server Management Studio to give the App Portal system account read access to this database.

5.   Click **Save**.

Connecting to Microsoft System Center Orchestrator

App Portal can integrate with the Microsoft System Center Orchestrator workflow tool. Orchestrator is a workflow management solution for the data center. Orchestrator lets you automate the creation, monitoring, and deployment of resources in your environment.

If App Portal is connected to System Center Orchestrator, App Portal will have the ability to trigger a workflow at various points during an App Portal request life cycle.

Orchestrator workflows can execute complex, long-running tasks such as creating AD User account, building virtual machines and performing complex logic such as loops and branches.

Task   **To connect to Microsoft System Center Orchestrator:**

1.   Select **Site Management > Settings > 3rd-Party Integration**. The **3rd-Party Integration** view opens.

2.   In the **Orchestrator Service URL** field, enter the URL of your System Center Orchestrator site.

Assigning System Center Orchestrator Runbooks Permissions

In order to add System Center Orchestrator actions to a catalog item on the **Actions** tab of the **Catalog Item Properties** dialog box, you must have at least **Read** permission on Runbooks in System Center Orchestrator.

Runbook access permissions are set using the System Center Orchestrator Runbook Designer. By default, only users in the Orchestrator user group have full access to Runbooks. You can give access to additional users to run, start, stop, view, and change Runbooks at either the folder level or the individual Runbook level.

Task   ***To view or modify the permissions of a runbook:***

1. Open the System Center Orchestrator Runbook Designer.

2. In the **Connections** pane, select the **Runbooks** folder. The **Runbook Designer Design** workspace opens.

3. Right-click the **Runbooks** folder (or an individual Runbook) and select **Permissions**. The **Permissions for Runbooks** dialog box opens.
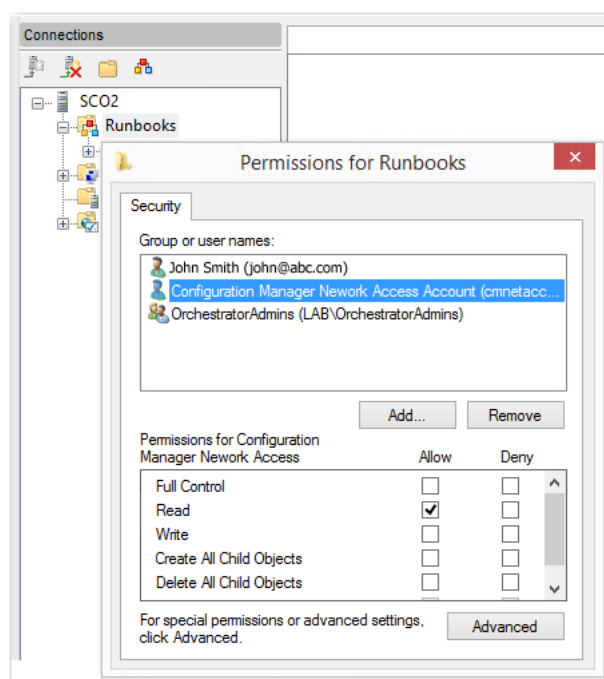
4. To give another user or security group access to Runbooks, click the **Add** button, and select the user or security group from the local computer or from the domain.

   - **Read permission**—If the user or security group should be able to view and run Runbooks, select the **Allow** check box next to **Read**.

   - **Write permission**—If the user or security group should be able to change Runbooks, select the **Allow** check box next to **Write**.

   - **Full control**—If the user or security group should be able to change permissions for Runbooks, select the **Allow** check box next to **Full Control**.

5. To close the **Permissions for Runbook** dialog box and save any changes, click **OK**.

Viewing Error, Email, Request Lifecycle, and Debug Logs

App Portal offers four types of log files that will help you troubleshoot App Portal issues.

- **Email log**—The **Email Log** view lists all emails that were sent to users, both those notifying the user of success and of failure. You can view and sort these email messages on this view. For more information, see Email Log.

- **Error log**—The **Error Log** view lists all errors generated by the system. You can view and sort these error messages on this view. For more information, see Error Log.

- **Request life cycle logging**—If you select the **Enable request life cycle logging** option on the **General** tab of the **Site Management > Settings > Web Site** view, App Portal will create individual log files for each App Portal request that list all events that have occurred for that request. These log files will be stored in the following location and will be named using the request number:

  `C:\Program Files (x86)\Flexera Software\App Portal\Logs\RequestLog`

  Here is an example of one of these log files:
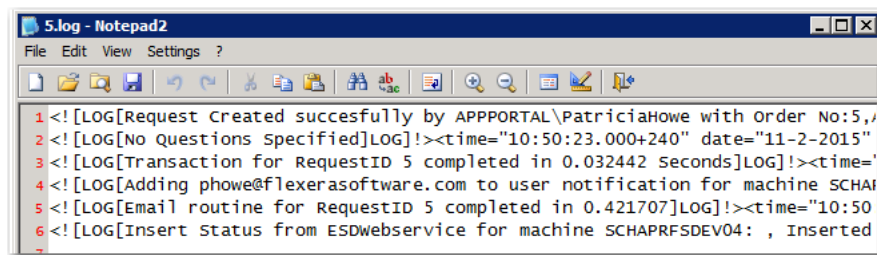
  A request's lifecycle log file may prove helpful if you are encountering an issue with an individual request. This feature should only be turned on when performing troubleshooting.

- **Debug log**—When you encounter a particularly complicated issue, one which could be caused by environmental issues and which cannot be easily reproduced on other systems, you may want to turn on App Portal's debug logging, which is an exhaustive log of all actions that occur while the log is turned on. For more information, see Creating and Viewing a Debug Log.

Creating and Viewing a Debug Log

When you encounter a particularly complicated issue, one which could be caused by environmental issues and which cannot be easily reproduced on other systems, you may want to turn on App Portal's debug logging, which can be viewed on the **Debug Log** view. Rather than just a log of error messages, a debug log is an exhaustive log of all events—such as actions, methods, stack trace, execution path—and provides a very low level detail of the entire request life cycle of the App Portal web site.

When you turn on debug logging, it is only in effect for the current App Portal user. In other words, if an administrator on Machine A enables debug logging, then App Portal will be logging only requests coming from Machine A.

Important • Because debug logging slows down the system considerably, it should only be turned on when performing troubleshooting, preferably before App Portal is in a production environment.

To turn on debug logging, perform the following steps.

Task   ***To create a debug log:***

1. On the **Admin** tab, open the **Site Management > Debug Log** view.

2. Click **Start Log**. A dialog box prompts you to enter a title for this log and a description of what you are testing.

3. Enter a title and description, and then click **Start**. The message at the top of the screen changes to `Debug logging is currently turned ON`.

4. Perform the App Portal steps that you are testing (such as checking out a particular catalog item, or viewing a specific App Portal page). Continue performing steps until you reproduce your issue.

   Note • *App Portal performance speed will be slow due to the extensive logging.*

5. Return to the **Debug Log** view. You will see that individual methods are listed.

6. Click **Select** to view details of a method.

7. Click **Back to Debug Log**.

8. To stop logging, click **Stop Log**. You are prompted to confirm that you want to save the session.
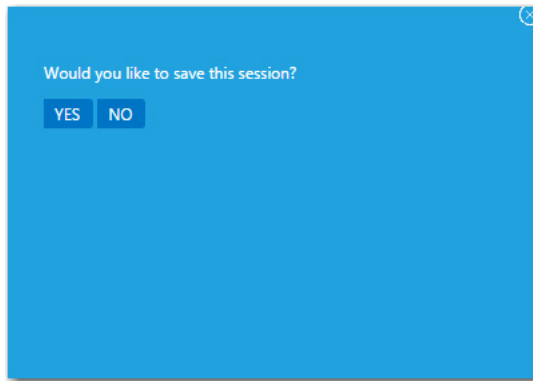
9. Click **Yes**. Logging is turned off and all of the methods that were logged are now listed.

10. To save the log files in a ZIP file, so that it could perhaps be sent to product support personnel, click **Save Logs**. You are prompted to confirm the creation of a ZIP file which will contain a set of `.csv` log files.
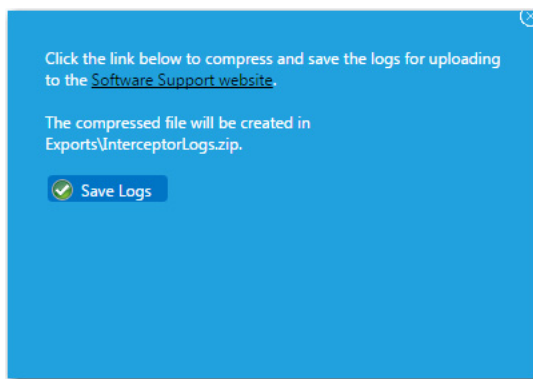
11. Click **Save Logs**. The ZIP file will be saved, by default, in your `Downloads` directory.

12. To import an individual `.csv` log file so that you can view it in the **Debug Log** view, click **Import Logs**. You are prompted to upload the file.
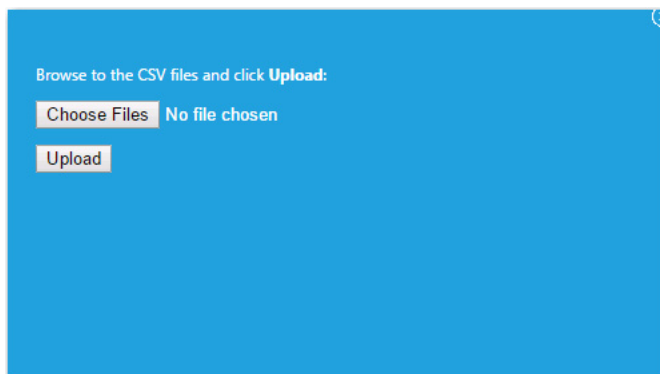
Securing HTTP Cookies Created by App Portal

If your App Portal website is running under HTTPS binding (`https://` is visible in the URL), then you need to make a configuration change so that HTTP cookies will only be transmitted under HTTPS communication.

Task   ***To secure HTTP cookies created by App Portal:***

1. Locate the following file on your App Portal Website server:

    `[App Portal Installation Location]\web\web.config`

2. Open the `web.config` file (as an Administrator) in a text editor.

3. In the `<httpCookies>` element, change the value of the `requireSSL` parameter from `false` to `true`:

    `<httpCookies httpOnlyCookies="true" requireSSL="true" />`

> ***Important •*** *If your organization is using HTTP binding (`http://` is visible in the URL), then the* ***requireSSL*** *parameter must remain set to* ***false****.*

Site Management Reference

Information about the App Portal functionality available on the **Site Management** view of the **Admin** tab is organized in the following sections:

Table 3-13 • Site Management Views

View	Description
Admin Security	Use to add the groups and users to Admin roles for specific areas of App Portal manageability. This secures the site settings to those listed groups and users.
Catalog Security	Use to enable permissions to see and manage the App Portal catalog. You can add the necessary groups and users to Admin roles for specific areas of Catalog manageability. This secures the site catalogs to the listed groups and users.
Settings	Use to configure App Portal settings, including the App Portal website, deployment technology, Active Directory, and email settings.
Imported Users and Computers	View a list of the users, computers, and user-computer relationships that have been imported into App Portal.

Table 3-13 • Site Management Views (cont.)

View	Description
Logs	View a list of various App Portal log files: • **Error Log**—View a list of all errors generated by the system. • **Email Log**—View a list of all emails that were sent to users, both those notifying the user of success and of failure. • **Debug Log**—Use to enable and view detailed log files which can be used to troubleshoot App Portal issues that are encountered.
Active Directory	Use to add properties, which determine the attributes that you want to utilize in App Portal approval, deployment, and provisioning processes. You can also use virtual properties to group similar properties together as a single logical name.
ITSM Integration	Use to configure out-of-the-box integration, via web services, with both ServiceNow and BMC Remedy IT Service Management (ITSM) systems. You can configure both incident and request management. You can also use App Portal's built-in reusable framework to integrate with other ITSM systems.
Cloud Integration	Use to configure App Portal integration with cloud applications: Box, Salesforce, and Office 365.
Categories	Use to organize the following objects into the following types of categories: Catalog, Command, Inventory, Note, Purchase, and Report.
Commands and Actions	Use to add script, web service, and request commands. These commands can be executed against a selected machine from the **Support Tools** tab in the software store or as part of a request at one or more stages during the request life cycle.
Communication	Manage email notifications (as well as other App Portal site content), license reclamation reasons, approve/reject reasons, languages, language text, and announcements.

Admin Security

On the **Admin Security** view, you add the necessary groups and users to admin roles for specific areas of manageability. This secures the site settings to the listed groups and users.
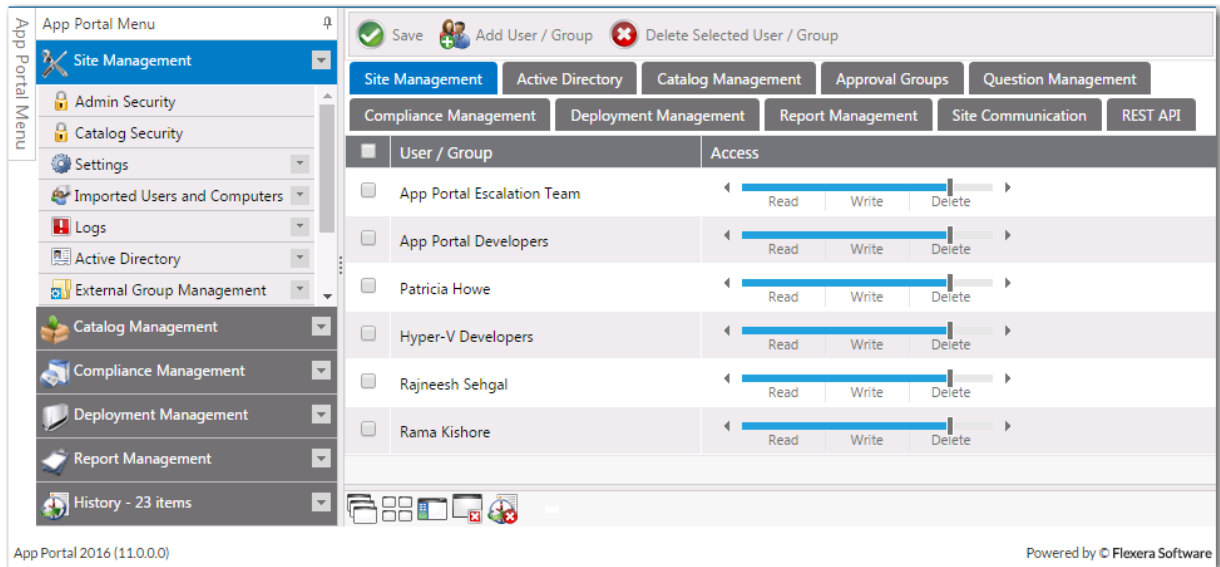
Figure 3-52: Admin Security View

On each of the tabs of the **Admin Security** view, you can view and edit the security settings (**Read**, **Write**, **Delete**) for *existing* users and groups for that particular role. Each role's permissions are described in Admin Security Roles.

However, you assign *initial* permissions to a user or group for *all roles* on the Admin Security Add User/Group Dialog Box that opens when you click **Add User/Group** on the **Admin Security View**.

Admin Security Add User/Group Dialog Box

On the **Admin Security Add User/Group** dialog box, which opens when you click **Add User/Group** on the **Admin Security** view, you assign *initial* permissions to a user or group for all admin roles.
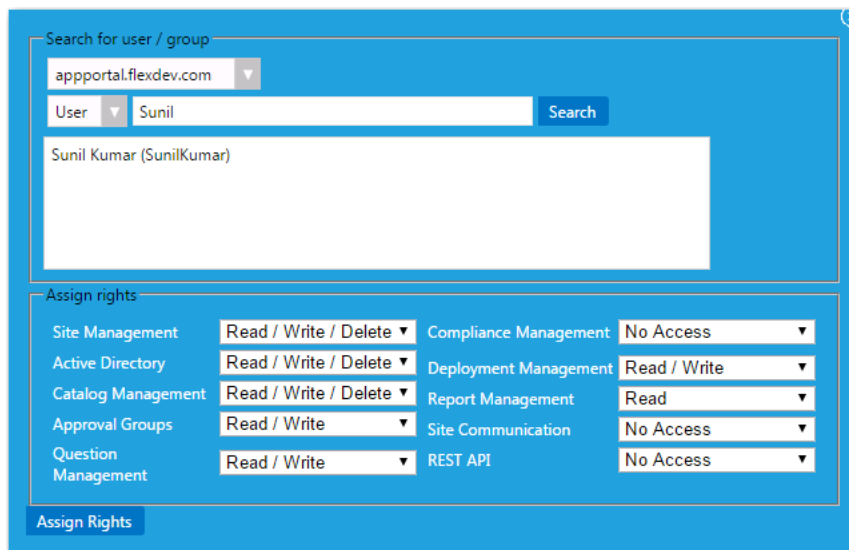
Figure 3-53: Admin Security Add User/Group Dialog Box

First you use the search fields to locate the user or group that you want to add, and then select the appropriate permissions from the **Assign rights** fields for each listed role, and then click **Assign Rights**.

Under **Assign rights**, the following roles are listed:

Table 3-14 • Admin Security Roles

Role	Permission
Site Management	Can view, create / modify, or delete configuration items under the following subnodes of **Site Management**: • Site Management > Admin Security • Site Management > Catalog Security • Site Management > Settings (all subnodes except Active Directory) • Site Management > Imported Users and Computers • Site Management > Logs • Site Management > ITSM & Cloud Integration • Site Management > Categories • Site Management > Commands and Actions
Active Directory	Can view, create / modify, or delete configuration items under the following nodes: • Site Management > Active Directory • Site Management > Settings > Active Directory
Site Communication	Can view, create / modify, or delete items under the following nodes: • Site Management > Communication
Catalog Management	Can view, create / modify, or delete items under the following nodes: • Catalog Management > Create New Catalog Item • Catalog Management > Current Catalog Items • Catalog Management > Catalog • Catalog Management > Catalog Categories • Catalog Management > Expressions • Catalog Management > Workflows • Catalog Management > Workflow Status
Approval Groups	Can view, create / modify, or delete items under the following nodes: • Catalog Management > Approval Groups
Question Management	Can view, create / modify, or delete items under the following nodes: • Catalog Management > Questions

Table 3-14 • Admin Security Roles (cont.)

Role	Permission
Compliance Management	Can view, create / modify, or delete items under the following nodes: • Compliance Management
Deployment Management	Can view, create / modify, or delete items under the following nodes: • Deployment Management
Report Management	Can view, create / modify, or delete items under the following nodes: • Report Management
Rest API	Enables access to all REST API endpoints.

Note • *Note that permissions are the "most restrictive model". For example, if a user is in two groups where one is granted Read permission and the other granted Write permission, the permissions will be Read; they are not cumulative.*

Catalog Security

When configuring App Portal, you will need to specify which users and groups can view and modify the App Portal catalog. This secures the App Portal site catalogs to the listed groups and users.

You configure catalog security on the **Catalog Security View**, which is opened by selecting **Catalog Security** under **Site Management** on the **Admin** tab.
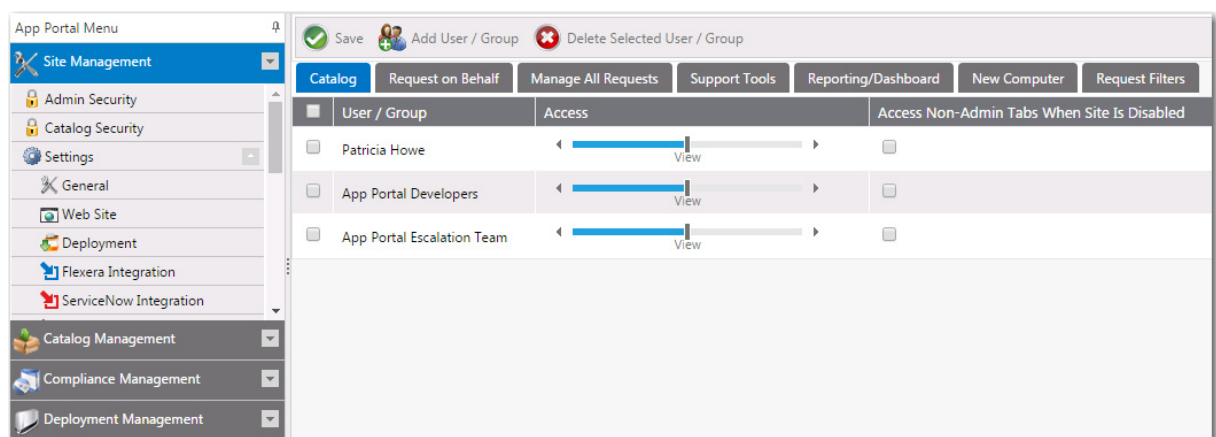
Figure 3-54: Catalog Security View

On each of the tabs of the **Catalog Security View**, you can view and edit the security settings for *existing* users and groups for that particular role.

However, you assign *initial* permissions to a user or group for all roles on the **Catalog Security Add User/Group** dialog box that opens when you click **Add User/Group** on the **Catalog Security View**.

To enable a user to view the non-administrative tabs of the App Portal / App Broker interface even when the end-user facing site is disabled (such as when using App Broker), select the **Access Non Admin Tabs When Site Is Disabled** option. For more information, see Providing Access to Non-Admin Tabs When App Portal Site is Disabled.

Catalog Security Add User/Group Dialog Box

On the **Catalog Security Add User/Group** dialog box, which opens when you click **Add User/Group** on the **Catalog Security** view, you assign *initial* permissions to a user or group for all catalog roles.

Figure 3-55: Catalog Security Add User/Group Dialog Box

First you use the search fields to locate the user or group that you want to add, then select the appropriate permissions from the **Assign rights** fields for each listed role, and then click **Assign Rights**.

Under **Assign rights**, the following roles are listed:

Table 3-15 • Catalog Security Roles

Role	Permission
Browse Catalog	Allows users to see the catalog hierarchy. If no group is defined, it is visible for all. Add groups to restrict access.
Request on Behalf	Determines whether members can perform "request on behalf" for catalog items enabled for request on behalf. Recommended members: Help Desk / Support Staff.
Manage All Requests	Can View, Create / Modify, or Delete request items under My Requests tab. Grants visibility to the "Show all requests" check box so users can see not only their own requests but all others as well. Recommended members: Help Desk / Support Staff.

Table 3-15 • Catalog Security Roles (cont.)

Role	Permission
Support Tools	Grants access to the **Support Tools** tab. Recommended members: Help Desk / Support Staff.
Reporting	Grants access to the "Reporting" tab. Recommended members: Help Desk / Support Staff / Business Analysts.
New Computer Deployment	Grants access to the "New Computer" button during a request on behalf action. Recommended members: PC Builders.
Request Filters	Not implemented.

Note • Permissions are the "most restrictive model". For example, if a user is in two groups where one is granted View permission and the other granted Modify permission, the permissions will be View; they are not cumulative.

Settings

You configure App Portal's website, deployment technology, Active Directory, Email, and other settings on the tabs of the **Settings** view, which is opened by selecting **Settings** under **Site Management** on the **Admin** tab.

Note • App Portal stores its configuration data in a database table WD_AppSettings *within the App Portal database.*

The **Settings** view includes the following sub-views:

- General

- Web Site

- Deployment

- Flexera Integration

- ServiceNow Integration

- 3rd-Party Integration

- Cloud Apps

- Single Sign On

- Email

- Timers

- Active Directory

- Wake On Lan

- Security

This section also includes the App Portal Logs Reference.

General

You configure general App Portal settings on the **Site Management > Settings > General** view,.

Figure 3-56: Settings > General View

The **General** view includes the following properties:

Table 3-16 • Settings >General View

Property	Description
Database Version	Version of the App Portal database.
Website Assembly Version	Version of App Portal as read from the database.
	📄
	*Note • The **Website Version** and **Website Assembly Version** should match.*
UI Assembly Version	Version of the UI controls used to build the App Portal user interface.
DB Connection	Server name and database name of the App Portal database.

Table 3-16 • Settings >General View

Property	Description
Web Services Version	Click to display details on the web services version of the App Portal website. The following information is listed: • **Site**—Name of the System Center Configuration Manager site where the web service is installed. • **Site Code**—The site code of the System Center Configuration Manager site where the web service is installed. • **Server**—The server name of the server where the web service is installed. • **Version**—The installed version of the App Portal web service on the listed server. 📄 *Note • Applies to System Center Configuration Manager deployment technology only.*
Licenses Owned	Number of App Portal licenses owned by your organization. 📄 *Note • If the customer exceeds the license count usage, App Portal will continue to function as normal, without any restriction in functionality. If the usage exceeds by 25%, App Portal displays the following warning in the header section, which is visible to both administrators and end users:* *Warning: Your license count for App Portal is exceeded by 25% or more.*
Licensed Used	Number of App Portal licenses used by your organization.
Licenses Remaining	Number of unused App Portal licenses at your organization.
License Entity	Identifies the type of license as either USER or DEVICE.
License Type	Identifies your App Portal license type. The expiration date and the number of days remaining are also listed.
Registered To	Lists the of your name of the person or company that your App Portal license is registered to. If you want to update your license file, or add a license file, click **Add/Update license key**. You will then be prompted to browse to the license file and upload it. For more information, see Managing Your App Portal License File. To generate a text file containing license information, click **Generate License Report**.
Enable site?	Enables/disables the App Portal storefront. When disabled, only administrators can access the site. Normal users will be redirected to the `SiteDisabled.htm` page. For more information, see Enabling App Portal Site for Your Enterprise.

Table 3-16 • Settings >General View

Property	Description
Require EULA?	Enables/disables the requirement for users to accept a usage agreement when first visiting the software store.
Expire EULA every x days	Determines whether or not the EULA expires, and how often it would expire. If this field is set to 0, the EULA will not expire.

Web Site

You specify website configuration, appearance, and behavior settings on the **Site Management > Settings > Web Site** view. The **Web Site** view includes the following tabs:

- General Tab

- Catalog Appearance Tab

- Catalog Behavior Tab

- Corporate Branding Tab

- Dashboard Tab

General Tab

On the **General** tab of the **Site Management > Settings > Web Site** view, you specify the configuration settings of the App Portal website.

Figure 3-57: Settings > Web Site View / General Tab

The **General** tab of the **Web Site** view includes the following properties:

Table 3-17 • Settings > Web Site View / General Tab

Property	Description
Licensed Collection	Use the **Select a Collection** list to identify a collection to set the scope of licensing. To use a collection to license, select a collection. ● **When a collection is selected**, only clients present in the collection will be able to access App Portal and have software delivered to them. ● **When a collection is not selected**, App Portal will count all active, non-obsolete, installed clients as licensed clients. For more information, see Difference Between "Licensed Collection and "Exclude Collection".
License View	When using collection licensing, it is subject to collection update intervals. If you cannot update the collection at a schedule necessary, you can define a view in the **App Portal** database that will identify the licensed clients. ● The view will not be subject to collection update schedules. ● The view requires a `ResourceID` and `MachineName` (computer name) column. Enter the name of the view in the **License View** field.

Table 3-17 • Settings > Web Site View / General Tab

Property	Description
Exclude collection	This is the inverse of the **Licensed Collection** field Any members of the selected collection will be banned from App Portal activity. **Difference Between "Licensed Collection and "Exclude Collection"** When you use the **Exclude collection** list to exclude a collection from App Portal activity, this is not the same as selecting that same collection from the **Licensed Collection** list along with selecting **Exclude Collection** because the license count is not altered. • **Licensed Collection**—The **Licensed Collection** list (and the **Include Collection** / **Exclude Collection** selection) is checked during each user visit to see if the user is included or excluded. The collection is also used to count the used licensed (**Include Collection**) or subtracted from the total count owned (**Exclude Collection**). • **Exclude collection**—The **Exclude collection** list is used to filter search results for a "request on behalf" scenario, making it possible to exclude servers from being requested against, on behalf of, but still license them to access the site from the console.
Request On Behalf DB View	To use a custom SQL view to display the eligible for Request On Behalf, specify the page name in this field, and then click **Test** to view the page.
Site Title	The name of the site title as it appears on the browser title bar.
Site DNS Address	Specify the DNS address of the site. • This address is used for links in emails back to the App Portal site. • By default the server name is used. • If you create an alias, enter the alias here as well.
Log File Path	Specify the path to the log files. If you wish to use a different drive or folder, change the value here. *Note • Be sure to include the trailing backslash.*
Logging Level	Specify the default logging level: • **Debug (testing only)**—Extensive, detailed logging including per visiting user. Use only for pre-production testing or if instructed by Flexera Software Support. • **Verbose**—Extensive logging including per visiting user. Use only for pre-production testing or if instructed by Flexera Software Support. • **Normal**—Basic logging of system activities. • **Errors only**—Only errors will be logged resulting in the least logging activity.

Table 3-17 • Settings > Web Site View / General Tab

Property	Description
Enable request life cycle logging	Select this option to create individual log files for each App Portal request that lists all events that have occurred for that application. These log files will be stored in the following location: `C:\Program Files (x86)\Flexera Software\App Portal\Logs\RequestLog` This feature should only be turned on when performing troubleshooting.
Log File Size KB	The data storage size for each log file created.
Primary computer discovery method	Specify how App Portal will determine the computer name. • **WebExtensions**—Discovery method supported in Chrome for Windows (version 29 and higher), Firefox for Windows (version 50 and higher), and Microsoft Edge (version 41 and higher) browsers using web extensions. Because Internet Explorer does not support web extensions, you will need to continue to use a computer discovery method in App Portal other than web extensions if you plan on using Internet Explorer. If **WebExtensions** is selected, an administrator must ensure that the respective WebExtensions installer has been deployed and installed on each user's machine. A link to the installer is provided in the description provided next to the **Primary computer discovery method** field. The installer is only available to administrators because it requires an install as administrator and also because an administrator will need to enter the correct App Portal web URL as part of the install process. For additional information, refer to Deploying WebExtensions to All Computers in a Network. • **Active X Control**—Highly accurate for determining the computer name. *Limitations*: Only fully supported in Internet Explorer. Also, moving forward Microsoft has dropped support for ActiveX Only in their Edge browser. • **Active Directory**—Computer is derived from Active Directory where the computer is "Managed By" the user. *Limitations*: Retrieves only computers managed by the user. • **Reverse DNS**—Uses the visiting users IP Address and performs a reverse DNS lookup. *Limitations*: This is a slow process and unreliable particularly if connected through VPN or wirelessly. • **SCCM**—Computer is derived from System Center Configuration Manager where the user is the top console user. *Limitations*: Assumes System Center Configuration Manager is updated and assumes Data Sync is complete.
Secondary computer discovery method	If the primary computer discovery method fails, this secondary discovery method will be used.
Fallback computer discovery method	If both the primary and secondary computer discovery methods fail, the fallback discovery method will be used.

Table 3-17 • Settings > Web Site View / General Tab

Property	Description
WebExtensions Computer discovery timeout (in seconds)	If **WebExtensions** is the **Primary Computer discovery method** selected, the administrator can set a timeout period using this option that sets the timeout period to use before reverting to the Secondary or Fallback computer discovery methods.
Check synced IP before Reverse DNS look up	If this option is selected, App Portal will look into the local table for an IP address match for the machine. If the IP address is not found, App Portal then will perform a reverse DNS look up. Because viewing a local table takes less time than performing a reverse DNS lookup, selecting this option could speed up performance. By default, this option is not selected.
Default Workflow	If you create a new catalog item and select the **Require Approval for Install?** option on the **Global** tab of the **New Catalog Item** dialog box, but do not add an approval workflow on the **Approval Process** tab, the approval workflow selected from this **Default Workflow** list will be used.
Default Approval Group	Select a approval group to identify a group of approvers that would be used in a case where no approvers for a calculated workflow step could be identified (such as if you specified that a user's manager is the approver for a workflow step, but that user does not have a manager).
Default Category	Select the default category for a catalog item.
Site Protocol	Specify if you want the protocol of the App Portal website to be **http** or **https**.
Web Service Protocol	Specify if you want the protocol of the App Portal web service to be **http** or **https**.
Web service port	If the Web Services are installed on a specific port, enter the port number here.
Cache method	Specify the cache method to be used on the App Portal website: • **IIS Cache**—Use IIS web server caching. • **AppFabric Cache**—Use Windows Server AppFabric distributed caching. AppFabric Caching features use a cluster of servers that communicate with each other to form a single, unified application cache system.
Enable Internet Language Translation	Select to enable internet language translation on the **Communication > Language Text** view.
Default Currency Symbol	Enter the default currency symbol to be used on the App Portal site, such the U.S. dollar sign or the British pound sign.

Table 3-17 • Settings > Web Site View / General Tab

Property	Description
Default ISO Currency	Enter the global currency code, from the ISO 4217 Currency Code list, for the currency that you want to use on the App Portal site. For example, enter **USD** for U.S. dollar, **CAD** for Canada dollar, or **INR** for India rupee. 📄 *Note • The ISO Currency Code list is published by the ISO: International Organization for Standardization (http://www.iso.org).*
Maximum package records to load from SCCM/Altiris	Controls how many records from System Center Configuration Manager or Altiris that are initially queried and displayed on the listing when using the **New Catalog Item Wizard**. 💡 *Tip • To search the entire server for a package or application, use the column filters above the listing.*

Deploying WebExtensions to All Computers in a Network

The following procedures provide steps that an I.T. Administrator needs to take in order to get App Portal WebExtensions successfully deployed to all computers in their network so that you do not have to grant install permissions to your Enterprise users.

- Deploying WebExtensions in Firefox (Windows)

- Deploying WebExtensions in Windows Chrome (Windows)

- Deploying WebExtensions in Microsoft Edge

Deploying WebExtensions in Firefox (Windows)

There are two options to deploy WebExtensions in Firefox for Windows to all computers in your network:

- **Option 1**—To deploy WebExtensions in Firefox for WIndows, an I.T. administrator needs to create an Active Directory Group Policy that allows for auto-install without giving the user the ability stop it. Mozilla's documentation can be found here: https://developer.mozilla.org/en-US/Add-ons/WebExtensions/Alternative_distribution_options/Add-ons_in_the_enterprise#Firefox_settings. Therefore, within the Active Directory Group Policy, an I.T. administrator needs to set `extensions.autoDisableScopes` to their desired preference.

- **Option 2 (Recommended by Mozilla)**—An I.T. administrator needs to deploy **Firefox ESR (Extended-Support Release)** within their enterprise. This can be downloaded and installed from https://www.mozilla.org/en-US/firefox/organizations/all/

Deploying WebExtensions in Windows Chrome (Windows)

Administrators that are deploying `App Portal WebExtensions.msi` onto enterprise user machines need to provide their respective Uniform Resource Identifier (*URI*) in the `APPPORTAL_CHROME_UPDATES_URI` property. App Portal sets the default value of this property to **http://localhost/esd/Downloads/Chrome/WebExtensions/UpdateXML.aspx**. Administrators need to swap *localhost* with their respective App Portal host name.

Deploying WebExtensions in Microsoft Edge

The following procedure provide steps that an I.T. Administrator needs to take in order to get App Portal WebExtensions successfully deployed to all computers in their network so that you do not have to grant install permissions to your Enterprise users.

Task   ***Administrators that are deploying App Portal WebExtensions.msi to enterprise user machines need to perform following steps***

1. Enable **Sideloading** in the respective client machines where web extension are to be installed. To do that, go to **Start > Settings > Update & Security > For developers** and then under the **Use developer features** section, choose the **Sideload apps** radio button.

2. Administrators that are deploying App Portal WebExtensions.msi to enterprise user machines need to provide their respective Uniform Resource Identifier (*URI*) in the APPPORTAL_CHROME_UPDATES_*URI* property. App Portal sets the default value of this property to **http://***localhost***/esd/Downloads/Chrome/WebExtensions/UpdateXML.aspx**. Administrators need to swap ***localhost*** with their respective App Portal host name.

Catalog Appearance Tab

On the **Catalog Appearance** tab of the **Site Management > Settings > Web Site** view, you specify the appearance settings of the App Portal website.

Figure 3-58: Settings > Web Site View / Catalog Appearance Tab

The **Catalog Appearance** tab of the **Web Site** view includes three sets of properties:

- Catalog Tab Strip

- Catalog Appearance

- Visual Styling

Catalog Tab Strip

The **Catalog Tab Strip** area of the **Catalog Appearance** tab of the **Web Site** view includes the following properties:

Table 3-18 • Catalog Tab Strip Area Properties

Property	Description
Enable Help Desk Tools Tab	Determines whether the **Support Tools** tab is displayed to users with the **Request on Behalf of** permission.
Display Application Survey Tab	Select this option to display the **App Survey** tab, which is where users can identify which applications they want to have redeployed onto a new computer using System Center Configuration Manager OSD. The results of the survey are added to Deployment Management AppSurvey Results, where technicians can review the surveys and apply the selected applications to the new computer.
Hide Profile Tab	When enabled, the **Profile** tab will not be visible. This will prevent the user from selecting an alternate approver or specifying a preferred language.
Hide Help Tab	When enabled, the **Help** tab will not be visible.
Always Show Approval Tabs	When enabled, the **Approve / Reject** tab and the **Processed** tabs will be visible to everyone, even if they are not an approver.

Catalog Appearance

The **Catalog Appearance** area of the **Catalog Appearance** tab of the **Web Site** view includes the following properties:

Table 3-19 • Catalog Appearance Area

Property	Description
Hide Inventory Column	Select to hide the **Inventory** column on the **My Requests** tab. When this column is visible, it displays one of the following icons: 🔒 License required 🔒 License not available 🔒 License not required

Table 3-19 • Catalog Appearance Area

Property	Description

Hide Approval Column	Select to the **Approval** column on the **My Requests** tab. When this column is visible, it displays one of the following icons:
	
	  Pending Approval
	
	  Approved
	
	  No Approval Required

Enable dynamic search hints	No longer used.
Show results with visibility restrictions	No longer used.
Show Keyword Search **Show Best Rating Search** **Show new items search** **Show most popular search**	Select these options to enable users to filter catalog items by: • Trending Keywords • Top Rated • What's New • Most Popular When these options are selected, catalog items in these categories are also listed on the App Portal home page.
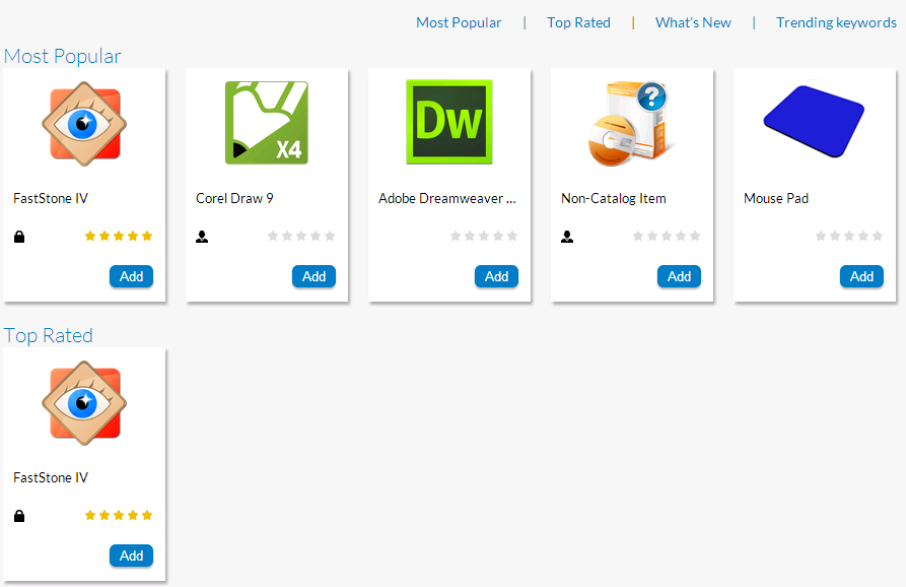
Table 3-19 • Catalog Appearance Area

Property	Description
Day limit for new items	If you select the **Show new items search** option, specify the number of days that an item would be listed in the **What's New** group.
Default Catalog View	Specify whether you want the catalog items to be displayed on the **Browse Catalog** tab, by default, in **Card** or **Grid** view.

Visual Styling

The **Visual Styling** area of the **Catalog Appearance** tab of the **Web Site** view includes the following properties:

Table 3-20 • Visual Styling Area

Property	Description
Company Logo URL	This field lists the location of the company logo that appears at the top left of all App Portal desktop screens. By default, the location of the App Portal logo is listed in this field: `/ap/Images/ap-logo.jpg` To customize the App Portal desktop site to display a different logo, enter the logo's location in this field. You can specify either a local file or a URL to a file at a remote location.
Company Logo URL - Mobile Site Home page	This field lists the location of the company logo that appears on the App Portal mobile site home page. By default, the location of the App Portal logo is listed in this field: `/apm/content/ap-logo.jpg` To customize the App Portal mobile site Home page to display a different logo, enter the logo's location in this field. You can specify either a local file or a URL to a file at a remote location.
Company Logo URL - Mobile Site Login page	This field lists the location of the company logo that appear on the App Portal mobile site Login page. By default, the location of the App Portal logo is listed in this field: `/apm/Images/AppPortalLogo.png` To customize the App Portal mobile site Login page to display a different logo, enter the logo's location in this field. You can specify either a local file or a URL to a file at a remote location.
URL for company support home page	When specified, an image will appear in the top right of the store front and will link to the URL specified.
Hover text for support icon	The text that appears when you hover over the support image when the URL is specified.
Enable Form Decoration	Use to enable or disable the styling of HTML elements (scrollbars, buttons, and text boxes) to match that of the theme selected.

Table 3-20 • Visual Styling Area

Property	Description
Splitter Height Offset	Specifies the height, in pixels, of the heading area of the App Portal website, which is the area of the website that displays the App Portal logo, the user name and the computer name. If you have customized your App Portal website to use a different logo, as described in Changing the Page Header Logo, you may want to increase or decrease this number.

Catalog Behavior Tab

On the **Catalog Behavior** tab of the **Web Site** view, you specify the behavior settings of the App Portal catalog. The **Catalog Behavior** tab includes two sets of properties:

- My Requests Options

- Behaviors

Browse Catalog Options

In the **Browse Catalog Options** section of the **Catalog Behavior** tab, you specify settings to govern how catalog items are displayed on the **Browse Catalog** tab and the mobile UI.

Figure 3-59: Settings > Web Site View / Catalog Behavior Tab / Browse Catalog Options

The **Browse Catalog Options** area of the **Catalog Behavior** tab of the **Web Site** view includes the following properties:

Table 3-21 • Browse Catalog Options Area

Property	Description
Number of catalog items to show for Most Popular	Number of catalog items to be displayed in the Most Popular grouping on the **Browse Catalog** tab.
Mobile UI browse catalog page size	Number of catalog items that will be loaded into the App Portal mobile site at a time. After the user scrolls through the specified number of items, another set of items will be loaded.

Table 3-21 • Browse Catalog Options Area

Property	Description
Display "Show Descriptions" option	Select this option to display the **Description** heading when viewing the catalog items in list view on the **Browse Catalog** tab.
Show installed apps	Select this option to list, on the **Browse Catalog** tab, catalog items that have already been installed on the user's device. If this option is not selected, installed applications will not be listed.
Enable express checkout	Click to enable express checkout on catalog items, so that an **Install Now** button is in addition to the **Add to Cart** button. For more information, see Enabling Express Checkout: Install Now Button.
Ignore Include enforcements if any Excluded enforcement is not satisfied	This option determines how App Portal should evaluate catalog item visibility when you have multiple conditions attached to a catalog item. If the machine/user has at least one **Exclude** condition being true, then this option determines whether or not the catalog item is displayed: ● **Option selected (most restrictive)**—Even if this catalog item has a number of **Include** conditions that are true, the catalog item is not displayed. ● **Option not selected (least restrictive)**—(Default) One of the following occurs: 　● **At least one Include condition is true**—If catalog item has any applicable **Include** conditions that are true, the catalog item will be displayed. 　● **No Include conditions are true**—If the catalog item does not have any **Include** conditions that are true, the catalog item will not be displayed. *Important •* If the machine/user have an associated **Exclude** condition, then this option does not play a role in determining whether or not to display the catalog item.

My Requests Options

In the **My Requests Options** section of the **Catalog Behavior** tab, you specify behavior settings relating to App Portal requests.

Figure 3-60: Settings > Web Site View / Catalog Behavior Tab / My Requests Options

The **My Requests Options** area of the **Catalog Behavior** tab of the **Web Site** view includes the following properties:

Table 3-22 • My Requests Options Area

Property	Description
My requests page auto refresh interval	Specifies the duration that the **My Requests** page refreshes for users. *Note • Only users in roles will have the auto-refresh enabled.*
Enable Real Time Status	When enabled, App Portal will check System Center Configuration Manager for the most recent status of a request if it is in progress. When disabled, the last status received from the bulk status update process (default is 5 minutes) will be used.
Allow users to cancel own requests	When enabled a user can cancel their requests at any stage of the request process. When disabled a user cannot cancel the request after it has been submitted to System Center Configuration Manager for delivery.

Table 3-22 • My Requests Options Area

Property	Description
Allow users to request to SCCM primary	By default, a user can request software to their current device that they are visiting the portal from. Selecting this option will also allow the user to request to all their primary according to the **User / Computer relationship** setting on the **General** tab of **Site Management > Settings**.
Allow users to rate requests	Select to enable a rating system that allows users to give a rating and textual feedback after an application has been successfully installed. The rating will be visible for others to see as they browse the catalog. The ability to rate an item is designated by a yellow star in the **Actions** column after installation.
Show pending requests to all approvers	When enabled, an approver will see all the requests for which they are an approver regardless if it is their turn to approve. The checkbox will not be displayed if it is not their turn to approve. When disabled, the approver will only see the request when it is their turn to approve the request.
Allow approvers to accept requests	If this option is selected, accepting a request marks an item as acknowledged by the approver. The App Portal user interface will update to indicate which approver (from a pool of approvers) has accepted the request so that the rest of the pool does not need to take any action. Accepting a request causes approval reminder emails to stop being sent to other approvers in the pool.
Allow approvers to recommend reject	If this option is selected, recommending rejection marks your objection to approval but does not stop the advancement of the approval process to the next level. If you recommend rejection and are the last approver in the approval process, then the item is rejected.
Allow users to do a search on partial Order #	Select this option to enable users to enter a partial order number in the search field. If this option is not selected, users will have to enter the full order number, including the prefix (such as FLX-235), in order to successfully search by order number.
Show Approve / Reject on My Requests	Select this option to display the **Approve** and **Reject** buttons on the **My Requests** tab. When this option is not selected, the approvers have to open the **Approve / Reject** tab and click on the request name to approve or reject the request. This option is often not selected when you use mandatory approver questionnaires where the approver will always have to open the request details to review and answer questions.
Enable Request Notes	Enable the addition of notes to existing requests. When this option is selected, the following icon will be displayed on the **My Requests** tab next to each request:
Allow users to see detailed deployment status	Select this option to enable users to view detailed deployment status information from System Center Configuration Manager / Altiris on the **My Requests** tab.

Table 3-22 • My Requests Options Area

Property	Description
Show machine policy refresh status to users	Select this option to display a small icon next to the installation status icon under the status column on the **My Requests** tab to indicate whether the machine policy refresh was successful. If this option is not selected, only those with the Catalog Security role of **Manage All Requests** will see this status icon.
Show installation process time	Select this option to display a timer, clock icon under the **Info** column on the **My Requests** tab to indicate the time that has elapsed since the installation request was issued to System Center Configuration Manager. When this option is not selected, only those with the Catalog Security role of **Manage All Requests** will see this status icon.
Show warning for installations processing longer than x hours	Display a warning to the user if an application installation takes longer than the number of hours specified.
Show alert for installations processing longer than x hours	Display an alert to the user if an application installation takes longer than the number of hours specified.
My Requests Status Position	When an item is approved, rejected, etc., a status pop-up opens, by default, in the bottom right of the screen. To change the position of this status pop-up, select another location from this dropdown list.
My Requests Status - Modal	Select this option to specify that when a status pop-up opens, it needs to be acknowledged by the user and manually closed. If this option is not selected, the status pop-up will remain open for the amount of seconds specified in the **My Requests Status - Auto Close Delay** field and will then automatically close.
My Requests Status - Auto Close Delay	Specify the length of time, in seconds, that a status pop-up will remain open on the screen. This option is not used when the **My Requests Status - Modal** option is selected.
Order Number Prefix	Enter the prefix that will appear prior to all request numbers. For example, if you entered `RJX-`, then request numbers would be `RJX-1003`, `RJX-1004`, etc.
Cloud Variable Name Prefix	The default value is `Cloud_`.
Custom Variable Name Prefix	The default value is `Custom_`.
Allow user to cancel a request if it is successful	Select this option to allow a user to cancel a request even after it has been successfully completed. If this option is not selected, cancellation of canceled requests will not be permitted.

Behaviors

In the **Behaviors** section of the **Catalog Behavior** tab of the **Site Management > Settings > Web Site** view, you can set options related to general website functionality.

Figure 3-61: Settings > Web Site View / Catalog Behavior Tab / Behaviors

The **Behaviors** area of the **Catalog Behavior** tab of the **Web Site** view includes the following properties:

Table 3-23 • Settings > Web Site View / Catalog Behavior Tab / Behaviors

Property	Description
Do tutorial on first visit	When enabled, the user will be redirected to the **Help** tab and open the `UserTutorial.htm` file specified in `Web\Help\UserTutorial.htm`. Content can be entered here to train the user on their first visit. Content can include a Flash tutorial or similar training information.
Display client diagnostics	Displays an informational page as necessary if there would be an expected problem deploying software to the visiting computer.
Use Default Approver	When enabled App Portal will use the approver specified in the **Email Settings > Default Approver**. This approver is used when an approver cannot be determined or if approval is specified but no approver is defined. If you do not want to allow the request to complete if an approver could not be found, deselect this option and the user will receive a notification indicating that the request cannot continue.
Application Survey Question Template ID	When the **Display Application Survey Tab** option is selected on the **Site Management > Settings > Web Site > Catalog Appearance** tab, this field sets the question template that is displayed on the **Application Survey** screen.
Allow Application Survey User Editing	Select this option to enable users to edit the list of applications displayed on the **Application Survey** screen. If this option is not selected, all items in the list are selected and users cannot edit them.

Table 3-23 • Settings > Web Site View / Catalog Behavior Tab / Behaviors

Property	Description
Require approval for support tools	When enabled, requests submitted using **Support Tools** will be subjected to the approval process specified, if any.
Always require authorization for LR campaigns containing more than x clients	This setting helps prevent unwanted emails being generated from license reclamation campaigns by accident. Should there be more than the specified number of computers identified for license reclamation in any single campaign, the campaign will require manual authorization of the reclamation records by choosing **Authorize All** under the license reclamation actions menu of a specific campaign. Specify the number of clients which has to be exceeded to trigger manual authorization. The default value is **1000**.
Reload Answers for Questions	If you have a set of questions where the list of available answers in one drop down list is dependent upon what was selected in a previous question, select this option to reload the questions after a selection is made. For example, if you had a set of three questions: 1. Country 2. State 3. City The **States** that you want to list in the second question depends upon the **Country** that was selected in the first question. And the **Cities** that you want to list in the second question depends upon which **State** was selected. If this option is selected, when a selection is made, the target questions are reloaded.
Catalog item reorder waiting period (in days) **Block catalog item reorder during waiting period**	In the **Catalog item reorder waiting period (in days)** field, enter the number of days a requester must wait before submitting a second request for the same catalog item. By default, this value is 7 days. If a requester attempts to submit a second request for the same catalog item within the specified time frame, one of the following will occur, depending upon whether or not the **Block catalog item reorder during waiting period** option is also selected: • **Selected**—The requester will be unable to submit the request. • **Not selected**—The requester will be permitted to submit the request, but a warning message will be displayed during checkout.

Corporate Branding Tab

On the **Corporate Branding** tab of the **Site Management > Settings > Web Site** view, you can customize the colors used in your App Portal site.

Figure 3-62: Settings > Web Site > Corporate Branding Tab

By default, App Portal's user interface is branded with a color theme that mostly consists of various shades of blue and gray. However, you can change the color theme on the **Corporate Branding** tab of the **Site Management > Settings > Web Site** view.

Important • If you have modified the CSS files shipped with previous releases of App Portal to customize the colors of the site, those changes will not be retained when you upgrade to App Portal 2015 R2. You will need to perform the steps in Customizing the App Portal User Interface Colors to customize the colors of your App Portal user interface.

There are two methods for changing the App Portal color theme to match your corporate colors:

● Changing the Base Color and Automatically Generating Other Colors

● Changing the Individual Component Colors

Changing the Base Color and Automatically Generating Other Colors

The easiest way to change the App Portal color theme is to simply change the color listed in the **Select base color** field. App Portal will then automatically generate color codes of various shades of that color that will be used throughout the site.

For example, suppose your company had a green logo with a HEX value of #006600. If you entered #006600 into the **Select base color** box and then clicked **Apply**, a preview of the colors that would be applied throughout your site, that are based on the specified base color, will appear in the **Your custom color** column.

Figure 3-63: Applying a Base Color With Preview of Colors in Your Custom Color Column

If you are satisfied with the colors listed in the **Your custom color**, click **Save**. The browser window will be refreshed and the new color theme will be displayed.

To return to the default Flexera Software colors, click the **Reset to default** button at the bottom of the **Corporate UI Branding** tab.

Changing the Individual Component Colors

You have the option of setting the color individually for each of the listed components of the App Portal application. This is a more difficult option because you have to specify slight variations in your corporate color to serve as hover colors and the background colors for drop down menus, etc.

Your first step would be to determine the colors that you want to use for each of the listed App Portal subcomponents.

Table 3-24 • App Portal Component Color Worksheet

Component	Sub Components	Your Custom Color
Nav bar	Background	
	Icons (unselected)	
	Hover	

Table 3-24 • App Portal Component Color Worksheet

Component	Sub Components	Your Custom Color
Browse categories menu	Menu header background	
	Categories background	
	Category (hover)	
Buttons	Primary	
	Primary (hover)	
	Secondary	
	Secondary (hover)	
Grid/Table	Header row background	
	Row (hover) background	
	Row (alternate) background	
View and dialog box tabs	Tabs (selected)	
	Background	
Highlight color	Search box button, Top border, Progress wheel	
Pop up dialog box	Background	
Others	View titles/subtitles	
	Hyperlink	
	Background of summary box on Checkout page (in progress)	
	Welcome menu hover	
	Dropdown menu hover	
	Admin tab navigation menu hover	
	Image button hover	

In the **Your custom color** column, you would enter the the colors you have selected and click **Save**. The browser window would then be refreshed and the new colors you specified will be displayed throughout the App Portal site.

To return to the default Flexera Software colors, you can click the **Reset to default** button at the bottom of the **Corporate UI Branding** tab.

Dashboard Tab

On the **Dashboard** tab of the **Site Management > Settings > Web Site** view, you specify options for the Software Deployment ROI, OS Deployment ROI, and SLA Dashboards.

You set dashboard reporting options on the **Dashboard** tab of the **Site Management > Settings > Web Site** view.

Figure 3-64: Settings > Web Site > Dashboard Tab

The **Dashboard** tab includes the following properties:

Table 3-25 • Settings > Web Site > Dashboard Tab

Property	Description
Provide adjustable variables for Software Requests	Enter the number of **Hours per request** and **Cost per hour** of a typical software request.
Provide adjustable variables for OSD Requests	Enter the number of **Hours per request** and **Cost per hour** of a typical OSD request.
No. of days the requests are waiting for approval	Enter the threshold number of days that a request needs to be waiting before it is listed in the **Deployment waiting approval for more than n days** card on the **SLA Dashboard**.
Threshold value for failed deployments in %	Enter the percentage of the total number of requests that need to fail before that category's card would be displayed in red (instead of gray) in the **SLA Dashboard** report.

Table 3-25 • Settings > Web Site > Dashboard Tab

Property	Description
Threshold value for rejected requests in %	Enter the percentage of the total number of requests that need to be rejected before that category's card would be displayed in red (instead of gray) in the **SLA Dashboard** report.
Threshold value for approval pending in %	Enter the percentage of the total number of requests that need to be awaiting approval before that category's card would be displayed in red (instead of gray) in the **SLA Dashboard** report.

Deployment

You specify deployment technology settings on the **Site Management > Settings > Deployment** view. The **Deployment** view consists of the following tabs:

- Common Tab
- ConfigMgr Tab
- SCCM 2012 Tab
- Altiris Tab
- AirWatch Tab
- Casper Tab
- MobileIron Tab

Common Tab

On the **Common** tab of the **Deployment** view, you need to select the deployment technology that App Portal should use to perform user syncing, computer syncing, evaluating collection membership, and other tasks.

You can connect App Portal to multiple deployment technologies: System Center 2012 Configuration Manager, Symantec Altiris, AirWatch (mobile applications), and Casper (Macintosh desktop applications). You can also specify a custom connection string to another third-party deployment technology. You are permitted to set up App Portal to perform some tasks with one deployment technology and other tasks with a different deployment technology.

Figure 3-65: Settings > Deployment View / Common Tab

The **Common** subtab includes the following properties:

Table 3-26 • Settings > Deployment View / Common Tab

Property	Description
Define order for detecting client deployment technology	If you have entered connection settings for more than one deployment technology, specify the order in which App Portal will check them to determine which deployment technology the end user's computer is a client of.
Syncing Users	Select the deployment technology that App Portal should use to sync users using built-in sync queries: ● **Not Defined** ● **ConfigMgr** ● **SCCM 2012** ● **Altiris** **Important •** *If you are going to specify a custom user sync connection string in the* Custom User Sync Settings *area below, set this field to* **Not Defined***.*

Table 3-26 • Settings > Deployment View / Common Tab

Property	Description
Syncing Computers	Select the deployment technology that App Portal should use to sync computers using built-in sync queries: • **Not Defined** • **ConfigMgr** • **SCCM 2012** • **Altiris** *Important • If you are going to specify a custom computer sync connection string in the Custom Computer Sync Settings and Custom User Computer Map Sync Settings areas below, set this field to* **Not Defined***.*
Evaluating collection membership	Select the deployment technology that App Portal should use to evaluate collection membership for standard conditions: • **Not Defined** • **ConfigMgr** • **SCCM 2012** • **Altiris**
Inventory / OS Deployment	Select the deployment technology that you want App Portal to use to perform OS deployments and to read inventory data: • **Not Defined** • **ConfigMgr** • **SCCM 2012** *Note • Not supported for Altiris unless also using FlexNet Manager Suite.*
Sync Page Size	Specify the batch size that App Portal should use to process users and computers. The default value is 100.
Sync Command Timeout (in seconds)	Specify the timeout value in seconds for the Sync Data command. The default value is 300.

Table 3-26 • Settings > Deployment View / Common Tab

Property	Description
Sync Data Now	Click to sync App Portal using the current selections. 📄 *Note •* *Until you sync user and computer data with the selected deployment technology, App Portal will not recognize the logged in user.* 📄 *Note •* *The sync also happens at 2:00 a.m. each morning. To configure the time, open the* ***Site Management > Settings > Timers*** *tab and edit the* ***Time of day to sync users and computers*** *field.*
Custom User Sync Settings	If you want App Portal to use custom user sync queries, enter those queries in the following text boxes: • **Custom User ID Sync SQL Query**—Query to obtain user IDs so that App Portal can process them in batch. See example in Custom User ID Sync SQL Query. • **Custom User Sync SQL Query**—Query to obtain all user columns. Some of the columns and their names are mandatory, as described in the provided query sample. See example in Custom User Sync SQL Query. • **Custom User Sync Connection String**—If you do not specify a custom connection string, App Portal will default to the connection string of the technology selected for **Syncing Users**. See example in Custom User Sync Connection String. 📄 *Important •* *If you are using a custom source for user syncing, be sure to set the Syncing Users property to* ***Not Defined***.
Custom Computer Sync Settings	If you want to use custom computer sync queries, enter those queries in the following text boxes: • **Custom Computer ID Sync SQL Query**—Query to obtain computer IDs so that App Portal can process them in batch. See example in Custom Computer ID Sync SQL Query. • **Custom Computer Sync SQL Query**—Query to obtain all computer columns. Some of the columns and their names are mandatory, as described in the provided query sample. See example in Custom Computer Sync SQL Query. • **Custom Computer Sync Connection String**—If you do not specify a custom connection string, App Portal will default to the connection string of the technology selected for **Syncing Users**. See example in Custom Computer Sync SQL Query. 📄 *Important •* *If you are using a custom source for computer syncing, be sure to set the Syncing Computers property to* ***Not Defined***.

Table 3-26 • Settings > Deployment View / Common Tab

Property	Description
Custom User Computer Map Sync Settings	If you want to use custom user computer map sync settings, enter those queries in the following text boxes: • **Custom User Computer Map ID Sync SQL Query**—Query to obtain user IDs and computer IDs so that App Portal can process them in batch. See example in Custom User Computer Map ID Sync SQL Query. • **Custom User Computer Map Sync SQL Query**—Query to obtain all user and computer columns. Some of the columns and their names are mandatory, as described in the provided query sample. See example in Custom User Computer Map Sync SQL Query. • **Custom User Computer Map Sync Connection String**—If you do not specify a custom connection string, App Portal will default to the connection string of the technology selected for **Syncing Users**. See example in Custom User Computer Map Sync Connection String.

Custom User Sync Settings

This section provides examples of code that could be used in the **Custom User Sync Settings** area of the **Deployment > Common** subtab:

• Custom User ID Sync SQL Query

• Custom User Sync SQL Query

• Custom User Sync Connection String

Custom User ID Sync SQL Query

The following is example code of a custom user ID sync SQL query:

Table 3-27 • Custom User ID Sync SQL Query Example

Type	Sample Code
Altiris	```SELECT DISTINCT Guid as UserResourceID, Name FROM vUser ORDER BY Name```
ConfigMgr **SCCM 2012**	```SELECT vru.ResourceID as UserResourceID FROM v_R_User vru ORDER BY vru.Name0```

📄

Note • *App Portal is specifically looking to read the mandatory* `UserResourceID` *column.*

📄

Note • *To verify your query and its columns, first click* **Save,** *and then click the* **Test User Sync Settings** *button.*

Custom User Sync SQL Query

The following is example code of a custom user sync SQL query:

Table 3-28 • Custom User Sync SQL Query Example

Type	Sample Code
Altiris	SELECT DISTINCT u.[Given Name] AS FirstName, u.[Surname] AS LastName, '' AS OS, u.[Office Location] AS Office, u.City as City, u.Zip AS PostalCode, u.Department AS Department, u.[Job Title] AS Title, u.Name AS UserName, u.Email AS Email, m.ManagerDN AS Manager, u.Guid AS UserResourceID, ad.[Distinguished Name] AS ADSPath, u.[Display Name] AS FullName, '' AS Name, u.Domain + '\\' + Name AS UniqueName, '' AS UserDomain, u.Company AS Company, ou.[Distinguished Name] AS UserOU FROM vUser u INNER JOIN Inv_Global_Active_Directory_Details ad on ad._ResourceGuid = u.Guid INNER JOIN Inv_OU_Membership ou on ou._ResourceGuid = u.Guid LEFT JOIN (SELECT ra.ParentResourceGuid, it.Name as Manager, ra.ChildResourceGuid, ad.[Distinguished Name] as ManagerDN FROM ResourceAssociation ra LEFT JOIN vItem it ON ra.ChildResourceGuid = it.Guid INNER JOIN Inv_Global_Active_Directory_Details ad on ad._ResourceGuid = it.Guid WHERE ra.ResourceAssociationTypeGuid = '049C633F-8413-42AE-93EA-F4EB7EDAFC65') m on m.ParentResourceGuid = u.Guid
ConfigMgr SCCM 2012	SELECT DISTINCT givenName0 AS FirstName, sn0 AS LastName, DisplayName0 AS DisplayName, Network_Operating_System0 AS OS, physicalDeliveryOfficeNam0 AS Office, l0 AS City, vru.postalCode0 AS PostalCode, department0 AS Department, title0 AS Title, User_Name0 AS UserName, mail0 AS Email, manager0 AS Manager, vru.ResourceID AS UserResourceID, distinguished_Name0 AS ADSPath, Full_User_Name0 AS FullName, Name0 AS Name, Unique_User_Name0 AS UniqueName, Windows_NT_Domain0 AS UserDomain, company0 AS Company, ra.User_OU_Name0 AS UserOU FROM v_R_User AS vru LEFT JOIN v_RA_User_UserOUName ra on ra.ResourceID = vru.ResourceID

Note • *App Portal is specifically looking to read the following mandatory columns:*

UserResourceID
FirstName
LastName
Office
City
PostalCode
Department
Title

```
UserName
Email
Manager
ADSPath
FullName
UniqueName [in the format of Domain\UserName]
UserDomain
Company
UserOU
```

📄

Note • *To verify your query and its columns, first click* **Save***, and then click the* **Test User Sync Settings** *button.*

Custom User Sync Connection String

The following is example code of a custom user sync connection string:

Table 3-29 • Custom User Sync Connection String Example

Type	Sample Code
Altiris ConfigMgr SCCM 2012	`Data Source=`*DBSERVERNAME*`;Initial Catalog=`*DBNAME*`;Integrated Security=True`

📄

Note • *If you do not specify a custom connection string, App Portal will default to the connection string of the technology selected for* **Syncing Users***.*

📄

Note • *To verify your connection string, first click* **Save***, and then click the* **Test User Sync Settings** *button.*

Custom Computer Sync Settings

This section provides examples of code that could be used in the **Custom Computer Sync Settings** area of the **Deployment > Common** subtab:

● Custom Computer ID Sync SQL Query

● Custom Computer Sync SQL Query

● Custom Computer Sync Connection String

Custom Computer ID Sync SQL Query

The following is example code of a custom computer ID sync SQL query:

Table 3-30 • Custom Computer ID Sync SQL Query Example

Type	Sample Code
Altiris	SELECT DISTINCT Guid AS ResourceID, Name AS MachineName FROM vComputerEx ORDER BY Name
ConfigMgr **SCCM 2012**	SELECT vrs.ResourceID, vrs.Netbios_Name0 FROM v_R_System vrs ORDER BY vrs.Netbios_Name0

📄

Note • App Portal is specifically looking to read the mandatory ResourceID *column.*

📄

Note • To verify your query and its columns, first click **Save***, and then click the* **Test Computer Sync Settings** *button.*

Custom Computer Sync SQL Query

The following is example code of a custom computer sync SQL query:

Table 3-31 • Custom Computer Sync SQL Query Example

Type	Sample Code
Altiris	SELECT DISTINCT c.Guid AS ResourceID, c.Name AS MachineName, c.[User] AS SMSUserName, '' AS ADSite, c.IsManaged AS Client, c.IsManaged AS Active, 0 AS ClientType, 0 AS Obsolete, c.Domain AS UserDomain, c.Domain AS MachineDomain, '' AS ManagedBy, ou.[Distinguished Name] AS SystemOU FROM dbo.vComputerEx c INNER JOIN Inv_OU_Membership ou ON ou._ResourceGuid = c.Guid

Table 3-31 • Custom Computer Sync SQL Query Example

Type	Sample Code
ConfigMgr SCCM 2012	```SELECT DISTINCT vrs.ResourceID, Netbios_Name0 AS MachineName, User_Name0 AS SMSUserName, AD_Site_Name0 AS ADSite, Client0 AS Client, Active0 AS Active, Client_Type0 AS ClientType, Obsolete0 AS Obsolete, User_Domain0 AS UserDomain, Resource_Domain_OR_Workgr0 as MachineDomain,vrs.Operating_System_Name_and0 as OperatingSystem, ra.System_OU_Name0 as SystemOU, (SELECT top 1 IP_Addresses0 FROM v_RA_System_IPAddresses WHERE v_RA_System_IPAddresses.IP_Addresses0 not like '%:%' --ignore ipv6 address AND v_RA_System_IPAddresses.ResourceID=vrs.ResourceID) AS [IPAddress] , ManagedBy0 as ManagedBy FROM dbo.v_R_System vrs left join v_RA_System_SystemOUName ra on ra.ResourceID = vrs.ResourceID```

📄

Note • App Portal is specifically looking to read the following mandatory columns:

ResourceID
MachineName
SMSUserName
ADSite
Client
Active
ClientType
Obsolete
UserDomain
MachineDomain
ManagedBy
SystemOU

📄

*Note • To verify your query and its columns, first click **Save**, and then click the **Test Computer Sync Settings** button.*

Custom Computer Sync Connection String

The following is example code of a custom computer sync connection string:

Table 3-32 • Custom Computer Sync Connection String Example

Type	Sample Code
ConfigMgr SCCM 2012 Altiris	`Data Source=DBSERVERNAME;Initial Catalog=DBNAME;Integrated Security=True`

📄

Note • *If you do not specify a custom connection string, App Portal will default to the connection string of the technology selected for* **Syncing Computers**.

📄

Note • *To verify your connection string, first click* **Save**, *and then click the* **Test Computer Sync Settings** *button.*

Custom User Computer Map Sync Settings

This section provides examples of code that could be used in the **Custom User Computer Map Sync Settings** area of the **Deployment > Common** subtab:

- Custom User Computer Map ID Sync SQL Query

- Custom User Computer Map Sync SQL Query

- Custom User Computer Map Sync Connection String

Custom User Computer Map ID Sync SQL Query

There are two examples of Custom User Computer Map ID Sync SQL queries:

- Primary Example

- Last Logon User Example

Primary Example

The following is example code of a custom user computer map ID sync SQL query for a primary device:

Table 3-33 • Custom User Computer Map ID Sync SQL Query / Primary Device

Type	Sample Code
ConfigMgr SCCM 2012 (Only)	```SELECT DISTINCT vrs.ResourceID, vrs.Netbios_Name0 AS MachineName FROM v_R_System AS vrs INNER JOIN vUsersPrimaryMachines ON vrs.ResourceID = vUsersPrimaryMachines.MachineID INNER JOIN v_R_User AS vru ON vUsersPrimaryMachines.UserResourceID = vru.ResourceID ORDER BY vrs.Netbios_Name0```
Altiris	```SELECT uc._ResourceGuid as [ResourceID], uc.Name AS [MachineName] FROM Inv_AeX_AC_Identification uc LEFT OUTER JOIN Inv_AeX_AC_Primary_User pu ON pu._ResourceGuid = uc._ResourceGuid ORDER BY uc.Name```

📄

Note • *App Portal is specifically looking to read the mandatory* `ResourceID` *and* `MachineName` *columns.*

📄

Note • *To verify your query and its columns, first click* **Save**, *and then click the* **Test User Computer Map Sync Settings**
button.

Last Logon User Example

The following is example code of a custom user computer map ID sync SQL query for a last logon user:

Table 3-34 • Custom User Computer Map ID Sync SQL Query / Last Logon User

Type	Sample Code
ConfigMgr **SCCM 2012**	SELECT DISTINCT vrs.ResourceID, vrs.Netbios_Name0 AS MachineName FROM v_R_System AS vrs LEFT OUTER JOIN v_R_User AS vru ON vrs.User_Name0 = vru.User_Name0 AND vrs.User_Domain0 = vru.Windows_NT_Domain0 ORDER BY vrs.Netbios_Name0
Altiris	SELECT uc._ResourceGuid AS [ResourceID], isnull(uc.[Name], uc.[Name]) AS [MachineName] FROM Inv_AeX_AC_Identification uc ORDER BY uc.Name

📄

Note • *App Portal is specifically looking to read the mandatory* `ResourceID` *and* `MachineName` *columns.*

📄

Note • *To verify your query and its columns, first click* **Save**, *and then click the* **Test User Computer Map Sync Settings**
button.

Custom User Computer Map Sync SQL Query

There are two examples of Custom User Computer Map Sync SQL queries:

- Primary Example
- Last Logon User Example

Primary Example

The following is example code of a custom user computer map sync SQL query for a primary device:

Table 3-35 • Custom User Computer Map Sync SQL Query / Primary Device

Type	Sample Code
ConfigMgr **SCCM 2012** (Only)	SELECT DISTINCT vrs.ResourceID, vru.Unique_User_Name0 AS UniqueName, vrs.Netbios_Name0 AS MachineName, 1 AS Active FROM v_R_System AS vrs INNER JOIN vUsersPrimaryMachines ON vrs.ResourceID = vUsersPrimaryMachines.MachineID INNER JOIN v_R_User AS vru ON vUsersPrimaryMachines.UserResourceID = vru.ResourceID
Altiris	SELECT * from (SELECT uc._ResourceGuid AS [ResourceID], uc.Name AS [MachineName], isnull([pu].[Domain] + N'\' , N'') + isnull([User] , N'') AS [UniqueName], 1 AS [Active] FROM Inv_AeX_AC_Identification uc LEFT OUTER JOIN Inv_AeX_AC_Primary_User pu ON pu._ResourceGuid = uc._ResourceGuid) uc

📄

Note • App Portal is specifically looking to read the following mandatory columns:

ResourceID
MachineName
UniqueName

📄

*Note • To verify your query and its columns, first click **Save**, and then click the **Test User Computer Map Sync Settings** button.*

Last Logon User Example

The following is example code of a custom user computer map sync SQL query for a last logon user:

Table 3-36 • Custom User Computer Map Sync SQL Query /Last Logon User

Type	Sample Code
ConfigMgr **SCCM 2012**	SELECT DISTINCT vrs.ResourceID, vrs.Netbios_Name0 AS MachineName, vru.Unique_User_Name0 AS UniqueName, 1 AS Active FROM v_R_System AS vrs LEFT OUTER JOIN v_R_User AS vru ON vrs.User_Name0 = vru.User_Name0 AND vrs.User_Domain0 = vru.Windows_NT_Domain0

Table 3-36 • Custom User Computer Map Sync SQL Query /Last Logon User

Type	Sample Code
| Altiris | ```
SELECT *

FROM

(

SELECT uc._resourceguid AS ResourceID, isnull( uc.[Name], uc.[Name]) AS [MachineName],
   isnull( uc.[Last Logon Domain] + N'\', N'' ) + isnull( uc.[Last Logon User], N'' )
   AS [UniqueName], 1 AS [Active]

FROM Inv_AeX_AC_Identification uc

) uc
``` |

📄

Note • App Portal is specifically looking to read the following mandatory columns:

ResourceID
MachineName
UniqueName

📄

Note • To verify your query and its columns, first click **Save***, and then click the* **Test User Computer Map Sync Settings**
button.

Custom User Computer Map Sync Connection String

The following is example code of a custom user computer map sync connection string:

Table 3-37 • Custom User Computer Map Sync Connection String

Type	Sample Code
ConfigMgr SCCM 2012 Altiris	`Data Source=DBSERVERNAME;Initial Catalog=DBNAME;Integrated Security=True`

📄

*Note • If you do not specify a custom connection string, App Portal will default to the connection string of the technology
selected for* **Syncing Users** *and* **Syncing Computers***.*

📄

Note • To verify your connection string, first click **Save***, and then click the* **Test User Computer Map Sync Settings** *button.*

ConfigMgr Tab

You specify System Center Configuration Manager (current branch) settings on the **Deployment > ConfigMgr** subtab of the **Settings** view, which is opened by selecting **Settings** under **Site Management** on the **Admin** tab.

Figure 3-66: Settings > Deployment View / ConfigMgr Tab

The **ConfigMgr** subtab includes the following properties:

Table 3-38 • Settings > Deployment View / ConfigMgr Tab

Property	Description
Central Site Server	Enter the machine name of the System Center Configuration Manager (current branch) server.
Central Site Database Server	Enter the machine name where the System Center Configuration Manager (current branch) server database resides.
Central Site Database Name	Enter the database name of the System Center Configuration Manager (current branch) server database.
Central Site Code	Defines the Central Site Code (in SITE_XXX format).
Limiting Collection For Device	By default, when creating a collection for a catalog item, App Portal uses "All System" as the limiting collection for device-based deployments. If you instead want to specify which limiting collection to use, enter a collection name in this field to set as the limiting collection ID for all device-based collections created by App Portal for device-based deployments.
Limiting Collection For User	By default, when creating a collection for a catalog item, App Portal uses "All Users as the limiting collection for user-based deployments. If you instead want to specify which limiting collection to use, enter a collection name in this field to set as the limiting collection ID for all user-based collections created by App Portal for user-based deployments.
Test	Click to test the connection settings that are entered. If the test is successful, the message [SERVER_NAME] settings are valid appears.

Table 3-38 • Settings > Deployment View / ConfigMgr Tab (cont.)

Property	Description
Enable workstation verification?	Enables/disables the actions in the **Select verification level** list. Users matching one of the specified attributes will not be required to accept the EULA.
	Depending on the User / Computer relationship, this will be the last user inventoried or the most logged on user.
	• **Select verification level**—Tells App Portal how to handle users who visit from machines that were not originally registered with App Portal. Select one of the following options:
	• **Warning**—Users will be prompted with a notification that they are not using the discovered machine.
	• **Disallowed**—Users will not be able to visit the App Portal Storefront from other machines.
	*Important • This field is disabled when the **User / Computer relationship** field is set to **Use SCCM last logon user**.*
User / Computer relationship	Specify the user/computer relationship that App Portal needs to use by selecting one of the following options:
	• **Use SCCM last logon user**—The user to computer relationship will use SMS last logon user.
	• **Use SCCM Primary Console Usage**—Makes use of the System Center Configuration Manager / SMS SP3 feature of tracking login duration to determine primary machine usage
	• **Use AD Computer Managed By**—Uses the AD Computer object "Managed By" attribute to determine the primary user of the computer. This setting requires inventory of the "ManagedBy" AD attribute in System Center Configuration Manager System Discovery.
	• **Use User Affinity**—In System Center Configuration Manager (current branch), you can directly define the users for a computer and the computers for a user. The option could also be referred to as "Use System Center Configuration Manager user and device assignment".
	*Note • When workstation verification is enabled, the user's current computer is checked against System Center Configuration Manager to determine if this device is their primary device. Therefore, the **Use SCCM last logon user** is not available for workstation verification because it is not as accurate as the other methods.*

Table 3-38 • Settings > Deployment View / ConfigMgr Tab (cont.)

Property	Description
Reporting Path	The full HTTP path to the System Center Configuration Manager reporting URL, including the trailing backslash. When not specified, the standard format will be used: http://<server>/sccmreporting_<site _code>/
Use v_ClassicDeploymentAssetDetails to get package deployment status	If status updates for packages and task sequences are not getting updated in your environment, select this option to instruct App Portal to obtain the deployment status from an alternate view in System Center Configuration Manager.
Validate available DP for software requests	App Portal can impersonate a client location request for content to ensure that the computer will have access to the System Center Configuration Manager content when a request is submitted. Disabling this option may cause a request to stall in "Waiting for Content" state if the content is not available for the computer. May require the registration (Regsvr32) of the smsmsgapi.dll in Web\Bin.
Use Central Site for All Deployments	All deployments will be generated from the central site as opposed to using each primary site. In some cases you may elect to do all your deployments from the Central Site instead of using each primary site. App Portal manages all the collections at each primary site, however if you still wish to use the Central site for all deployments select this option. Your deployment times will be subject to intra-site replication delays.
Client polling interval	Enter the client polling interval of the System Center Configuration Manager client. This value is used to calculate date and time data for email messages when explaining when a request should begin no later than.
MDT Database Name	If Microsoft Deployment Toolkit (MDT) is installed on the Central Administration Site (CAS) server, enter the database name here (such as MDT) to obtain the list of supported MDT variables for OSD.
User Computer Relationship View	Specify the System Center Configuration Manager view to use to read the user/computer relationship. Possible values are: • v_UserMachineRelationship • vUsersPrimaryMachines
Use SCCM server for machine policy refresh	When a user requests software, his machine is added to a catalog-item specific collection in System Center Configuration Manager (current branch). By default, this list only refreshes once per hour. If you select this option, System Center Configuration Manager (current branch) will trigger a policy refresh on desktop machines.

Table 3-38 • Settings > Deployment View / ConfigMgr Tab (cont.)

Property	Description
Enable Collection Cleanup on Failure	If this setting is selected, upon deployment failure, App Portal will remove the device from the collection.
Success Status IDs	Identifies the status IDs from System Center Configuration Manager that constitute a successful installation.
Failure Status IDs	Identifies the status IDs from System Center Configuration Manager that constitute a failed installation.
Program Collection Cleanup Status IDs	Identifies the status IDs from System Center Configuration Manager where App Portal should remove the machine from the collection for requests that have Enable Collection Clean-up enabled.
Enable Rerun Advertisement for Status IDs	Identifies the status IDs from System Center Configuration Manager where App Portal should allow an advertisement to be rerun for requests that **Enable Rerun** is enabled.

SCCM 2012 Tab

You specify System Center 2012 Configuration Manager settings on the **Deployment > SCCM 2012** subtab of the **Settings** view, which is opened by selecting **Settings** under **Site Management** on the **Admin** tab.

Figure 3-67: Settings > Deployment View / SCCM 2012 Tab

The **SCCM 2012** subtab includes the following properties:

Table 3-39 • Settings > Deployment View / SCCM 2012 Tab

Property	Description
Central Site Server	Enter the machine name of the System Center 2012 Configuration Manager Server.

Table 3-39 • Settings > Deployment View / SCCM 2012 Tab (cont.)

Property	Description
Central Site Database Server	Enter the machine name where the System Center 2012 Configuration Manager Server database resides.
Central Site Database Name	Enter the database name of the System Center 2012 Configuration Manager Server database.
Central Site Code	Defines the Central Site Code (in SITE_XXX format).
Limiting Collection For Device	By default, when creating a collection for a catalog item, App Portal uses "All System" as the limiting collection for device-based deployments. If you instead want to specify which limiting collection to use, enter a collection name in this field to set as the limiting collection ID for all device-based collections created by App Portal for device-based deployments.
Limiting Collection For User	By default, when creating a collection for a catalog item, App Portal uses "All Users as the limiting collection for user-based deployments. If you instead want to specify which limiting collection to use, enter a collection name in this field to set as the limiting collection ID for all user-based collections created by App Portal for user-based deployments.
Test	Click to test the connection settings that are entered. If the test is successful, the message [SERVER_NAME] settings are valid appears.
Enable workstation verification?	Enables/disables the actions in the **Select verification level** list. Users matching one of the specified attributes will not be required to accept the EULA.
	Depending on the User / Computer relationship, this will be the last user inventoried or the most logged on user.
	• **Select verification level**—Tells App Portal how to handle users who visit from machines that were not originally registered with App Portal. Select one of the following options:
	• **Warning**—Users will be prompted with a notification that they are not using the discovered machine.
	• **Disallowed**—Users will not be able to visit the App Portal Storefront from other machines.
	*Important • This field is disabled when the **User / Computer relationship** field is set to **Use SCCM last logon user**.*

Table 3-39 • Settings > Deployment View / SCCM 2012 Tab (cont.)

Property	Description
User / Computer relationship	Specify the user/computer relationship that App Portal needs to use by selecting one of the following options: • **Use SCCM last logon user**—The user to computer relationship will use SMS last logon user. • **Use SCCM Primary Console Usage**—Makes use of the System Center Configuration Manager / SMS SP3 feature of tracking login duration to determine primary machine usage • **Use AD Computer Managed By**—Uses the AD Computer object "Managed By" attribute to determine the primary user of the computer. This setting requires inventory of the "ManagedBy" AD attribute in System Center Configuration Manager System Discovery. • **Use User Affinity**—In System Center 2012 Configuration Manager, you can directly define the users for a computer and the computers for a user. The option could also be referred to as "Use System Center 2012 Configuration Manager user and device assignment". *Note • When workstation verification is enabled, the user's current computer is checked against System Center Configuration Manager to determine if this device is their primary device. Therefore, the* **Use SCCM last logon user** *is not available for workstation verification because it is not as accurate as the other methods.*
Reporting Path	The full HTTP path to the System Center Configuration Manager reporting URL, including the trailing backslash. When not specified, the standard format will be used: http://<server>/sccmreporting_<site _code>/
Use v_ClassicDeploymentAssetDetails to get package deployment status	If status updates for packages and task sequences are not getting updated in your environment, select this option to instruct App Portal to obtain the deployment status from an alternate view in System Center Configuration Manager.
Validate available DP for software requests	App Portal can impersonate a client location request for content to ensure that the computer will have access to the System Center Configuration Manager content when a request is submitted. Disabling this option may cause a request to stall in "Waiting for Content" state if the content is not available for the computer. May require the registration (`Regsvr32`) of the `smsmsgapi.dll` in `Web\Bin`.

Table 3-39 • Settings > Deployment View / SCCM 2012 Tab (cont.)

Property	Description
Use Central Site for All Deployments	All deployments will be generated from the central site as opposed to using each primary site. In some cases you may elect to do all your deployments from the Central Site instead of using each primary site. App Portal manages all the collections at each primary site, however if you still wish to use the Central site for all deployments select this option. Your deployment times will be subject to intra-site replication delays.
Client polling interval	Enter the client polling interval of the System Center Configuration Manager client. This value is used to calculate date and time data for email messages when explaining when a request should begin no later than.
MDT Database Name	If Microsoft Deployment Toolkit (MDT) is installed on the Central Administration Site (CAS) server, enter the database name here (such as MDT) to obtain the list of supported MDT variables for OSD.
User Computer Relationship View	Specify the System Center Configuration Manager view to use to read the user/computer relationship. Possible values are: • `v_UserMachineRelationship` • `vUsersPrimaryMachines`
Use SCCM server for machine policy refresh	When a user requests software, his machine is added to a catalog-item specific collection in System Center Configuration Manager. By default, this list only refreshes once per hour. If you select this option, System Center Configuration Manager will trigger a policy refresh on desktop machines.
Enable Collection Cleanup on Failure	If this setting is selected, upon deployment failure, App Portal will remove the device from the collection.
Success Status IDs	Identifies the status IDs from System Center Configuration Manager that constitute a successful installation.
Failure Status IDs	Identifies the status IDs from System Center Configuration Manager that constitute a failed installation.
Program Collection Cleanup Status IDs	Identifies the status IDs from System Center Configuration Manager where App Portal should remove the machine from the collection for requests that have Enable Collection Clean-up enabled.
Enable Rerun Advertisement for Status IDs	Identifies the status IDs from System Center Configuration Manager where App Portal should allow an advertisement to be rerun for requests that **Enable Rerun** is enabled.

OS Deployment Tab

After you have specified a default OS deployment technology, as described in Specifying the Default OS Deployment Technology, you need to also specify global OS deployment settings for that deployment technology on the **OS Deployment** tab of the **Site Management > Settings > Deployment** view.

Figure 3-68: OS Deployment Tab of Site Management > Settings > Deployment View

On the **OS Deployment** tab, you can specify the following types of global settings:

- **Application migration**—You can enable the migration of existing installed applications from the source machine to the target machine (when performing either a computer upgrade or when performing a side-by-side migration). You can also specify whether to enable the requester to either migrate all existing applications or only those that they select during checkout.

- **Installation of additional applications**—You can select an option to enable the requester to select additional applications to install during OS deployment.

- **OSD site server settings**—You need to provide settings specific to the default OS deployment technology that you selected, as described in Specifying the Default OS Deployment Technology.

The **OS Deployment** tab includes the following properties.

Table 3-40 • OS Deployment Tab Properties

Property	Description
Enable application migration and installation of additional applications	Select this option to enable a requester to select existing applications to migrate during the checkout of an OSD task sequence catalog item.
	If this option is selected, along with the **Auto detect installed apps** option on the **Deployment > Roles** tab of the **Catalog Item Properties** dialog box for an OSD task sequence catalog item, the Choose Existing Applications to Migrate Panel panel of the Checkout Wizard will be displayed during the checkout of an OSD task sequence catalog item.
	Also, if this option is selected, applications will be listed in the **Applications Included** column of the roles table on the **Choose Roles** panel of the Checkout Wizard (which is displayed if roles are associated with a task sequence catalog item). If this option is not selected, this column will be empty; only the names of the roles will be listed.
	*Note • This option must be selected in order to enable its sub-options: **Enable requester to specify which existing applications to migrate** and **Prompt requester to select additional applications to install**.*
	Note • For more information, see Global vs. Catalog Item Level Settings for Migrating or Installing New Applications During OS Deployment.
Enable requester to specify which existing applications to migrate	This option is enabled if you select the **Enable application migration and installation of additional applications** option.
	● **If this option is selected**, when the **Choose Existing Applications to Migrate** panel of the Checkout Wizard is displayed, the requester will be able to select which of the applications on the existing computer will be migrated to the target computer.
	● **If this option is not selected**, all applications on the existing computer will automatically be selected and you will be unable to deselect them.
	*Note • To prevent an application from being listed on the **Choose Existing Applications to Migrate** panel, select the **Core application** option on the **General > Global** tab of the catalog item's Catalog Item Properties dialog box.*

Table 3-40 • OS Deployment Tab Properties

Property	Description
Prompt requester to select additional applications to install	If this option is selected, the Choose Additional Applications to Install During OS Deployment Panel will be displayed in the Checkout Wizard, prompting the requester of an OSD task sequence catalog item to select additional applications to install on the target computer. *Note •* *This option is enabled if you select the* **Enable application migration and installation of additional applications** *option.* *Note •* *To prevent an application from being listed on the* **Choose Additional Applications to Install During OS Deployment** *panel, select the* **Core application** *option on the* **General > Global** *tab of the catalog item's Catalog Item Properties dialog box.*
Path to inboxes	Specify the path to the System Center Configuration Manager In Boxes, such as: `\\FLEXDCCM\sms_flx\inboxes\` This path is used to transfer the Discovery Data Record (DDR) for user and computer discovery, when the new computer is created during a "bare metal" scenario. *Important •* *Specify the path to the same System Center Configuration Manager technology you selected in the* **Inventory / OS Deployment** *field on the* **Site Management > Settings > Deployment > Common** *tab.* *Note •* *When System Center Configuration Manager runs a discovery, it creates DDRs. The information contained in a DDR varies depending upon the discovered resource. For example, it can include the NetBIOS name of a computer, the IP address and IP subnet of a computer or device, and the computer operating system name.*
Default OSD site server	Choose the System Center Configuration Manager site where new computer objects will be imported when using bare metal OS deployment.
Default OSD time zone	Enter the default time zone for new computers imported into System Center Configuration Manager as a part of an OS deployment. For example, enter **-6** to indicate that the time zone is 6 hours behind Coordinated Universal Time (UTC), the world's time standard.

Table 3-40 • OS Deployment Tab Properties

Property	Description
Store OSD packages as computer variables	If you select this option, when applications are targeted to an OS deployment, the applications will be stored on the computer object as variables. This allows for the MDT process to automatically install the applications without any further customizations. If you do not select this option, you will need to obtain the applications using SQL or web service calls.
Base application variable name	This base variable will be used to deploy applications as part of the **Install Applications** step in a System Center Configuration Manager OSD task sequences. It should match the value specified in the **Install Applications** task sequence step exactly. The variable name and value will be appended to the variables list of the System Center Configuration Manager object. The default value is COALESCEDAPPS.
Base package variable name	This base variable will be used to deploy packages as part of the **Install Software** step in a System Center Configuration Manager OSD task sequence. It should match the value specified in the **Install Software** task sequence step exactly. The variable name and value will be appended to the variables list of the System Center Configuration Manager Computer object. The default value is PACKAGES.
Coalesce digits for OSD variable (applications)	This setting, which works in conjunction with the **Base application variable name** COALESCEDAPPS, is used during OS deployment when App Portal writes applications that need to be migrated as computer variables. This value sets the number of digits used in variable names. For example: ● If this field is set to **2** and App Portal has to write three applications, then the variables App Portal would write would be COALESCEDAPPS01, COALESCEDAPPS02, COALESCEDAPPS03. ● If this field is set to **3** and App Portal has to write three applications, then the variables App Portal would write would be COALESCEDAPPS001, COALESCEDAPPS002, COALESCEDAPPS003. ...and so forth.

Table 3-40 • OS Deployment Tab Properties

Property	Description
Coalesce digits for OSD variable (packages)	This setting, which works in conjunction with the **Base package variable name** PACKAGES, is used during OS deployment when App Portal writes packages that need to be migrated as computer variables. This value sets the number of digits used in variable names. For example: ● If this field is set to **2** and App Portal has to write three packages, then the variables App Portal would write would be PACKAGES01, PACKAGES02, PACKAGES03. ● If this field is set to **3** and App Portal has to write three packages, then the variables App Portal would write would be PACKAGES001, PACKAGES002, PACKAGES003. ...and so forth.
Use single task sequence for capture and deployment	Determines whether both the source and target computers are inserted into the same collection for side-by-side migrations. *Important • If this option is used, you must properly configure your task sequence to perform only specific steps based on computer variable values. Failure to do so can result in the source computer being reimaged!*
Overwrite existing resources for computer import	You could select this option to overwrite existing resources for computer import. However, for operating system deployments, leave this option unselected.
Task sequence collection cleanup status IDs	Identifies the status IDs that would cause the removal of a computer from the task sequence collections. The use case is that the computer is not removed from the collection at an early enough stage to prevent the task sequence from rerunning after the computer is rebooted. *Note • You also need to select the **Remove from collection when complete?** option on the **Deployment > Global** tab of the Catalog Properties dialog box.*

Altiris Tab

You specify Altiris Client Management Suite settings on the **Deployment > Altiris** subtab of the **Settings** view, which is opened by selecting **Settings** under **Site Management** on the **Admin** tab.

Figure 3-69: Settings > Deployment View / Altiris Tab

The **Altiris** subtab includes the following properties:

Table 3-41 • Settings > Deployment View / Altiris Tab

Property	Description
Central Site Server	Enter the machine name of the Altiris Notification Server. Make sure that ASDK is installed on this machine.
Central Site Database Server	Enter the machine name where the Altiris Notification Server database resides.
Central Site Database Name	Enter the database name of the Altiris Notification Server database.
Test	Click to test the connection settings that are entered. If the test is successful, the message [SERVER_NAME] settings are valid appears.

Table 3-41 • Settings > Deployment View / Altiris Tab

Property	Description
User / Computer relationship	Specify the user/computer relationship that App Portal needs to use by selecting one of the following options: • **Use last logon user**—Use the last logon user. • **Use User Affinity**—Use the primary device assigned to user.
Computer Collection Folder	Enter the name of the folder to use to create App Portal computer filters.
User Collection Folder	Enter the name of the folder to use to create App Portal user filters.
Advertisement Folder	Enter the name of the folder to use to create App Portal advertisements.
Policy Folder ID (GUID)	Enter the Policy Folder GUID that App Portal will use to search for policies to attach to a catalog item.
Policy Changed Collection Update Offset	Enter the number of minutes duration to wait after a device is added to a collection before initiating a policy update.
Use Central Site for All Deployments	This option is always selected, because App Portal only communicates with the central site.
Update Machine Policy on Altiris Management Agent	After adding the user/computer to a filter for deployment, App Portal can update the policy on the Altiris Management Agent on the client to receive the deployment. However, in order to do this, the App Portal system account needs remote WMI access on all the machines. If the remote WMI permissions are granted, enable this option to allow App Portal to remotely update client policy.

Custom Policy Status SQL Query	Enter an SQL query to override the built-in App Portal deployment status checking SQL command for policy based deployments.
	
	For example, you could use the following SQL query:
	
	`select Status from Evt_AeX_SWD_Execution where AdvertisementId =`
	`  'PolicyGUID' and _ResourceGuid = 'ComputerResourceGUID'`
	
	📄
	
	Note • PolicyGUID and ComputerResourceGUID should be replaced with actual values.
	
	One of the following status texts will be returned:
	
	• **Success**—Command executed, successfully
	
	• **Failure**—Failed, Terminated

Table 3-41 • Settings > Deployment View / Altiris Tab

Property	Description
Custom Policy Status SQL Connection String	Enter the connection string of the SQL Server database for the **Custom Policy Status SQL Query** that you entered. If empty, App Portal will use the default notification server database. For example, you could use the following SQL query: `Data Source=`*`DBServer`*`;Initial Catalog=`*`DBName`*`;Integrated Security=True` *Note • DBServer and DBName should be replaced with actual values.* *Important • The App Portal system account must have read access to the database. If none is provided, it defaults to the CMS database*

AirWatch Tab

With App Portal, you can deliver a universal enterprise app store: both desktop and mobile applications together. You can connect App Portal to an AirWatch server and create catalog items for Apple iOS and Google Android mobile apps, both internal and public store. This gives you license compliance, deployment automation, and control.

You specify AirWatch settings on the **Deployment > AirWatch** subtab of the **Settings** view, which is opened by selecting **Settings** under **Site Management** on the **Admin** tab.

Note • Users and from AirWatch will be synced to App Portal during the normal sync process.

Figure 3-70: Settings > Deployment View / AirWatch Tab

The **AirWatch** tab includes the following properties:

Table 3-42 • Settings > Deployment View / AirWatch Tab

Property	Description
AirWatch URL	Enter the URL to your instance of AirWatch.
User Name	Enter the **User Name** to your AirWatch instance.
Password	Enter the **Password** to your AirWatch instance.
API Key	Enter the key that was provided to you by AirWatch.
Test	Click to test connection settings. If successful, the following message is displayed: `AirWatch Server settings are valid.`

Table 3-42 • Settings > Deployment View / AirWatch Tab

Property	Description
Success status values **Failure status values**	When App Portal publishes a request to AirWatch, AirWatch returns a status message to indicate success or failure of the deployment: • **Success**—AirWatch returns `Installed` or `Managed`. • **Failure**—AirWatch returns `NotInstalled`. If, at some future time, AirWatch changes their status messages to something different, you can update these values. If you enter new values, enter the values in pipe-delimited format, such as: `Installed|Managed`

Casper Tab

With App Portal, you can deliver a universal enterprise app store that includes both Windows and Macintosh OS X desktop applications. You can connect App Portal to a JAMF Casper Suite 9.6.4 server and create catalog items for OS X desktop applications. This gives you license compliance, deployment automation, and control.

You specify Casper settings on the **Deployment > Casper** subtab of the **Settings** view, which is opened by selecting **Settings** under **Site Management** on the **Admin** tab.

Important • *In order for App Portal to be successfully integrated with Casper, your Casper account needs to have a specific set of minimum permissions. For more information, see* Required Casper Account Permissions.

Figure 3-71: Settings > Deployment View / Casper Tab

The **Casper** tab includes the following properties:

Table 3-43 • Settings > Deployment View / Casper Tab

Property	Description
Casper URL	Enter the URL to your Casper server.
	📄
	Note • App Portal and Casper communicate using Casper's JSS API. By default, Casper uses port 8443 for inbound SSL traffic to the JSS. You will need to include the port number in the Casper URL when configuring your settings. If you have modified the inbound SSL port within your JSS configuration, specify your custom port number in the Casper URL.

Table 3-43 • Settings > Deployment View / Casper Tab (cont.)

Property	Description
User Name	Enter the **User Name** to your Casper server.
Password	Enter the **Password** to your Casper server.
App Portal policy folder	Enter the folder/category in Casper under which the policies created by App Portal will reside.
Policy template name	Enter the name of the policy in Casper which can be used as a template.
Computer group template name	Enter the name of the static group in Casper which can be used as a template.
Test	Click to test the connection settings.
Casper XPath Mapping	This area of provides a means for you to adapt to changes to the Casper APIs that may occur in future releases of Casper.
	App Portal uses these XPaths to access values from the API results sent from Casper. If any of these change in the Casper API in the future, you can make the corresponding necessary changes here.
	There is no need to modify these XPath mapping settings. But, If, at some future time Casper changes their XPath mapping settings to something different, you can update these values by editing the fields in this area.

Table 3-43 • Settings > Deployment View / Casper Tab (cont.)

Property	Description
Casper Machine Name Configuration	The **Casper Machine Name Configuration** area of the **Casper** tab provides a means for you to change user computer mappings that App Portal utilizes for Casper. By default, App Portal maps to Casper using email addresses. Changing the mapping lets you map to Casper with **UserName** Or **FullName** Or **DisplayName**. In some environments, the user name has a unique ID which helps uniquely identify each user. If you enter additional properties in the **Casper Machine Name Configuration** section and a sync is performed, the Macintosh machine name will get appended with the additional properties and the entire string will be treated as a machine name. For example: ● If the Macinstoch machine name is **MacABC** and you have configured an additional property as **mac_address** then the machine name will be the entire string: **MacABC; 0C:4D:E9:CD:EC:C4**. ● If you have configured the additional property as **serial_number,udid** then the machine name will look similar to the following: **MacABC; C07NG0W4DWYL; AEB468FF-904B-5D76-8167-392761E942CD.** 📄 *Note • When checking out Casper catalog items, the mapping to Casper must be considered when specifying the machine name. Consider the following steps:* 1. Select the **Enable request to manual list?** option for a Casper catalog item. 2. On the resulting **Choose Target** panel of the **Checkout** view (available for requesters who have been assigned the Request to Manual list), select the **Add machine names or user IDs manually** option. 3. On the **Checkout** screen where you **Enter Target /Users**, enter the Macintosh name in the format that corresponds to the currently configured mapping to Casper. When additional properties are specified in the **Additional properties for device sync** field of the **Casper Machine Name Configuration** section (in the **Casper** tab of the **Site Management > Settings > Deployment** view), then the machine name must be entered as the entire string in a format such as **MacABC; 0C:4D:E9:CD:EC:C4** or **MacABC; C07NG0W4DWYL; AEB468FF-904B-5D76-8167-392761E942CD** depending on the additional properties you specified.

MobileIron Tab

You can connect App Portal to a MobileIron server and create catalog items for Apple iOS and Google Android mobile applications. This gives you license compliance, deployment automation, and control.

You specify MobileIron settings on the **MobileIron** tab of the **Site Management > Settings > Deployment** view.

You specify MobileIron settings on the **Deployment > MobileIron** subtab of the **Settings** view, which is opened by selecting **Settings** under **Site Management** on the **Admin** tab.

📄

Note • For more information, see Entering MobileIron Settings.

Figure 3-72: Settings > Deployment View / MobileIron Tab

The **MobileIron** tab includes the following properties:

Table 3-44 • Settings > Deployment View / MobileIron Tab

Property	Description
MobileIron URL	Enter the URL to your MobileIron server.
User Name	Enter the **User Name** to your MobileIron server.
Password	Enter the **Password** to your MobileIron server.
Test	Click to test the connection settings.

Flexera Integration

You enter Flexera Service Gateway, FlexNet Manager Suite, ServiceNow, Remedy, Orchestrator Service, and Workflow Manager settings on the **Site Management > Settings > Flexera Integration** view on the **Admin** tab.

Figure 3-73: Settings > Flexera Integration View

The **Site Management > Settings > Flexera Integration** view includes the following properties.

Table 3-45 • Settings > Flexera Integration View

Property	Description
Enable App Portal API	Select to enable the App Portal API (`http://server/esd/api.asmx`) to be accessible. By default, this option is not selected. 📄 *Note • You should modify NTFS permissions on the* `api.asmx` *file to prevent unauthorized access prior to enabling the API.*
Enable Advanced License Check with FlexNet Manager Suite	Select this option to instruct App Portal to consider not only available licenses during license check, but also second use rights, upgrade/downgrade rights, and exemption by device role rights (such as an MSDN subscription), all based upon information stored in FlexNet Manager Suite. For more information, see Performing Advanced License Check.
Flexera Service Gateway Server Name	If you have also purchased FlexNet Manager Suite, you can use App Portal to manage application licenses. App Portal communicates with FlexNet Manager Suite via the Flexera Service Gateway component. To connect App Portal to the Flexera Service Gateway, enter the name of your Flexera Service Gateway server.
FNMS Tenant UID (MSP Only)	If using a multi-tenant instance of FlexNet Manager Suite, enter the FlexNet Manager Suite UID, a value that uniquely identifies a tenant in a multi-tenant instance of FlexNet Manager Suite.
FlexNet Manager Suite Cloud Settings	If you are integrating App Portal with FlexNet Manager Suite Cloud, enter the access token that was provided by your system administrator in the F**lexNet Manager Suite Cloud Access Token** field.
FlexNet Manager Suite On-Premises Settings	If you are integrating App Portal with FlexNet Manager Suite On Premises, and your App Portal system account does not have access to FlexNet Manager Suite On Premises, enter a **Username** and **Password** with appropriate credentials.
FlexNet Manager Suite Database Connection Settings	In order to use the **My Apps** feature, the App Portal system account needs to have read access to the FlexNet Manager Suite database. First, enter the **Database Server Name** and **Database Name** of the FlexNet Manager Suite database. Then, use Microsoft SQL Server Management Studio and give the App Portal system account read access to this database.
Enable My Apps Feature?	Select this option to enable the **My Apps** tab, where users can view a list of all of the applications installed on their device(s) and address automatic and administrator-defined alerts to ensure that those applications comply with corporate software policies. 📄 *Important • In order to enable the **My Apps** tab, you must be also connected to FlexNet Manager Suite via the Flexera Service Gateway. For more information, see Enabling the My Apps Tab.*

Table 3-45 • Settings > Flexera Integration View

Property	Description
Enable My Apps Email Notifications?	Select this option to instruct App Portal to automatically send out an email notification to users each time an alert is generated for one of their installed applications.
Smart Uninstaller is deployed for License Reclamation?	Select this option to automatically include the `AppPortal.SmartUinstall.exe` file with deployed Windows Installer packages so that they could be automatically uninstalled as part of a license reclamation even an uninstallation program was not defined in the deployment technology for that application. *Note • Valid option for Windows Installer packages only.* *Note • For more information, see Configuring SmartUninstall in Your System Center Configuration Manager Environment.*
License Reclamation Threshold	Identify the number of days that applications need to be unused in order to trigger the generation of an unused software alert, prompting users to either keep or uninstall the application.
Bypass Question for uninstall checkout	Select this option to specify that if a user is submitting a request for the uninstall of a catalog item, they will not be prompted to answer the catalog item's associated questions.
Workflow Manager URL	You can configure an App Portal catalog item so that a Workflow Manager workflow request is automatically created when that catalog item is requested. In this field, enter the URL to the Workflow Manager site that a user will be redirected to when they request a Workflow Manager-associated catalog item. *Note • When the Workflow Manager workflow request is completed, the status of the request in App Portal changes to* **Complete***.*

ServiceNow Integration

You enter ServiceNow settings on the **Site Management > Settings > ServiceNow Integration** view on the **Admin** tab.

ServiceNow Integration

ServiceNow Integration

ServiceNow Instance URL (e.g. https://instance.service-now.com)   `https://ven01764.service-now.com/`

ServiceNow User Name   `admin`

ServiceNow Password   `••••••••••••••••••`

Test   Create Default ITSM Operations

ServiceNow Requested Item State Mapping

App Portal Status	ServiceNow Requested Item State
Pending	`2`
Success	`3`
Failure	`4`

Test

ServiceNow Request State Mapping

Update ServiceNow Request State   ☐

App Portal Status	ServiceNow Request State
Pending	`in_process`
Success	`closed_complete`
Failure	`closed_incomplete`

Test

ServiceNow Employee App Provisioning

ServiceNow Employee App Provision Requests data table   `x_fls_appportal_task_sequence_requests`

Click on Delete Employee App Provision Operations button to edit Employee App Provision Requests data table name.

Test   Delete Employee App Provision Operations

ServiceNow Catalog Item Integration

Sync catalog items with ServiceNow   ☑

ServiceNow Variable Set Name   `App Portal Variable Set`

ServiceNow Import Set table for saving App Portal catalog details   `x_fls_appportal_import_service`

Click on delete catalog operations button to edit Import set table name.

Test   Delete Catalog Operations and Mapping

Enable all software catalog items to sync with Service Now   Enable

ServiceNow Catalog Operations

Import Set create operation   `Create ServiceNow Request For Cloud`

Import Set update operation   `Update ServiceNow Task Sequence Request`

Import Set delete operation   `Archive ServiceNow Import Set Record`

Sync Catalog Now

Figure 3-74: Settings > ServiceNow Integration View

App Portal / App Broker offers three types of integration with ServiceNow, and the settings that you need to configure on the ServiceNow Integration view depend upon which integration methods you are implementing and whether or not you have purchased App Broker.

Table 3-46 • ServiceNow Integration View Settings Areas

Product	Task	Areas in ServiceNow Integration View to Configure
App Portal	Creating incidents in ServiceNow Creating requests for cloud accounts in ServiceNow	• ServiceNow Integration
App Broker for ServiceNow	Requesting catalog items from ServiceNow UI	• ServiceNow Integration • ServiceNow Request State Mapping • ServiceNow Catalog Item Integration • ServiceNow Catalog Operations
	Requesting OSD task sequence catalog items from Employee App Provision Request Wizard in ServiceNow	• ServiceNow Integration • ServiceNow Employee App Provisioning

The **Site Management > Settings > ServiceNow Integration** view includes the following properties

Table 3-47 • Settings > ServiceNow Integration View

Area / Property		Description
ServiceNow Integration	**ServiceNow Instance URL**	Enter the URL of your ServiceNow instance in the following format: `https://`*yourinstance*`.service-now.com` **Important •** *Do not use any special characters in the URL field. The only special character that is permitted is _ (underscore). Dashes (-) and other special characters are not permitted.*

Table 3-47 • Settings > ServiceNow Integration View

Area / Property		Description
	ServiceNow User Name	Enter your ServiceNow user account name. ***Important •*** *The account used to connect to ServiceNow must have access to invoke web methods in ServiceNow. This account also needs to have been granted the following ServiceNow permissions:* • `Itil` • `soap_create` • `soap_query_update` • `soap_script`
	ServiceNow Password	Enter your ServiceNow password.
	Test	Click to test the connection to the ServiceNow instance.
	Create Default ITSM Operations	Click to create the ITSM operations in App Portal for the Incident Management and Request Management features in ServiceNow.
ServiceNow Item State Mapping	**App Portal Status / ServiceNow Requested Item State**	This section provides support to update the Requested Item (RITM) state in ServiceNow according to status transition in App Portal with respect to an individual catalog requested item (along with the existing ServiceNow Request Status changes).
ServiceNow Request State Mapping	**Update ServiceNow Request State**	Enabling this checkbox will update the ServiceNow Request State of ServiceNow Catalog with respect to the mapping of the App Portal request status. When this checkbox is unchecked, this mapping configuration is ignored. Currently there is limitation of this checkbox setting, as it will work efficiently when there is single catalog requested in ServiceNow.

Table 3-47 • Settings > ServiceNow Integration View

Area / Property	Description
App Portal Status / ServiceNow Request State	In this area, you can map App Portal request status to ServiceNow request state. App Portal / App Broker can only return three different statuses to ServiceNow: • **Pending** • **Success** • **Failure** You can manually map the above App Portal request statuses to ServiceNow request states. In the **ServiceNow Request Status** fields, enter the ServiceNow state that App Portal status maps to. For example, ServiceNow could have the following defined states: • Pending Approval • Approved • Closed Complete • Closed Incomplete • Closed Canceled • Closed Rejected • Closed Skipped In this case, you could enter **Pending** in the **Pending** field, **Closed Complete** in the **Success** field, and **Closed Incomplete** in the **Failure** field. Click **Test** to test the configuration of the ServiceNow state mapping with the App Portal status. *Note • Whenever you get updates from System Center Configuration Manager (such as a successful or failed deployment), you could update the request state in ServiceNow (as defined by the administrator).*

Table 3-47 • Settings > ServiceNow Integration View

Area / Property		Description
ServiceNow Employee App Provisioning	**ServiceNow Employee App Provision Requests data table**	Specify the table where request data from the ServiceNow Employee App Provision Request wizard will be stored:
		`x_fls_appportal_task_sequence_requests`
		The data in this table will be pushed to the App Portal database with the help of a ServiceNow workflow.
	Test	Click to test the connection to the table.
	Create Employee App Provision Operations	Click to create operations in App Portal for the Employee App Provision Request wizard. The **ServiceNow - Update Task Sequence Request Management Service** would then added to App Portal and listed on the **Site Management > ITSM Integration** view.

Table 3-47 • Settings > ServiceNow Integration View

Area / Property		Description
ServiceNow Catalog Item Integration	**Sync catalog items with ServiceNow**	Select this option to automatically sync all new catalog items to the connected ServiceNow catalog. The catalog items will be synced in a background task.
	ServiceNow Variable Set Name	Enter `App Portal Variable Set` in this field.
		The variables defined in this variable set determine what fields are displayed in ServiceNow when requesting an App Portal catalog item in the standard ServiceNow interface.
		By default (with App Broker integration with ServiceNow), the App Portal Variable Set contains a drop down for the user to select which computer they would like to deploy the software to.
		If you want to display more options on this screen, perhaps to collect more information from the user during ServiceNow checkout (such as answering questions, uploading documents, or selecting an approval manager), you can create your own variable set, as long as it contains a variable named **election** that prompts the requester to select a device from a drop-down list.
	ServiceNow Import Set table for saving App Portal catalog details	Enter the following import set table name in this field:
		`x_fls_appportal_import_service`
		An App Portal-provided "transformer" transforms uploaded App Portal catalog item data and inserts it into this master catalog item table in ServiceNow.
		Note • If you would like to create your own import set table that points to your own "transformer" (to transform data the way that you want it to be transformed), specify the name of that import set table in this field.
	Test	Click to validate the entries.

Table 3-47 • Settings > ServiceNow Integration View

Area / Property		Description
ServiceNow Catalog Item Integration (Continued)	**Create Catalog Operations**	Click to create ServiceNow catalog operations. The **ServiceNow - Catalog Import Set Management Service** would then be listed on the **Site Management > ITSM Integration** view.
	Enable all software items to sync with ServiceNow	For existing App Portal customers who already have defined catalog items, click **Enable** to sync all existing catalog items with the ServiceNow catalog. If do you not click this button, only new and updated catalog items will be synced.
ServiceNow Catalog Operations	Enter the names of the ServiceNow operations that create, update, and delete a ServiceNow Import Set. 📄 *Note • These fields are only displayed after you click **Create Catalog Operations** under **ServiceNow Catalog Item Integration**.*	
	Import Set create operation	By default, this value is `Create ServiceNow Import Set Record`.
	Import Set update operation	By default, this value is `Update ServiceNow Import Set Record`.
	Import Set delete operation	By default, this value is `Delete ServiceNow Import Set Record`.
	Sync Catalog Now	Click to sync ServiceNow with the App Portal catalog.

3rd-Party Integration

You enter proxy, BMC Remedy, and System Center Orchestrator settings on the **Site Management > Settings > 3rd-Party Integration** view on the **Admin** tab.

Figure 3-75: Settings > 3rd-Party Integration View

The **Site Management > Settings > 3rd-Party Integration** view includes the following properties.

Table 3-48 • Settings > 3rd-Party Integration View

Property	Description
Proxy Settings	If you are using a proxy server to connect to another application, such as ServiceNow, enter the following: ● **Proxy Server Name**—Enter the proxy server name, such as PROXY.APPPORTAL.FLEXDEV.COM. ● **Proxy Server Port**—Enter the port used for the proxy server. ● **By Pass Proxy for Local Address**—Select this option if you want to bypass the proxy server for local addresses.

Table 3-48 • Settings > 3rd-Party Integration View

Property	Description
Remedy Integration	If you are integrating App Portal with the BMC Remedy ITSM system, enter the following: • **Remedy Instance**—Enter the URL of your Remedy instance in the following format: `http://yourinstance:0000/arsys/WSDL/public/yourinstance` • **Remedy User Name**—Enter your Remedy user account name. • **Remedy Password**—Enter your Remedy password. *Note • In App Portal 2015, you were required to enter a URL for both the Remedy Incident Create URL and the Remedy Incident Query URL. Starting with App Portal 2015 R2, you only need to enter a Remedy Instance URL in order to create a connection to both the Remedy incident and request systems.* *Important • Do not use any special characters in the URL fields. The only special character that is permitted is _ (underscore). Dashes (-) and other special characters are not permitted.*
Orchestrator Service URL	If you want to integrate App Portal with the Microsoft System Center Orchestrator workflow tool, enter the URL to this tool.

Cloud Apps

If you integrate App Portal with a cloud application, App Portal will be able to include a catalog item that, when checked out on the Browse Catalog tab, will automatically create an account in that cloud application for the requester. The requester will then receive an email that includes account login details.

App Portal provides out-of-the-box support for three cloud applications: Box, Salesforce, and Microsoft Office 365. App Portal will automatically create the following three "cloud application" catalog items.

Figure 3-76: Out-of-the-Box Cloud Catalog Items

To enable this feature, you need to connect App Portal to these cloud applications on the **Site Management > Settings > Cloud Apps** view.

Important • *Because some of the settings need to be stored locally, when you enter cloud application connection settings, you must be on the machine where App Portal is installed.*

Obtaining the Credentials

Your first step in enabling App Portal support for cloud applications is to create a custom cloud application for your organization on the cloud application vendor's website. You will obtain the credentials and end points required to integrate App Portal with that cloud application. For information, see the following sites:

Table 3-49 • Cloud Application Vendor Links

Cloud Application Vendor	Help Topic
Box.com	https://box-content.readme.io/docs/box-platform
Salesforce	http://www.salesforce.com/platform/getting-started/
Microsoft Office 365	http://dev.office.com/

Entering Connection Settings

You enter connection settings to Box, Salesforce, and Microsoft 365 cloud applications on the tabs of the **Site Management > Settings > Cloud Apps** view.

Figure 3-77: Cloud Apps View

Then, after you enter the initial connection settings on one of the these tabs, you will need to generate an access token and then generate default operations.

On the tabs of the **Site Management > Settings > Cloud Apps** view, you need to enter connection settings, which you will obtain when you create your corporate account with the cloud application vendor:

- Box Tab

- Salesforce Tab

- Office 365 Tab

Box Tab

You enter connection settings to Box on the **Box** tab of the **Site Management > Settings > Cloud Apps** view.

Figure 3-78: Cloud Apps / Salesforce Tab

On the **Box** tab of the **Cloud Apps** view, you need to enter the following properties, which were obtained when your corporate Box account was created:

Table 3-50 • Settings > Cloud Apps View / Box Tab

Property	Description
ClientID	Enter the client ID that was provided to you by Box.
Client Secret	Enter the client secret code that was provided to you by Box.
Redirect Url	Enter the redirect URL that was provided to you by Box. The redirect endpoint is the endpoint in the client application where the resource owner is redirected to, after having granted authorization at the authorization endpoint.
Authorization end point	Enter the endpoint on the authorization server where the resource owner logs in, and grants authorization to the client application.
Token end point	Enter the endpoint on the authorization server where the client application exchanges the authorization code, client ID and client secret, for an access token.
Api Url	Enter the API URL for Box.

Table 3-50 • Settings > Cloud Apps View / Box Tab

Property	Description
Save and Generate Access Token	Click to generate the access token for Box. A message box will open stating that the Box credentials were saved successfully, and prompting you to perform additional tasks to generate a token. Click **OK** on the dialog box. A web page will then open where you will be prompted to grant access to Box. Enter your user ID and password to Box, and then click the **Grant access** button. A message will then appear in App Portal confirming the successful creation of the access token: The access token is saved in the App Portal database. Whenever a Box account is requested, App Portal will use this token to authenticate the user.
Generate default operations	After you click the **Save and Generate Access Token** button, click this button to generate the default operations for Box. A message will open stating that the operations were created successfully. 📄 **Note •** *Optionally, you can open the Site Management > Cloud Integration view to view the default operations that were created.*

Salesforce Tab

You enter connection settings to Salesforce on the **Salesforce** tab of the **Site Management > Settings > Cloud Apps** view.

Figure 3-79: Cloud Apps / Salesforce Tab

On the **Salesforce** tab of the **Cloud Apps** view, you need to enter the following properties, which were obtained when your corporate Salesforce account was created:

Table 3-51 • Settings > Cloud Apps View / Salesforce Tab

Property	Description
ClientID	Enter the client ID that was provided to you by Salesforce.
Client Secret	Enter the client secret code that was provided to you by Salesforce.
Redirect Url	Enter the redirect URL that was provided to you by Salesforce. The redirect endpoint is the endpoint in the client application where the resource owner is redirected to, after having granted authorization at the authorization endpoint.
Authorization end point	Enter the endpoint on the authorization server where the resource owner logs in, and grants authorization to the client application.
Token end point	Enter the endpoint on the authorization server where the client application exchanges the authorization code, client ID and client secret, for an access token.
Api Url	Enter the API URL for Salesforce.

Table 3-51 • Settings > Cloud Apps View / Salesforce Tab

Property	Description
Save and Generate Access Token	Click to generate the access token for Salesforce. A message box will open stating that the Salesforce credentials were saved successfully, and prompting you to perform additional tasks to generate a token. The page at localhost says: Salesforce credentials saved successfully. 1) On click of 'OK' button, you will be taken to a Salesforce web page to authorize Access and Refresh token generation. 2) Enter the Admin credential and click on Sign in button. 3) You will then be redirected back to App Portal page with a message confirming successful generation of the tokens Note: Pop-ups may be blocked on your browser. Update the browser settings to enable pop-ups for the App Portal site. ☐ Prevent this page from creating additional dialogs. OK Click **OK** on the dialog box. A web page will then open where you will be prompted to grant access to Salesforce. Enter your user ID and password to Salesforce, and then click the **Grant access** button. A message will then appear in App Portal confirming the successful creation of the access token: Save and Generate Access Token (Access and Refresh Tokens generated Successfully.) Generate default operations The access token is saved in the App Portal database. Whenever a Salesforce account is requested, App Portal will use this token to authenticate the user.
Generate default operations	After you click the **Save and Generate Access Token** button, click this button to generate the default operations for Salesforce. A message will open stating that the operations were created successfully. 📄 *Note • Optionally, you can open the Site Management > Cloud Integration view to view the default operations that were created.*

Office 365 Tab

You enter connection settings to Microsoft Office 365 on the **Office 365** tab of the **Site Management > Settings > Cloud Apps** view.

Figure 3-80: Cloud Apps / Office 365 Tab

On the **Office 365** tab of the **Cloud Apps** view, you need to enter the following properties, which were obtained when your corporate Office 365 account was created:

Table 3-52 • Cloud Apps View / Office 365 Tab

Property	Description
Client ID	Enter the client ID that was provided to you by Microsoft.
Client Secret	Enter the client secret code that was provided to you by Microsoft.
Redirect Url	Enter the redirect URL that was provided to you by Microsoft. The redirect endpoint is the endpoint in the client application where the resource owner is redirected to, after having granted authorization at the authorization endpoint.
Authorization end point	Enter the endpoint on the authorization server where the resource owner logs in, and grants authorization to the client application.
Token end point	Enter the endpoint on the authorization server where the client application exchanges the authorization code, client ID and client secret, for an access token.
Api Url	Enter the API URL for Office 365.

Table 3-52 • Cloud Apps View / Office 365 Tab

Property	Description
Save and Generate Access Token	Click to generate the access token for Office 365. A message box will open stating that the Office 365 credentials were saved successfully, and prompting you to perform additional tasks to generate a token.

Click **OK** on the dialog box. A web page will then open where you will be prompted to grant access to Office 365.

Enter your user ID and password to Office 365, and then click the **Grant access** button. A message will then appear in App Portal confirming the successful creation of the access token:

The access token is saved in the App Portal database. Whenever an Office 365 account is requested, App Portal will use this token to authenticate the user.

Property	Description
Generate default operations	After you click the **Save and Generate Access Token** button, click this button to generate the default operations for Office 365. A message will open stating that the operations were created successfully.

📄

*Note • Optionally, you can open the **Site Management > Cloud Integration** view to view the default operations that were created.*

Single Sign On

You can configure single sign-on authentication for your users, enabling them to access the App Portal app store (including the mobile version) on-the-go from locations outside the corporate network or VPN.

Single sign-on is configured on the **Site Management > Settings > Single Sign On** view.

Figure 3-81: Site Management > Settings > Single Sign-On View

On the **Single Sign-On** view, you can specify single sign-on settings for both the standard user interface (**OpenID Connect**, **OAuth 2.0**, **SAML 2.0**, and **Custom**) and the mobile user interface (**SAML 2.0** only).

App Portal supports for the following authentication types:

Table 3-53 • App Portal's Supported Authentication Types

Interface	Authentication Type	Description
Standard User Interface	**None**	When single sign-on is not enabled, Windows Authentication is used.
	SAML 2.0	SAML (Security Assertion Markup Language) 2.0 is an XML-based, open-standard data format for enabling web browser single sign-on.
	OAuth 2.0	OAuth is an open standard for authorization, commonly used as a way for users to log in to third party websites using their Google, Facebook, Microsoft, Twitter, etc. accounts without exposing their password.
	OpenID	OpenID is an open standard and decentralized authentication protocol which allows users to be authenticated by co-operating sites (known as relying parties) using a third-party service.
	Custom	To implement a custom single sign-on authentication type, you would need to write a custom SSL page (`.aspx`) to redirect to. App Portal is installed with a boilerplate custom SSL page named `CustomSignon.aspx`, which your services team can customize for your organization.
		Important • When using single sign-on, App Portal needs to be configured to run with anonymous authentication in IIS. By default, Windows Authentication is selected.
Mobile User Interface	**None**	When single sign-on is not enabled for the mobile user interface, forms authentication is used.
	SAML 2.0	SAML (Security Assertion Markup Language) 2.0 is an XML-based, open-standard data format for enabling web browser single sign-on.

The **Single Sign-On** view includes the following properties:

Table 3-54 • Single Sign-On View Properties

Single Sign-On Type	Field	Description
SAML 2.0	**Identity provider certificate**	Click **Browse** select the authentication certificate that you obtained from your identity provider platform.
	Single sign-on URL	Enter the URL that you obtained from your identity provider platform.
	Signature node XPath	The default setting is `//ds:Signature`. Adjust this signature node XPath as needed, per your identity provider platform.

	Attribute node XPath	The default setting is below. Adjust this attribute node XPath as needed, per your identity provider platform.
		
		`/saml2p:Response/saml2:Assertion/saml2:Subject/`
		`saml2:NameID`

	Redirect Url Parameter	The **Redirect Url Parameter** declaration, which is set by default to `RelayState`, is optional extra information that may be sent along with a SAML message. This parameter may specify a URL the service provider should redirect to once single sign-on completes.

Table 3-54 • Single Sign-On View Properties

Single Sign-On Type	Field	Description
OpenID Connect	**Single sign-on URL**	Enter the URL that you obtained from your identity provider platform.
	Authentication request end point	Enter the URL that you obtained from your identity provider platform.
	Client ID	Enter the client ID that you obtained from your identity provider platform.
	Redirect URL	Enter the following: http://*YOURAPPPORTALSERVER*/esd/OpenIdSignOn.aspx
	State	Enter any value that will passed back to App Portal by the identity provider platform post login for validation. The **State** value helps to validate that the correct ID Token is received. Also, this value comes as a Key in the Form element.
	Nonce	Enter any value that will passed back to App Portal by the identity provider platform post login for validation. The **Nonce** value helps to validate that the correct ID Token is received. Also, it is used to mitigate replay attacks.
	Bypass Token Validation	When the client application receives the ID Token from the identity provider platform, it is the responsibility of the client to validate the ID Token. This validation process involves a number of steps which would get performed when the **Bypass token validation** option is not selected. If you want to bypass token validation, select the **Bypass token validation** option.
	Generate "Initiate Login URL"	Click to generate a URL based upon the entered information. Copy this URL, return to the account settings page of your identity provider platform and paste this URL into the **Initiate login URL** field.

Table 3-54 • Single Sign-On View Properties

Single Sign-On Type	Field	Description
OAuth 2.0	Client Id	Enter the ID provided by your identity provider platform.
	Client Secret	Enter the "client secret" provided by your identity provider platform.
	Authorization end point	Enter URL provided by your identity provider platform.

	Call back Url	Enter the following URL:
		
		`http://YOURAPPPORTALSERVER/esd/`
		`oauth2SignOn.aspx?MethodToInvoke=CallBack`

	Scope	Enter URL provided by your identity provider platform.
	Profile end point	Enter URL provided by your identity provider platform.
	Token end point	Enter URL provided by your identity provider platform.
Custom	Single sign-on URL	When you select this option, the settings defined in your custom SSL page are displayed.

Email

You specify default email settings on the **Mail Server** tab of the **Site Management > Settings > Email** view. There are to two subtabs:

- Outgoing Email Subtab
- Incoming Email Subtab

Outgoing Email Subtab

The following shows the **Outgoing Mail** subtab of the **Site Management > Settings > Email.**

Figure 3-82: Site Management > Settings > Email > Outgoing Email (top half of options)

Below the default email settings, is a group of **Email Notification Options**:

Figure 3-83: Site Management > Settings > Email > Outgoing Email (bottom half of options)

The **Site Management > Settings > Email > Outgoing Email** view includes the following properties:

Table 3-55 • Outgoing Email Properties

Property	Description
SMTP Relay Server	IP address or Domain name of SMTP server that will accept relays from the server where App Portal is installed.
SMTP Port	Port for the SMTP server.
SSL	Select this option to use SSL to send email.
SMTP User Name	Enter the SMTP user name. 📄 _____ ***Note •*** *If using Active Directory, leave this field blank.*

Table 3-55 • Outgoing Email Properties (cont.)

Property	Description
SMTP Password	Enter the SMTP password . 📄 _____ **Note •** *If using Active Directory, leave this field blank.*
SMTP Timeout	Seconds to allow for email processing
Email Batch Size	The number of emails processed in each batch
Pause Between Emails	The delay between sending each email to the SMTP server.
Email Retry Count	The number of times to retry failed emails.
Email Retry Delay	The delay between retrying failed emails.
Purge Email History	The number of days to retain email records
Email Prefix	The from field prefix of email messages sent from App Portal **user**@domain.com
Email Suffix	The from field suffix of email messages sent from App Portal user@**domain.com**
HTML Email Format	Decide whether to send email in HTML or plain text. (HTML Recommended)
Enable Custom User View (vCustomUser) for email variables	App Portal allows for a number of email variables to include in email messages. You can have additional email variables for user data by creating a vCustomUser view containing a UserResourceID column. Each column in the view will become an email variable to use in email messages.
Email Address for Site Alerts	Enter any email addresses to send administrative site alerts.
Email Address for Inventory Alerts	Enter any email addresses to send administrative inventory alerts.
Send License Install Alerts	Enable to send alerts to the procurement email list when a licensed application is installed and there are no available licenses.
Send Cancel Email	Select who should receive emails when a request is cancelled. Uses the "Cancelled Request" email template.
Send Request Email	Select who should receive notification when a new request is generated.
Send install success email	Select who should receive notification when an installation is successful.
Send install failure email	Select who should receive notification when an installation fails.

Table 3-55 • Outgoing Email Properties (cont.)

Property	Description
Send accept email	Select who should receive notification when a request is accepted.
Send approval email	Select who should receive notification when a request is approved.
Send reject email	Select who should receive notification when a request is rejected.
Send schedule reminder email	Select this option to send a reminder notification email the indicated number of days prior to the scheduled date.
Send readiness reminder email	Select this option to send a reminder notification email the indicated number of days prior to the start date. Also, enter a number to indicate how often this notification email should be repeatedly sent until the scheduled date is reached.

Incoming Email Subtab

The following shows the **Incoming Mail** subtab of the **Site Management > Settings > Email.** Here, you set up the email settings for a monitoring email service to enable flexible approval. Flexible approval functionality enables flexibility for an approver to approve or reject requests outside the enterprise network and without logging into App Portal. This provides a speedy on-the-go approval (or rejection) process, and subsequent delivery of the request without delays. The monitoring email address is used to receive email approvals or rejections from an approver. Once the **Incoming Email** subtab fields are set, an approver can approve or reject requests by simply replying to an email notification using predefined keywords (e.g., **Approve** or **Reject** or any others that are defined in the keyword notification templates) along with any additional comments. The system further parses through these email responses and takes action of approving or rejecting the request accordingly based on the keyword provided in the reply.

Figure 3-84: Site Management > Settings > Email > Incoming Email

The **Site Management > Settings > Email > Incoming Email** view includes the following properties:

Table 3-56 • Incoming Email Properties

Property	Description
Mail Server Type	The Mail Server type used by the approver: **IMAP** or **POP3**.
Mail Server	The IP address or Domain name of the IMAP or POP3 mail server.
Port	The port for the Mail Server of type IMAP or POP3.
SSL	Select this option to use SSL to receive email. Out of the box, this is enabled.
Email	The email address of the App Portal monitoring mailbox that receives replies from the approver.
Password	The email password of the App Portal monitoring mailbox that receives replies from the approver.
Test	Click the **Test** button to validate **Incoming Email** configurations. This displays the settings along with a message. If settings are valid, the validation message says "`Incoming Email configuration settings are valid.`" If settings are not valid, a validation message says, "`Incoming Email configuration settings are invalid! Please recheck the Server, Port, and SSL details.`"

Table 3-56 • Incoming Email Properties (cont.)

Property	Description
Scanning Interval	The frequency (set in minutes) to monitor the mailbox which receives email responses from the Approver.

Timers

You specify timing intervals on the **Timers** tab of the **Settings** view, which is opened by selecting **Settings** under **Site Management** on the **Admin** tab.

Figure 3-85: Settings View / Timers Tab

The **Timers** tab of the **Site Management > Settings** view includes the following properties:

Table 3-57 • Timers Tab Properties

Property	Description
Reminder email interval for items pending approval	The interval for reminder to approve requests emails (Hours)
New success / failure notification interval	The interval to send new success and failure emails (Minutes)
Low inventory notification interval	The interval to send low license emails (Hours)
Collection cleanup interval	The interval to clean collections (Minutes)
Inventory sync interval	The interval to sync inventory data from the deployment server (Minutes)
Constraint Schedule Cleanup Interval	The interval in which to constrain scheduled cleanups.
Check for new insert collection jobs	The interval in which to check for new collection inserts
Frequency to check for new rerun advertisement jobs	The interval in which to check to rerun advertisements
Frequency to check for new policy refresh jobs	The interval in which to check for new policy refreshes
Delay between policy refresh and collection insert	The delay between inserting a machine into a collection and refreshing the clients policy
Frequency to update last status state	The interval in which to update status data from the deployment server database
Maximum retry time for Advertisement Rerun	If a computer is not online when a rerun job is required the process will stop checking after the elapsed time.
Automatically fail software requests with no status after xx hours	Determines the number of hours to wait without receiving any status messages from the deployment server (after successful collection insert).
Automatically fail software requests with no change in status after xx hours	Determines the number of hours to wait without receiving any change in status from deployment server.
Code execution timer log threshold value	If a service process runs for more than the specified number of seconds, it will be logged in a log file containing the phrase `CodeTimer` and the process name, such as: `CodeTimer_EmailTimer_Elapsed.log`

Table 3-57 • Timers Tab Properties (cont.)

Property	Description
SCCM Application CI_ID Sync Interval	After an System Center Configuration Manager application is added to a catalog item, App Portal will periodically execute the sync cycle to keep the application in sync with any app model property changes that have been made by the System Center Configuration Manager administrator in System Center Configuration Manager. Enter the number of minutes to indicate how often you want to execute the sync cycle.
Time of day to sync users and computers	By default, App Portal syncs its users and computers with its connected deployment technology at 2:00 a.m. each morning. To change the sync time, select a different time from this field. Hours of the day are listed in 24-hour format.

Active Directory

You can disable distribution groups on the **Active Directory** tab of the **Settings** view, which is opened by selecting **Settings** under **Site Management** on the **Admin** tab.

Figure 3-86: Settings View / Active Directory Tab

All other Active Directory integration options, including forest and domain information, are located on the **Site Management > Active Directory > Integration** view. For more information, see Configuring Active Directory Settings.

Wake On Lan

Note • Displayed when connected to a System Center Configuration Manager server.

Wake on LAN (WOL) is supported in App Portal to wake a machine. By default, App Portal will attempt to wake a computer if it is not online by sending a Subnet Broadcast WOL packet. Many networks do not support subnet broadcasting. In those cases we support the System Center Configuration Manager Companion product which uses a peer based WOL.

You specify WOL settings on the **Wake On Lan** tab of the **Settings** view, which is opened by selecting **Settings** under **Site Management** on the **Admin** tab.

Figure 3-87: Settings > Wake On Lan View

The **Site Management > Settings > Wake On Lan** view includes the following properties:

Table 3-58 • Wake On Lan View Properties

Property	Description
Enable SCCM Companion Wake on LAN	Enable System Center Configuration Manager Companion WOL
Path to ICA.exe	The path to the System Center Configuration Manager Companion ICA.exe command line utility.
Companion Server	The server that is running System Center Configuration Manager Companion software.
Companion Port	The port that System Center Configuration Manager Companion listens on for ICA requests.
Enable SCCM Wake on Lan	Enabled System Center Configuration Manager WOL
WOL Port	The port that System Center Configuration Manager listens on for ICA requests.
Packet Type	Select one of the following transmission methods: ● **Unicast** ● **Broadcast** ● **AMT**

Security

You specify security settings on the **Security** tab of the **Settings** view, which is opened by selecting **Settings** under **Site Management** on the **Admin** tab.

Figure 3-88: Settings View / Security Tab

The **Security** tab of the **Site Management > Settings** view includes the following properties:

Table 3-59 • Security Tab Properties

Property	Description
Maximum targets for request on behalf	When requesting on behalf of other users the number of users that can be selected is limited to the value specified.
Maximum items for shopping cart	Limits the maximum number of items that can be requested at one time.

Table 3-59 • Security Tab Properties (cont.)

Property	Description
Limit request on behalf targets to:	**Machines in User's Current OU and Child OUs** When requesting items on behalf of other users, the scope of the target machines will be limited to the machine objects in the user's current OU and child OUs. **Security Group Matching** Uses Active Directory security groups to define a list of authorized users and the scope of authorized machines for which those users can make a request. Security groups require a specific naming convention as follows: ● **Active Directory security group with Name =** `ESD_User_<Identifier>`—Contains the user objects. ● **Active Directory security group with Name =** `ESD_Computer_<Identifier>`— Contains the computer objects authorized for the `ESD_User_<Identifier>` group. For example: User A, User B, and User C in security group `ESD_User_USA` can request on behalf to Computer A, Computer B, and Computer C in `ESD_Computer_USA` security group. **Security Group and Collection Matching** Uses an Active Directory security group to define a list of authorized users, while matching that to a Configuration Manager collection that defines the scope of authorized machines for which those users can make a request. Security groups require a specific naming convention as follows: ● **Active Directory security group with Name =** `ESD_Collection_<CollectionID>`— Contains the user objects ● **Configuration Manager collection with Collection ID =** `<CollectionID>`—Contains the computer objects authorized for the `ESD_ Collection_<CollectionID>` group. For example: User A, User B, and User C in security group `ESD_Collection_SMS00001` can request on behalf to Computer A, Computer B, and Computer C in the Collection ID `SMS00001` (All Systems). *Note • Evaluating collection membership is only supported for a single deployment technology, the deployment technology specified in the **Inventory** field on the **Common** tab of the **Site Management > Settings > Deployment** view.*

Imported Users and Computers

When configuring App Portal, you need to specify which users and groups can view and modify settings on the various App Portal views. You add users and groups and assign permissions to them on the **Admin Security** view of the **Admin** tab, as described in Managing Admin and Catalog Permissions.

You can also view a list of the users, computers, and user-computer relationships that have been imported into App Portal on the **Imported Users and Computers** views, and a list of all users who have unlicensed software installed.

To access these views, select either **Users**, **Computers**, **User Computer Relationships**, or **Users Exceeding Licenses** under **Site Management > Imported Users and Computers**.

- Users View
- Computers View
- User Computer Relationships View
- Users Exceeding Licenses

Users View

On the **Users** view, you can view a list of the users that have been imported into App Portal, as described in Managing Admin and Catalog Permissions.

To access this view, select **Site Management > Imported Users and Computers > Users**

Figure 3-89: Imported Users and Computers / Users View

Computers View

On the **Computers** view, you can view a list of the computers that have been imported into App Portal, as described in Managing Admin and Catalog Permissions.

To access this view, select **Site Management > Imported Users and Computers > Computers.**

Figure 3-90: Imported Users and Computers / Computers View

User Computer Relationships View

On the **User Computer Relationships** view, you can view a list of the user-computer relationships that have been imported into App Portal, as described in Managing Admin and Catalog Permissions.

To access this view, select **Site Management > Imported Users and Computers > User Computer Relationships.**

Figure 3-91: Imported Users and Computers / User Computer Relationships View

Users Exceeding Licenses

On the **User Exceeding Licenses** view, which is only displayed when user-based licensing is being used, you can view a list of all users who have unlicensed software installed. If machine-based licensing is used, this view will not be displayed.

To access this view, select **Site Management > Imported Users and Computers > Users Exceeding Licenses.**

Figure 3-92: Imported Users and Computers / Users Exceeding Licenses View

Logs

You can view a list of the error, email, and debug logs on the **Logs** views.

To access these views, select either **Error Log**, **Email Log**, or **Debug Log** under **Site Management > Logs**.

- Error Log

- Email Log

- Debug Log

Note • For information on the content of log files, see App Portal Logs Reference.

Error Log

The **Error Log** view under **Site Management > Logs** lists all errors generated by the system. You can view and sort these error messages on this view.

Figure 3-93: Error Log View

On the **Error Log** view, you also have the following options:

- **Clear Log**—Click to clear the error list, deleting all error messages.

- **Save Logs**—Click to compress and save the logs for uploading to the Flexera Software Support website. The compressed file will be created in `Exports\AppPortalLogs.zip`.

Note • For information on the content of log files, see App Portal Logs Reference.

Email Log

The **Email Log** view under **Site Management > Logs** list all emails that were sent to users, both those notifying the user of success and of failure. You can view and sort these email messages on this view.

☐	To Address	Date Processed	Status	Attempts Remaining	Priority	Subject
☐	phowe@flexerasoftware.com	11/1/2015 1:27:34 PM	Sent	n/a	0	Your App Portal Order (Order N...

Figure 3-94: Email Log View

On the **Email Log** view, you have the following options:

- **View**—Double click email to view it in the **Email Details** dialog box.

- **Refresh**—Click to refresh the list of emails that have encountered an error.

- **Resend/Retry**—Click to resend the selected email message.

- **Delete**—Click to delete the selected email message.

Note • For information on the content of log files, see App Portal Logs Reference.

Debug Log

When you encounter a particularly complicated issue, one which could be caused by environmental issues and which cannot be easily reproduced on other systems, you may want to turn on App Portal's debug logging, which can be viewed on the **Debug Log** view under **Site Management > Logs**.

Rather than just a log of error messages, a debug log is an exhaustive log of all events—such as actions, methods, stack trace, execution path—and provides a very low level detail of the entire request life cycle of the App Portal web site.

When you turn on debug logging, it is only in effect for the current App Portal user. In other words, if an administrator on Machine A enables debug logging, then App Portal will be logging only requests coming from Machine A.

Important • Because debug logging slows down the system considerably, it should only be turned on when performing troubleshooting, preferably before App Portal is in a production environment.

When debug logging is turned off, the text `Debug logging is currently turned OFF` is displayed in a red band.

Figure 3-95: Debug Log View / Logging Off

When debug logging is turned on, `Debug logging is currently turned ON` is displayed and, if any actions have been taken, methods are listed on the **Debug Log** view.

Figure 3-96: Debug Log View / Logging On

Click **Select** to view the details of individual method log file.

Figure 3-97: Log File Details of a Method

The **Debug Log** view includes the following properties:

Table 3-60 • Debug Log View

Property	Description
Start Log	Click to start debug logging. You will be prompted to enter a title and description of what you are testing. After you have provided that information, the text Debug logging is currently turned ON is displayed.
Stop Log	Click to stop logging. You are prompted to save the session.
Clear Log	Click to clear the view so that the last set of logs are no longer displayed.
Save Logs	Click to save the current log files in a ZIP file so that it could perhaps be sent to product support personnel.
Import Logs	Click to import a log file in .CSV format.
Select	Click to view the details of individual method log file.
Machine	Machine where the logged action took place.
User	User performing the logged action.

Table 3-60 • Debug Log View

Property	Description
Method Name	Method that was used.
Arguments	Arguments that were executed.
Return Value	Value that was returned from the method.

Note • For information on the content of log files, see App Portal Logs Reference.

Active Directory

The **Site Management > Active Directory** view has the following subviews:

- Integration View

- Property Mapping View

- Virtual Properties View

- User Impersonation View

Integration View

You manage Active Directory forests on the **Site Management > Active Directory > Integration** view.

Figure 3-98: Integration View Under Site Management > Active Directory

To enable App Portal to communicate with an additional Active Directory forest, you need to add it by clicking **Add Forest**. The Configure Forest view opens.

Figure 3-99: Configure Forest View

The Configure Forest view includes the following properties:

Table 3-61 • Configure Forest View

Property	Descriptoin
Root Domain Forest Server / Path	Enter the path to the root domain Active Directory forest path that you are adding.
Choose authentication type	Select **Provided Credentials** or **Integrated** to identify the authentication type of this forest.
	If you choose **Provided Credentials**, you also need to enter the appropriate **User name** and **Password**.
Test	Click to test the connection
Save	Click to save your edits.

Deleting a Domain from a Forest

If you do not want one of the listed domains in an Active Directory forest to have access to App Portal, click **Delete** to delete that specific domain.

Figure 3-100: List of Domains in a Forest

For more information, see Configuring Active Directory Settings and Adding an Active Directory Forest.

Property Mapping View

The **Property Mapping** subview of the **Site Management > Active Directory** view includes the **Allow Inventory Allocation** and **Allow Deployment** options.

Figure 3-101: Property Mapping Toolbar

Properties determine the attributes that you want to utilize in App Portal approval, deployment, and provisioning processes. App Portal includes the most common properties.

Allow Inventory Allocation

When an attribute is specified for Inventory Allocation, the attribute will be displayed in the dropdown list for inventory allocation. You should only identify attributes for inventory allocation that represent groups of users. Suitable properties include office and department. Attributes not suitable for inventory allocation include last name, manager, etc. as they typically do not represent groups of users.

Allow Deployment

By enabling a property for deployment you can select this property to view all users that match this property when using the request on behalf of feature. Rather than searching by user or computer selecting a property will show all users and their associated computers for selection.

Virtual Properties View

Virtual Properties allow you to group similar properties together as a single logical name. Virtual properties are used primarily for Inventory Allocation. Future versions will support virtual properties in other areas.

The **Virtual Properties** subview of the **Active Directory** view includes two subviews: **New Virtual Property** and **View Virtual Properties**.

- New Virtual Property

- View Virtual Properties

New Virtual Property

The **New Virtual Property** subview is opened by selecting **Active Directory > Virtual Properties >New Virtual Property** under **Site Management**.

Figure 3-102: New Virtual Property Subview

The **New Virtual Property** subview includes the following properties:

Table 3-62 • New Virtual Property Subview Properties

Property	Description
Virtual Property Name	Specify a logical name that will represent the properties specified in the current property list.

Table 3-62 • New Virtual Property Subview Properties

Property	Description
Property Source	Identify the Active Directory property from where to extract its values. Select one of the following values: • **Active Directory User Property**—Select this option to extract values from an Active Directory user property. If you select this option, you are prompted to select properties by using the arrow keys to move them from the **Available** to the **Current** list. • **User Organizational Unit**—Select this option to extract values from a User Organizational Unit. When you select this option, a tree view of Organizational Units will be displayed in the **Available** area. Click and drag to move properties from the tree to the **Current** list. • **Computer Organizational Unit**—Select this option to extract values from a Computer Organizational Unit. When you select this option, a tree view of Organizational Units will be displayed in the **Available** area. Click and drag to move properties from the tree to the **Current** list.

View Virtual Properties

All virtual properties are listed on the **View Virtual Properties** subview.

Figure 3-103: View Virtual Properties Subview

To edit an existing virtual property, double-click on it. A view similar to the New Virtual Property view opens, where you perform edits.

User Impersonation View

On the **User Impersonation** view, which is opened by selecting **Settings > User Impersonation** under **Site Management**, you can create user impersonation accounts.

Figure 3-104: User Impersonation View

Click **New** or double-click on an existing impersonated account to open the User Impersonation Properties Dialog Box.

User Impersonation Properties Dialog Box

The **User Impersonation Properties** dialog box is opened by clicking **New** or double-clicking on an existing impersonated account on the **Site Management > User Impersonation** view.

Figure 3-105: User Impersonation Properties Dialog Box

The **User Impersonation Properties** dialog box includes the following properties:

Table 3-63 • User Impersonation Properties Dialog Box

Property	Description
Select the account to impersonate	Enter the name of the account you want to impersonate.
Search box	Use the search box to find the accounts that have the permissions that you want to impersonate.
Add Selected Accounts	Select a user in the Search results area and click **Add Selected Accounts** to add the user to the **Current accounts** list.
Current accounts	List of selected users.

ITSM Integration

App Portal includes out-of-the-box integration, via web services, with both ServiceNow and BMC Remedy IT Service Management (ITSM) systems. You can also use App Portal's built-in reusable framework to integrate with other ITSM systems.

You manage ITSM integration on the **ITSM Integration** view, which is opened by selecting **Site Management > ITSM Integration**.

Figure 3-106: ITSM Integration View

For additional information see the following topics:

Table 3-64 • Steps to Integrate with ServiceNow or Remedy

Topic	Description
Connecting to ServiceNow or BMC Remedy and Creating Default Operations	Explains how to connect to your ServiceNow or Remedy instance on the **Site Management > Settings > ServiceNow** or **3rd-Party Integration** view, and how to create default operations.
Editing ITSM Services	Explains how to edit the properties of an existing ITSM web service.
Configuring Operations	App Portal only interacts with a portion of the parameters of each operation: parameters that relate to create, read, update, or delete tasks. Therefore, App Portal automatically defines the parameters associated with those tasks.

This section explains how you can, if desired, edit those parameters or define new parameters on the **Configure Operation** view, which lists all of the parameters associated with the selected operation. |
| **Setting ITSM Actions on Catalog Items** | In order for a catalog item request to trigger an event in an ITSM system, you need to define ITSM-specific actions on that catalog item. This is done on the **Actions** tab of the **Catalog Item Properties** dialog box. |

Table 3-64 • Steps to Integrate with ServiceNow or Remedy

Topic	Description
Deploying via API to Enable App Portal Approvals in an External ITSM System	Explains how to delay deployment of a catalog item until a response from the ITSM system would trigger the deployment via App Portal's API.
Integrating With the ServiceNow User Interface	Explains how to display App Portal within the ServiceNow user interface.
Integrating With Another ITSM System	Explains how to integrate with an ITSM system other than ServiceNow or Remedy.

Cloud Integration

App Portal includes out-of-the-box integration with Box, Salesforce, and Microsoft Office 365 cloud applications. You can also use App Portal's built-in reusable framework to integrate with other cloud applications.

You manage cloud integration on the **Cloud Integration** view, which is opened by selecting **Site Management > Cloud Integration**.

Figure 3-107: Cloud Integration View

For additional information see the following topics:

Table 3-65 • Cloud Integration Topics

Topic	Description
Integrating With Box, Salesforce and Office 365	Explains how to configure out-of-the-box support for Box, Salesforce, and Office 365 cloud applications.
	• Connecting to Box, Salesforce, and Office 365
	• Using Out-of-the-Box Catalog Items for Box, Office 365, Salesforce
	• Creating Cloud Catalog Items to Request Box, Office 365, and Salesforce Access Using ITSM System
Integrating With Other Cloud Applications	Explains how to configure support for other cloud applications.
	• Adding Web Services for a New Cloud Application
	• Adding a New Cloud Application System
	• Adding Operations for Cloud Applications
	• Setting Cloud Application Actions on Catalog Items
Creating a Cloud Catalog Item	Explains how you can use the **New Catalog Item Wizard** to create a cloud catalog item that will obtain an account for the specified cloud application for the requester.
Defining Custom Variables for Cloud Catalog Items	App Portal provides automatically configures Box, Salesforce, and Microsoft Office 365 catalog items with custom variables which are required for the account request to be completed. This section explains how to view and edit these variables on the **Cloud Apps** tab of the **Catalog Item Properties** dialog box.

Categories

Categories are used to organize objects and are defined on several views on the **Admin** tab. Catalog item categories are defined in on the **Catalog Management > Catalog Categories** view.

Figure 3-108: Catalog Categories Subview of Catalog Management

Additional types of categories are specified on the following subnodes of the **Admin** tab.

Table 3-66 • Categories Subnodes

Main Node	Subnode
Catalog Management	• Catalog Categories
Site Management > Categories	• Command Categories • Note Categories
Report Management	• Report Categories • Dashboard Categories
Compliance Management	• Inventory Categories 📄 **Note •** *These categories are not used if you are performing compliance management using the **My Apps** feature, which requires integration with FlexNet Manager Suite.*

Buttons

The **Categories** subviews include the following buttons:

Table 3-67 • Categories Subviews Buttons

Item	Description
Add Category	Enter a name for a new category. If you wish to make the new category a child of an existing category, highlight the category you wish to be the parent before selecting **Add Category**.

Table 3-67 • Categories Subviews Buttons

Item	Description
Delete Category	Deletes the highlighted category. Any request within the deleted category will be moved to the top most category.
Set Category Owner	Use to specify an owner of a category. Category owners can manipulate the items within their categories. Owners access their categories on the **Profile > My Categories** tab.
Set Category Security	To apply security to a category, highlight the category and click **Set Category Security**. Then, on the **Category Security** dialog box, specify the Groups, OUs, property values, or collections you wish to access the category. For more information, see Creating a Catalog Category.

Context Menu Commands

The following context menu (right-click menu) commands are available in the **Categories** subviews:

Table 3-68 • Categories Subviews / Context Menu Commands

Item	Description
Move to root	If you wish to make a child category a root category, highlight the child category and select **Move to root** from the context menu.
Rename	Use to rename a category.
Delete	Use to delete a category.
Set owner	Use to specify an owner of a category. Category owners can manipulate the applications within their categories.
Set security	Use to apply security to a category.

Adjusting Tree Items

You can use the following methods to adjust the items in the tree:

Table 3-69 • Adjusting Tree Items

Method	Description
Use "drag and drop" to re-parent a category	The category tree supports drag and drop. If you wish to move a category to another place in the tree, drag it to the new location and release the mouse button
Direct link	When a category is highlighted the direct URL to that category is presented. When entered, the catalog will display items within that category by default and the category will be selected.

Commands and Actions

Commands allow arbitrary commands to be executed against a selected machine from the **Support Tools** tab in the software store or as part of a request at one or more stages during the request life cycle.

- Client commands and server commands that are executed run under the context of the visiting user and are invoked using JavaScript.

- Server commands run under the context of the App Portal account specified during setup.

- Use of commands executed from the client requires modification of Internet Explorer security settings to allow Active X content.

Commands and actions are defined on the **Site Management > Commands and Actions** view. The **Commands and Actions** view has three subviews:

- Script Commands

- Web Service Commands

- Request Commands

Script Commands

The **Commands and Actions > Script Commands** view lists the current commands and a summary of their settings. Double-click a command name to edit the command.

Figure 3-109: Commands and Actions > Script Commands View

To create a new command, click the **New Command** button. The **New Command** dialog box opens.

Figure 3-110: New Command Dialog Box

The **New Command** dialog box includes the following properties:

Table 3-70 • New Command Dialog Box Properties

Command	Description
Command name	Specify the name of the command. This command name will appear in the menu list.
Command description	Describes the command. The description shows when you hover over the command name in the menu list.
Execute From Server	When this option is selected, the command will be executed from the server using the security context of the service account. Server commands are exposed as actions that can be invoked at different stages during the request process and also on workflow steps. See **Request Management > Request Actions** for global actions and the **Actions** tab when editing a request for request specific actions.

Table 3-70 • New Command Dialog Box Properties

Command	Description
Execute From Client	When this option is selected, the command will be executed from the client using the client's security. The browser must allow client side Active X content.

Command File	Defines the command to execute. Server command files are uploaded to the web server and stored in the `Uploads\Commands` directory. The command accepts numerous variables available listed under the **Command Arguments Variables**.
	
	Sample command syntax is:
	
	• **Client Side Command**:
	
	`ping ##Name0##`
	
	• **Server Side Command**:
	
	`NewMainframeAccount.vbs computer:##Netbios_Name0## user:##User_Name0##`
	
	The following is a sample of a client command on the **Support Tools** tab:

Command Argument Variables	Variables that are available for use in the **Command arguments** field. Select a variable and click **Add** to add the variable to the **Command arguments** field.

Command arguments	Defines the syntax that should be appended after the command file. Available variables are supplied in the drop down lists.
	
	Sample command syntax:
	
	`##Name0##`
	
	`computer:##Netbios_Name0## user:##User_Name0##`

Strip HTML from arguments	Select to remove HTML commands from arguments.
Category	Select a category for the command. The categories appear as menu items as shown for the **Test** category shown in the image above (in the **Command File** description). 📄 *Note • Only available when **Execute From Client** is selected.*

Table 3-70 • New Command Dialog Box Properties

Command	Description
Pick Image	Select an image to represent the command. 📄 *Note • Only available when **Execute From Client** is selected.*
Collection filter	Select a collection to filter the command based on collection membership. The computer must be present in the specified collection for the command to be visible. This is useful for filtering commands based on OS, installed software, or other criteria. 📄 *Note • Only available when **Execute From Client** is selected.*
Visible	Allows you to hide the command without deleting it. 📄 *Note • Only available when **Execute From Client** is selected.*

Web Service Commands

A web service action allows the connection to a web service. Each method can become its own action and its parameters supplied by App Portal Request variables. Web service actions execute just like the command actions.

The **Commands and Actions > Web Service Commands** view lists defined Web Service actions.

Figure 3-111: Commands and Actions > Web Service Commands View

To create a new web service action, click the **New Web Service Command** button. The **New/Edit Web Service Action** dialog box opens. The fields displayed on this dialog box varies depending on the selections you make.

- **Create a new web service / not connected**—If, under **Web Service Action**, you select **Create a new web service**, the following fields are displayed *before* you have specified a valid URL and connected to the service:

Figure 3-112: New Web Service Action Dialog Box / Create a New Web Service / Not Connected

- **Create a new web service / connected**—Under **Web Service Action**, you select **Create a new web service**, the following fields are displayed *after* you have connected to the new web service:

Figure 3-113: New Web Service Action Dialog Box / Create a New Web Service / Connected

- **Use existing web service**—Under **Web Service Action**, if you select **Use existing web service** and select a web service from the list, the following fields are displayed:

Figure 3-114: New Web Service Action Dialog Box / Create a New Web Service / Connected

The **New Web Service Action** dialog box includes the following properties:

Table 3-71 • New Web Service Action Dialog Box Properties

Category	Description
Enter a descriptive name	Provide a unique name for this web service and method.
Provide the URL to the web service	Enter the path to the web service. Do not include ?WSDL as that is automatically appended to the request in order to read its schema.
Select the authentication type	Select one of the following options: ● **Integrated**—Uses the identity of the account specified during setup. ● **Provided**—Enter your own User ID and Password.
Select the web service type	Some web services are complex and require a helper class to allow the customer to easily interact with them. We create or help you create special interfaces as required.
Connect	Click to connect to the specified web service.
Select the desired method	After connecting to the web service you can choose the method to invoke. The method will be examined and the parameters made available.

Table 3-71 • New Web Service Action Dialog Box Properties

Category	Description
Specify the parameters	Each parameter and expected object type is listed. App Portal can pass string and integer values to web services. More complex objects like datasets and arrays are not currently supported.
	Enter static values or variables for the Parameter Value. Enter static values for the Default Value in the case where the value is not available (a blank office value for example). If the web service requires the value and no default is specified an error may occur and prevent processing of the request. Please be careful to add defaults whenever possible.

Request Commands

Request Actions allows custom commands to be executed at stages during the Request life cycle. There are two types of actions that can be invoked across seven stages.

Request Action Types

There are two types of request action types:

- **Command Execution**—Uses a command previously created under **Site Management > Commands and Actions > Request Commands**. Those commands specified as **Execute from Server** are available. When the request stage is processed, the command will be invoked and passed the variables identified in the command.

- **Web Service Action**—Allows the connection to a web service. Each method can become its own action and its parameters supplied by App Portal Request variables. Web service actions execute just like the Command Actions.

Adding an Action

When you have your actions created they can be added to the events during the request life cycle. Select an action and event from the list and choose add to add it to the event tree. These actions will execute when the event completes. A log file for reference of actions is WebServiceAction.log.

Figure 3-115: Site Management > Commands and Actions > Request Commands View

Communication

Information about App Portal communications is organized into the following sections:

- Notifications

- License Reclamation Reasons

- Approve / Reject Reasons

- Languages

- Language Text

- Announcements

- Currency

Notifications

Notifications are emails and messages that are used to communicate status and events to App Portal users. They can be modified to suit your company's language preferences and content.

You view and edit email templates and message text on the **Communication > Notifications** view.

- HTML Email Format Option

- Specifying Notification Language

- Notification Editor

- List of Notification Email Templates and Messages

HTML Email Format Option

HTML formatting of email communication is only enabled if the **HTML Email Format** option is selected on the **Site Management > Settings > Email** view.

Figure 3-116: Enabling HTML Formatting of Emails

Specifying Notification Language

App Portal provides a number of notification messages, in both email and web form, to communicate status and events within the software. These notification messages are customizable in content and language. A number of variables are provided that can be placed in most email templates to offer a wealth of information.

The notifications can be language specific. By default English is the primary language. You can add additional languages to App Portal from the **Communication > Languages** node.

The current language being edited is selected in the **Select a language** list on the **Communication > Notifications** view.

Note • The ***Flexible Approval*** *tab will be enabled only if* ***Incoming Mail*** *server details are configured*

		Custom	Conditions	CC	BCC
Application Survey - Current PC			0	No	No
Application Survey - New PC			0	No	No
Application Survey - Survey Complete			0	No	No
Cancelled Request			0	No	No
Empty search result			0	No	No
Error Message Display			0	No	No
EULA			0	No	No
Help Page			0	No	No
Microsoft Office 365 Account Created Successfully			0	No	No
No SMS Client			0	No	No
Not Licensed			0	No	No
Notes			0	No	No
Reminder to approve requests			0	No	No
Salesforce Account Created Successfully			0	No	No
Software/General Catalog Item Request Order			0	No	No
Submit Request			0	No	No
Welcome			0	No	No

Figure 3-117: Selecting a Language

Notification Editor

You edit a notification in a multi-tabbed editor, which is opened by double-clicking the notification name on the **Notifications** view. This editor consists of four tabs: **Notification**, **Recipients**, **Conditions**, and **Preview**.

- Editing Content on the Notification Tab

- Viewing Source HTML on the Notification Tab

- Setting Recipient Options on the Recipients Tab

- Specifying Conditions on the Conditions Tab

- Previewing an Email Notification on the Preview Tab

Editing Content on the Notification Tab

To edit a notification, double click the notification name to open a multi-tabbed editor.

On the **Notification** tab, you can edit the **Subject** line (if it is an email template) and the notification text. Formatting can be performed using the tool bar.

Variables are inserted by enclosing a variable name in double-hash tags (##VariableName##). On some notifications, information about the inserted variables is listed above the **Subject** line.

Figure 3-118: Editing a Notification

Viewing Source HTML on the Notification Tab

If you prefer to format the notification content using HTML/CSS tags, click the "source" button on the tool bar to display the HTML markup.

Figure 3-119: View HTML Markup Option

Setting Recipient Options on the Recipients Tab

For most email notifications, you can add additional email addresses on the **Recipients** tab. Enter the email addresses one per line in the **CC Addresses** and **BCC Addresses** lists.

Figure 3-120: Email Recipient Options

Specifying Conditions on the Conditions Tab

For most email notifications, you can filter the recipient against membership rules to determine whether the recipient should receive the notification. You add these conditions on the **Conditions** tab.

If a match is found against one of the conditions, then the notification is not sent to the recipient. Recipients include both the requester and target user of the request.

Figure 3-121: Notification Condition

In the above example, if the target user or the requester is in the **Admin User New** Security Group, the notification will not be sent.

Previewing an Email Notification on the Preview Tab

You can view a preview of how an email notification for a specific request will look when viewed by the user by opening the **Preview** tab of the editor dialog box, and entering the numeric ID of a request in the Enter a request ID to preview data box.

Figure 3-122: Preview Tab of Notification Editor Dialog Box

List of Notification Email Templates and Messages

On the **Site Management > Communication > Notifications** view, email templates and system messages are listed on four tabs: **Global**, **Software**, **General**, **License Reclamation**, and **Flexible Approval**.

Table 3-72 • Notifications List

Tab	Notifications	Description
Global	**Application Survey - Current PC**	This text is displayed on the **App Survey** tab; it explains how the user can complete the survey to identify the applications that they want to have redeployed onto their current computer using System Center Configuration Manager OSD.
	Application Survey - New PC	This text is displayed on the **App Survey** tab; it explains how to restore selected applications onto a new computer.
	Application Survey - Survey Complete	This text is displayed on the **App Survey** tab when the user has completed the survey.
	Canceled Request	This is the template for an email notification that is sent out when a user cancels an App Portal request before it is completed.
	Empty search result	This text is displayed when a search on the Browse Catalog tab returns no results.
	Error Message Display	This end user license agreement text is displayed when App Portal experiences an exception and crashes.
	EULA	This text is displayed to the user upon first logon if the **Require EULA?** option on the **Site Management > Settings > General** tab is selected.
	Help Page	The content of this notification is displayed on the **Help** page, which is opened by clicking the help icon on the **Browse Catalog** tab.
	New User Discovery (DDR)	*Note • Not currently used.*
	No SMS Client	*Note • Not currently used.*

Table 3-72 • Notifications List (cont.)

Tab	Notifications	Description
Global (continued)	**Not Licensed**	This text is displayed to the user if the current machine does not belong to a group that has an App Portal license.
	Notes	This email notification is sent out when a note is added to a request on the My Requests tab.
	Reminder to approve requests	This email notification is sent out to an approver that has pending requests to approve.
	Software/General Catalog Item Request Order	This email notification is sent out to the requester when software and/or general catalog items have been requested.
	Welcome	This text is displayed at the top of the **Browse Catalog** tab, above the list of catalog items.
Software	**My Apps - Action Alert Text**	This text is displayed to the user on the **My Current Alerts** subtab of the **My Apps** tab when an administrator has created an Alert Action catalog item that applies to one of the user's installed applications. For example: `Action Alert: You are required to perform an action` **`Uninstall Blacklisted Software`** `for` **`Calculator 6.1.`** `To perform this action, click here.` 📄 **Note •** *Alert Action catalog items are a specialized type of catalog item that uses FlexNet Manager Suite application recognition and licensing data to identify installed application/device combinations that need attention, such as unused applications, unlicensed applications, or applications targeted for another reason. App Portal then sends out alerts to the identified device owners to prompt them to take action to resolve the issues.*
	My Apps - Alert Action Responded Text	This text is displayed to the user on the **My Resolved Alerts** subtab of the **My Apps** tab when an Alert Action was responded to.
	My Apps - Alert Email Notification	This email notification is sent out to an App Portal user when App Portal discovers that the user has compliance alerts.

Table 3-72 • Notifications List (cont.)

Tab	Notifications	Description
Software (continued)	My Apps - License Reclamation Action Responded Text	This text is displayed to the user on the **My Resolved Alerts** subtab of the **My Apps** tab when an Unused Software Alert was responded to.
	My Apps - License Reclamation Alert Text	This text is displayed to the user on the **My Current Alerts** subtab of the **My Apps** tab when App Portal determines that the user has unused software installed on their machine.
	OSD - Unknown Computer Build	When you attempt to deploy an operating system to a computer that is not built yet, App Portal displays this message to you to identify the build ID of the operating system. When you are ready to deploy the operating system to the computer, you would use this build number.
	Software - Approval Required	 **Note** • *This notification is no longer used. It has been replaced by the Software - Request for Approval notification.*
	Software - Data	This email notification identifies the data fields for a particular catalog item request that will be displayed within the following email notifications: ● Software - Request for Approval ● Software/General Catalog Item Request Order The ##RequestData## variable in these email templates will be replaced with the contents of the **Software - Data** notification at runtime.
	Software - Install Failed	This email notification is sent out when the installation of a catalog item has failed. This email identifies the package title, request ID, requester, and target machine.
	Software - Install Successful	This email notification is sent out when the installation of a catalog item has been completed successfully. This email identifies the package title, request ID, requester, and target machine.
	Software - Lease Expiring	This email notification is sent out when a license lease for a software package is about to expire. This email identifies the package title, license expiration date, and target machine.

Table 3-72 • Notifications List (cont.)

Tab	Notifications	Description
Software (continued)	**Software - License notification**	This email notification is sent out when a software package that requires a license has been installed. This email identifies the package title, target machine, requester, and license information.
	Software - No Approval	 *Note • This notification is no longer used. It was replaced by the Software/General Catalog Item Request Order notification, which is the template for an email notification that is sent out to the requester when either a Software or General catalog item has been requested.*
	Software - Request Approved - Auto Delivery	This email notification is sent out to a requester after their request for a catalog item has been approved and the **Allow scheduling immediately after approval?** option is selected on the **General > Global** tab of the **Catalog Item Properties** dialog box for the requested catalog item. This email states that the catalog item will be automatically installed.
	Software - Request Approved - Manual Delivery	This email notification is sent out to a requester after their request for a catalog item has been approved. This email prompts the user to click the **Install** icon to submit an installation request.
	Software - Request for Approval	This email notification is sent out to an approver after a requester has requested a software catalog item which requires approval. This email prompts the approver to either Approve or Reject the request. It also provides a link that enables the approver to review the data that was submitted when the catalog item was requested.
	Software - Request Rejected	This email notification is sent out to a requester after their request for a catalog item has been rejected. This email lists the reason for the rejection and the approver who rejected the request.
	Software - Scheduled Installation - Reminder	This email notification is sent out to a requester to remind them that the software that they requested will be installed on their computer on a specific date.

Table 3-72 • Notifications List (cont.)

Tab	Notifications	Description
Software (continued)	**Software - User Readiness**	This email notification informs a user that their machine is ready for a specific software catalog item to be installed. This email lists the recommended date for installation, and prompts the user to request the catalog item.
	Software - User Readiness - Reminder	This email notification informs a user that they have not yet scheduled the installation of a software catalog item that they have previously been informed that their machine is ready for. This email lists the recommended date for installation, and prompts the user to request the catalog item.
General	**General - Approval Required**	**Note •** *This notification is no longer used. It has been replaced by the General - Request For Approval notification.*
	General - Data	This email notification identifies the data fields for a particular general catalog item request that will be displayed within the following email notifications: ● General - Request for Approval ● Software/General Catalog Item Request Order The ##RequestData## variable in these email templates will be replaced with the contents of the **General - Data** notification at runtime.
	General - No Approval	**Note •** *This notification is no longer used. It was replaced by the Software/General Catalog Item Request Order notification, which is the template for an email notification that is sent out to the requester when either a Software or General catalog item has been requested.*
	General - Request Approved	This email notification is sent out to a requester after their request for a general catalog item has been approved.

Table 3-72 • Notifications List (cont.)

Tab	Notifications	Description
General (continued)	**General - Request For Approval**	This email notification is sent out to an approver after a requester has requested a general catalog item which requires approval. This email prompts the approver to either Approve or Reject the request. It also provides a link that enables the approver to review the data that was submitted when the catalog item was requested.
	General - Scheduled Request - Reminder	This email notification is sent out to a requester to remind them that the general catalog item that they requested will be installed on their computer on a specific date.
	General - User Readiness	This email notification is sent out to a user to inform them that their machine is ready for a specific general catalog item to be installed.
	General - User Readiness - Reminder	This email notification is sent out to a user to inform them that they have not yet scheduled the installation of a general catalog item that they have previously been informed that their machine is ready for. This email lists the recommended date for installation, and prompts the user to request the general catalog item.
	Request for Review	This email notification is sent from an approver to another user to ask them to review a specific request. This email lists the notes associated with the request.
	Request for Review Submitted	This email notification is sent to an approver to inform them that a user has responded to his request to review the request. This email lists the notes associated with the request, and prompts the approver to Approve or Reject the request.

Table 3-72 • Notifications List (cont.)

Tab	Notifications	Description
License Reclamation *Note • These notifications are only used if managing licenses using System Center Configuration Manager. If using FlexNet Manager Suite, license information is displayed on the **My Apps** tab.*	**License Reclamation - ARP Entry only**	This email notification is sent to a user to ask them whether they still require a software application that is installed on their machine, and to inform the user that they have a mechanism to automatically uninstall the application. The user is prompted to either uninstall at a later date, uninstall automatically, or keep the software.
	License Reclamation - Keep Program	This email notification is sent to a user after they have indicated that they would like to keep a software application, and prompts them to click a button to confirm that they want to keep the software.
	License Reclamation - Keep Program - after submit	This text is displayed to the user after they have clicked **Submit** to respond to a **License Reclamation - Keep Program** email.
	License Reclamation - Survey - Keep	This text is displayed to the user to prompt them to confirm that they still use a specific software application.
	License Reclamation - Survey - Remove	This text is displayed to the user to prompt them to confirm that they no longer use a specific software application.
	License Reclamation - Uninstall Program	This text is displayed to a user after they have responded that they want to uninstall a software application, and prompts them to click a button to confirm that they want it to be uninstalled.
	License Reclamation - Uninstall Program - after submit	This text is displayed to the user after they have clicked **Submit** to respond to a License Reclamation - Uninstall Program email.
	License Reclamation - Survey	This email notification is sent to a user to ask them whether they still require a software application that is installed on their machine. The user is prompted to either uninstall or keep the software.
	License Reclamation Notification	This email notification is sent to a user to inform them that they have not used a software application for a specific amount of time, and prompts them to either uninstall at a later date, uninstall automatically, or keep the software.

Table 3-72 • Notifications List (cont.)

Tab	Notifications	Description
Flexible Approval *Note • These notifications are used for flexible approval functionality that enables flexibility for an approver to take approve or reject actions outside the enterprise network and without logging into App Portal.*	**Flexible Approval - Approval Keywords**	This template is not sent to approvers. Instead, it is used to define approval keywords for use in the **General** and **Software** subtab **Request for Approval** templates. Out of the box, **Approved** is displayed. Multiple keywords can be added, with comma separators. Special characters should not be added. The content in this notification template body replaces the variable ##APPROVALKEYWORDS## available in the **Flexible Approval - Keyword Information** email template.
	Flexible Approval - Generic Acknowledgement	This email notification template is sent to an approver when the current user is not the approver or when the approval level is already processed.
	Flexible Approval - Keywords Information	This email notification template is not sent to an approver. Instead, the content in this notification body replaces the variable ##EMAILAPPROVALPLACEHOLDER## in the **General** and **Software** subtab **Request for Approval** templates.
	Flexible Approval - Mailto Links	This email notification template is not sent to an approver. Instead, this notification displays MAILTO links for Approve and Reject as variables ##MAILTOAPPROVE##, ##MAILTOREJECT##. This template is embedded into the **Flexible Approval - Keyword Information** notification template as variable ##EMAILAPPROVALMAILTOLINKS## and is resolved to show the Approve and Reject links.
	Flexible Approval - No Response Acknowledgment Mail	This email notification template is sent to an approver when the approver approves or rejects the request with invalid keywords (e.g., keywords that have not been defined in the **Flexible Approval** - **Approval Keywords** or **Flexible Approval** - **Reject Keywords** notification templates).
	Flexible Approval - Question Template Acknowledgment	This email notification is sent to an approver when the approver approves or rejects a request that contains a question template that has approver questions to answer. Here, the approver has to login to the App Portal website to perform the approval or rejection action after answering the questions.
	Flexible Approval - Reject Keywords	This template is not sent to approvers. Instead, it is used to define rejection keywords for use in the **General** and **Software** subtab **Request for Approval** templates. Out of the box, **Rejected** is displayed. Multiple keywords can be added, with comma separators. Special characters should not be added. The content in this notification template body replaces the variable ##REJECTKEYWORDS## available in the **Flexible Approval - Keywords Information** notification template.

Table 3-72 • Notifications List (cont.)

Tab	Notifications	Description
Flexible Approval (Continued)	**Flexible Approval - Request Already Approved Acknowledgment**	This email notification template is sent to the approver when the approver tries to approve or reject a request that has already been approved.
	Flexible Approval - Request Already Rejected Acknowledgment	This email notification template is sent to the approver when the approver tries to approve or reject a request that already has been rejected.
	Flexible Approval - Request Cancelled Acknowledgment	This email notification template is sent to the approver when the approver tries to approve or reject a request that is already been cancelled / catalog item is archived from the App Portal user interface.
	Flexible Approval - Standard Rejection Reason	This template will not be sent to approver and this notification is used to configure the standard rejection comments, when user does not enter any comments during email reply with Reject keyword, the system will set this reasons Out of the box and displays in the Notes tab of request details dialog in My Request page.
	Flexible Approval - Successful Approval Notification Response	This email notification template is sent to the approver when the approver approves the request by replying with an Approve keyword through email and the approval is successful.
	Flexible Approval - Successful Reject Notification Response	This email notification template is sent to the approver when the approver rejects the request by replying with a Reject keyword through email and the rejection is successful,

License Reclamation Reasons

Note • *This node is not displayed if you are using FlexNet Manager Suite for compliance management.*

On the **Communication > License Reclamation Reasons** view, enter values to appear in the drop lists for when users select to either keep or uninstall when using license reclamation.

Figure 3-123: Reasons for License Reclamation

To add a new reason, click **Add New Reason**. On the pop-up dialog box, enter a name for the reason in the **Reason** text box, and specify whether it is an **Approve Reason** or a **Reject Reason**.

Figure 3-124: Add New Reason Dialog Box for License Reclamation Reasons

Click **Edit** to edit the text of a reason and click **Delete** to delete a reason.

Approve / Reject Reasons

On the **Communication > Approve / Reject Reasons** view, enter values to appear in the drop lists for when users select to either approve or reject an item pending approval.

Figure 3-125: Approve / Reject Reasons

To add a new reason, click **Add New Reason**. On the pop-up dialog box, enter a name for the reason in the **Reason** text box, and specify whether it is an **Keep Reason** or a **Remove Reason**.

Figure 3-126: Add New Reason Dialog Box for Approve / Reject Reasons

Click **Edit** to edit the text of a reason and click **Delete** to delete a reason.

Languages

App Portal provides out-of-the-box localization support for its customer user interface, providing a choice of the following 14 languages:

- Chinese (Simplified)
- Dutch
- English
- French
- German
- Italian

- Japanese

- Korean

- Portuguese

- Portuguese (Brazil)

- Russian

- Spanish

- Spanish (Mexico)

- Thai

App Portal's localization support includes the following features:

- **End user screens and email notifications**—The localization support applies to the end user screens and the notifications/email messages.

- **Ability to localize questions and answers**—App Portal also provides you with an interface to localize the questions and answers that you associate with a catalog item request. The out-of-the-box questions and answers that are shipping with the product are already translated.

- **Language auto-detected by browser**—App Portal will automatically detect the language of the requesting browser from the user's culture settings and display that language. It will not be necessary for the end user to make a selection to change the displayed language.

- **Ability to add support for additional languages**—If you want to display App Portal's end user interface in a language other than those 14 that are supported, App Portal provides you with an interface to upload translated text in additional languages.

Additional language are activated on the **Languages** view.

Figure 3-127: Communication > Languages View

On the Languages view, all activated languages are listed. To activate an additional language, click the drop down list under **Available Languages**, select one or more additional languages, and then click **Add**.

Figure 3-128: Activating an Additional Language on the Languages View

The language that App Portal uses is determined by the browser culture settings of the user. However, some notifications are sent outside of the browser's session, such as a successful installation email. The site does not know what the language of the target user is.

You can create collections to help identify the proper language to use in these cases. Collections starting with the prefix ESD_Language_<LanguageName> will show in the list. Select the collection that matches the selected language from the **Select Collection** list

For more information, see the following topics:

- Activating Languages

- Uploading Additional Languages

- Localizing Questions and Answers

- Editing Text Strings in the Language Text View

Language Text

As described in Uploading Additional Languages, you can add new languages by adding translated text to existing Excel files and then uploading the files to App Portal. You can also edit existing text strings by editing those Excel files and re-uploading them.

However, an easier way of editing user interface text strings may be to use the **Communication > Language Text** view. On the **Language Text** view, you can display the user interface text strings for any of the activated languages, and modify the text strings for that language. The edits that you make will be immediately saved in the App Portal database.

Figure 3-129: Communication > Language Text View

From the **Select a language** list, select the language of the text strings that you would like to edit. Edit the text strings in the **Translation** column.

You can click **Show Untranslated Items** to only display text strings that have not been translated. Click the button again to go back to viewing the entire list.

Click **Save Translation** to save your edits, and click **Publish Translation** to publish your edits to the App Portal database.

*Note • If, after editing text strings on the **Language Text** view, you want to go back to the default translations, you just need to re-upload the original Excel files, as described in Uploading Additional Languages.*

Announcements

You use the **Communication > Announcements** view to add announcements to the App Portal site, as described in Adding Announcements to the Page Header.

Figure 3-130: Communication > Announcements View

Announcements are displayed on the top right corner of the user portal.

Figure 3-131: Announcement Displayed on the App Portal Site

New Announcement Dialog Box

To create a new announcement, click the **New** button at the top of the **Announcements** view to open the **New Announcement** dialog box.

Figure 3-132: New Announcement Dialog Box

The **New Announcement** dialog box includes the following properties:

Table 3-73 • New Announcement Dialog Box

Property	Description
Announcement title	Enter a brief title for this new announcement.
Expire date	Enter the date and time after which you no longer want this announcement displayed. If you do not enter an **Expire date**, the announcement will not expire.
Announcement	In this text editor, enter the text of the announcement. Use the toolbar buttons to perform formatting. Click the **HTML** button at the bottom of the editor to edit the HTML code of the announcement.
Save announcement	Click to save the announcement.

After you add an announcement, the next time the browser window is refreshed, the **Announcement title**, along with the beginning text of the announcement will be displayed. If a user clicks on the announcement title, a browser window opens displaying the full text of the message.

If more than one announcement is added, the announcements will automatically be rotated in the page header.

Adding Conditions

On the **Conditions** tab of the **New Announcement** dialog box, you can add a condition to restrict the announcement to be displayed for only those users who meet the defined condition.

Conditions can be based on user attributes including group and OU membership, AD property value, and deployment system collection membership for both users and computers.

For more information on adding conditions, see Add Condition Dialog Box.

Currency

The **Currency** view is used to specify the currencies and the exchange rates to use for each country. This enables App Portal to adjust the cost value displayed to the user.

Figure 3-133: Communication > Currency View

Site Feedback

You can enable a site feedback widget for your App Portal site so that users can report feedback or problems. Users are able to select whether they have feedback or are experiencing a problem, and can also specify which site module that their feedback pertains to. On the **Site Feedback** view, you can enable or disable the Site Feedback widget, and view feedback that was submitted.

Figure 3-134: Communication > Site Feedback View

On the **Site Feedback** view, the following properties are displayed:

Table 3-74 • Site Feedback View Properties

Property	Description
Username	User name of person who submitted the issue.
Machine	Machine name from which the issue was submitted.
Report	Identifies this issue as either a **Problem** or **Feedback**.
Status	Identifies the status of the issue as one of the following: ● New ● Open ● Review ● Reject ● Needs Clarification ● Hold ● Backlog ● Close *Note • The status of a feedback issue can be specified on the Site Feedback Issue Details view.*
Module	App Portal module selected when the issue was submitted.

Table 3-74 • Site Feedback View Properties

Property	Description
Files	Number of files uploaded with this feedback issue.
Created (UTC)	Date and time that the issue was submitted.
Turn on Site Feedback **Turn Off Site Feedback**	Click to toggle on/off the App Portal Site Feedback feature. When Site Feedback is on, the App Portal **Feedback** widget is displayed in the lower right corner of non-admin App Portal pages.
Modules	Click to open the Site Feedback Modules, where you can customize the list of modules listed in the **Which site module?** list on the Submit Feedback form.

Site Feedback Issue Details

On the **Site Feedback Issue Details** view, which is opened by clicking **Select** next to the issue name on the **Site Feedback** view, you can view the text of the submitted feedback issue and a list of the files that were uploaded with the issue. On this view you can also specify the status of the submitted issue.

Figure 3-135: Site Feedback Issue Details View

In the table at the top of the **Site Feedback Issue Details** view, the following properties are displayed:

Table 3-75 • Site Feedback Issue Details View

Property	Description
Unique Name	User name of person who submitted the issue.
Machine Name	Machine name from which the issue was submitted.
Created (UTC)	Date and time that the issue was submitted.
Report Type	Identifies this issue as either a **Problem** or **Feedback**.
Module	App Portal module selected when the issue was submitted.
Uploads	Number of files uploaded with this feedback issue.

Response Status Area

After addressing the feedback issue, you can change its status by selecting one of the following values from the **Response Status** list and clicking **Update**:

- New
- Open
- Review
- Reject
- Needs Clarification
- Hold

- Backlog

- Close

Comments Area

In the **Comments** area of the **Site Feedback Issue Details** view, you can view the text of the issue that was submitted.

Uploads Area

The **Uploads** area of the **Site Feedback Issue Details** view lists the files that were uploaded with the submitted issue. To download a file, click the **Download** link next to the file name.

Site Feedback Modules

When a user submits a feedback issue, they are prompted to select an App Portal feature from the **Which site module?** list to categorize the issue they are submitting:

Figure 3-136: Which site module? list

On the **Site Feedback Modules** view, you can customize this list of feedback modules to hide items, show previously hidden items, and add new items. By default, the following modules are listed:

Table 3-76 • App Portal Feedback Modules

Category	Subcategory	Sub-Subcategory
Main site	Browse Catalog	
	My Requests	Viewing/modifying request details information
		Searching for requests
		Adding notes
		Actions (Uninstall, Cancel, Reinstall, Rate)
	Approve\Reject	Approving requests
		Reassigning requests
		Rejecting requests
		Requesting additional info
	Processed	Viewing request details information
	My Apps	Viewing installed applications
		Viewing Software Policy Score chart
		Resolving alerts
		Uninstalling installed application
	Profile	Viewing user information
		Viewing User Readiness records
	Reporting	Viewing reports
		Saving reports
	Dashboard	Viewing ROI reports
		Exporting reports
	App Survey	Selecting applications
		Answering questions
		Reviewing selections

Table 3-76 • App Portal Feedback Modules

Category	Subcategory	Sub-Subcategory
Mobile Site	Searching for catalog items	
	Requesting catalog items	
	Viewing categories	
	Viewing catalog item descriptions	
	Other	
Notifications	Clicking a link within notifications	

Important • *Only site modules that do not have child modules are selectable by end users.*

To open the **Site Feedback Modules** view, click the **Modules** button on the **Site Feedback** view.

Figure 3-137: Site Feedback Modules View

The **Site Feedback Modules** view includes the following properties:

Table 3-77 • Site Feedback Modules Properties

Property	Description
Tree Structure	Lists all of the currently displayed modules in a tree format.

Table 3-77 • Site Feedback Modules Properties

Property	Description
Hide Site Module	To hide a module, select the module name from the **Select a module to hide list** and then click **Hide**. *Important •* *If you hide a parent module group, all of its child modules will also be hidden from the* **Which site module?** *list on the Submit Feedback form.*
Show Site Module	To show a previously hidden module, select the module name from the **Select a site module to show** list and then click **Show**.
Add New Site Module	To add a new module to the list, first enter a name for the module in the **Enter module name** text box. Then, select one of the listed items from the **Select a parent group** and click **Show**. *Note •* *You cannot create a new root-level parent group, which are* **Main site**, **Mobile site**, *and* **Notifications**.

Reporting

Reporting allows for the display of App Portal data in a read-only, searchable, and exportable view. You can create new reports, edit existing reports, and create and edit report categories.

Figure 3-138: Reporting > Report Management View

App Portal can display the following types of reports:

● **Standard reports**—Starting with App Portal 7.5, App Portal includes support for reports generated using Microsoft SQL Reporting Services. Over 40 standard reports are shipped with App Portal, and you have the ability to create your own custom reports, as described in Creating a New Standard RDLC-Based Report.

- **Legacy reports**—Legacy reports are derived from SQL views and stored procedures. These report views and procedures begin with v_Rep for report views and sp_Rep for stored procedures. Prior to App Portal 7.5, this was the only type of report that was available in App Portal.

New Legacy Report Dialog Box

Note • This feature is available for System Center Configuration Manager deployment technology only.

You can create a new legacy report that derives data from an available stored SQL view or procedure. You can link columns to external reports from System Center Configuration Manager by passing the correct query string values.

You create a new legacy report on the **New Legacy Report** dialog box, which is opened by clicking **New Legacy Report** on the **Reporting** view.

Figure 3-139: New Legacy Report Dialog Box

The **New Legacy Report** dialog box includes the following properties:

Table 3-78 • New Legacy Report Dialog Box

Properties	Description
Report Name	Enter a name to identify this report.

Table 3-78 • New Legacy Report Dialog Box

Properties	Description
Report Category	Select a category to associate the report to.
	*Note • You can create and secure categories in the **Report Categories** node under **Site Management > Categories**. Each category can have its own security provision for it so that the reports within that category can only be viewed by those users with access.*
Report View	Select the SQL view or procedure to derive the report data from.
Example	After you click **Save**, additional fields are displayed along with an example:
	`ReportID=10&Machine=##ColumnName##`
	In this example, the selected report has a column, `Machine`, that is linked to an System Center Configuration Manager report with a report ID of `10`. Report ID 10 requires a variable called `Machine` which contains a machine name. When the user selects a machine from the machine column, they will be directed to System Center Configuration Manager report ID 10.

New/Edit Report (RDLC) Dialog Box

App Portal is shipped with over 40 standard RDLC-based reports (reports that are generated using Microsoft SQL Reporting Services). By default, all of these reports are listed on the **Report Management > Reporting** view, which makes them available to view on the **Reporting** tab.

However, if you have removed a standard report from this list (as described in Removing a Report from the Reporting Tab) or have created a new standard report that you want to make available on the **Reporting** tab (as described in Creating a New Standard RDLC-Based Report), you will need to add the report to the **Report Management > Reporting** view. This is done using the New Standard Report dialog box, which is opened by clicking **New Standard Report** on the **Reporting** view.

Figure 3-140: New Standard Report Dialog Box

The **New Standard Report** dialog box includes the following properties:

Table 3-79 • New Standard Report Dialog Box

Properties	Description
Report Name	Select the report that you want to add to the **Reporting** tab.
	If you have previously deleted a standard report or have created a new standard report (as described in Creating a New Standard RDLC-Based Report), there should be a report listed in the **Report** list.
	However, if all standard reports are already being displayed on the **Reporting** tab, then this list will be empty.

Table 3-79 • New Standard Report Dialog Box

Properties	Description
Report Category	Select a category to associate the report to. 📄 *Note • You can create and secure categories in the **Report Categories** node under **Site Management > Categories**. Each category can have its own security provision for it so that the reports within that category can only be viewed by those users with access.*

App Portal Logs Reference

App Portal logs activities in several locations. There are log files for activities on the App Portal website, for the App Portal web service, and for the App Portal Windows service. There are also log files created for each App Portal request submitted and for each App Portal user.

- App Portal Website and Web Service Activity Log Files

- App Portal Requests Log Files

- App Portal Users Log Files

App Portal Website and Web Service Activity Log Files

The following log files, which are found in the Logs subdirectory of the App Portal installation directory, record activity related to the App Portal website and web service.

Table 3-80 • App Portal Website Activity Log Files

Log File	Description
ActiveDirectory_Error.log	This log file is updated if App Portal encounters any Active Directory-related exceptions such as an LDAP connection failure or if a user is not able to read from Active Directory.
ActiveDirectory.jog	Lists details about Active Directory-related information.
AirWatch_Error.log	Lists any errors that occur during mobile app deployment on AirWatch.
AirWatchDeployment.log	Lists AirWatch deployment information for Android, iOS, and Windows applications.
AirWatchIntegration.log	Lists integration details as well as the connection failure exception.
CodeTimer_CreateRequest.log	Lists Information on the execution process, including the amount of time each request took to complete.
CollectionClean.log	Tracks the activity of the collection cleaning process.

Table 3-80 • App Portal Website Activity Log Files (cont.)

Log File	Description
CollectionInsert.log	Handles the collection insert requests. The database is queried for new insert requests, and the service will contact the primary site server via the App Portal Web Service. The corresponding log file on the primary site server is the ESDWebService.log file.
DatabaseCalls_Error.log	Lists all of the information related to database connection errors.
DataSync.log	Lists all of the information related to user and computer syncing.
DataSyncException.log	Lists all of the errors or exceptions that occur during data sync.
EmailServices.log	Handles all the email notification processes for App Portal.
ESDService.log	Tracks general settings and actions for the App Portal Service.
ESDWebService.log	This log file is present only on servers with the App Portal Web Service. It tracks the actual insertion process of a machine into a collection.
FNMSIntegration.log	Lists the entire integration detail with FlexNet Manager Suite.
Integration.log	Provides all the information on third-party integration with App Portal (FlexNet Manager Platform, Workflow Manager, Microsoft System Center Orchestrator).
InventoryUpdate.log	Tracks the updating of inventory data from your deployment system.
ITSMSystemStatusCheck.log	Lists the status and the progress on each ITSM ticket in ServiceNow and Remedy; updates the same in App Portal.
LicenseReclamation.log	Lists the processing of lease end and license reclamation activities.
MI.log	Used by developers to see results from the MobileIron API.
MobileIron_Error.log	Lists exceptions related to MobileIron.
MobileIronDeployment.log	Details related to MobileIron catalog checkout pages of App Portal.
MobileIronIntegration.log	Includes details related to create catalog, edit catalog, and label creation.
MobileStatusUpdate.log	Tracks the status of requests processed in AirWatch after requests are placed from App Portal; also updates each status back to App Portal.
MyApps_Exceptions.log	Lists any exceptions that occur regarding My Apps alert generation, as well as during My Apps processing. It also includes exceptions that occur related to upgrade/retirement campaigns.

Table 3-80 • App Portal Website Activity Log Files (cont.)

Log File	Description
MyApps_ProcessAlerts.log	This log file contains all the details on My Apps processing, as well as the detail on the processed alerts for entire machine. It also includes details regarding upgrade/retirement campaigns.
MyApps\(MachineName).log	Includes details relating to upgrade/retire campaigns such as matching alerts found for a particular machine, number of apps found, and creating alerts.
RerunAdvertisement.log	Tracks the task of rerunning advertisements on the client.
RunPolicy.log	Tracks the task of running the machine policy on the client.
StatusUpdate.log	Tracks the status of requests processed in System Center Configuration Manager after requests are placed from App Portal; also updates each status back to App Portal.
WebAPIException.log	Lists any exceptions that occur during a web API run.
WebSite.log	Lists general settings and actions for the App Portal website. Startup errors or unhandled exceptions are logged in this file.
WebsiteMVC.log	Lists the error logs related to the Browse Catalog and Checkout pages of App Portal.

App Portal Requests Log Files

If enabled, request-level information for each request is recorded in a separate log file. These log files are found in the Logs\RequestLog subdirectory of the App Portal installation directory, and are named using the request number, such as 1.log, 2.log, etc.

Figure 3-141: Request Log File

To enable request-level logging, open the **Settings > Web Site > General** tab under **Site Management** and select the
Enable request life cycle logging option.

App Portal Users Log Files

User session data and error messages for each App Portal user and group is recorded in a separate log file. These log files
are found in the Logs\UserLog subdirectory of the App Portal installation directory, and are uniquely named with the user
or group name.

Figure 3-142: User Log File

4

Managing Your Catalog

Before software can be deployed using App Portal, a program or deployment must be created in Microsoft System Center Configuration Manager, managed software delivery policy must be created in Altiris, or a mobile application must be configured on AirWatch. An App Portal catalog item is an application, package, software product, policy, or task sequence that has been published in App Portal deployment through the software store front. There are three types of requests of catalog items: Software, General, and Groups.

This section explains how to create catalog items and set catalog item properties.

Table 4-1 • Managing Your Catalog

Section	Description
Creating Catalog Items	Explains how to create **Software**, **General**, **Cloud**, **Task Sequence**, **AirWatch Mobile Application**, and **Group** catalog items, and how to bundle catalog items.
Enabling Express Checkout: Install Now Button	Explains how to enable express checkout for catalog items, enabling users to bypass the checkout process if certain conditions are met.
Managing Approval Workflows	Explains how to create approval workflows to define how a request will be routed for review.
Managing Questions and Question Templates	Describes how to create questions, add questions to a question template, and how to attach a question template to a catalog item:
Setting Catalog Item Properties	Explains how to set the properties of a catalog item including those related to approval, questions asked at submission, deployment to System Center Configuration Manager, deployment to Altiris, FlexNet Manager Suite licensing, visibility conditions, notifications, and permissions. Also explains how to set properties specific to mobile applications.
Creating Alternate Targets	Explains how to create alternate targets that can be suggested to the user if they are prevented from checking out the catalog item to the target that they originally selected.

Table 4-1 • Managing Your Catalog

Section	Description
Using Expressions to Control Form Validation	Explains how to link expressions to form fields to assure that data is entered into forms in a consistent format and contains valid information.
Catalog Management Reference	Describes the **Catalog Management** views and dialog boxes that are used when managing your App Portal catalog items.

Creating Catalog Items

An App Portal catalog item is an application/package/program from a connected deployment system that is listed on the **Browse Catalog** tab, making it available for selection in the App Portal storefront. You can create the following types of catalog items:

Table 4-2 • Types of Catalog Items

Type	Description
Software Catalog Items	When creating a **Software** catalog item, App Portal connects to a deployment system and you select one of the listed items to make available in App Portal. You can create the following types of **Software** catalog items: ● Applications (System Center 2012 Configuration Manager only) ● Packages ● Virtual Applications ● Task Sequences (used to deploy operating systems) ● Software Products (Altiris only) ● Policies (Altiris only)
Cloud Catalog Item	App Portal provides out-of-the-box support for three cloud applications: Salesforce, Box, and Microsoft Office 365. These three catalog items are automatically created during App Portal installation. After you connect App Portal to your corporate account with these cloud application vendors, you can offer these catalog items on your Browse Catalog tab to enable end users to request an account to use these cloud applications.
AirWatch Mobile Application Catalog Item	When creating an AirWatch Mobile Application catalog item, App Portal connects to an AirWatch instance, and you select a mobile application to make available in App Portal. You can create a catalog item for a Google Android, Mac iOS, or Windows Phone mobile app.
Casper macOS Application Catalog Item	When creating a Casper catalog item, App Portal connects to a Casper server and you select one of the listed Apple macOS desktop applications to make available in App Portal.

Table 4-2 • Types of Catalog Items

Type	Description
General Catalog Items	When creating a **General** catalog item, you manually add a new catalog item and set its properties. General catalog items are usually used for non-software assets, such as a headset or a mouse, that you want to make available for request on App Portal. They can also be used to enable someone to make a request for a software item that is not in the catalog.
Group Catalog Items	When creating a **Group** catalog item, you select multiple catalog items to bundle into a group. End users would then be able to request this group of software by adding only one item to his cart on the **Browse Catalog** tab.

Note • To create an Alert Action catalog item, see Creating a New Custom Alert Action Catalog Item.

In this section, you will learn how to create a catalog category, create a catalog item, create a catalog group, and create a catalog item template.

- Creating a Catalog Category

- Creating a New Catalog Item Using the Wizard

- Creating a New Catalog Item (Advanced)

- Creating a Group Catalog Item

- Creating a Catalog Item Template

Creating a Catalog Category

Catalog items are organized using categories. Categories, which are listed in the **Browse Categories** tree on the **Browse Catalog** tab, are visible to end users when they are creating an App Portal request. When an end user selects a category on the **Browse Catalog** tab, the catalog items in that category are listed:

Figure 4-1: Browse Catalog Tab With Microsoft Category Selected

Note • A catalog item can be a member of multiple categories.

When you create a category, you have the option of setting category security and setting a category owner:

- **Set Category Security**—To control which users and/or groups are permitted to view (and request) the catalog items in that category, you can set category security.

  When determining whether to display a catalog item to a user, App Portal performs two permissions checks:

  - **First**, App Portal checks to determine if the user has permission to view catalog items in the selected category.

  - **Next**, App Portal checks to determine if any of the catalog items in the selected category also belong to another category; if so, App Portal checks the permissions on those categories.

  - **Then**, if the user has permission to view all of the categories that a catalog item belongs to, the catalog item will be displayed.

  A user cannot simultaneously have permission to view a catalog item and also be restricted from viewing it. Since categories are not just for organization, but also for security, App Portal applies the most restrictive permission.

- **Set Category Owner**—To give specific users permission to manipulate the applications in a category, you can assign category owners.

To create a catalog category, perform the following steps.

Task   ***To create a catalog category:***

1. Open the App Portal **Admin** tab.

2. Select **Catalog Management > Catalog Categories**. Existing categories are listed in the right pane.

3. In the category tree, select the category that you would like to add a subcategory to, and then click **Add Category**. You are prompted to enter a **New Category Name**.

4. Enter a name to identify the category and click **Add**. The new category is now listed in the tree.

5. **Set Category Owner**—To give specific users permission to manipulate the applications in a category, you can assign category owners by performing the following steps:

    a. On the **Catalog Categories** view, select a category in the tree.

    b. Click **Set Category Owner**. The **Set Category Owner** dialog box opens:

    c. Open the **Add Owners** tab.

    d. Use the search fields to locate the user or group that you would like to assign as an owner.

    e. Select a user or group in the **Search Results** box and click **Select**.

6. To set category security to control which users and/or groups are permitted to view (and request) the applications in a category, perform the following steps:

    a. On the **Catalog Categories** view, select a category in the tree.

    b. Click **Set Category Security**. The **Catalog Security** dialog box opens:

    c. Open the tab of the condition type that you want to add: **Group and OU**, **AD Property**, or **Collections**.

    d. Click **Add Condition**. The **Add Condition** dialog box opens.

    e. Use the search box to search for the group, OU, property, or collection that you want to add, and select the checkbox next to the item in the search results list.

f. Click the **Select** button to add the condition. After you add a condition to any of the three subtabs (**Group and OU**, **AD Property**, or **Collections**), that condition is listed on that subtab.

g. After the condition is added, specify the enforcement option you want to take effect by making a selection in the **Enforcement** column: **Include** or **Exclude**.

h. Click **Save**.

Creating a New Catalog Item Using the Wizard

You can use the **New Catalog Item Wizard** to create general catalog items; software catalog items from SCCM 2012, Altiris, or Casper deployment technologies; AirWatch mobile application catalog items; and SCCM task sequence catalog items.

- Creating a General Catalog Item

- Creating a ConfigMgr / SCCM 2012 Software Catalog Item

- Creating an Altiris Software Catalog Item

- Creating a Casper macOS (OS X) Desktop Application Catalog Item

- Creating an AirWatch Mobile Application Catalog Item

- Creating a MobileIron Mobile Application Catalog Item

- Creating a Cloud Catalog Item

- Creating a Task Sequence Catalog Item for OSD Deployment

After creating a catalog item using the wizard, you can then edit its properties or set additional, advanced properties on the **Catalog Item Properties** dialog box.

Note • You can also create a new catalog item using the Catalog Item Properties dialog box, as described in Creating a New Catalog Item (Advanced).

*Important • To create an AirWatch mobile application catalog item, you must use the **New Catalog Item Wizard**. After you have created the mobile application catalog item, you can then set additional properties on the **Catalog Item Properties** dialog box.*

Creating a General Catalog Item

General catalog items are usually used for non-software assets, such as a headset or a mouse, that you want to make available for request on App Portal. They can also be used to enable someone to make a request for a software item that is not in the catalog.

To create a **General** catalog item using the **New Catalog Item Wizard**, perform the following steps:

Task   **To create a General catalog item:**

1. If you want to create a licensed **General** catalog item, make sure that you have performed the steps in Connecting to the Flexera Service Gateway.

2. Open the App Portal **Admin** tab.

3. Under **Catalog Management**, select **New Catalog Item Wizard**. The **Catalog Item Type** panel of the **New Catalog Item Wizard** opens.

4. Select **General Catalog Item** and click **Next**. The **Catalog Item Title and Category** panel opens.

5. In the **Title** field, enter a title to identify this catalog item in your App Portal storefront.

6. From the **Category** field, select a category to specify this catalog item's location in the App Portal catalog. You are required to select at least one category, but you may select more than one.

7. In the **Brief Description** field, enter the text that you want to display under the catalog item **Title** in the App Portal storefront (when viewed in list view).

8. By default, a generic icon is associated with this catalog item. To associate a custom icon to this catalog item, click **Change** to open the **Image Selection** dialog box and select a `.gif`, `.jpg`, or `.png` icon file.

    💡

    Tip • For best results, the uploaded image should be 80 px by 80 px or larger.

9. Optionally, from the **Template** list, select an existing template to apply advanced settings to this catalog item.

    📄

    Note • For more information, see Creating a Catalog Item Template.

10. In the **Search Keywords** text box, enter single words that an end user might enter when searching for this catalog item.

11. In the **Full Description** text area, enter a longer description of this catalog item, and use the items on the toolbar to format it.

    The text entered in the **Title**, **Brief Description**, and **Full Description** fields will be displayed as follows:

    - **Title**—The text entered in the **Title** field along with the catalog item icon, will be displayed when viewing this catalog item on the **Browse Catalog** tab.

    - **Brief Description**—When viewing catalog items in list view, the brief description will also be visible:

    - **Full Description**—The text entered in the **Full Description** field will be displayed when a catalog item is viewed in its detail view, which is opened by clicking on the catalog item name in either the list or card view.

12. When you are finished editing the fields on the **Catalog Item Title and Category** panel, click **Next**. If you are connected to the Flexera Service Gateway, the **Flexera ID** panel opens

13. To track licenses for this catalog item using its Flexera ID, use the column filters to locate this catalog item in FlexNet Manager Suite, select it, and click **Next**. The **Ready to Create** panel opens.

14. If, after this catalog item is created, you want to immediately open this catalog item's **Catalog Item Properties** dialog box, where you can specify advanced settings, select the **Load advanced view after creating the catalog item** option.

15. Review the summary information and then click **Create** to create this new catalog item. The catalog item will now be listed on the **Browse Catalog** tab in the category you selected.

Note • After creating a catalog item, you can edit its basic and advanced settings on the ***Catalog Item Properties*** *dialog box, as described in* Setting Catalog Item Properties.

Creating a ConfigMgr / SCCM 2012 Software Catalog Item

You can use the **New Catalog Item Wizard** to create a new ConfigMgr / SCCM 2012 **Software** catalog item containing either an application or a package.

*Important • While the instructions in this section assume you are adding a single package or application from ConfigMgr / SCCM 2012 to a new **Software** catalog item, you can include software from multiple deployment technologies to the same **Software** catalog item by selecting more than one source on the **Software Source** panel of the **New Catalog Item Wizard**.*

Task   *To create a new Software catalog item from SCCM 2012:*

1. If you want to create a licensed **Software** catalog item, make sure that you have performed the steps in Connecting to the Flexera Service Gateway.

2. Under **Catalog Management**, select **New Catalog Item Wizard**. The **Catalog Item Type** panel of the **New Catalog Item Wizard** opens.

3. Select **Software Catalog Item** and click **Next**. The **Software Source** panel opens.

4. Select **SCCM 2012** and then select the **Application** or **Package** option.

5. Click **Next**. The **SCCM 2012 Applications** or **SCCM 2012 Packages** panel opens.

6. Locate and select the application or package on the SCCM 2012 server that you want to associate with this new catalog item.

Important • Only a specified number of applications or packages are initially listed in this grid. To search the entire SCCM server for an application or package, use the column filters.

7. Click **Next**. The **Catalog Item Title and Category** panel opens.

8.   In the **Title** field, enter a title to identify this catalog item in your App Portal storefront. By default, the name of the package or application that you selected is listed in this field.

9.   From the **Category** field, select a category to specify this catalog item's location in the App Portal catalog. You are required to select at least one category, but you may select more than one.

10. In the **Brief Description** field, enter the text that you want to display under the catalog item **Title** in the App Portal storefront (when viewed in list view).

11. By default, a generic icon is associated with this catalog item. To associate a custom icon to this catalog item, click **Change** to open the **Image Selection** dialog box and select a `.gif`, `.jpg`, or `.png` icon file.

Tip • For best results, the uploaded image should be 80 px by 80px or larger.

12. Optionally, from the **Template** list, select an existing template to apply advanced settings to this catalog item.

Note • For more information, see Creating a Catalog Item Template.

13. In the **Search Keywords** text box, enter single words that an end user might enter when searching for this catalog item.

14. In the **Full Description** text area, enter a longer description of this catalog item, and use the items on the toolbar to format it.

The text entered in the **Title**, **Brief Description**, and **Full Description** fields will be displayed as follows:

● **Title**—The text entered in the **Title** field along with the catalog item icon, will be displayed when viewing this catalog item on the **Browse Catalog** tab.

● **Brief Description**—When viewing catalog items in list view, the brief description will also be visible:

● **Full Description**—The text entered in the **Full Description** field will be displayed when a catalog item is viewed in its detail view, which is opened by clicking on the catalog item name in either the list or card view.

15. When you are finished editing the fields on the **Catalog Item Title and Category** panel, click **Next**. If you are connected to FlexNet Manager Suite via the Flexera Service Gateway, the **Flexera ID** panel opens.

16. To track licenses for this catalog item using its Flexera ID, use the column filters to locate this application or package in FlexNet Manager Suite, select it, and click **Next**.

One of the following panels opens, depending upon whether you are adding an application or a package from SCCM:

● **Application**—The **SCCM 2012 Deployment Settings** panel opens.

● **Package**—The **SCCM 2012 Package Deployment Settings** panel opens.

17. **If you are adding an application** from SCCM, perform the following steps on the **SCCM 2012 Deployment Settings** panel:

    a. From the **Select Deployment Method** list, select one of the following options to specify whether this catalog item will be deployed to a computer or to a user:

        ● **Deploy to computer**

        ● **Deploy to user**

    b. To add an uninstall collection to this catalog item, select the **Create Uninstall Collection** option. When this option is selected, users will be able to submit an uninstall request from App Portal, and System Center Configuration Manager will uninstall the application. App Portal will inform the user when the uninstall is complete.

18. **If you are adding a package** from SCCM, perform the following steps on the **SCCM 2012 Package Deployment Settings** panel:

    a. From the following lists, select at least one existing program from the SCCM server:

        ● **Select Program for Install**

        ● **Select Program for Uninstall**

        ● **Select Program for Repair**

    b. Under **Program for OS Deployment Task Sequence**, select a matching program name for the program function.

    c. Under **Select Sites to Publish**, select the sites where this request will be available, the locations you wish to publish the catalog item to. An advertisement and collection will be created at the site(s) selected.

    d. Specify **Advertisement Settings**.

    e. Specify **Distribution Settings**.

19. Click **Next**. The **Ready to Create** panel opens.

20. If, after this catalog item is created, you want to immediately open this catalog item's **Catalog Item Properties** dialog box, where you can specify advanced settings, select the **Load advanced view after creating the catalog item** option.

21. Review the summary information and then click **Create** to create this new catalog item. The catalog item will now be listed on the **Browse Catalog** tab in the category you selected.

*Note • After creating a catalog item, you can edit its basic and advanced settings on the **Catalog Item Properties** dialog box, as described in Setting Catalog Item Properties.*

Creating an Altiris Software Catalog Item

When connected to Altiris Client Management Suite, you can create a **Software** catalog item that contains a Software Product or a Managed Software Delivery Policy from the Altiris server.

- Creating a Software Catalog Item for an Altiris Software Product

- Creating a Software Catalog Item for an Existing Altiris Policy

*Important • While the instructions in this section assume you are adding a software product or policy from Altiris to a new **Software** catalog item, you can include software from multiple deployment technologies to the same **Software** catalog item by selecting more than one source on the **Software Source** panel of the **New Catalog Item Wizard**. See Creating a ConfigMgr / SCCM 2012 Software Catalog Item.*

Creating a Software Catalog Item for an Altiris Software Product

When creating a **Software** catalog item for an Altiris software product, App Portal connects to the Altiris server and you select one of the listed items to make available in App Portal.

To create a new **Software** catalog item for an Altiris software product, perform the following steps:

*Important • While the instructions in this section assume you are adding a software product from Altiris to a new **Software** catalog item, you can include software from multiple deployment technologies to the same **Software** catalog item by selecting more than one source on the **Software Source** panel of the **New Catalog Item Wizard**. See Creating a ConfigMgr / SCCM 2012 Software Catalog Item.*

Task   ***To create a new Software catalog item for an Altiris software product:***

1. If you want to create a licensed **Software** catalog item, make sure that you have performed the steps in Connecting to the Flexera Service Gateway.

2. Under **Catalog Management**, select **New Catalog Item Wizard**. The **Catalog Item Type** panel of the **New Catalog Item Wizard** opens.

3.   Select **Software Catalog Item** and click **Next**. The **Software Source** panel opens.

4.   Select **Altiris** and then select the **Software Product** option and click **Next**. The **Altiris Software Products** panel opens.

5. Locate and select the software product that you want to associate with this new catalog item.

Important • *Only a specified number of software products are initially listed in this grid. To search the entire Altiris server for a software product, use the column filters.*

6. Click **Next**. The **Catalog Item Title and Category** panel opens.

7. In the **Title** field, enter a title to identify this catalog item in your App Portal storefront. By default, the name of the software product that you selected is listed in this field.

8. From the **Category** field, select a category to specify this catalog item's location in the App Portal catalog. You are required to select at least one category, but you may select more than one.

9. In the **Brief Description** field, enter the text that you want to display under the catalog item **Title** in the App Portal storefront (when viewed in list view).

10. By default, a generic icon is associated with this catalog item. To associate a custom icon to this catalog item, click **Change** to open the **Image Selection** dialog box and select a `.gif`, `.jpg`, or `.png` icon file.

Tip • For best results, the uploaded image should be 80 px by 80px or larger.

11. Optionally, from the **Template** list, select an existing template to apply advanced settings to this catalog item.

Note • For more information, see Creating a Catalog Item Template.

12. In the **Search Keywords** text box, enter single words that an end user might enter when searching for this catalog item.

13. In the **Full Description** text area, enter a longer description of this catalog item, and use the items on the toolbar to format it.

The text entered in the **Title**, **Brief Description**, and **Full Description** fields will be displayed as follows:

- **Title**—The text entered in the **Title** field along with the catalog item icon, will be displayed when viewing this catalog item on the **Browse Catalog** tab.

- **Brief Description**—When viewing catalog items in list view, the brief description will also be visible:

- **Full Description**—The text entered in the **Full Description** field will be displayed when a catalog item is viewed in its detail view, which is opened by clicking on the catalog item name in either the list or card view.

14. When you are finished editing the fields on the **Catalog Item Title and Category** panel, click **Next**. If you are connected to FlexNet Manager Suite via the Flexera Service Gateway, the **Flexera ID** panel opens.

15. To track licenses for this catalog item using its Flexera ID, use the column filters to locate this application or package in FlexNet Manager Suite, select it, and click **Next**. The **Altiris Advertisement Settings** panel opens.

16. From the **Select Deployment Method** list, select one of the following options:

   - **Deploy to user**

   - **Deploy to computer**

17. From the **Select Program for Install**, **Select Program for Uninstall**, and **Select Program for Repair** lists, select the program name that you would like to add for each function.

Note • You are required to select at least one program.

18. Click **Next**. The **Ready to Create** panel opens.

19. If, after this catalog item is created, you want to immediately open this catalog item's **Catalog Item Properties** dialog box, where you can specify advanced settings, select the **Load advanced view after creating the catalog item** option.

20. Review the summary information and then click **Create** to create this new catalog item. The catalog item will now be listed on the **Browse Catalog** tab in the category you selected.

*Note • After creating a catalog item, you can edit its basic and advanced settings on the **Catalog Item Properties** dialog box, as described in Setting Catalog Item Properties.*

Creating a Software Catalog Item for an Existing Altiris Policy

An Altiris managed software delivery *policy* simplifies advanced software deliveries by enabling you to deliver software as a unit, which can include multiple software resources as well as dependencies. For example, you can create a single policy that installs an application and its associated patches and service packs. Policies can also run any task at any stage of the delivery. For example, it can run a task that performs a restart or runs a script.

To create a **Software** catalog item for an existing Altiris policy, perform the following steps:

*Important • While the instructions in this section assume you are adding a single policy from Altiris to a new **Software** catalog item, you can include software from multiple deployment technologies to the same **Software** catalog item by selecting more than one source on the **Software Source** panel of the **New Catalog Item Wizard**. See Creating a ConfigMgr / SCCM 2012 Software Catalog Item.*

Task   *To create a new Software catalog item for an existing Altiris policy:*

1. If you want to create a licensed **Software** catalog item, make sure that you have performed the steps in Connecting to the Flexera Service Gateway.

2. Under **Catalog Management**, select **New Catalog Item Wizard**. The **Catalog Item Type** panel of the **New Catalog Item Wizard** opens.

3.   Select **Software Catalog Item** and click **Next**. The **Software Source** panel opens.

4.   Select **Altiris** and then select the **Managed Software Delivery Policy** option and click **Next**. The **Altiris Policies** panel opens.

5. Locate and select the policy that you want to associate with this new catalog item.

> **Important •** *Only a specified number of policies are initially listed in this grid. To search the entire Altiris server for a policy, use the column filters.*

6. Click **Next**. The **Catalog Item Title and Category** panel opens.

7. In the **Title** field, enter a title to identify this catalog item in your App Portal storefront. By default, the name of the policy that you selected is listed in this field.

8. From the **Category** field, select a category to specify this catalog item's location in the App Portal catalog. You are required to select at least one category, but you may select more than one.

9. In the **Brief Description** field, enter the text that you want to display under the catalog item **Title** in the App Portal storefront.

10. By default, a generic icon is associated with this catalog item. To associate a custom icon to this catalog item, click **Change** to open the **Image Selection** dialog box and select a `.gif`, `.jpg`, or `.png` icon file.

> *Tip • For best results, the uploaded image should be 80 px by 80px or larger.*

11. Optionally, from the **Template** list, select an existing template to apply advanced settings to this catalog item.

> *Note • For more information, see Creating a Catalog Item Template.*

12. In the **Search Keywords** text box, enter single words that an end user might enter when searching for this catalog item.

13. In the **Full Description** text area, enter a longer description of this catalog item, and use the items on the toolbar to format it.

    The text entered in the **Title**, **Brief Description**, and **Full Description** fields will be displayed as follows:

    ● **Title**—The text entered in the **Title** field along with the catalog item icon, will be displayed when viewing this catalog item on the **Browse Catalog** tab.

- **Brief Description**—When viewing catalog items in list view, the brief description will also be visible:

- **Full Description**—The text entered in the **Full Description** field will be displayed when a catalog item is viewed in its detail view, which is opened by clicking on the catalog item name in either the list or card view.

14. When you are finished editing the fields on the **Catalog Item Title and Category** panel, click **Next**. If you are connected to FlexNet Manager Suite via the Flexera Service Gateway, the **Flexera ID** panel opens.

15. To track licenses for this catalog item using its Flexera ID, use the column filters to locate this application or package in FlexNet Manager Suite, select it, and click **Next**. The **Altiris Policy Settings** panel opens.

16. From the **Select Policy Deployment Method** list, select one of the following options:

- **Deploy to user**

- **Deploy to computer**

17. The **Select Software Delivery Item** list lists all of the software delivery items that are included in the selected Altiris policy. Select the software delivery item that you want this new **Software** catalog item to contain.

18. From the **Select Deployment Type** list, select one of the following items to match the purpose of the selected software delivery item:

- **Install**

- **Uninstall**

- **Repair**

19. Click **Next**. The **Ready to Create** panel opens.

20. If, after this catalog item is created, you want to immediately open this catalog item's **Catalog Item Properties** dialog box, where you can specify advanced settings, select the **Load advanced view after creating the catalog item** option.

21. Review the summary information and then click **Create** to create this new catalog item. The catalog item will now be listed on the **Browse Catalog** tab in the category you selected.

*Note • After creating a catalog item, you can edit its basic and advanced settings on the **Catalog Item Properties** dialog box, as described in Setting Catalog Item Properties.*

Creating a Casper macOS (OS X) Desktop Application Catalog Item

When App Portal is connected to a Casper server, you can use the **New Catalog Item Wizard** to create a catalog item for an Apple maxOS desktop application. All macOS desktop applications configured on the connected Casper server can be associated with an App Portal catalog item and made available in App Portal.

*Note • If a user does not have a registered Apple macOS desktop machine, that user will not see any macOS applications displayed on the **Browse Catalog** tab.*

To create a Casper macOS desktop application catalog item, perform the following steps.

Task   ***To create a Casper macOS desktop application catalog item:***

1. Make sure that you have connected App Portal to a Casper server, as described in Entering Casper Settings.

2. Under **Catalog Management**, select **New Catalog Item Wizard**. The **Catalog Item Type** panel of the **New Catalog Item Wizard** opens.

3. Select **Software Catalog Item** and click **Next**. The **Software Source** panel opens.

4. Select **Casper Package** and click **Next**. The **Casper Packages** panel opens, listing all of the macOS applications on the Casper server.

5. Select the macOS application that you want to associate with this new catalog item.

6. Click **Next**. The **Catalog Item Title and Category** panel opens.

7. In the **Title** field, enter a title to identify this catalog item in your App Portal storefront. By default, the name of the package or application that you selected is listed in this field.

8. From the **Category** field, select a category to specify this catalog item's location in the App Portal catalog. You are required to select at least one category, but you may select more than one.

9. In the **Brief Description** field, enter the text that you want to display under the catalog item **Title** in the App Portal storefront (when viewed in list view).

10. By default, a generic icon is associated with this catalog item. To associate a custom icon to this catalog item, click **Change** to open the **Image Selection** dialog box and select a `.gif`, `.jpg`, or `.png` icon file.

> *Tip • For best results, the uploaded image should be 80 px by 80 px or larger.*

11. In the **Search Keywords** text box, enter single words that an end user might enter when searching for this catalog item.

12. In the **Full Description** text area, enter a longer description of this catalog item, and use the items on the toolbar to format it.

    The text entered in the **Title**, **Brief Description**, and **Full Description** fields will be displayed as follows:

    - **Title**—The text entered in the **Title** field along with the catalog item icon, will be displayed when viewing this catalog item on the **Browse Catalog** tab.

- **Brief Description**—When viewing catalog items in list view, the brief description will also be visible:

- **Full Description**—The text entered in the **Full Description** field will be displayed when a catalog item is viewed in its detail view, which is opened by clicking on the catalog item name in either the list or card view.

13. When you are finished editing the fields on the **Catalog Item Title and Category** panel, click **Next**. If you are connected to FlexNet Manager Suite via the Flexera Service Gateway, the **Flexera ID** panel opens.

14. To track licenses for this catalog item using its Flexera ID, use the column filters to locate this application or package in FlexNet Manager Suite, select it, and click **Next**. The **Casper Package Deployment Settings** panel opens.

15. If you want this App Portal catalog item to support uninstallation of the application, select the **Create Uninstall Policy** option. If this option is selected, two policies will be created in Casper: one for installation and one for uninstallation.

16. Select a Casper distribution point for this package from the **Select Distribution point** list. Distribution points are servers used to host files for distribution to computers.

17. Click **Next**. The **Ready to Create** panel opens.

18. If, after this catalog item is created, you want to immediately open this catalog item's **Catalog Item Properties** dialog box, where you can specify advanced settings, select the **Load advanced view after creating the catalog item** option.

19. Review the summary information and then click **Create** to create this new catalog item. The catalog item will now be listed on the **Browse Catalog** tab in the category you selected.

Note • After creating a catalog item, you can edit its basic and advanced settings on the **Catalog Item Properties** *dialog box, as described in* Setting Catalog Item Properties.

Enabling the "Create Uninstall Policy" Option for a Casper Package

App Portal allows the uninstallation policy to be created for a Casper package only if the **Allow package to be uninstalled** option has been selected on the **Options** tab when editing package properties within Casper Management settings (**Management Settings > Computer Management > Packages**).

Figure 4-2: Selecting the "Allow package to be uninstalled" Option on Options Tab of Casper Package Properties

When this option is not selected, App Portal disables the **Create Uninstall Policy** option on the **Casper Package Deployment Settings** panel of the **New Catalog Item Wizard** (and the **Deployment > Casper** tab of the `Catalog Item Properties` dialog box).

Figure 4-3: Disabled "Create Uninstall Policy" Option

When the **Create Uninstall Policy** option is selected, App Portal creates both an Install and Uninstall policy. Therefore, unless you select the **Create Uninstall Policy** option for a Casper package, users will not be able to request this package in the App Portal storefront.

Creating an AirWatch Mobile Application Catalog Item

When App Portal is connected to an AirWatch instance, you can use the **New Catalog Item Wizard** to create a mobile application catalog item containing an Apple iOS, Google Android, or Windows Phone mobile app. All mobile apps configured on the connected AirWatch instance, both internal and public store, can be associated with an App Portal catalog item and made available in App Portal.

You can add multiple versions of a mobile application to the same catalog item in order to accommodate different operating systems and different . For example, a single catalog item named ABC Application could contain the following versions of the same mobile app:

- ABC Application / iOS iPhone Version

- ABC Application / iOS iPad Version

- ABC Application / Android Version

- ABC Application / Windows Phone Version

When the end user requests this mobile application, the version appropriate to the user's registered device will be delivered.

Note • You can also link a mobile application to its corresponding desktop version so that end users requesting one will be asked whether they want to also receive the other. See Linking a Mobile Application with a Desktop Application.

Note • If a user does not have a registered mobile device, that user will not see any mobile applications displayed on the ***Browse Catalog*** *tab. Also, if a user has only iOS mobile registered, Android-only mobile applications will not be visible on the* ***Browse Catalog*** *tab for that user, and vice versa.*

To create an AirWatch mobile application catalog item, perform the following steps.

Task   ***To create an AirWatch mobile application catalog item:***

1. Make sure that you have connected App Portal to an AirWatch instance, as described in Entering AirWatch Settings.

2. Under **Catalog Management**, select **New Catalog Item Wizard**. The **Catalog Item Type** panel of the **New Catalog Item Wizard** opens.

3.   Select **Mobile Application Catalog Item** and click **Next**. The **Mobile Application** panel opens.

4.   Select **AirWatch Application**.

5.   Select the platform(s) of the mobile application you want to add to this catalog item: **Android Application**, **iOS Application**, and/or **Windows Application**.

6.   Click **Next**. If you selected **Android Application**, the **AirWatch Android Applications** panel opens, listing all of the Android applications on the AirWatch instance.

7.   Select the Android application that you want to add and click **Next**. If you selected **iOS Application** on the **Mobile Application** panel, the **AirWatch iOS Applications** panel opens.

8.   Select the iOS mobile application that you want to associate with this new catalog item.

9.   Next to **Supported** , select **iPhone** and/or **iPad** to indicate the that this mobile application supports.

10. Click **Next**. If you selected **Windows Application** on the **Mobile Application** panel, the **AirWatch Windows Applications** panel opens.

11. Select the Windows Phone mobile application that you want to associate with this new catalog item.

12. Next to **Supported** , select **Windows Phone** and/or **Windows Phone 8** to indicate the that this mobile application supports.

13. Click **Next**. The **Catalog Item Title and Category** panel opens.

14. In the **Title** field, enter a title to identify this catalog item in your App Portal storefront. By default, the name of the package or application that you selected is listed in this field.

15. From the **Category** field, select a category to specify this catalog item's location in the App Portal catalog. You are required to select at least one category, but you may select more than one.

16. In the **Brief Description** field, enter the text that you want to display under the catalog item **Title** in the App Portal storefront (when viewed in list view).

17. By default, a generic icon is associated with this catalog item. To associate a custom icon to this catalog item, click **Change** to open the **Image Selection** dialog box and select a `.gif`, `.jpg`, or `.png` icon file.

Tip • *For best results, the uploaded image should be 80 px by 80 px or larger.*

18. In the **Search Keywords** text box, enter single words that an end user might enter when searching for this catalog item.

19. In the **Full Description** text area, enter a longer description of this catalog item, and use the items on the toolbar to format it.

The text entered in the **Title**, **Brief Description**, and **Full Description** fields will be displayed as follows:

- **Title**—The text entered in the **Title** field along with the catalog item icon, will be displayed when viewing this catalog item on the **Browse Catalog** tab.

- **Brief Description**—When viewing catalog items in list view, the brief description will also be visible:

- **Full Description**—The text entered in the **Full Description** field will be displayed when a catalog item is viewed in its detail view, which is opened by clicking on the catalog item name in either the list or card view.

20. When you are finished editing the fields on the **Catalog Item Title and Category** panel, click **Next**. The **Ready to Create** panel opens.

21. If, after this catalog item is created, you want to immediately open this catalog item's **Catalog Item Properties** dialog box, where you can specify advanced settings, select the **Load advanced view after creating the catalog item** option.

22. Review the summary information and then click **Create** to create this new catalog item. The catalog item will now be listed on the **Browse Catalog** tab in the category you selected.

*Note • After creating a catalog item, you can edit its basic and advanced settings on the **Catalog Item Properties** dialog box, as described in Setting Catalog Item Properties.*

Creating a MobileIron Mobile Application Catalog Item

When App Portal is connected to a MobileIron instance, you can use the **New Catalog Item Wizard** to create a mobile application catalog item containing an Apple iOS or Google Android mobile app. All mobile apps configured on the connected MobileIron instance can be associated with an App Portal catalog item and made available in App Portal.

You can add multiple versions of a mobile application to the same catalog item in order to accommodate different operating systems and different . For example, a single catalog item named ABC Application could contain the following versions of the same mobile app:

●   ABC Application / iOS iPhone Version

●   ABC Application / iOS iPad Version

●   ABC Application / Android Version

When the end user requests this mobile application, the version appropriate to the user's registered device will be delivered.

Note • You can also link a mobile application to its corresponding desktop version so that end users requesting one will be asked whether they want to also receive the other. See Linking a Mobile Application with a Desktop Application.

Note • If a user does not have a registered mobile device, that user will not see any mobile applications displayed on the **Browse Catalog** *tab. Also, if a user has only iOS mobile registered, Android-only mobile applications will not be visible on the* **Browse Catalog** *tab for that user, and vice versa.*

To create a MobileIron mobile application catalog item, perform the following steps.

Task   **To create a MobileIron mobile application catalog item:**

1. Make sure that you have connected App Portal to a MobileIron instance, as described in Entering MobileIron Settings.

2. Under **Catalog Management**, select **New Catalog Item Wizard**. The **Catalog Item Type** panel of the **New Catalog Item Wizard** opens.

3. Select **Mobile Application Catalog Item** and click **Next**. The **Mobile Application** panel opens.

4. Select **MobileIron Application**.

5. Under **MobileIron Application**, select the platform(s) of the mobile application you want to add to this catalog item:
    Android Application and/or **iOS Application**.

6. Click **Next**. If you selected **Android Application**, the **MobileIron Android Applications** panel opens, listing all of the
    Android applications on the MobileIron instance.

7. Select the Android application that you want to add and click **Next**. If you selected **iOS Application** on the **Mobile
    Application** panel, the **iOS Applications** panel opens.

8.   Select the iOS mobile application that you want to associate with this new catalog item.

9.   Click **Next**. The **Catalog Item Title and Category** panel opens.

10. In the **Title** field, enter a title to identify this catalog item in your App Portal storefront. By default, the name of the package or application that you selected is listed in this field.

11. From the **Category** field, select a category to specify this catalog item's location in the App Portal catalog. You are required to select at least one category, but you may select more than one.

12. In the **Brief Description** field, enter the text that you want to display under the catalog item **Title** in the App Portal storefront (when viewed in list view).

13. By default, a generic icon is associated with this catalog item. To associate a custom icon to this catalog item, click **Change** to open the **Image Selection** dialog box and select a `.gif`, `.jpg`, or `.png` icon file.

Tip • For best results, the uploaded image should be 80 px by 80 px or larger.

14. In the **Search Keywords** text box, enter single words that an end user might enter when searching for this catalog item.

15. In the **Full Description** text area, enter a longer description of this catalog item, and use the items on the toolbar to format it.

The text entered in the **Title**, **Brief Description**, and **Full Description** fields will be displayed as follows:

- **Title**—The text entered in the **Title** field along with the catalog item icon, will be displayed when viewing this catalog item on the **Browse Catalog** tab.

- **Brief Description**—When viewing catalog items in list view, the brief description will also be visible:

- **Full Description**—The text entered in the **Full Description** field will be displayed when a catalog item is viewed in its detail view, which is opened by clicking on the catalog item name in either the list or card view.

16. When you are finished editing the fields on the **Catalog Item Title and Category** panel, click **Next**. The **Ready to Create** panel opens.

17. If, after this catalog item is created, you want to immediately open this catalog item's **Catalog Item Properties** dialog box, where you can specify advanced settings, select the **Load advanced view after creating the catalog item** option.

18. Review the summary information and then click **Create** to create this new catalog item. The catalog item will now be listed on the **Browse Catalog** tab in the category you selected.

📄

*Note • After creating a catalog item, you can edit its basic and advanced settings on the **Catalog Item Properties** dialog box, as described in Setting Catalog Item Properties.*

Creating a Cloud Catalog Item

When App Portal is connected to a cloud application, you can use the **New Catalog Item Wizard** to create a cloud catalog item that will obtain an account for the specified cloud application for the requester.

App Portal provides out-of-the-box support for Box, Office 365, and Salesforce, and a catalog item for each oif those cloud applications is automatically created:

Figure 4-4: Default Cloud Catalog Items

These catalog items can be used to directly request an account from the cloud application vendor.

However, if you have connected to a cloud application other than Box, Office 365, or Salesforce (as described in Integrating With Other Cloud Applications), you will need to create a new cloud catalog item. You will also need to create a cloud catalog item if you want to use an ITSM system to request a Box, Office 365, or Salesforce account instead of requesting it directly from the vendor.

To create a cloud catalog item, perform the following steps.

📋

Task   **To create a cloud catalog item:**

1.   Make sure that you have connected App Portal to at least one cloud application, as described in Connecting to Box, Salesforce, and Office 365.

2.   Under **Catalog Management**, select **New Catalog Item Wizard**. The **Catalog Item Type** panel of the **New Catalog Item Wizard** opens.

3. Select **Cloud Catalog Item** and click **Next**. The **Cloud Account Type** panel opens.

4. Select the type of cloud application you want to add to this catalog item: **Box, Office 365, Salesforce, or Others.**

5. Click **Next**. The **Catalog Item Title and Category** panel opens.

6. In the **Title** field, enter a title to identify this catalog item in your App Portal storefront, such as `Box Account` or `Office 365 Account`..

7. From the **Category** field, select the **Cloud** category to specify this catalog item's location in the App Portal catalog.

8. In the **Brief Description** field, enter the text that you want to display under the catalog item **Title** in the App Portal storefront (when viewed in list view).

9. By default, a generic icon is associated with this catalog item. To associate a custom icon to this catalog item, click **Change** to open the **Image Selection** dialog box and select a `.gif`, `.jpg`, or `.png` icon file.

Tip • For best results, the uploaded image should be 80 px by 80 px or larger.

10. In the **Search Keywords** text box, enter single words that an end user might enter when searching for this catalog item.

11. In the **Full Description** text area, enter a longer description of this catalog item, and use the items on the toolbar to format it.

The text entered in the **Title**, **Brief Description**, and **Full Description** fields will be displayed as follows:

- **Title**—The text entered in the **Title** field along with the catalog item icon, will be displayed when viewing this catalog item on the **Browse Catalog** tab.

- **Brief Description**—When viewing catalog items in list view, the brief description will also be visible:

- **Full Description**—The text entered in the **Full Description** field will be displayed when a catalog item is viewed in its detail view, which is opened by clicking on the catalog item name in either the list or card view.

12. When you are finished editing the fields on the **Catalog Item Title and Category** panel, click **Next**. If you are connected to the Flexera Service Gateway, the **Flexera ID** panel opens

13. To track licenses for this catalog item using its Flexera ID, use the column filters to locate this catalog item in FlexNet Manager Suite, select it, and click **Next**. The **Ready to Create** panel opens.

14. If, after this catalog item is created, you want to immediately open this catalog item's **Catalog Item Properties** dialog box, where you can specify advanced settings, select the **Load advanced view after creating the catalog item** option.

15. Review the summary information and then click **Create** to create this new catalog item. The catalog item will now be listed on the **Browse Catalog** tab in the category you selected.

Note • *After creating a catalog item, you can edit its basic and advanced settings on the* **Catalog Item Properties** *dialog box, as described in* Setting Catalog Item Properties.

Creating a Task Sequence Catalog Item for OSD Deployment

A task sequence is a mechanism used in System Center 2012 Configuration Manager for performing multiple steps or tasks on a client computer at the command-line level without requiring user intervention. Task sequences are used by SCCM to deploy operating systems.

To create a task sequence catalog item, perform the following steps:

Task   ***To create a task sequence catalog item:***

1. If you want to create a licensed **Software** catalog item, make sure that you have performed the steps in Connecting to the Flexera Service Gateway.

2. Under **Catalog Management**, select **New Catalog Item Wizard**. The **Catalog Item Type** panel of the **New Catalog Item Wizard** opens.

3. Select **Task Sequence** and click **Next**. The **SCCM 2012 Task Sequences** panel opens.

4. Select the task sequence that you want to associate with this catalog item.

5. If the selected task sequence is used to deploy an operating system, select the **Is OS Deployment?** option.

6. Click **Next**. The **Catalog Item Title and Category** panel opens.

7. In the **Title** field, enter a title to identify this catalog item in your App Portal storefront. By default, the name of the task sequence that you selected is listed in this field.

8. From the **Category** field, select a category to specify this catalog item's location in the App Portal catalog. You are required to select at least one category, but you may select more than one.

9. In the **Brief Description** field, enter the text that you want to display under the catalog item **Title** in the App Portal storefront.

10. By default, a generic icon is associated with this catalog item. To associate a custom icon to this catalog item, click **Change** to open the **Image Selection** dialog box and select a `.gif`, `.jpg`, or `.png` icon file.

Tip • For best results, the uploaded image should be 80 px by 80 px or larger.

11. Optionally, from the **Template** list, select an existing template to apply advanced settings to this catalog item.

Note • For more information, see Creating a Catalog Item Template.

12. In the **Search Keywords** text box, enter single words that an end user might enter when searching for this catalog item.

13. In the **Full Description** text area, enter a longer description of this catalog item, and use the items on the toolbar to format it.

The text entered in the **Title**, **Brief Description**, and **Full Description** fields will be displayed as follows:

- **Title**—The text entered in the **Title** field along with the catalog item icon, will be displayed when viewing this catalog item on the **Browse Catalog** tab.

- **Brief Description**—When viewing catalog items in list view, the brief description will also be visible:

- **Full Description**—The text entered in the **Full Description** field will be displayed when a catalog item is viewed in its detail view, which is opened by clicking on the catalog item name in either the list or card view.

14. When you are finished editing the fields on the **Catalog Item Title and Category** panel, click **Next**. If you are connected to FlexNet Manager Enterprise Suite, the **Flexera ID** panel opens.

15. To track licenses for this catalog item using its Flexera ID, use the column filters to locate this application or package in FlexNet Manager Suite, select it, and click **Next**. The **SCCM 2012 Task Sequence Deployment Settings** dialog box opens.

16. Specify the following deployment settings:

Property	Description
Make the advertisement mandatory	Select this option to make this task sequence a mandatory installation for all clients of the associated advertised group.
Mandatory over slow links?	Select this option to require that the installation is run even when a client has a slow connection. If this option is not selected, the SCCM client agent will not perform the installation if the client has a slow connection, but will perform the installation if the client is connected over a regular LAN connection.
Advertisement Priority	Specify the priority of the advertisement: **High**, **Medium**, or **Low**.
Ignore maintenance windows	Select to have the advertised program ignore maintenance windows while the program is running.
Allow system restart outside of maintenance windows	Select to allow the advertised program to restart the client even if the restart would occur outside a maintenance window.
Show the task sequence progress	Select to make the task sequence progress bar visible to users.
Make this task sequence available to boot media and PXE	Select to make the advertisement available to boot media and PXE clients.
Program rerun behavior	Specifies whether the advertised program will be rerun on the client computer if it has previously been run before the scheduled mandatory time. Select one of the following options: • **Never rerun advertised program**—The program will not be rerun on the client if the program has previously been run on the client, even if the program originally failed or the program files have been changed. • **Always rerun**—The program will always be rerun on the client when the advertisement is scheduled, even if the program has already been successfully run. • **Rerun if failed previous attempt**—The program will be rerun when the advertisement is scheduled only if it failed on the previous run attempt. • **Rerun if succeeded on previous attempt**—The program will be rerun only if it has previously run successfully on the client. *Important • This option is only enabled if **Make the advertisement mandatory** is also selected.*

Property	Description
Download options	Select one of the following options to specify how content will be downloaded from the distribution points when a distribution point is available locally:
	● **Download content locally when needed by running task sequence**
	● **Download all contents locally before starting task sequence**
	● **Access content directly from a distribution point when needed by the running task sequence**
When no local distribution point is available, use a remote distribution point	Select this option to specify that when no distribution point is available locally, run the program directly from a remote distribution point.
When no protected distribution point is available, use an unprotected distribution point	Select this option to permit a client to use an unprotected distribution point if content is not immediately available on its protected distribution point.
	If this option is not selected, the client will not use unprotected distribution points.

17. Click **Next**. The **Ready to Create** panel opens.

18. If, after this catalog item is created, you want to immediately open this catalog item's **Catalog Item Properties** dialog box, where you can specify advanced settings, select the **Load advanced view after creating the catalog item** option.

19. Review the summary information and then click **Create** to create this new catalog item. The catalog item will now be listed on the **Browse Catalog** tab in the category you selected.

*Note • After creating a catalog item, you can edit its basic and advanced settings on the **Catalog Item Properties** dialog box, as described in Setting Catalog Item Properties.*

Creating a New Catalog Item (Advanced)

In addition to creating a new software item using the **New Catalog Item Wizard**, you can choose to create a catalog item using the **New Catalog Item Properties** dialog box, which enables you to configure advanced settings during catalog item creation. For detailed instructions, see:

- Creating a New Catalog Item (Advanced) From SCCM

- Creating a New Catalog Item (Advanced) From Altiris

Note • You must use this advanced method to create catalog items containing virtual applications from SCCM.

Important • To create an AirWatch mobile application catalog item, you must use the wizard interface as described in Creating an AirWatch Mobile Application Catalog Item. After you have created the mobile application catalog item, you can then set additional properties on the Catalog Item Properties dialog box.

*Note • If you would prefer to quickly create a catalog item by only specifying the required options using a wizard interface, you can use the **New Catalog Item Wizard**, as described in the following topics:*

- *Creating a General Catalog Item*
- *Creating a ConfigMgr / SCCM 2012 Software Catalog Item*
- *Creating an Altiris Software Catalog Item*
- *Creating a Task Sequence Catalog Item for OSD Deployment*

Creating a New Catalog Item (Advanced) From SCCM

To create a new catalog item from SCCM 2012 using the multi-tabbed **New Catalog Item Properties** dialog box, perform the following steps:

Task   *To create a new catalog item from SCCM using the New Catalog Item Properties dialog box:*

1. Open the **Admin** tab, and click on **Catalog Management**:

2. Under **Create New Catalog Item**, click on **New Software Catalog Item**. The **General > Global** tab of the **New Catalog Item Properties** dialog box opens.

Note • *Until you enter settings and click* **Save***, only the* **General** *tab of the* **New Catalog Item Properties** *dialog box is enabled.*

3. On the **General > Global** tab of the **New Catalog Item Properties** dialog box, click on the **Category** list and select a category for this catalog item.

📄

Note • For information on creating a catalog category, see Creating a Catalog Category.

4. To require the requester to answer some questions when they submit a request for this catalog item, select a template from the **Question Template** list.

📄

Note • A question template is a group of questions to ask the end user at the time of request. For more information, see Managing Questions and Question Templates and Attaching a Question Template.

5. Select any other desired properties on the **General** tab, as described in General Tab.

6. Open the **Title & Description** subtab of the **General** tab, and enter a title for this new catalog item.

7. Click **Save** to create the new catalog item. A message appears stating that a catalog item has been created.

8. Open the **Deployment > Global** subtab and specify any desired deployment options, as described in Global Subtab.

9. Open the **Deployment > SCCM 2012** subtab.

10. Click **Add Package**. The **Add Package** dialog box opens, displaying subtabs that list all of the applications, packages, task sequences, and virtual applications in the connected SCCM 2012 server:

11. Open the subtab of the type of item you want to add to this catalog item: **Applications**, **Packages**, **Task Sequences**, or **Virtual Applications**.

12. Select one of the listed items and click **Add Program**. The SCCM Deployment Dialog Box for the selected item opens, displaying different options in the **SCCM Object** area, depending upon the type of **Software** catalog item you are creating:

13. **For applications**, perform the following steps:

    a.   From the **Select deployment method** list, select **Deploy to user** or **Deploy to computer**.

    b.   You can choose to **Create Uninstall Collection**.

14. **For packages**, perform the following steps:

    a.   Select the matching program name for each program function: **Install**, **Uninstall**, and **Repair**.

       ● If you have enabled **Uninstall** or **Repair** in the global settings, the uninstall and repair programs are required.

       ● You can have multiple installation programs for different languages within a single request.

       ● If programs are specified for more than one language, the requester will select the language during the checkout process.

    b.   Under **Program for OS Deployment Task Sequence**, select a matching program name for the program function.

15. Under **Select sites to publish**, select the sites where this request will be available, the locations you wish to publish the catalog item to. An advertisement and collection will be created at the site(s) selected.

16. Select any other desired properties on the **SCCM Deployment** dialog box, as described in Attaching a Program to Deploy a Catalog Item to System Center Configuration Manager.

17. Click **Save**. The deployment or program is now listed on the **Deployments** or **Programs/Task Sequences** subtab of the **Catalog Item Properties** dialog box.

18. You can now edit additional settings, if desired, on the **Catalog Item Properties** dialog box, as described in Setting Catalog Item Properties.

Creating a New Catalog Item (Advanced) From Altiris

To create a new catalog item from Altiris using the multi-tabbed **New Catalog Item Properties** dialog box, perform the following steps:

Task　　**To create a new catalog item from Altiris using the New Catalog Item Properties dialog box:**

1. Open the **Admin** tab, and click on **Catalog Management**:

2. Under **Create New Catalog Item**, click on **New Software Catalog Item**. The **General > Global** tab of the **New Catalog Item Properties** dialog box opens.

*Note • Until you enter settings and click **Save**, only the **General** tab of the **New Catalog Item Properties** dialog box is enabled.*

3. On the **General > Global** tab of the **New Catalog Item Properties** dialog box, click on the **Category** list and select a category for this catalog item.

    Note • For information on creating a catalog category, see Creating a Catalog Category.

4. To require the requester to answer some questions when they submit a request for this catalog item, select a template from the **Question Template** list.

    Note • A question template is a group of questions to ask the end user at the time of request. For more information, see Managing Questions and Question Templates and Attaching a Question Template.

5. Select any other desired properties on the **General** tab, as described in General Tab.

6. Open the **Title & Description** subtab of the **General** tab, and enter a title for this new catalog item.

7. Click **Save** to create the new catalog item. A message appears stating that a catalog item has been created.

8. Open the **Deployment > Global** subtab and specify any desired deployment options, as described in Global Subtab.

9. Open the **Deployment > Altiris** subtab.

10. To add a software product from Altiris, perform the following steps:

*Note • For instructions on adding an Altiris policy, skip to Step **11.***

a. Click **Add Software Product**. The **Add Software Product** dialog box opens, listing all of the software products in the connected Altiris server:

b. Select the software product that you want to add and click **Add Program**. The **Altiris Software Product Deployment** dialog box opens:

c.   From the **Select deployment method** list, select **Deploy to user** or **Deploy to computer**.

d.   If you have multiple installation programs for different languages within a single request, select the **Show all languages** option.

> **Note •** *If programs are specified for more than one language, the requester will select the language during the checkout process.*

e.   Select the matching program name for each program function: **Install**, **Uninstall**, and **Repair**.

   ● If you have enabled **Uninstall** or **Repair** in the global settings, the uninstall and repair programs are required.

   ● You can have multiple installation programs for different languages within a single request.

   ● If programs are specified for more than one language, the requester will select the language during the checkout process.

f.   Under **Select sites to publish**, select the sites where this request will be available, the locations you wish to publish the catalog item to.

g.   Click **Save**. The deployment or program is now listed on the **Deployments** or **Programs/Task Sequences** subtab of the **Catalog Item Properties** dialog box.

11.   **To add a policy from Altiris**, perform the following steps:

a.   On the **Deployment > Altiris** tab, click **Add Existing Policy**. The **Add Existing Policy** dialog box opens.

b.   Select a policy and click **Next**, the **Software Delivery Item** tab opens.

c. From the **Select Deployment Method** list, select one of the following options:

- **Deploy to user**

- **Deploy to computer**

d. The **Select Software Delivery Item** list lists all of the software delivery items that are included in the selected Altiris policy. Select the software delivery item that you want this new **Software** catalog item to contain.

e. From the **Select Deployment Type** list, select one of the following items to match the purpose of the selected software delivery item:

- **Install**

- **Uninstall**

- **Repair**

f. Click **Add Program**. The policy is now listed on the **Deployment > Altiris** tab.

12. Proceed with editing the properties on the remaining tabs of the **Catalog Item Properties** dialog box, as described in Setting Catalog Item Properties.

Creating a Group Catalog Item

Catalog items can be configured to be selected as a bundle of separate applications. This is called a *group catalog Item*.

Figure 4-5: Group Catalog Item (Indicated by Special Icon)

If a requester adds a group catalog item to their cart, all of the applications in that group are added to the cart. However, if the **Allow removal from bundle?** option is selected for a catalog item on its **Catalog Item Properties** dialog box, the requester can choose to remove that catalog item from the bundle before adding it to their cart by clearing the checkbox.

To create a group catalog item, perform the following steps.

Task   **To create a group catalog item:**

1. Open the **Admin** tab.

2. Under **Catalog Management**, select **Create New Catalog Item > New Group Catalog Item**. The **General > Global** tab of the **Catalog Item Properties** dialog box opens.

Note • *Until you enter settings and click* ***Save****, only the* ***General*** *tab of the* ***Catalog Item Properties*** *dialog box is enabled.*

3. From the **Category** list, select a category for this group catalog item.

4. Open the **Title & Description** tab and enter a title for this bundle of catalog items.

5. Click **Save**. The other tabs of the dialog box are now enabled.

6. Open the **Catalog Items** tab. Catalog items are listed in the **Available Catalog Items to Group** list, and no catalog items are listed in the **Current Grouped Catalog Items** list.

7. In the **Available Items to Group** list, select the catalog items that you want to add to the group and then click **Group Programs**. The selected catalog items are now listed in the **Current Grouped Catalog Items** list.

8.   Set options on the following tabs, if desired:

   ●   Controlling Visibility of a Catalog Item by Adding Conditions

   ●   Attaching an Approval Workflow to a Catalog Item

   ●   Assigning Permissions to a Catalog Item

Creating a Catalog Item Template

When you create a new catalog item, you can select an existing template to load settings from a previously created catalog item. For catalog items with a complex set of properties, creating a template to use during catalog item creation could prove to be quite beneficial.

Task   **To create a catalog item Template:**

1. Open the **Admin** tab, and click on **Catalog Management**:

2. Locate an existing catalog item that you would like to use as a template.

3. Double-click that catalog item to open its **Catalog Item Properties** dialog box.

4. On the **General > Global** tab, enter a name for the template in the **Template Name** text box.

5. Click **Save**. The next time that you create a new catalog item, you will be able to select this template when creating a new catalog item:

- **New Catalog Item Wizard**—The template will be listed in the **Template** list on the **Catalog Item Title and Category** panel.

- **New Catalog Item Properties Dialog Box**—The template will be listed in the **Load settings from template** list on the **General > Global** tab.

*Note • After you click **Save** on the **New Catalog Item Properties** dialog box the first time, the **Load settings from template** property will no longer be listed on the **General > Global** tab.*

Enabling Express Checkout: Install Now Button

When requesting a catalog item, you can give users the option of bypassing the checkout process by clicking the **Install Now** button.

Figure 4-6: Install Now Button on Browse Catalog Tab

When the user clicks the **Install Now** button, a catalog item request is automatically generated for that single catalog item, bypassing the checkout experience altogether. In the event that the user has more than one associated device, a pop-up window will prompt the user to select the desired target system.

Figure 4-7: Choose Target Dialog Box

To enable express checkout, select the **Enable express checkout** option on the **Catalog Behavior** tab of the **Site Management > Settings > Web Site** view.

Figure 4-8: Enable Express Checkout Option

Even when express checkout is enabled, not all catalog items will display an **Install Now** button. Also, in some instances, you cannot use express checkout even when the **Install Now** button is displayed.

- Conditions Preventing Display of Install Now Button

- Conditions That Prevent Use of Express Checkout

Conditions Preventing Display of Install Now Button

If any of the following conditions are met, the **Install Now** button will not be displayed even when the **Enable express checkout option** is selected.

Table 4-3 • Conditions Preventing Display of Install Now Button

Condition	Description
Question templates	If the catalog item has an associated question template, the **Install Now** button is not displayed.
Custom approvers	If the catalog item has an approval workflow associated with it that prompts the requester to select a custom approver, the **Install Now** button is not displayed. *Note • If the catalog item has a standard approval workflow associated with it, the **Install Now** button will be displayed. When the requester clicks **Install Now**, a message will be displayed stating that installation will begin once the request has been approved.*
Constraints, Leasing, or Allow switch to? settings	If the catalog item has **Constraints, Leasing**, or **Allow switch to?** settings defined, the **Install Now** button is not displayed.
Task sequence catalog items	For OSD/task sequence catalog items, the **Install Now** button is not displayed.
Cloud catalog items	For cloud catalog items—such as Box, Office 365 or Salesforce—the **Install Now** button is not displayed.

Table 4-3 • Conditions Preventing Display of Install Now Button

Condition	Description
General catalog items	For **General** catalog items, the **Install Now** button is not displayed.
Group catalog items	For **Group** catalog items, the **Install Now** button is not displayed.
File upload	If a catalog item has the **Allow File Upload?** option selected on the **General > Global** tab of the **Catalog Item Properties** dialog box, which enables a user to upload a file during checkout, the **Install Now** button is not displayed.
User defined scheduling	If a catalog item has the **Enable user defined scheduling?** option selected on the **General > Global** tab of the **Catalog Item Properties** dialog box, the **Install Now** button is not displayed.

Conditions That Prevent Use of Express Checkout

Even if the **Install Now** button is displayed, you cannot perform express checkout in the following scenarios:

- **Multiple catalog item request**—You can only use the **Install Now** button to request one catalog item at a time. If you want to request more than one catalog item in the same request, you are required to add all catalog items to the cart and proceed through the regular checkout process.

- **Request on behalf**—If you are requesting a catalog item on behalf of another user, you cannot use the **Install Now** button to submit the request. You instead are required to add the catalog item to the cart and proceed through the regular checkout process.

Managing Approval Workflows

Approval workflows are applied to catalog items to define how a request will be routed for review. In each step of an approval workflow, a user or group reviews the request.

- About Approval Workflows

- Creating a New Approval Workflow

- Setting Additional Workflow Step Properties

- Managing Approval Groups

- Managing Workflow Status

- Configuring a Workflow Step to Execute a Custom Action

- Using the Custom Approver Feature

About Approval Workflows

Approval workflows can be dynamic or static, and can have conditions applied to them.

- Dynamic vs. Static Workflow Steps

- Using Conditions

Dynamic vs. Static Workflow Steps

Each workflow step (also referred to as a level) can be either dynamic or static:

- **Dynamic** steps are evaluated based on user and computer conditions. For example, if the workflow step is defined as **Manager**, the end user's manager will be required to approve the request.

- **Static** steps are the same regardless of who requests it or where it goes. For example, if the workflow step is assigned to a specific user, that same user will be required to approve all requests for this catalog item, no matter which end user requests it.

Workflows are defined and listed on the **Workflows View**, which is opened by selecting **Workflows** under **Site Management** on the **Admin** tab.

Using Conditions

Workflows and workflow steps can have conditions applied to them. Conditions determine whether the workflow and / or workflow step should be applied to the given situation.

- **Single workflow applied to catalog item**—When you assign a single workflow to a catalog item, the conditions of the *workflow* are not evaluated; only the *workflow step* conditions are evaluated.

- **Multiple workflows applied to catalog item**—When you apply more than one workflow to a catalog item, the conditions of the workflow as well as the steps within that workflow are evaluated.

Conditions can be based on user attributes including group and OU membership, AD property value, deployment system collection membership for both users and computers, and catalog item properties such as cost and inventory availability. Conditions can also be based upon the answer that a user gives to a question (from the catalog item's associated Question Template) when requesting a catalog item.

Creating a New Approval Workflow

To create a new approval workflow, perform the following steps.

Task   ***To create a new approval workflow:***

1.   On the **Admin** tab, select **Workflows** under **Site Management**. The **Workflows View** opens.

2.   Click **New Workflow**. The **General** tab of the **Workflow Properties** dialog box opens.

3.   In the **Workflow Name** field, enter a friendly name to identify this workflow, such as `Finance Application Workflow` or `Engineering Application Workflow`.

4.   In the **Workflow Description** field, provide details about the workflow and its use.

5.   From the **Process Type** list, select one of the following options:

- **Linear**—The approval process functions in a linear fashion. Each approver must approve the request in order as defined in each workflow step.

- **Pool**—Anyone in any workflow step can approve the request. It takes only one approver to approve the request. All approvers will be notified of the request.

- **Pool within Group**—This option will allow anyone within a workflow to approve the request before it is forwarded to the next workflow step.

6. To enable the requester to change who the members of the workflow step are, select the **Allow requester to define workflow** option.

7. Open the **Workflow Steps** tab.

Note the following regarding workflow steps:

- Workflow steps are executed from top to bottom.

- Each step can be configured with conditions to determine whether the step will be used.

- Steps can contain direct members, static approval groups, and dynamic approval groups.

- Steps can also execute custom actions when that step is processed.

8. Click **Add New Level**. A dialog box pops up prompting you to make a selection.

9.   To add a static set of approvers, select a group in one of the following approval group categories:

●   **User Approval Group (Static)**

●   **Property Approval Group (Static)**

●   **OU Approval Group (Static)**

●   **Collection Approval Group (Static)**

*Note • To create a new approval group, select **Approval Groups** under **Site Management**.*

Note • Approvers within these types of groups are static; they do not change based on user or computer conditions.

10. If you want to add a dynamic set of approvers, select one of the following under **Dynamic Approval Groups**:

Option	Description
Manager	Uses the Manager attribute from Active Directory.
Computer - Managed By	Uses the Managed By attributes of the computer object in Active Directory.

Option	Description
<Property Defined Group>	Uses the approvers specified for the property defined.
	For example, create a property-based approval group for the IT Department. Then, specify the group to use the department attribute and the values include `IT Department`, `Info Tech`, and `Information Technology` values from the department attribute in Active Directory. This action exposes the **Department** attribute under the Dynamic Approval Group.
	Adding the **Department** as a workflow step will cause the workflow to look at the requesting users department, search for a value that matches `IT Department`, `Info Tech`, or `Information Technology` and use the corresponding approvers identified for that group.

📄

Note • *In order to effectively use dynamic approval groups you should have Approval Groups created for every value of the property you choose to use.*

📄

Note • *Dynamic approval groups display properties, not actual groups. When you create a dynamic approval group for at least one property (department, OU, collection, etc.) that property is exposed here.*

11. Click **Add Selected Group**. The new workflow step is now listed on the **Workflow Steps** tab.

📄

Note • *For more options available to you regarding workflow steps, see* *Setting Additional Workflow Step Properties.*

12. Open the **Conditions** tab of the **Workflow Step Properties** dialog box, which lists any conditions that are applied to the workflow step.

The conditions that you apply to a workflow step determine when the step should apply.

- Conditions specified here are limited to **Include**, meaning you define conditions when you want the item to apply.

- Adding a **Question Condition** enables you to base the condition on an answer that an end user gives when submitting the request.

- An additional condition, **Catalog Item**, offers the ability to include a step based on the license availability and cost of a catalog item.

13. To add a condition to a workflow step based on **Group and OU**, **AD Property**, or **Collections**, perform the following steps:

    a. Open the **Group and OU**, **AD Property**, or **Collections** tab and click **Add Condition**. A dialog box pops up and prompts you search for a group or OU, AD property, or collection.

    b.   Select one or multiple items and click **Select**. The selected items are now listed on the **Conditions** tab. Close the pop-up dialog box.

- If you selected OUs, select the **Apply to OU and child OUs** option, if desired.

- If you selected an **AD Property**, use the lists in the **Operator** and **Enforcement** (if necessary) columns to specify the condition.

- If you selected a **Collection**, use the **Enforcement** list to specify the condition, if necessary.

14. To add a condition to a workflow step based on the answer the end user provides to a question asked during request submission, perform the following steps:

    a.   First, make sure that you have created a Question Template that contains a question with a single-response answer (**Dropdown List**, or **Radio Button List**), as described in Managing Questions and Question Templates.

    b.   On the **Workflow Step Properties** dialog box, open the **Conditions > Question Condition** tab.

    c.   From the **Please select the Question Condition** list, select the question that you want to use to create this condition.

    d.   From the **Please select the Question Condition Value** list, select the response that would satisfy this condition.

    e.   Click **Save**.

15. If you want to add a condition to the entire workflow, open the **Conditions** tab of the **Workflow Properties** dialog box and perform the steps listed above to add a condition.

Workflows and workflow steps can have conditions applied to them. Conditions determine whether the workflow and / or workflow step should be applied to the given situation:

- **Single workflow applied to catalog item**—When you assign a single workflow to a catalog item, the conditions of the *workflow* are not evaluated; only the *workflow step* conditions are evaluated.

- **Multiple workflows applied to catalog item**—When you apply more than one workflow to a catalog item, the conditions of the workflow as well as the steps within that workflow are evaluated.

16. Open the **Applies To** tab, which you can use to identify which catalog items that this workflow applies to.

Note • *If more than one workflow is applied to a single catalog item, the conditions on the workflow will be evaluated to determine which one to use. If more than one workflow applies to a given catalog item, the first workflow identified will be used.*

Note • *Be cautious not to create conditions that overlap.*

17. Open the **Simulate** tab, on which you can enter a user ID or a computer name so that you can simulate the approval process for that user or computer.

18. Enter the user ID or computer name and click **Show approval process**. The approval process is displayed:

19. Click **Save**. The new approval workflow is now listed on the **Workflows View**.

Setting Additional Workflow Step Properties

You can modify additional properties of a workflow step by double-clicking the step on the **Workflow Steps** tab of the **Workflow Properties** dialog box.

Figure 4-9: Workflow Step Properties Dialog Box

You can edit three types of workflow step properties:

- Setting Workflow Step Options

- Applying Conditions to a Workflow Step

- Defining a Custom Action on a Workflow Step

Setting Workflow Step Options

The **Options** tab of a workflow step's **Properties** dialog box includes the following properties:

Table 4-4 • Workflow Step Properties

Property	Description
Approver Type	Select one of the following options:
	- **Reviewer**
	- **Purchaser**
Set Status	Select a custom status for this workflow step.
	Workflow status is created and managed under **Settings > Workflow Status**. Setting a status other than Default Status will set the request with the identified status when that workflow step is in progress.
Set Action	Software installations are typically triggered and allowed for installation after all workflow steps have occurred. If you wish to have this action occur earlier in the workflow process, identify the step in which you want the software install action to occur.

Table 4-4 • Workflow Step Properties

Property	Description
Question template	Select a question template to link to the specified workflow step. When a question template is linked to a workflow step, the approvers at that step will be presented with those questions. If there are required questions within the question template, the request cannot move to the next workflow step until all required questions have been answered.
Allow Approval Level User Edit	Select this option if you wish to allow this specific approval step to be identified by the requester. With this option enabled the requester will be able to change the users within this step.

Applying Conditions to a Workflow Step

The **Conditions** tab of a workflow step's **Properties** dialog box lists any conditions that are applied to the workflow step.

Figure 4-10: Conditions Tab of Workflow Step Properties Dialog Box

The conditions that you apply to a workflow step or the workflow itself determines when the step or workflow should apply. Conditions specified here are limited to **Include**, meaning you define conditions when you want the item to apply. An additional condition, **Catalog Item**, is present only for workflow step and workflow conditions. This condition offers the ability to include a step or apply a workflow based on the license availability and cost of a catalog item.

Defining a Custom Action on a Workflow Step

You can have a workflow step execute a custom action. Custom actions are defined under **Site Management > Commands and Actions**. You can use a custom action to execute an executable, script, web service, etc.

Figure 4-11: External Actions Tab of Workflow Step Properties Dialog Box

Managing Approval Groups

Approval groups are used to group users or groups together to identify a group of approvers. Approval groups are then linked to catalog items indicating that the catalog item should go through workflow process.

- Creating a New Approval Group

- Editing an Approval Group

- Setting the Default Approval Group

Creating a New Approval Group

To create a new Approval Group, perform the following steps:

Task   ***To create a new Approval Group:***

1. Under **Site Management > Approval Groups**, select the **New Group** node. The **Workflow Type** tab of the **New Approval Group** dialog box opens.

2. Enter a **Group Name** for the approval group

3. Select a **Group Type**:

   - **User group**—Users organized in a specific order. You apply user groups directly to a workflow step. User groups are used when the approvers do not change.

   - **Active Directory Property Group**—These groups allow you to relate users to AD properties like departments and offices. Create these groups when you want to route requests based on these attributes. E.g. marketing approvers or Chicago office approvers.

   - **Organizational Unit**—These groups allow you to relate users to AD OUs. Create these groups when you want to route requests based on user or computer location within the AD OU hierarchy.

   - **User Collection**—Enables you to relate users to collections on your deployment system. Create these groups when you want to route requests based on user collection membership within your deployment system.

   - **Computer Collection**—Enables you to relate users to collections on your deployment system. Create these groups when you want to route requests based on computer collection membership within your deployment system.

4. From the **Workflow family** list, select an Approval workflow family. Approval workflow families are created and managed on the **Approval Groups > Families** view under **Site Management**.

5. Click **Next**. If you have selected any **Group type** other than **User group**, the **Workflow Properties** tab opens, where you can group the properties for the group type selected.

6. On the **Workflow Properties** tab, if required, use the search fields to populate the **Available** properties list. Then use follow the instructions to move the properties from the **Available** box to the **Current** box.

7. Click **Next**. The **Workflow Members** tab opens.

8. On the **Workflow Members** tab, first search for users or groups to populate the search results box. Then select a user or group and click the arrow to move it to the Selected list.

9. Click **Save** to create the **Approval Group**.

10. Under **Approval Groups**, click the **User Groups**, **Property Groups**, **OU Groups**, or **Collection Groups** node to view the newly created group.

Editing an Approval Group

To edit an existing approval group, perform the following steps:

___

Task   **To edit a approval group:**

1. Under **Site Management > Approval Groups**, select the node containing the approval group that you want to edit: **User Groups**, **Property Groups**, **OU Groups**, or **Collection Groups**.

    Existing approval groups are listed in the right pane.

2. Double-click on the approval group that you wish to edit. The **Approval Group Properties** dialog box for that approval group opens.

3. Edit the approval group properties, as described in Creating a New Approval Group.

Setting the Default Approval Group

To set the default approval group, perform the following steps:

___

Task   **To set the default approval group:**

1. Under **Site Management**, open the **Settings > Web Site** view and, open the **General** tab.

2. From the **Default Approval Group** field, select a approval group.

    The default approval group is used in the event approval is specified and no approvers are defined or you are using a dynamic approval process and the approvers could not be determined (such as if you specified manager approval and the user does not have a manager defined).

3. Click **Save**.

Managing Workflow Status

Workflow steps allow the customization of the status regarding the workflow process. You customize status on the **Site Management > Workflow Status** view.

Figure 4-12: Workflow Status

You can create your own workflow status to convey the progress, state, or otherwise identify what is happening at the particular workflow step.

Task   ***To create a workflow status:***

1. Under **Site Management** select **Workflow Status**. The Workflow Status view opens.

2. Click **Add Status**. The **Create New Status** dialog box opens.

3. In the **Status Name** field, enter a name to identify this new status.

4. In the **Status Description** field, enter a description of the meaning of this status.

5. From the **Status Icon** list, select an icon that will indicate this new status in the App Portal user interface.

Configuring a Workflow Step to Execute a Custom Action

You can have a workflow step execute a custom action. Custom actions are defined under **Site Management > Commands and Actions**. You can use a custom action to execute an executable, script, web service, etc.

Commands allow arbitrary commands to be executed against a selected machine from the support tools section in the software store or as part of a request at one or more stages during the request life cycle. **Client Commands** and **Server Commands** that are executed run under the context of the visiting user and are invoked using JavaScript. Server commands run under the context of the App Portal account specified during setup. Use of commands executed from the client requires modification of Internet Explorer security settings to allow Active X content.

Commands and actions are defined on the three subviews of **Site Management** > Commands and Actions:

●   Script Commands

●   Web Service Commands

●   Request Commands

To configure a workflow step to execute a custom action, perform the following steps:

Task   *To configure a workflow step to execute a custom action:*

1. Create a script, web service, or request command, as described in the following three topics:

   - Script Commands

   - Web Service Commands

   - Request Commands

2. Open the **Site Management** > **Workflows** view and double-click a workflow to open the **Workflow Properties** dialog box.

3. Open the **Workflow Steps** tab.

4. Either click **Add New Level** to create a new workflow step or double-click on an existing workflow step. The **Workflow Step Properties** dialog box opens.

5. Open the **External Actions** tab.

6. From the **Select a service** and **Select a method or command** lists, select the appropriate service and command.

7. Click **Save**.

Using the Custom Approver Feature

If the built-in feature of selecting approvers using workflows does not satisfy your requirements, you can define a custom query to select approvers based on the Active Directory attributes of logged-in end users. To implement the ability to specify custom approvers, perform the following steps:

Task   ***To use the custom approver feature:***

1. Enable the custom approver feature by executing the SQL query below:

   ```
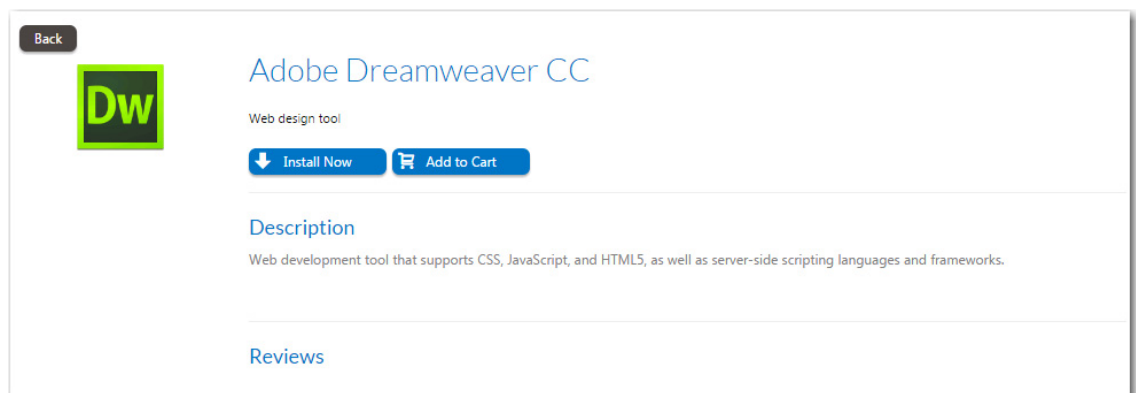   update WD_AppSettings set Value = 'True' where KeyName = 'UseCustomApproverSearch'
   ```

   Note • *If you want to pass the user name of the logged in user to the stored procedure, then you need to use the* sAMAccountName *as the custom variable:*

   ```
   update wd_appsettings set Value = 'sAMAccountName' where KeyName = 'CustomApproverSearchVariable'
   ```

2. Define the AD user property that will be used to filter the approvers.

   - The value of this property for the currently logged in user is passed to the custom stored procedure.

   - The default attribute is Department.

   This means that if the feature is enabled, and the end user chooses the custom approval option, App Portal will load all the users in the department that the user belongs to.

3. To switch the AD property that App Portal needs to use, change the SQL below accordingly:

   ```
   update WD_AppSettings set Value = 'Department' where KeyName = 'CustomApproverSearchVariable'
   ```

4. Restart IIS or go to the **Admin > Settings** view and click **Save** to reload the cache.

5. Verify that the stored procedure sp_Search_Custom_Approver exists.

   If needed, you can use the following SQL to create the stored procedure:

   ```
   IF EXISTS (
       SELECT *
       FROM sysobjects
       WHERE id = object_id(N'[dbo].[sp_Search_Custom_Approver]')
       )
   BEGIN
       DROP PROCEDURE [dbo].[sp_Search_Custom_Approver]
   END
   GO
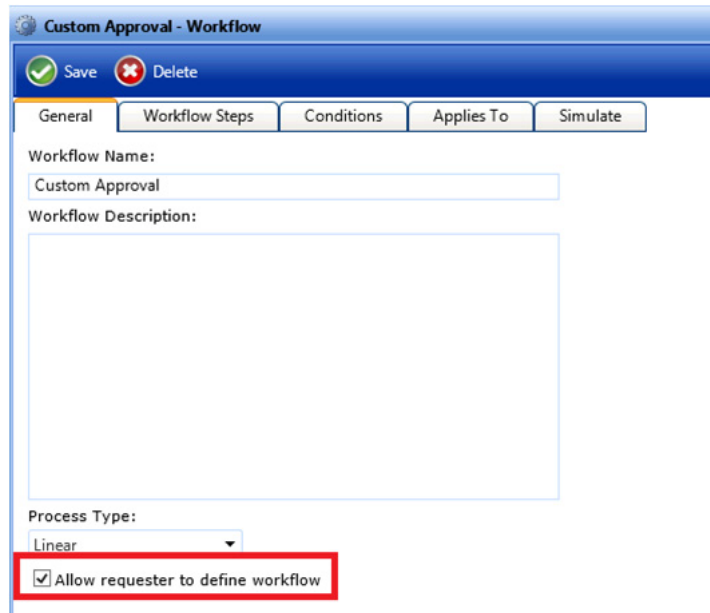
   CREATE PROCEDURE [dbo].[sp_Search_Custom_Approver] @Variable VARCHAR(500), @Level int,
   @ApprovalTemplateID int, @TotalCost float
   AS
   BEGIN
       -- SET NOCOUNT ON added to prevent extra result sets from
       -- interfering with SELECT statements.
       SET NOCOUNT ON;

       -- Insert statements for procedure here
       SELECT DISTINCT ADSPath, UserName, Department, Office, FullName FROM vUser where Department LIKE
   '%' +  @Variable + '%'
   END
   GO
   ```

6. Edit the stored procedure as needed.

7. Create a new approval workflow and choose the **Allow requester to define workflow** option.

8. Create a new workflow step, assign a default approver, and choose the **Allow Approval Level User Edit** and **Force Approval Level User Edit** options.

9. Attach the approval workflow to a catalog item. When you checkout the software, you will see the following screen with the option to specify the approver:

10. Clicking on the **Specify Approver** button will call the stored procedure and pass in the value of the approval property defined in Step 2 to the stored procedure, which will return the results accordingly. In this case, it will return all the users in the **Department** of Schaumburg.

Managing Questions and Question Templates

When submitting a software request, sometimes the end user needs to answer a set of questions that will give App Portal the information it needs in order to fulfill that software request.

For example, in order to approve a software request, a manager may want to know the name of the project that the end user is working on that requires this application. Or, in order to determine licensing requirements, the manager may want to know how frequently the end user will use this application or the time of day that it would be used.

In App Portal, you use the **Question Manager** to create questions, then group those questions into question templates using the **Template Manager**. This section explains how to create questions, add questions to a question template, and how to attach a question template to a catalog item:

● Creating Questions

● Creating Questions With Conditions

- Creating a Question Template

- Default Question Templates

After you have created a Question Template, you can then attach it to a catalog item, as described in Attaching a Question Template.

Note • *For information on localizing questions and answers, see Localizing Questions and Answers.*

Tip • *In addition to associating a question template to a catalog item, you can also associate a question template with a workflow step. When a question template is linked to a workflow step, the approvers at that step will be presented with those questions. If there are required questions within the question template, the request cannot move to the next workflow step until all required questions have been answered. For example, the approver might be requested to enter a budget code for the expense. For more information, see Managing Approval Workflows.*

Creating Questions

Before you can create a Question Template, which can be attached to a catalog item, you first need to create questions.

To create a new question, perform the steps listed in Creating a New Question. If the question has an input type of **Checkbox List**, **Dropdown List**, or **Radio Button List**, you will also need to provide the list of answers, as described in Creating a Question Containing a Selection List.

Creating a New Question

To create a new question, perform the following steps.

Task   **To create a new question:**

1. Open the **Admin** tab.

2. Under **Site Managemen**t, select **Questions** > **Question Manager**. The **Question Manager View** opens.

3.   Click **Add Question**. The **Question Properties** dialog box opens.

4.   In the **Question Title** field, enter text to identify this question in App Portal.

5. In the **Question to be asked** text box, enter the question that will be displayed to the end user, such as:

```
What is the business purpose for obtaining this application?
```

6. In the **Question details** text box, enter some descriptive text about the question. This information, when present, is displayed as a pop-up dialog when the control is focused or the mouse hovers over it.

7. If you want to write the response to this question to a computer variable of the targeted and/or source machine, perform the following steps:

    a. If you want the response to the question to be written to the computer variable of the targeted and/or source machine, enter the response in the **Apply response to computer variable** field.

    b. From the **Apply variable to** list, select **Source**, **Target**, or **Source and Target** to apply the variable to the respective computer objects when being used as part of an OSD Task Sequence Catalog Item.

    c. From the **Apply to build type** list, choose **Bare Metal**, **In-Place Migration**, **Side-by-Side Migration**, or **Not Specified** to apply the variable to the respective scenario when being used as part of an OSD Task Sequence Catalog Item.

    d. When a variable value is applied to a computer object, the value of the variable can be masked, just like when you type in a password. To mask the variable, select the **Mask Variable** option. There are cases where you would not want the response to the question to be visible in the user interface, such as when it is a password.

8. Under **Target**, select one of the following options:

- **Requestor**
- **Approver**
- **Either**

9. If you want to specify that the question is not optional, select the **Required** check box

10. Under **Focus**, select one of the following options:

- **Request Specific**—Select this option to indicate that the question is related to the entire request (such as asking for the end user's cost center). When this option is selected, the question will only be asked once per request, and the question will be displayed at the top of the **Respond to Questionnaire** panel of the checkout procedure.

  Note • Even if more than one catalog item in the cart has an associated question template that contains the same Request-Specific question, the question is not repeated. It is only asked once per request.

- **Item Specific**—Select this option to indicate that the question is related to an individual catalog item. When this option is selected, the question will be displayed on the lower portion of the **Respond to Questionnaire** panel. in the table next to the catalog item.

11. Under **Question Format**, select one of the following options:

- **Single Line**—Input will allow for a single line of data.
- **Multiline / Rich Text Box**—Input will allow for multiple lines of text.
- **Checkbox List / Dropdown List / Radio Button List**—Input will allow for multiple selections. If you select one of these options, you will also need to open the **Answer** tab of the **Question Properties** dialog box and enter the possible answers for this multiple selection question, as described in Creating a Question Containing a Selection List.

- **Date / Time / Date and time**—Input will allow for a date / time entry.

12. Click **Save** and close the **Question Properties** dialog box. The new question is now listed on the **Question Manager View**.

Creating a Question Containing a Selection List

To create a question that has an input type of **Checkbox List**, **Dropdown List**, or **Radio Button List**, perform the following steps:

Task   ***To add a question that contains a selection list:***

1. Create a new question, as described in Steps 1 through 9 in Creating a New Question. For example, to ask the user to select their department from a list, enter the following:

Field	Entry
Question Title	`Department`
Question to be asked	`What is your department?`
Question details	`Select your department from the list.`

2. Under **Focus**, select **Request Specific**.

3. Under **Question Format**, select **Checkbox List**, **Dropdown List**, or **Radio Button List**.

4. Click **Save**. You are notified that the question was created successfully, and, because you selected **Checkbox List**, **Dropdown List**, or **Radio Button List** as the question format, the **Answers** tab is enabled, where you need to enter the values for the list.

5. Open the **Answers** tab.

6. Click **Add new record**. Additional entry fields are displayed.

7. In the **Answer Text** field, enter the value that will be displayed in the drop down list, such as `Engineering`.

8. In the **Answer Value** field, enter the value that will be recorded for this selection, such as `ENG`.

9. Click **Insert**. The answer is displayed in the list.

10. Repeat the above steps to enter all additional answers, such as: `Marketing (MKTG)`, `Accounting (ACCT)`, and `Administration (ADMIN)`.

11. Click **Save** and close the **Question Properties** dialog box. The new question is now listed on the **Question Manager View**.

Creating Questions With Conditions

You can assign two types of conditions to a question:

- **Standard condition**—Condition based on user attributes including group and OU membership, AD property value, and deployment system collection membership for both users and computers.

- **Question condition**—Condition is based upon the answer to another single-selection question (which must be in the format of **Dropdown List** or **Radio Button List**).

Assigning a Standard Condition

To assign a standard condition to a question, perform the following steps:

Task   ***To assign a standard condition:***

1.   Open the **Question Manager** view and double-click on an existing question. The **Question Properties** dialog box opens.

2.   Open the **Standard Condition** tab.

3.   Click **Add Condition** to open the **Condition Properties** dialog box and add a **Group and OU**, **AD Property**, or **Collections** condition, as described in Add Condition Dialog Box.

4.   Click **Save**.

Assigning a Question Condition

To assign a question condition to a question, which is a condition is based upon the answer to another single-selection question, perform the following steps:

Task   ***To assign a question condition:***

1.   Open the **Question Manager** view and make sure that you have already created at least one question with the **Question Format** of **Radio Button List** or **Dropdown List**.

2.   Double-click on the question that you want to add a condition to. The **Question Properties** dialog box opens.

3.   Open the **Question Condition** tab.

4.   From the **Please select the Question Condition** list, select a question.

5.   From the **Please select the Question Condition Value** list, select the answer to the selected question that the end user will have to select in order for this question to be displayed.

6.   Click **Save**.

Creating a Question Template

To create a new question template, perform the following steps:

Task   ***To create a new Question Template:***

1. Open the **Admin** tab.

2. Under **Site Managemen**t, select **Questions** > **Template Manager**. The **Template Manager View** opens.

3. Click **Add Template**. The **Question Template Properties** dialog box opens.

4. In the **Template Name** field, enter `Business Reason`.

5. In the **Available Questions** list, select **Reason** and click the right arrow button to move it to the **Current Questions** list.

6. Move the **Department** question from the **Available Questions** list to the **Current Questions** list.

7. Click **Save**. A message stating that the template was successfully created is displayed.

8. Close the **Question Template Properties** dialog box. The new question template is now listed on the **Template Manager View**.

Default Question Templates

When App Portal is installed, several default Question Templates are created. The following table lists those default question templates and their purpose.

Table 4-5 • Default Question Templates

Type	Template Name	Purpose
Software or General Catalog Item	**Software**	Associate with a **Software** catalog item to prompt the end user to provide information when requesting that catalog item.
	Non-Catalog Item	Associate with a non-catalog item to prompt the end user to provide the information necessary to obtain a software or hardware asset that is not listed in the App Portal catalog.
Alert Action Catalog Item	**KeepTemplate**	Associate with an Alert Action catalog item to prompt the user to enter information when they choose to keep an unused application.
	ProofOfPurchaseTemplate	Associate with an Alert Action catalog item to prompt the user to provide proof of purchase of an installed application.
	UninstallationWithNoProgramTemplate	Associate with an Alert Action catalog item to prompt the end user to explain why the application (without a program template) should be uninstalled.

📄

Note • For more information, see Attaching a Question Template.

Setting Catalog Item Properties

The **Catalog Item Properties** dialog box is a multi-tabbed form that you use to create a new catalog item and to set its properties. A detailed list of all of the properties and options available on the Catalog Item Properties dialog box can be found in Catalog Item Properties Dialog Box.

This section explains how to specify the properties for several of the most common scenarios:

- Setting Approval Options

- Attaching a Question Template

- Enabling a Catalog Item to Be Requested on Behalf of Another User / Device

- Adding Notes to a Catalog Item

- Attaching a Program to Deploy a Catalog Item to System Center Configuration Manager

- Defining Custom Variables for a Catalog Item

- Setting FlexNet Manager Suite Licensing Options

- Controlling Visibility of a Catalog Item by Adding Conditions

- Adding an Action to a Catalog Item

- Customizing Email Notifications for a Catalog Item

- Assigning Permissions to a Catalog Item

- Setting Properties Specific to Mobile Application Catalog Items

- Connecting a Catalog Item to a Workflow Manager Workflow Request

- Connecting a Catalog Item With System Center Orchestrator

Setting Approval Options

Approval workflows, which are applied to catalog items, define how a request will be routed for review. This section explains the two steps you need to perform to attach an Approval Workflow to a catalog item:

- Attaching an Approval Workflow to a Catalog Item

- Specifying Approval Settings

Attaching an Approval Workflow to a Catalog Item

Approval workflows, which are applied to catalog items, define how a request will be routed for review. In each step of an approval workflow, a user or group reviews the request. Workflows are defined and listed on the **Workflows View**, which is opened by selecting **Workflows** under **Site Management** on the **Admin** tab.

In this section, you will learn how to attach an approval workflow to a catalog item.

Note • For information on creating an approval workflow, see Managing Approval Workflows.

To attach an approval workflow to a catalog item, perform the following steps:

Task   **To attach an approval workflow to a catalog item:**

1. Open the **Admin** tab.

2. Under **Catalog Management > Current Catalog Items**, select the group that contains the catalog item you want to attach a workflow to. The catalog item is listed in the right pane.

3. Double-click the catalog item. The **General > Global** tab of the catalog item's properties dialog box opens

4. Under **Approval Options**, select the **Require Approval for Install?** option.

5. Open the **Approval Process** tab and make sure that the **Workflow** subtab is selected.

6. Click **Add Workflow**. A pop-up dialog box opens, prompting you to select a workflow.

7. From the **Select a workflow to add** list, select a workflow and click **Add Selected Workflows**. The workflow is now listed on the **Workflow** subtab of the **Approval Process** tab.

8. To view a simulation of the approval process for this catalog item, open the **Simulate** subtab.

9. In the **Enter a user ID in Domain\name format or a computer name** field, enter your domain and user name and then click **Show approval process**. The levels in the selected approval workflow are listed:

10. Close the **Catalog Item Properties** dialog box.

Note • *For more information on workflows, see Managing Approval Workflows.*

Specifying Approval Settings

You have several options that you can set to specify how a catalog item's approval workflow will proceed. You can also set conditions on an approval workflow.

Task   **To specify approval settings:**

1. Double-click on a catalog item to open the **Catalog Item Properties** dialog box, and then open the **Approval** tab.

2. Select the **Require approval when assignment is present** option to force a request for this catalog item to go through an approval process.

3. Select the **Disable approval for leased installations** option to disable requests for this catalog item from using the approval process.

4. To create conditions—based on Active Directory Groups or OUs, Active Directory properties, and collections—that will force requests for the catalog item to go through an approval process, perform the following steps:

   a. Open the subtab of the type of condition you want to add: **Group and OU**, **AD Property**, or **Collections**.

   b. Click **Add Condition**. The **Add Condition** dialog box opens.

   c. Search for the group, OU, AD property, or collection you want to add and place a checkmark next to a item in the search results.

   d.   Click the Sel**ect** button to add the condition. The condition is listed on the **Approval** tab.

   e.   After the condition is added, specify the **Enforcement** option you want to take effect: **Include** or **Exclude**.

   f.   Click **Save**.

Attaching a Question Template

*Note • For AirWatch Mobile Application catalog items, the **MobileCatalogQuestionTemplate** containing the* **MobileCatalogQuestion** *is always attached and cannot be changed. See Specifying the Mobile Application Catalog Item Question.*

When submitting a software request, sometimes the end user needs to answer a set of questions that will give App Portal the information it needs in order to fulfill that software request.

For example, in order to approve a software request, a manager may want to know the name of the project that the end user is working on that requires this application. Or, in order to determine licensing requirements, the manager may want to know how frequently the end user will use this application or the time of day that it would be used. The request will not be submitted until all required questions have been answered.

After you create a question template, as described in Managing Questions and Question Templates, you need to attach a question template to a catalog item.

Task | **To attach a question template to a catalog item:**

1. Open the **Admin** tab.

2. Under **Catalog Management > Current Catalog Items**, select the group that contains the catalog item you want to edit. The catalog items are listed in the right pane.

3. Double-click the catalog item that you want to edit. The catalog item's **Catalog Item Properties** dialog box opens.

4. Select the **General** tab and make sure that the **Global** subtab is selected.

5. From the **Question Template** list, select a question template.

6. Click **Save**. The question template is now attached to the catalog item. When a requester adds this catalog item to his cart, he will be prompted to answer the questions on this question template on the **Questions** tab of the **Request Details View**.

Enabling a Catalog Item to Be Requested on Behalf of Another User / Device

You can configure a catalog item so that a user can request that catalog item for another person or another person's device. App Portal offers several different "request on behalf" options for a catalog item, which are specified on the **General > Global** tab of the **Catalog Item Properties** dialog box.

Figure 4-13: Request Options on the General > Global Tab of Catalog Item Properties Dialog Box

If any of these "request on behalf" options are selected, the requester will be able to use the selected method(s) to search for (or specify) users or to identify the target(s) of the request. The following "request on behalf" options are available:

Table 4-6 • "Request on Behalf" Options

Option	Administrator selects this option on the Catalog Item Properties dialog box	Requester selects this option on the Choose Target panel	Description
To search all users by machine name, full name, or user name	**Enable request on behalf?**	**Search for people or computers**	Requester can search by machine name, full name, or user name to locate the target device(s) / user(s) of the request. See Request on Behalf by or Users.
To search all users by Active Directory account attributes	**Enable request to AD property?**	**Search using account attributes**	Requester can search by Active Directory account attributes to locate the target device(s) / user(s) of the request. See Request on Behalf by Active Directory Property.
To search only users who report to the requester by machine name, full name, or user name	**Enable request for AD manager?**	**People who report to me**	Requester can search a list of direct reports by machine name, full name, or user name to locate the target device(s) / user(s) of the request. See Request On Behalf By Manager's Direct Reports.
To manually enter a list of machine names or user IDs	**Enable request to manual list?**	**Add machine names or user IDs manually**	Requester can manually add a list of machine names or user IDs to identify the target device(s) / user(s) of the request. See Request on Behalf by Entering a List of Machine Names or User IDs.

Note • *In order to have access to these "request on behalf" options, the requester must have been assigned the* **Request on Behalf** *role under* **Catalog Management > Catalog Security***.*

Request on Behalf Option Details

The following options are available when configuring a catalog item so that a user can request that catalog item for another person or another person's device.

- Request on Behalf by or Users

- Request on Behalf by Active Directory Property

- Request On Behalf By Manager's Direct Reports

- Request on Behalf by Entering a List of Machine Names or User IDs

- Using a Custom View to Display Eligible for Request on Behalf

Request on Behalf by or Users

If the **Enable request on behalf?** option is selected for a catalog item, the **Search for people or computers** option is listed on the **Choose Target** panel of the **Checkout** view for requesters who have been assigned the **Request on Behalf** role.

Choose Target

Specify the target location for these catalog items.

○ Me on machine ITAAPMARK7
○ ITAAPMARK
➤ ● Search for people or computers

Figure 4-14: Search for people or computers option

If this option is selected, the **Choose Target / Users for Request on Behalf** panel opens, where the requester can use the **Filter By** fields to search for or users. When the desired user or device is located, the requester selects the user or device and then clicks **Add Selected Records**. The user or device is now listed at the bottom of the screen in the **Selected** list.

Figure 4-15: Choose Target /Users for Request on Behalf Panel of Checkout / Users or

After the requester selects the target and clicks **Next**, the that were selected will be listed on the **Submit Request** panel.

Figure 4-16: Selected on the Submit Request Panel

Request on Behalf by Active Directory Property

If the **Enable request to AD property?** option is selected for a catalog item, the **Search using account attributes** option is listed on the **Choose Target** panel of the **Checkout** view.

Figure 4-17: Search Using Account Attributes Option

If this option is selected, the **Choose Target /Users for Request on Behalf** panel opens, where the requester can use the **Search** fields to search for or users using Active Directory attributes. The requester can also choose to use the **Filter By** list to filter the list by device name or user name.

Figure 4-18: Choose Target /Users for Request on Behalf Panel of Checkout View / AD Properties

When the desired user or device is located, the requester selects the user or device and then clicks **Add Selected Records**. The user or device is now listed at the bottom of the screen in the **Selected** list.

Request On Behalf By Manager's Direct Reports

If the **Enable request to AD manager?** option is selected for a catalog item, the **People who report to me** option is listed on the **Choose Target** panel of the **Checkout** view.

Figure 4-19: Search Direct Report Group Option

If this option is selected, the **Choose Target / Users for Request on Behalf** panel opens, where the requester, who is a manager, can use the **Filter By** fields to search a list of his direct reports for or users. When the desired user or device is located, the requester selects the user or device and then clicks **Add Selected Records**. The user or device is now listed at the bottom of the screen in the **Selected** list.

Request on Behalf by Entering a List of Machine Names or User IDs

If the **Enable request to manual list?** option is selected for a catalog item, the **Add machine names or user IDs manually** option is listed on the **Choose Target** panel of the **Checkout** view.

Figure 4-20: Option to Add Machine Names or User IDs Manually

If this option is selected, the **Enter Target /Users** panel opens, where the requester can enter a target device/user in the text box and then click **Add** to add it to the **Selected** list.

Figure 4-21: Choose Target /Users for Request on Behalf Panel of Checkout View / Entering a List

Using a Custom View to Display Eligible for Request on Behalf

To use a custom SQL view to display the eligible for Request On Behalf, enter the custom page name in the **Request On Behalf DB View** field on the **Web Site > General** tab of the **Site Management > Settings** view.

Adding Notes to a Catalog Item

You may want to document a special issue or event associated with a particular catalog item. To do this, you can add notes to a catalog item on the **Notes** tab of the **Catalog Item Properties** dialog box.

Task   ***To add a note to a catalog item:***

1.   Under **Catalog Management > Current Catalog Items**, select the group that contains the catalog item you want to edit. The catalog items are listed in the right pane.

2.   Double-click the catalog item that you want to edit. The catalog item's **Catalog Item Properties** dialog box opens.

3.   Open the **Notes** tab.

4.   Click **Add New Note**. A pop-up dialog box opens.

5.   In the **Note** text box, enter the text of the note.

6.   Click **Add Note**. The note is now listed on the **Notes** tab, along with the name of the person who added the note and the date and time.

7. To view and edit a note, click **Edit** next to the note text. A drop down editing area appears below the note name.

8. Edit the text in the text box and click **Update** to save your edits.

Attaching a Program to Deploy a Catalog Item to System Center Configuration Manager

You can add programs to deploy a catalog item to System Center Configuration Manager through App Portal.

Task   ***To attach a program to deploy a catalog item to SCCM:***

1. Open the **Catalog Item Properties** dialog box of a catalog item.

2. Open the **Deployment > SCCM 2012** subtab that contains the catalog item's associated application or package.

3. Click **New Deployment** (for applications) or **Add Program** (for packages). The **SCCM Deployment** dialog box opens, displaying different options in the **SCCM Object** area, depending upon the type of catalog item you are creating:

4. For applications, perform the following steps:

    a. From the **Select deployment method** list, select **Deploy to user** or **Deploy to computer**.

    b. You can choose to **Create Uninstall Collection**.

5. For packages, perform the following steps:

    a. Select the matching program name for each program function: **Install**, **Uninstall**, and **Repair**.

        ● If you have enabled **Uninstall** or **Repair** in the global settings, the uninstall and repair programs are required.

        ● You can have multiple installation programs for different languages within a single request.

        ● If programs are specified for more than one language, the requester will select the language during the checkout process.

    b. Under **Program for OS Deployment Task Sequence**, select a matching program name for the program function.

6. Under **Select sites to publish**, select the sites where this request will be available, the locations you wish to publish the catalog item to. An advertisement and collection will be created at the site(s) selected.

7. In the **Advertisement settings** area of this dialog box, specify the following properties:

Property	Description
Make the advertisement mandatory	Determines whether the Advertisement is created as a mandatory advertisement.
Mandatory over slow links?	Select this option to require that the installation is run even when a client has a slow connection. If this option is not selected, the SCCM client agent will not perform the installation if the client has a slow connection, but will perform the installation if the client is connected over a regular LAN connection.
Advertisement Priority	Specify the priority of the advertisement: **High**, **Medium**, or **Low**.
Ignore maintenance windows	Determines if the advertisement should ignore maintenance windows.

Property	Description
Allow system restart outside of maintenance windows	Select to allow the advertised program to restart the client even if the restart would occur outside a maintenance window.
Program rerun behavior	Specifies whether the advertised program will be rerun on the client computer if it has previously been run before the scheduled mandatory time. Select one of the following options: • **Never rerun advertised program**—The program will not be rerun on the client if the program has previously been run on the client, even if the program originally failed or the program files have been changed. • **Always rerun**—The program will always be rerun on the client when the advertisement is scheduled, even if the program has already been successfully run. • **Rerun if failed previous attempt**—The program will be rerun when the advertisement is scheduled only if it failed on the previous run attempt. • **Rerun if succeeded on previous attempt**—The program will be rerun only if it has previously run successfully on the client. *Important • This option is only enabled if **Make the advertisement mandatory** is also selected.*

8. In the **Distribution settings** area of this dialog box, specify the following properties:

Property	Description
When a Distribution Point is available locally	Select one of the following options to specify how content will be downloaded from the distribution points when a distribution point is available locally: • **Run program from distribution point**—Run program directly from a distribution point. • **Download program from distribution point**—Download program from the distribution point to the client computer before attempting to run the program.
When no Distribution Point is available locally	Select one of the following options to specify how content will be downloaded from the distribution points when no distribution point is available locally: • **Do not run program**—Do not run program. • **Download program from remote distribution point**—Download the program from a remote distribution point to the client computer before attempting to run the program. • **Run program from a remote distribution point**—Run program directly from a remote distribution point.

Property	Description
When no protected distribution point is available, use an unprotected distribution point	Select this option to permit a client to use an unprotected distribution point if content is not immediately available on its protected distribution point.

If this option is not selected, the client will not use unprotected distribution points. |

9. Click **Save**. Deployments will be created for each selected site:

10. For verification, select the check box next to each item and click **Get details** to verify the deployment of these new items created successfully in SCCM.

When you click **Get details**, additional information is displayed in the **Advertisement**, **Collection**, **Program**, and **Package ID** fields.

11. To add variables to collection, click the **Collection Variables** button. The following form opens, where you can specify collection variables.

12. To add variables to computers click the **Computer Variables** button. The following form opens, where you can specify computer variables.

Adding an Uninstall Collection to an SCCM Application

When software is distributed using System Center Configuration Manager, because users may not have local admin rights, they may be unable to uninstall applications using standard methods, such as using the Windows Add/Remove Programs function.

Therefore, in order to enable the uninstallation of an application that will be distributed using System Center 2012 Configuration Manager, it may be necessary to add an uninstall collection to a catalog item.

To add an uninstall collection, select the **Create Uninstall Collection** option on the **SCCM Deployment** dialog box when creating a deployment for the catalog item.

Figure 4-22: Create Uninstall Collection Option on SCCM Deployment Dialog Box

When this option is selected, users will be able to submit an uninstall request from App Portal, and System Center Configuration Manager will uninstall the application. App Portal will inform the user when the uninstall is complete.

Defining Custom Variables for a Catalog Item

You can define custom variables for both standard catalog items and cloud catalog items.

- Defining Custom Variables for Standard Catalog Items

- Defining Global Custom Variables for Standard Catalog Items

- Defining Custom Variables for Cloud Catalog Items

Defining Custom Variables for Standard Catalog Items

On the **Custom Variables** tab of the Catalog Item Properties dialog box, you can add custom variables to associate with a catalog item.

A catalog item's associated custom variables will be available for use in external web actions or script commands. For example, you may want to use the same action for Standard, Professional, Enterprise editions of a catalog item and you could use a custom variable to differentiate the messages.

Figure 4-23: Custom Variables Tab of the Catalog Item Properties Dialog Box

Note • *To make a custom variable globally available, you should add it to the **Catalog Management > Catalog > Custom Variables** view. Variables defined there will be available on the **Custom Variables** tab of all future catalog items. For more information, see Defining Global Custom Variables for Standard Catalog Items.*

On the **Custom Variables** tab of the Catalog Item Properties dialog box, you can add a new variable or edit an existing variable:

- Adding a New Variable

- Editing an Existing Variable

Adding a New Variable

To add a new variable, click **Add New Variable**. A pop-up dialog opens where you can enter a **Variable Name**, **Value,** and **Description**. Click **Add Variable** to save the variable.

Figure 4-24: Add New Variable

Editing an Existing Variable

To edit a variable, lick **Edit** next to a variable name. An area drops down below the variable where you can edit and update the variable. Click **Update** to save your edits.

Figure 4-25: Variable Editing Area

Defining Global Custom Variables for Standard Catalog Items

A catalog item's associated custom variables will be available for use in external web actions or script commands. For example, you may want to use the same action for Standard, Professional, Enterprise editions of a catalog item and you could use a custom variable to differentiate the messages.

You can add custom variables directly to a catalog item on the **Custom Variables** tab of the **Catalog Item Properties** dialog box, However, to make a custom variable globally available, you can add it to the **Catalog Management > Catalog > Custom Variables** view. Variables defined here will be available on the **Custom Variables** tab of all future catalog items.

Figure 4-26: Catalog Management > Catalog > Custom Variables View

*Note • This feature is not applicable to Cloud catalog items. There is no **Custom Variables** tab on the Catalog Item Properties dialog box for a Cloud catalog item, and variables defined on the **Catalog Management > Catalog > Custom Variables** view are not available to Cloud catalog items. See Defining Custom Variables for Cloud Catalog Items.*

On the **Catalog Management > Catalog > Custom Variables** view, you can add new variables and edit existing variables.

- Adding a New Variable

- Editing an Existing Variable

Adding a New Variable

To add a new variable, click **Add New Variable**. A pop-up dialog opens where you can enter a **Variable Name**, **Value,** and **Description**. Click **Add Variable** to save the variable.

Figure 4-27: Add New Variable

Editing an Existing Variable

To edit a variable, lick **Edit** next to a variable name. An area drops down below the variable where you can edit and update the variable. Click **Update** to save your edits.

Figure 4-28: Variable Editing Area

Defining Custom Variables for Cloud Catalog Items

App Portal provides out-of-the-box support for three cloud applications—Box, Salesforce, and Microsoft Office 365—and automatically configures these catalog items with custom variables which are required for the account request to be completed. These variables can be viewed on the **Cloud Apps** tab of the **Catalog Item Properties** dialog box for Cloud catalog items.

Figure 4-29: Custom Variables on the Cloud Apps Tab of the Catalog Item Properties Dialog Box

On the **Cloud Apps** tab of a Cloud catalog item, you can view and edit existing variables, and create new variables.

Note • While you can define global custom variables for standard catalog items on the Catalog Management > Catalog > Custom Variables view, there is no comparable functionality for Cloud catalog items. To create "global" custom variables for a Cloud catalog item, you need to use a template, as described in Creating a Catalog Item Template.

Editing an Existing Variable

To edit a variable, lick **Edit** next to a variable name. An area drops down below the variable where you can edit and update the variable. Click **Update** to save your edits.

Figure 4-30: Variable Editing Area

Adding a New Variable

To add a new variable, click **Add New Variable**. A pop-up dialog opens where you can enter a **Variable Name**, **Value,** and **Description**. Click **Add Variable** to save the variable.

Figure 4-31: Add New Variable

Setting FlexNet Manager Suite Licensing Options

If you have also purchased FlexNet Manager Suite, you can use App Portal to manage application licenses.

- **Flexera Service Gateway**—App Portal communicates with FlexNet Manager Suite via the Flexera Service Gateway component. You need to enter the Flexera Service Gateway server name and FlexNet Manager Suite credentials on the **Site Management > Settings > Flexera Integration** view.

- **Linking a catalog item to FlexNet Manager Suite**—After a catalog item has been added to App Portal, you need to open the **FlexNet Manager Suite** tab of the App Portal **Catalog Item Properties** dialog box and search the FlexNet Manager Suite libraries to locate the application's Flexera ID.

- **App Portal can reserve licenses**—After App Portal is connected to FlexNet Manager Suite and an application's Flexera ID has been selected, whenever an end user requests that application from App Portal, App Portal will automatically connect to FlexNet Manager Suite and request that an application license be reserved for that end user, if a license is available.

To map a **Software** catalog item to FlexNet Manager Suite, perform the following steps:

Task   ***To map a catalog item to FlexNet Manager Suite:***

1. Double-click on an existing catalog item to open the **Catalog Item Properties** dialog box.

2. Open the **FlexNet Manager Suite** tab.

3. Enter application information in the **Product Name**, **Version**, **Edition**, and **Publisher** fields, and then click **Search**. Possible matches are listed.

4. From the list of search results, select the appropriate entry. The selected item will be highlighted.

5. Click **Save**. The catalog item is now mapped to a software entry in FlexNet Manager Suite, and the product information is now listed at the top of the dialog box. Also, additional options are displayed.

6. If you would like App Portal, during checkout, to display an icon that indicates whether there are licenses available for this product, select the **Check for license position during checkout** option.

Note • For more information on displaying license information during checkout, see Displaying Available Licenses During Checkout.

7. If you would like App Portal, during checkout, to consider not only available licenses, but also second use rights, upgrade/downgrade rights, and exemption by device role rights (all based upon information stored in FlexNet Manager Suite), select the **Check for advanced license during checkout** option.

Note • For more information on performing an advanced license check during checkout, see Performing Advanced License Check.

8. From the **Select the licensing availability scope** list, select one of the following options to specify how FlexNet Manager Suite will determine the available license count for this catalog item:

- **Global Only**—When determining available license count, FlexNet Manager Suite will return the number of licenses that are available to the entire enterprise.

- **Enterprise Groups Only**—When determining available license count, FlexNet Manager Suite will return only the number of licenses that are available to that user or computer.

- **Check Enterprise Groups and fallback to Global if not available**—When determining available license count, FlexNet Manager Suite will first check the number of licenses that are available to that user or computer; then, if no license is available, FlexNet Manager Suite will return the number of licenses that are available to the entire enterprise.

Note • For more information, see Mapping Tab under FlexNet Manager Suite Tab.

9. Click **Save** to save your selection.

10. Open the **License Reclamation** tab.

11. Set licensing properties as described in License Reclamation Tab.

12. Optionally, set alert action targets as described in the following topics:

- Creating a New Custom Alert Action Catalog Item

- Triggering a Proof of Purchase Alert

- Converting a General Catalog Item to an Alert Action Catalog Item.

13. Click **Save**.

14. Close the **Catalog Item Properties** dialog box.

15. To check to confirm that you have created a licensed catalog item, perform the following steps:

a. Open the **Browse Catalog** tab and select the category that contains the catalog item that you just added. The catalog item should display a black lock icon:

b. Add the item to the cart and open the cart. A lock icon will be displayed next to the catalog item name to indicate the catalog item's license status:

One of the following lock icons will be displayed:

Icon		Meaning
License Required		A license is required for this catalog item, and one is available. If this catalog item is purchased, a license will be automatically reserved for that end user.
License Not Available		A license is required for this catalog item, but no licenses are available.

If a lock icon is not displayed, it means that no license is required for the catalog item.

Controlling Visibility of a Catalog Item by Adding Conditions

Visibility controls whether a catalog item is visible for a user based on conditions. For each condition you can choose **Include** or **Exclude**. If a user matches an include condition, the item is visible. If the user matches an exclude condition, the item is not visible.

Exclude conditions are evaluated first. If a user matches an exclude condition, no further processing occurs and the item is not visible. If there are both exclude and include conditions specified, the user must not match exclude conditions and must match include conditions for the item to be visible.

By default, all catalog items are visible when the **Is Enabled** Global option is specified. Use the **Visibility** tab of the **Catalog Item Properties** dialog box to further customize the visibility of items.

On the **Global** tab, you can create conditions based on Active Directory Groups or OUs, Active Directory properties, and collections.

Important • The creation of a condition based upon Active Directory device groups is not supported.

To create a condition, perform the following steps:

Task   **To create a condition:**

1. Open the **Visibility** tab of the catalog item's **Catalog Item Properties** dialog box.

2. On the **Global > Group and OU** tab, click the **Add Condition** button.

3. Search for the group or OU you want to add and place a check mark next to the item found.

4. Click the **Select** button to add the condition.

5. After the condition is added, specify the **Enforcement** option you want to take effect: **Include** or **Exclude**.

6. Click **Save**.

7. Follow a similar procedure to add conditions to the **AD Property** and **Collections** tabs.

Adding an Action to a Catalog Item

You can add an action to a catalog item so that a set of commands will be triggered as part of a request at one or more stages during the request life cycle, such as when the catalog item is requested, when it is approved, etc.

You can use the On Check Status event to set up integration between App Portal and an ITSM system.

📄

Note • *By default, the only actions that exist in App Portal are ServiceNow and Remedy ITSM actions (if you are integrated with a ServiceNow or Remedy ITSM system), Cloud application actions (if you are integrated with Box, Office 365, or Salesforce), and Workflow Manager actions. In order to add any other actions, you have to first create the action on the* **Site Management > Commands & Actions > Script Commands**, **Web Service Commands**, *or* **Request Commands** *view. For more information, see* [*Commands and Actions*](#)

To add an action to a catalog item, perform the following steps:

📋

Task   **To add an action:**

1. Open the **Actions** tab of the catalog item's **Catalog Item Properties** dialog box.

2. Select an action from the **Select a service** list.

If you select **Command Execution** from the **Select a service** list, a command previously created under **Site Management > Commands and Actions > New Command** is used. Those commands specified as **Execute from Server** are available. When the request stage is processed, the command will be invoked and passed the variables identified in the Command.

The other options from the **Select a service list** are:

- **Workflow Manager Action**

- **Remedy - Create Incident Management Service**

- **Remedy - Query Incident Management Service**

- **Remedy - Incident Status Management Service Wrapper**

- **Remedy - Create Request Management Service**

- **Remedy - Service Request Status Management Service Wrapper**

- **ServiceNow - Create Incident Management Service**

- **ServiceNow - Create Request Management Service**

- **Box**

- **Office 365**

- **Salesforce**

Note • For more information on adding an ITSM action to a catalog item, see Setting ITSM Actions on Catalog Items.

3. Select an event from the **Current Events and Actions** list.

4. Select a method or command from the **Select a method or command** list.

5. Select a status from the **Add a status** list to identify what the catalog item's status will be when this action is executed.

6. Click **Save** to add the action to the event tree on the left. These actions will execute when the event completes.

Note • For troubleshooting purposes, the log file for reference of actions is `WebServiceAction.log`*.*

Customizing Email Notifications for a Catalog Item

On the **Notifications** tab, you can specify custom notifications to replace the default notifications for different actions.

Figure 4-32: Notifications Tab

You can edit a custom notification message by double-clicking on the notification in this list and entering your custom message. The standard variables apply for custom messages.

You can edit each email as described in Editing Notification Email Templates and Messages.

Assigning Permissions to a Catalog Item

To assign permissions to a catalog item, perform the following steps.

Task   ***To assign permissions:***

1.   Open the **Permissions** tab of the catalog item's **Catalog Item Properties** dialog box.

2.   Click the **Add User/Group** button to open the search dialog box.

3. Select **User** or **Group** from the **Search for user / group** field.

4. Enter search criteria in the search field and click **Search**.

5. Select a permission from the **Assign rights** list.

6. Click the **Assign Rights** button when completed.

Setting Properties Specific to Mobile Application Catalog Items

After you create an AirWatch mobile application catalog item using the **New Catalog Item Wizard**, as described in Creating an AirWatch Mobile Application Catalog Item, you can open the mobile application's **Catalog Item Properties** dialog box and set the following additional properties that are unique to mobile applications:

- Specifying the Versions Associated with a Mobile Application Catalog Item

- Specifying the Mobile Application Catalog Item Question

- Linking a Mobile Application with a Desktop Application

Specifying the Versions Associated with a Mobile Application Catalog Item

You are permitted to add multiple versions of a mobile application to the same catalog item in order to accommodate different operating systems (iOS, Android) and different (iPhone, iPad). When using the **New Catalog Item Wizard** to create the catalog item, you are restricted to adding just one iOS mobile application and one Android mobile application. However, on the **AirWatch** tab of the **Catalog Item Properties** dialog box you can add additional versions or delete existing ones.

When adding additional versions of a mobile application, you are restricted to having a unique platform / device / Location Group ID combination. For example, a single catalog item could include the following versions of the XYZ mobile application because each one has a unique combination of platform / device / location:

- XYZ Application / Android / Chicago Location

- XYZ Application / Android / New York Location

- XYZ Application / iOS / iPad / Chicago Location

- XYZ Application / iOS / iPhone / Chicago Location

- XYZ Application / iOS / iPad / New York Location

- XYZ Application / iOS / iPhone / New York Location

You cannot add more than one version of a mobile application that has the same platform (iOS/Android), device (iPad/iPhone), and Location Group ID to the same catalog item.

Note • *Android applications do not have any phone vs. tablet device distinction.*

To specify the mobile application versions associated with a catalog item, perform the following steps:

Task   **To specify the mobile application versions associated with a catalog item:**

1. Open the **AirWatch** tab of a mobile application catalog item's **Catalog Item Properties** dialog box.

The mobile application versions currently associated with the catalog item are listed, and the following information is displayed:

Property	Description
AirWatch Package Name	Name of package on the AirWatch instance.
Platform	Identifies the platform of the mobile application to be either **iOS** or **Android**.
AirWatch Supported Device	Identifies the supported device of the mobile application: either **iPad** or **iPhone** for iOS , or **Android** for Android .
AirWatch ID	Number identifying the application on the AirWatch server.

Property	Description
Location Group Id	Number identifying the Active Directory location group that was specified for this mobile application when it was added to AirWatch. Only users within the mobile application's same location group hierarchy will have access to that mobile application.

2. To add another mobile application version, perform the following steps:

   a. Click **Add Android Application** or **Add iOS Application**. The **Add Mobile Application** dialog box opens, listing mobile applications on the connected AirWatch instance.

   b. Search for and select the mobile application version that you would like to add.

   c. Click **Add Application**.

3. To delete an existing mobile application version from the catalog item, select it and then click **Delete**.

4. Click **Save**.

Specifying the Mobile Application Catalog Item Question

For AirWatch mobile application catalog items, the MobileCatalogQuestionTemplate containing the MobileCatalogQuestion is always attached and cannot be removed. You cannot specify a different question template. However, you can edit the contents of the question.

Task   ***To specify the mobile application catalog item question:***

1. On the **Admin** tab, select **Questions > Question Manager** under **Site Management**. The **Question Manager** view opens.

2. Double-click on MobileCatalogQuestion to open it in an editor.

3. Edit the question, as described in Creating Questions.

Linking a Mobile Application with a Desktop Application

A user can request both a desktop application and its associated mobile app in the same request. App Portal will deploy the desktop application using System Center Configuration Manager or Symantec Altiris, while it will use AirWatch to deploy the mobile application.

You can link a mobile application catalog item with its associated desktop catalog item so that when one of the linked applications is requested, the user will be informed that the other linked catalog item is also available.

- **Requesting a desktop catalog item**—If a user adds a desktop catalog item that is linked to a mobile catalog item to the cart, the user will be informed during checkout that they can optionally install the mobile catalog item onto their mobile device:

If the user selects to also request the mobile application, both catalog items will be included on the same request, but two different request IDs will be created:

- **Requesting a mobile catalog item**—When a user clicks **Add** to add a mobile catalog item that is linked to a desktop catalog item to the cart, a message box will open asking the user whether they would like to also add the desktop catalog item to the cart.

To link a mobile application catalog item to a desktop catalog item, perform the following steps.

Task   ***To link a mobile catalog item to a desktop catalog item:***

1.   Open the **Link Desktop Catalog** tab of a mobile application catalog item's **Catalog Item Properties** dialog box.

2.   Use the **Search** field to locate the desktop catalog item that you want to link to, select it, and then click **Save**.

Connecting a Catalog Item to a Workflow Manager Workflow Request

If you have also purchased Workflow Manager, you can connect an App Portal catalog item to a Workflow Manager workflow request. App Portal communicates with Workflow Manager via the Flexera Service Gateway component.

In App Portal, you open a catalog item's Catalog Item Properties dialog box and select an event that you want to trigger a Workflow Manager workflow (such as On Submit Approval) and the Workflow Manager project that you want to use.

A workflow request will then be created in Workflow Manager when someone requests this catalog item. When Workflow Manager completes the workflow request, the status in App Portal changes to Complete.

Important • In order for App Portal to communicate with Workflow Manager, App Portal must be connected to the Flexera Service Gateway. See Connecting to the Flexera Service Gateway.

Task   ***To connect a catalog item to a Workflow Manager workflow request:***

1. Open a catalog item's **Catalog Item Properties** dialog box.

2. Open the **Actions** tab.

3. In the **Current Events and Actions** column, select the event that you want to trigger the submission of a Workflow Manager workflow request (such as `On Submit Approval`).

4. From the **Select a service list**, select **Workflow Manager Action**. Automatically, **Submit Workflow** will be selected from the **Select a method or command** list.

5. From the **Add Workflow Manager Project** list, select the project that you want to associate this catalog item with.

6. Click **Add**. The action is now listed in the **Current Events and Actions** list.

Connecting a Catalog Item With System Center Orchestrator

App Portal can integrate with the Microsoft System Center Orchestrator workflow tool. Orchestrator is a workflow management solution for the data center. Orchestrator lets you automate the creation, monitoring, and deployment of resources in your environment.

If App Portal is connected to System Center Orchestrator, App Portal will have the ability to trigger a workflow at various points during an App Portal request lifecycle.

Orchestrator workflows can execute complex, long-running tasks such as creating AD User account, building virtual machines and performing complex logic such as loops and branches.

Important • In order for App Portal to communicate with Workflow Manager, App Portal must be connected to the System Center Orchestrator. See Connecting to Microsoft System Center Orchestrator.

Important • In order to add a System Center Orchestrator action to a catalog item, you must have at least Read permission on Runbooks in System Center Orchestrator. For instructions, see Assigning System Center Orchestrator Runbooks Permissions.

Task   ***To connect a catalog item to System Center Orchestrator:***

1. Open a catalog item's **Catalog Item Properties** dialog box.

2. Open the **Actions** tab.

3. In the **Current Events and Actions** column, select the event that you want to trigger the submission of a System Center Orchestrator workflow (such as `On Submit Approval` or `On Fail Install`).

4. From the **Select a service** list, select **Orchestrator Action**. Automatically, **Orchestrator Method** will be selected from the second drop down list.

5. From the **Add Orchestrator Runbook** list, select an existing Orchestrator Runbook.

Note • A System Center Orchestrator Runbook contains the instructions for an automated task or process.

6. Provide the information requested per the selected Orchestrator Runbook.

7. Click **Add**. The action is now listed in the **Current Events and Actions** list.

Prompting Requester to Upload a File During Checkout

You can choose to prompt the requester to upload a file to a request during the checkout of a catalog item, perhaps to associate a purchase order or other file associated with your organization's business practices. If the **Allow File Upload?** option on the catalog item's Catalog Item Properties dialog box is selected, the Upload Files panel of the Checkout wizard will open, prompting the user to upload one or multiple files.

you can select the Allow File Upload option

Select this option to enable end users to upload files to this catalog item during checkout.

If a catalog item has the **Allow File Upload?** option selected on the **General > Global** tab of the **Catalog Item Properties** dialog box, which enables a user to upload a file during checkout, the **Install Now** button is not displayed.

Task   ***To prompt requester to upload a file during checkout of a catalog item:***

1.   Open the **Catalog Item Properties** dialog box for a catalog item.

2.   Under **Request options**, select **Allow File Upload?**.

3.   Click **Save**.

Creating Alternate Targets

Sometimes when a user selects a catalog item and goes to check it out, they are prevented from doing so for various reasons:

- **Machine is not found**—If the user's machine is not found by App Portal, they will be prevented from checking out.

- **Machine not on network**—If a user's machine is not on the network, it means that the standard method for installing software using System Center Configuration Manager or Altiris cannot be used.

- **Version user wants is not in the catalog**—If a user wants a more recent version of an application than the version that is in the catalog, they would not want to check out the older version; instead they would want to indicate that they would like the IT department to purchase the latest version.

To enable you to accommodate all of these types of situations using the current checkout structure available on the **Browse Catalog** tab (the App Portal storefront), you can create alternate targets that would be available for selection whenever a user attempts to check out a software catalog item, as shown on the **Choose Target** panel of the **Checkout Wizard**.

Figure 4-33: Choose Target Panel of Checkout Wizard Displaying Alternate Targets

Note • *Alternate targets are only displayed for* **Software** *catalog items, not* **General** *catalog items.*

To create alternate targets, perform the following steps:

Task   **To create an alternate target:**

1. For each alternate target that you want to create, first create a general catalog item, as described in Creating a New Catalog Item Using the Wizard.

2. On the **Admin** tab, open the **Catalog Management > Administration > Alternate Targets** view.

3. Click **Add New Alternate Target**. The **Create New Alternate Target** dialog box opens.

4. In the **Alternate Target Text** field, enter the name of this new alternate target, which is the text that will be displayed on the **Choose Target** panel of the **Checkout Wizard**.

5. From the **General Catalog** Item list, select the General catalog item that you would like to associate with this alternate target.

6. Click **Save**. The alternate target will now be displayed on the **Choose Target** panel of the **Checkout Wizard**.

Note • If a user selects one of the alternate targets during checkout, the general catalog item associated with the selected alternate target will be checked out rather than the software catalog item that was originally selected.

Using Expressions to Control Form Validation

Expressions control form validation. By linking expressions to form fields, you can assure that data entered into forms is in a consistent format and contains valid information. Expressions are supported for the JavaScript language.

By default, App Portal includes the following expressions, which are listed on the **Expressions View**:

Figure 4-34: Default Expressions on the Expressions View

For more information about JavaScript regular expressions, visit:

http://www.regular-expressions.info/javascript.html

Expressions are defined and listed on the **Expressions** subview of the **Admin > Site Management** view.

- Creating a New Expression
- Editing an Existing Expression
- Adding an Expression to a Question

Creating a New Expression

To define a new expression, perform the following steps:

Task   **To define an expression:**

1. On the **Admin** tab, open the **Expressions** subview of the **Site Management** view. The **Expressions** view opens.

2. Click **Add New Expression**. The following form opens:

3. In the **Name** field, enter a descriptive name for this new validation expression. The name that you enter here will identify this expression in the **Answer Format** list on the **Create New Question** dialog box.

4. In the **Expression** field, enter an expression that will validate the user-entered response to its associated question. For example, if the question asked the user to input their zip code, the expression must check to see if the user enters 5 numeric characters.

   Important • *For information on writing JavaScript regular expressions, see the Regular-Expressions.info site at:*

   http://www.regular-expressions.info/javascript.html

5. In the **Sample Format** field, enter the format that the expression validates. This value will be displayed under the form field requiring validation.

6. Click **Add Expression**.

Editing an Existing Expression

To edit an existing expression, perform the following steps:

Task **To edit an existing expression:**

1. On the **Admin** tab, open the **Expressions** subview of the **Site Management** view. The **Expressions** view opens, listing all defined expressions.

2. Click **Edit** next to the expression that you want to edit. The following form opens:

3. Edit the **Name**, **Expression**, and **Sample Format** fields, as described in Creating a New Expression on page 549.

   Important • *For information on writing JavaScript regular expressions, see the Regular-Expressions.info site at http://www.regular-expressions.info/javascript.html.*

4. Click **Update**.

Adding an Expression to a Question

Expressions control form validation. By linking expressions to form fields, you can assure that data entered into forms is in a consistent format and contains valid information. Expressions are supported for the JavaScript language.

To add an expression to a question for validation, perform the following steps:

Task   ***To add an expression to a question:***

1.   On the **Admin** tab, open the **Question Manager** subview of the **Site Management >Questions** view. The **Question Manager** view opens, listing all defined questions.

2.   Double-click on an existing question to open the **Question Properties** dialog box.

3.   On the **Question** tab of the **Question Properties** dialog box, select an appropriate expression from the **Answer Format** list.

4.   Click **Save**.

Catalog Management Reference

This section includes reference information for views, wizards, and dialog boxes—accessed under the **Catalog Management** node—that are used to create and manage catalog items.

Table 4-7 •

Section	Description
Current Catalog Items View	Describes the catalog item lists available **Current Catalog Items**.
New Catalog Item Wizard	Lists the properties available on the **New Catalog Item Wizard**, which can be used to create **General** catalog items; **Software** catalog items from System Center Configuration Manager, Altiris, Casper, and AirWatch deployment technologies; System Center Configuration Manager **Task Sequence** catalog items; and **Alert Action** catalog items.
Catalog Item Properties Dialog Box	Describes the **Catalog Item Properties** dialog box, a multi-tabbed form that you use to create a new catalog item and edit the properties of an existing catalog item.
Administration Node	Lists the existing catalog items that have Catalog Templates defined. Use this view to easily locate templates to change their settings.
Expressions Node	Use to define and view expressions, which are used to control form validation. By linking expressions to form fields, you can assure that data entered into forms is in a consistent format and contains valid information.
Workflows Node	Use to define approval workflows, which determine how a request should be routed for review and approval.
Approval Groups Node	Use to create approval groups, which are used to group users or groups together to identify a group of approvers.
Workflow Status Node	Use to create workflow statuses to convey the progress, state, or otherwise identify what is happening at a particular workflow step.

Table 4-7 •

Section	Description
Questions Node	Use to create questions and to group them into question templates. If a catalog item has an associated question template, the user is prompted to answer those questions during request submission.

Current Catalog Items View

The **Current Catalog Items View** lists all of the catalog items in the selected catalog category. If the **View All Items** node is selected, all catalog items are listed.

Figure 4-35: Current Catalog Items / View All Items View

The **Current Catalog Items View** includes the following summary information:

Table 4-8 • Current Catalog Items View

Property	Description
ID	Number identifying the catalog item.
Catalog Title	Name identifying the catalog item.
Type	Specifies whether the catalog item is a Software Catalog Item (**Application** or **Package**), a **Group Catalog Item**, or a **General Catalog Item**.
Created	Date and time catalog item was added.
Licensed	Indicates whether or not the item requires a license.
Enabled	Indicates whether or not the **Is enabled?** option on the **General > Global** tab of the **Catalog Item Properties** dialog box is selected.

Table 4-8 • Current Catalog Items View

Property	Description
Approval	Indicates whether an approval is required for this catalog item. Approval is required if the **Require Approval for Install?** option is selected on the **General > Global** tab of the **Catalog Item Properties** dialog box.

New Catalog Item Wizard

You can use the **New Catalog Item Wizard** to create **General** catalog items; **Software** catalog items from System Center Configuration Manager, Altiris, Casper, and AirWatch deployment technologies; System Center Configuration Manager **Task Sequence** catalog items; and **Alert Action** catalog items.

- Catalog Item Type Panel

- Software Source Panel

- Mobile Application Panel

- Cloud Account Type Panel

- ConfigMgr/SCCM 2012 Applications Panel

- ConfigMgr/SCCM 2012 Packages Panel

- Casper Packages Panel

- Altiris Software Products Panel

- Altiris Policies Panel

- AirWatch iOS Applications Panel

- AirWatch Android Applications Panel

- AirWatch Windows Applications Panel

- MobileIron Android Applications Panel

- MobileIron iOS Applications Panel

- Catalog Item Title and Category Panel

- Flexera ID Panel

- ConfigMgr/SCCM 2012 Deployment Settings Panel

- ConfigMgr/SCCM 2012 Package Deployment Settings Panel

- Casper Package Deployment Settings Panel

- Altiris Advertisement Settings Panel

- Altiris Policy Settings Panel

- Ready to Create Panel

Tip • After creating a catalog item using the New Catalog Item Wizard, you can edit its basic and advanced settings on the Catalog Item Properties dialog box, as described in Setting Catalog Item Properties.

Note • You can also create a new catalog item using the Catalog Item Properties dialog box, which displays all of the advanced settings available to you. See Creating a New Catalog Item (Advanced)

Catalog Item Type Panel

On the **Catalog Item Type** panel of the **New Catalog Item Wizard**, you select the type of catalog item that you want to create.

Figure 4-36: Catalog Item Type Panel / New Catalog Item Wizard

Select one of the following options:

Table 4-9 • Catalog Item Type Panel / New Catalog Item Wizard

Option	Description
General Catalog Item	Select to create a catalog item usually for non-software assets, such as a headset or a mouse, that you want to make available for request in App Portal. They can also be used to enable someone to make a request for a software item that is not in the catalog.
Software Catalog Item	Select this option to connect to a deployment system and select one of the following items to make available in App Portal: ● Applications (System Center 2012 Configuration Manager only) ● Packages (System Center Configuration Manager only) ● Virtual Applications (System Center Configuration Manager only) ● Software Products (Altiris only) ● Policies (Altiris only)

Table 4-9 • Catalog Item Type Panel / New Catalog Item Wizard

Option	Description
Task Sequence	Select this option to make a task sequence available for request in App Portal. A task sequence is a mechanism used in System Center 2012 Configuration Manager to perform multiple steps or tasks on a client computer at the command-line level without requiring user intervention. Task sequences are used by SCCM to deploy operating systems.
Mobile Application Catalog Item	If App Portal is connected to an AirWatch or MobileIron instance, this option is listed. Select this option to make an iOS, Android, or Windows mobile application available in App Portal.
Cloud Catalog Item	Select this option to create a catalog item for a cloud application. During App Portal installation, catalog items are automatically created for the three cloud applications that App Portal provides out-of-the-box support for: Box, Salesforce, and Office 365.

Click **Next** to continue.

Software Source Panel

On the **Software Source** panel of the **New Catalog Item Wizard**, which opens if you select **Software Catalog Item** on the **Catalog Item Type** panel, you select the source deployment technology and deployment type of the new catalog item that you are creating.

*Note • The **Software Source** panel is only displayed when creating a software catalog item, and only lists the deployment technologies that your App Portal instance is connected to.*

The **Software Source** panel includes the following properties:

Table 4-10 • Software Source Panel / New Catalog Item Wizard

Property	Description
ConfigMgr / SCCM 2012	Select to add an application or package from the connected System Center Configuration Manager server to App Portal. Then, specify whether you are adding an **Application** or **Package**. *Note • For information on setting up a connection to ConfigMgr and SCCM 2012, see Entering System Center Configuration Manager (Current Branch) Deployment Technology Settings and Entering System Center 2012 Configuration Manager Deployment Technology Settings.*

Table 4-10 • Software Source Panel / New Catalog Item Wizard

Property	Description
Altiris	Select to add software product or policy from the connected Altiris server to App Portal. Then, specify whether you are adding a **Software Product** or a **Managed Software Delivery Policy**. 📄 *Note • An Altiris managed software delivery policy simplifies advanced software deliveries by enabling you to deliver software as a unit, which can include multiple software resources as well as dependencies. For example, you can create a single policy that installs an application and its associated patches and service packs. Policies can also run any task at any stage of the delivery. For example, it can run a task that performs a restart or runs a script.* 📄 *Note • For information on setting up a connection to Altiris, see* Entering Altiris Client Management Suite Settings*.*
Casper Package	Select to create a catalog item for an Apple macOS desktop application on a Casper server. 📄 *Note • For information on setting up a connection to a Casper server, see* Entering Casper Settings*.*

Click **Next** to continue.

Mobile Application Panel

On the **Mobile Application** panel of the **New Catalog Item Wizard**, which opens if you select **Mobile Application Catalog Item** on the **Software Source** panel, select the deployment and application type of the mobile application you want to add to this catalog item.

Figure 4-37: Mobile Application Panel / New Catalog Item Wizard

You can add multiple versions of a mobile application to the same catalog item in order to accommodate different operating systems and different . For example, a single catalog item named ABC Application could contain the following versions of the same mobile app:

- ABC Application - iOS iPhone Version

- ABC Application - iOS iPad Version

- ABC Application - Android Version

- ABC Application - Windows Version

When the end user requests this mobile application, the version appropriate to the user's registered device will be delivered.

Note • *The* *Mobile Application* *panel is only displayed when creating a mobile application catalog item.*

Cloud Account Type Panel

On the **Cloud Account Type** panel of the New Catalog Item Wizard, select the type of cloud application you want to add to this catalog item: **Box, Office 365, Salesforce, or Others.**

Figure 4-38: Cloud Account Type Panel / New Catalog Item Wizard

ConfigMgr/SCCM 2012 Applications Panel

On the **ConfigMgr/SCCM 2012 Applications** panel of the **New Catalog Item Wizard**, which opens if you select **ConfigMgr** or **SCCM 2012** and then **Application** on the **Software Source** panel, you select the application that you want to add to this catalog item.

Figure 4-39: ConfigMgr/SCCM 2012 Applications Panel / New Catalog Item Wizard

To increase performance, App Portal initially loads only a specified number of applications into this list. It loads the number of applications specified in the **Maximum package records to load from SCCM/Altiris** field on the **Admin > Settings > Web Site > General** tab. This value is, by default, 100.

Therefore, to search the entire ConfigMgr/SCCM 2012 server for a specific application, you need to use the **App ID**, **Manufacturer**, **Name**, and **Version** column filters.

Click on the application that you want to associate with this catalog item and click **Next**.

ConfigMgr/SCCM 2012 Packages Panel

On the **ConfigMgr/SCCM 2012 Packages** panel of the **New Catalog Item Wizard**, which opens if you select **ConfigMgr** or **SCCM 2012** and then **Package** on the **Software Source** panel, you select the package that you want to add to this catalog item.

Figure 4-40: ConfigMgr/SCCM 2012 Packages Panel / New Catalog Item Wizard

To increase performance, App Portal initially loads only a specified number of packages into this list. It loads the number of packages specified in the **Maximum package records to load from SCCM/Altiris** field on the **Admin > Settings > Web Site > General** tab. This value is, by default, 100.

Therefore, to search the entire ConfigMgr/SCCM 2012 server for a specific package, you need to use the **App ID**, **Manufacturer**, **Name**, and **Version** column filters.

Click on the package that you want to associate with this catalog item and click **Next**.

Casper Packages Panel

On the **Casper Packages** panel of the **New Catalog Item Wizard**, which opens if you select **Casper Package** on the **Software Source** panel, you select the Apple macOS desktop application that you want to add to this catalog item.

Figure 4-41: Casper Packages Panel / New Catalog Item Wizard

Select a package and click **Next** to continue.

Altiris Software Products Panel

On the **Altiris Software Products** panel of the **New Catalog Item Wizard**, which opens if you select **Altiris** and then **Software Product** on the **Software Source** panel, you select the Altiris software product that you want to add to this catalog item.

Figure 4-42: Altiris Software Products Panel / New Catalog Item Wizard

To increase performance, App Portal initially loads only a specified number of software products into this list. It loads the number of software products specified in the **Maximum package records to load from SCCM/Altiris** field on the **Admin > Settings > Web Site > General** tab. This value is, by default, 100.

Therefore, to search the entire Altiris server for a specific software product, you need to use the **Software ID**, **Publisher**, **Name**, and **Version** column filters.

Click on the software product that you want to associate with this catalog item and click **Next**.

Altiris Policies Panel

On the **Altiris Policies** panel of the **New Catalog Item Wizard**, which opens if you select **Altiris** and then **Managed Software Delivery Policy** on the **Software Source** panel, you select the Altiris policy that you want to add to this catalog item.

Figure 4-43: Altiris Policies Panel / New Catalog Item Wizard

To increase performance, App Portal initially loads only a specified number of policies into this list. It loads the number of policies specified in the **Maximum package records to load from SCCM/Altiris** field on the **Admin > Settings > Web Site > General** tab. This value is, by default, 100.

Therefore, to search the entire Altiris server for a specific policy, you need to use the **Policy ID** and **Name** column filters.

Click on the policy that you want to associate with this catalog item and click **Next**.

AirWatch iOS Applications Panel

On the **AirWatch iOS Applications** panel of the **New Catalog Item Wizard**, which opens if you select **AirWatch Application > iOS Application** on the **Mobile Application** panel, you select the iOS mobile application that you want to associate with this catalog item. This panel lists all of the iOS mobile applications on your connected AirWatch instance.

Figure 4-44: AirWatch iOS Applications Panel / New Catalog Item Wizard

Next to **Supported** , select **iPhone** and/or **iPad** to indicate the that this mobile application supports.

📄

*Note • You are permitted to add multiple versions of a mobile application to the same catalog item in order to accommodate different operating systems (iOS, Android) and different (iPhone, iPad). After you have created the mobile application catalog item, you can open the **AirWatch** tab of the **Catalog Item Properties** dialog box and add additional versions or delete existing ones. For more information, see Specifying the Versions Associated with a Mobile Application Catalog Item.*

AirWatch Android Applications Panel

On the **AirWatch Android Applications** panel of the **New Catalog Item Wizard**, which opens if you select **AirWatch Application > Android Application** on the **Mobile Application** panel, you select the Android mobile application that you want to associate with this catalog item. This panel lists all of the Google Android mobile applications on your connected AirWatch instance.

Figure 4-45: AirWatch Android Applications Panel / New Catalog Item Wizard

AirWatch Windows Applications Panel

On the **AirWatch Windows Applications** panel of the **New Catalog Item Wizard**, which opens if you select **AirWatch > Windows Application** on the **Mobile Application** panel, you select the Windows Phone mobile application that you want to associate with this catalog item. This panel lists all of the Windows Phone mobile applications on your connected AirWatch instance.

Figure 4-46: AirWatch Windows Applications Panel / New Catalog Item Wizard

Next to **Supported** , select **Windows Phone** and/or **Windows Phone 8** to indicate the that this mobile application supports.

📄

Note • *You are permitted to add multiple versions of a mobile application to the same catalog item in order to accommodate different operating systems (iOS, Android, Windows) and different (Windows Phone, Windows Phone 8). After you have created the mobile application catalog item, you can open the* ***AirWatch*** *tab of the* ***Catalog Item Properties*** *dialog box and add additional versions or delete existing ones. For more information, see* Specifying the Versions Associated with a Mobile Application Catalog Item.

MobileIron Android Applications Panel

On the **MobileIron Android Applications** panel of the **New Catalog Item Wizard**, which opens if you select **MobileIron Application** on the **Mobile Application** panel, you select the Android mobile application that you want to associate with this catalog item. This panel lists all of the Google Android mobile applications on your connected MobileIron instance.

Figure 4-47: MobileIron Android Applications Panel / New Catalog Item Wizard

MobileIron iOS Applications Panel

On the **MobileIron iOS Applications** panel of the **New Catalog Item Wizard**, which opens if you select **MobileIron Application** on the **Mobile Application** panel, you select the iOS mobile application that you want to associate with this catalog item. This panel lists all of the iOS mobile applications on your connected MobileIron instance.

Figure 4-48: MobileIron iOS Applications Panel / New Catalog Item Wizard

Catalog Item Title and Category Panel

On the **Catalog Item Title and Category** panel of the **New Catalog Item Wizard**, you specify the title, descriptions, category, icon, template, and search keywords for this new catalog item.

Figure 4-49: Catalog Item Title and Category Panel / New Catalog Item Wizard

The **Catalog Item Title and Category** panel includes the following properties:

Table 4-11 • Catalog Item Title and Category Panel / New Catalog Item Wizard

Property	Description
Title	Enter a title to identify this catalog item in your App Portal storefront.
Category	Select a category to specify this catalog item's location in the App Portal catalog. You are required to select at least one category, but you may select more than one.
Brief Description	Description of the catalog item that is displayed under the heading **Description** when catalog items are viewed in list view on the **Browse Catalog** tab.
Image	By default, a generic icon is associated with this catalog item. To associate a custom icon to this catalog item, click **Change** to open the **Image Selection** dialog box and select a `.gif`, `.jpg`, or `.png` icon file. *Tip • For best results, the uploaded image should be 80 px by 80 px or larger.*
Template	Optionally, from the **Template** list, select an existing template to apply advanced settings to this catalog item. *Note • For more information, see Creating a Catalog Item Template.*

Table 4-11 • Catalog Item Title and Category Panel / New Catalog Item Wizard

Property	Description
Search Keywords	Enter single words that an end user might enter when searching for this catalog item in the App Portal store front.
Full Description	Enter a more detailed description of this catalog item. This text will be displayed when a catalog item is viewed in its detail view, which is opened by clicking on the catalog item name in either the list or card view.

Click **Next** to continue.

Flexera ID Panel

App Portal communicates with FlexNet Manager Suite via the Flexera Service Gateway component. If you are connected to FlexNet Manager Suite via the Flexera Service Gateway, the **Flexera ID** panel opens.

Note • *You can use FlexNet Manager Suite to manage licenses for this catalog item.*

Figure 4-50: Flexera ID Panel / New Catalog Item Wizard

To track licenses for this catalog item using its Flexera ID, use the column filters (**Product**, **Edition**, **Version**, and **Publisher**) to locate this catalog item in FlexNet Manager Suite, select it, and click **Next** to continue.

ConfigMgr/SCCM 2012 Deployment Settings Panel

If you are adding an application from ConfigMgr/SCCM 2012, you need to specify deployment settings on the **ConfigMgr/SCCM 2012 Deployment Settings** panel.

Figure 4-51: ConfigMgr/SCCM 2012 Deployment Settings Panel / New Catalog Item Wizard

The **ConfigMgr/SCCM 2012 Deployment Settings** panel includes the following properties:

Table 4-12 • ConfigMgr/SCCM 2012 Deployment Settings Panel / New Catalog Item Wizard

Property	Description
Select Deployment Method	Select one of the following options to specify whether this catalog item will be deployed to a computer or to a user: ● **Deploy to computer** ● **Deploy to user**
Create Uninstall Collection	Select this option to add an uninstall collection to this catalog item. When this option is selected, users will be able to submit an uninstall request from App Portal, and System Center Configuration Manager will uninstall the application. App Portal will inform the user when the uninstall is complete.

ConfigMgr/SCCM 2012 Package Deployment Settings Panel

If you are adding a package from ConfigMgr/SCCM 2012, you need to specify deployment settings on the **ConfigMgr/SCCM 2012 Package Deployment Settings** panel.

On the **ConfigMgr/SCCM 2012 Package Deployment Settings** panel, you are required to select at least one program for deployment. On this panel you can also specify advertisement and distribution settings for the selected package.

Figure 4-52: ConfigMgr/SCCM 2012 Package Deployment Settings Panel / New Catalog Item Wizard

The **ConfigMgr/SCCM 2012 Package Deployment Settings** panel includes the following properties:

Table 4-13 • ConfigMgr/SCCM 2012 Package Deployment Settings Panel / New Catalog Item Wizard

Property	Description
Select Program for Install **Select Program for Uninstall** **Select Program for Repair**	From these lists, select at least one existing program from the System Center Configuration Manager server.
Program for OS Deployment Task Sequence	Select a matching program name for the program function.
Make the advertisement mandatory	Select this option to make this advertisement mandatory.
Mandatory over slow links?	Select this option to require that the installation is run even when a client has a slow connection. If this option is not selected, the System Center Configuration Manager client agent will not perform the installation if the client has a slow connection, but will perform the installation if the client is connected over a regular LAN connection.
Advertisement Priority	Specify the priority of the advertisement: **High**, **Medium**, or **Low**.
Ignore maintenance windows	Select to have the advertised program ignore maintenance windows while the program is running.
Allow system restart outside of maintenance windows	Select to allow the advertised program to restart the client even if the restart would occur outside a maintenance window.

Table 4-13 • ConfigMgr/SCCM 2012 Package Deployment Settings Panel / New Catalog Item Wizard

Property	Description
Program rerun behavior	Specifies whether the advertised program will be rerun on the client computer if it has previously been run before the scheduled mandatory time. Select one of the following options: ● **Never rerun advertised program**—The program will not be rerun on the client if the program has previously been run on the client, even if the program originally failed or the program files have been changed. ● **Always rerun**—The program will always be rerun on the client when the advertisement is scheduled, even if the program has already been successfully run. ● **Rerun if failed previous attempt**—The program will be rerun when the advertisement is scheduled only if it failed on the previous run attempt. ● **Rerun if succeeded on previous attempt**—The program will be rerun only if it has previously run successfully on the client. *Important • This option is only enabled if **Make the advertisement mandatory** is also selected.*
When a Distribution Point is available locally	Select one of the following options to specify how content will be downloaded from the distribution points when a distribution point is available locally: ● **Run program from distribution point**—Run program directly from a distribution point. ● **Download program from distribution point**—Download program from the distribution point to the client computer before attempting to run the program.
When no Distribution Point is available locally	Select one of the following options to specify how content will be downloaded from the distribution points when no distribution point is available locally: ● **Do not run program**—Do not run program. ● **Download program from remote distribution point**—Download the program from a remote distribution point to the client computer before attempting to run the program. ● **Run program from a remote distribution point**—Run program directly from a remote distribution point.
When no protected distribution point is available, use an unprotected distribution point	Select this option to permit a client to use an unprotected distribution point if content is not immediately available on its protected distribution point. If this option is not selected, the client will not use unprotected distribution points.

Casper Package Deployment Settings Panel

If you are adding an macOS desktop package from Casper, you need to specify deployment settings on the **Casper Package Deployment Settings** panel.

Figure 4-53: Casper Package Deployment Settings Panel / New Catalog Item Wizard

The **Casper Deployment Settings** panel includes the following properties:

Table 4-14 • Casper Deployment Settings Panel / New Catalog Item Wizard

Property	Description
Create Uninstall Policy	If you want this App Portal catalog item to support uninstallation of the application, select this option. If this option is selected, two policies will be created in Casper: one for installation and one for uninstallation. In addition, App Portal will create two static computer groups: one will be added to the install policy, and the other will be added to the uninstall policy. When users place requests for the catalog item, computers get added to the static computer group and then Casper takes care of deployment. *Note • App Portal does not support Casper Remote.*
Select Distribution point	Select a Casper distribution point from this list. Distribution points are servers used to host files for distribution to computers.

Altiris Advertisement Settings Panel

If you are adding a software product from Altiris, you need to specify deployment settings on the **Altiris Advertisement Settings** panel.

Chapter 4   Managing Your Catalog
Catalog Management Reference

Figure 4-54: Altiris Advertisement Settings Panel / New Catalog Item Wizard

The **Altiris Advertisement Settings** panel includes the following properties:

Table 4-15 • Altiris Advertisement Settings Panel / New Catalog Item Wizard

Property	Description
Select Deployment Method	Select one of the following options: • **Deploy to user** • **Deploy to computer**
Select Program for Install **Select Program for Uninstall** **Select Program for Repair**	From these lists, select the program name that you would like to add for each function. 📄 *Note • You are required to select at least one program.*

Altiris Policy Settings Panel

If you are adding a managed software delivery policy from Altiris, you need to specify deployment settings on the **Altiris Policy Settings** panel.

Figure 4-55: Altiris Policy Settings Panel / New Catalog Item Wizard

The **Altiris Policy Settings** panel includes the following properties:

Table 4-16 • Altiris Policy Settings Panel / New Catalog Item Wizard

Property	Description
Select Policy Deployment Method	Select one of the following options: • **Deploy to user** • **Deploy to computer**
Select Software Delivery Item	This list lists all of the software delivery items that are included in the selected Altiris policy. Select the software delivery item that you want this new **Software** catalog item to contain.
Select Deployment Type	Select one of the following items to match the purpose of the selected software delivery item: • **Install** • **Uninstall** • **Repair**

Ready to Create Panel

The **Ready to Create** panel of the **New Catalog Item Wizard** lists a summary of the selections you made in the wizard.

Figure 4-56: Ready to Create Panel / New Catalog Item Wizard

If you want to open the catalog item's **Catalog Item Properties** dialog box immediately after it is created, select the **Load advanced view after creating the catalog item** option. On the Catalog Item Properties Dialog Box dialog box you can specify advanced settings.

Review the summary information and then click **Create** to create this new catalog item. When the catalog item creation is complete, a dialog box opens stating that the creation was successful.

Catalog Item Properties Dialog Box

The **Catalog Item Properties** dialog box is a multi-tabbed form that you use to create a new catalog item and edit the properties of an existing catalog item. After a catalog item is created, the name of the dialog box changes to the name of the catalog item.

There are several ways to open the **Catalog Item Properties** dialog box:

Table 4-17 • Ways to Open the Catalog Item Properties Dialog Box

When you want to ...	Do this ...
To create a new Software Catalog Item	Under **Catalog Management > Create New Catalog Item**, select the **New Software Catalog Item** node.
	Note • You can also create a new Software catalog item using the New Catalog Item Wizard, as described in Creating a New Catalog Item Using the Wizard.

Table 4-17 • Ways to Open the Catalog Item Properties Dialog Box

When you want to …	Do this …
To create a new General Catalog Item	Under **Catalog Management > Create New Catalog Item**, select the **New General Catalog Item** node. 📄 *Note •* *You can also create a new **General** catalog item using the New Catalog Item Wizard, as described in* Creating a New Catalog Item Using the Wizard*.*
To create a new Group Catalog Item	Under **Catalog Management > Create New Catalog Item**, select the **New Group Catalog Item** node.
To edit an existing catalog item	On the **Catalog Management > Current Catalog Items** view, double-click an existing catalog item.

The **Catalog Item Properties** dialog box includes the following main tabs:

- General Tab
- Notes Tab
- Deployment Tab
- AirWatch Tab
- Link Desktop Catalog Tab
- FlexNet Manager Suite Tab
- Catalog Items Tab
- Visibility Tab
- Approval Tab
- Approval Process Tab
- Custom Variables Tab
- Cloud Apps Tab
- Security Groups Tab
- Actions Tab
- Notifications Tab
- Permissions Tab

General Tab

The **General** tab of the **Catalog Item Properties** dialog box includes the following subtabs:

- Global Subtab

- Title & Description Subtab

- Alert Subtab

- Inventory Subtab

- Upgrade/Replacement Subtab

- Alternates Subtab

- Requirements Subtab

- Reviews Subtab

Global Subtab

The **General > Global** tab of the **Catalog Item Properties** dialog box includes global, approval, request, scheduling, and image options.

Figure 4-57: Catalog Item Properties Dialog Box / General > Global Tab

The **General > Global** tab of the **Catalog Item Properties** dialog box includes the following properties:

Table 4-18 • Catalog Item Properties Dialog Box / General > Global Tab Properties

Property	Description
Load settings from template	When you create a new request, you can specify a template to load settings from previously created requests. *Note • Only listed before application or package is saved.*
Is enabled?	Select this option to make the catalog item visible within App Portal regardless of other permission settings.

Table 4-18 • Catalog Item Properties Dialog Box / General > Global Tab Properties

Property	Description
Category	Select a category to associate the new catalog item with. Categorize are used by the program for searching on the Browse Catalog tab. A package can be a member of multiple categories.
Class	Select a class to associate the new catalog item with.
Question Template	Select a Question Template for use by the new catalog item. A question template is a group of questions to ask at the time of request.
Template Name	If you wish to make the settings specified in this request available as a template for other requests, enter a descriptive name here.
Expire on	Select a future date to mark this request inactive (disabling globally visible setting).
Require Approval for Install?	Select this option to require an approval prior to installing this software.
Do not inherit bundle Approval process	Select this option to prevent this catalog item from inheriting the approval workflow assigned to the group catalog item that contains it.
Allow removal from bundle?	Select this option to enable an end user to remove this catalog item from a group catalog item when submitting a request.
	For example, if a group catalog item contained a computer, monitor, and a set of headphones, if this option was selected for the headphones catalog item, an end user requesting this group catalog item would be permitted to remove the headphones from the bundle and request just the computer and monitor.
Do not sync the catalog with ServiceNow	This field enables/disables syncing of this OSD task sequence catalog items in ServiceNow.
	• **If this option is selected**, the catalog item will not be synced into ServiceNow and will not be available as a Service Catalog in ServiceNow.
	• **If this option is not selected**, the catalog item will be synced into ServiceNow and will be available as a Service Catalog in ServiceNow.
Request options	Select the options in this category that you want to enable, as described in Request Options.
Scheduling options	Select the options in this category that you want to enable, as described in Scheduling Options.
Image	Change the **Image** Icon that will be shown next to the new catalog item.
Direct link	A direct link to the package or application.

📄

Note • Only listed after package or application has been saved.

Request Options

The **Request Options** area of the **General > Global** tab of the **Catalog Item Properties** dialog box includes the following options:

Table 4-19 • Request Options

Property	Description
Enable request on behalf?	Select this option to enable the requester to request catalog items for another person or device. Requester can search by machine name, full name, or user name to locate the target device(s) / user(s) of the request.
	If this option is selected, the **Search for people or computers** option will be listed on the **Choose Target** panel of the Checkout view for those requesters who have been assigned rights to the **Request on Behalf** catalog security role.
	*Important • In order to have access to these "request on behalf" options, the requester must have been assigned the **Request on Behalf** catalog security role under **Catalog Management > Catalog Security**. See Managing Catalog Permissions.*
	Note • For more information, see Enabling a Catalog Item to Be Requested on Behalf of Another User / Device.
Enable request to AD property?	Select this option to enable the requester to search by Active Directory account attributes to locate the target device(s) / user(s) of the request.
	If this option is selected, the **Search using account attributes** option will be listed on the **Choose Target** panel of the Checkout view for those requesters who have been assigned rights to the **Request on Behalf** catalog security role.
Enable request for AD manager?	Select this option to enable the requester to search a list of direct reports by machine name, full name, or user name to locate the target device(s) / user(s) of the request.
	If this option is selected, the **People who report to me** option will be listed on the **Choose Target** panel of the Checkout view for those requesters who have been assigned rights to the **Request on Behalf** catalog security role.
Enable request to manual list?	Select this option to enable the requester to manually add a list of machine names or user IDs to identify the target device(s) / user(s) of the request.
	If this option is selected, the **Add machine names or user IDs manually** option will be listed on the **Choose Target** panel of the Checkout view for those requesters who have been assigned rights to the **Request on Behalf** catalog security role.
Allow File Upload?	Select this option to enable end users to upload files to this catalog item during checkout.

Table 4-19 • Request Options

Property	Description
Allow switch to?	Select this option to specify that this catalog item is available to be an alternate catalog item for another catalog item. It will be listed on the **General > Alternates** tab of the **Catalog Item Properties** dialog box. See Alternates Subtab.
Enable unknown computer deployment (OSD Only)?	Enables deployment of OSD task sequence catalog items to unknown computers.
	If this option is selected, the **Build an unknown computer and migrate my data from MACHINENAME to the new computer** option is listed on the **Choose Target** panel during of the Checkout Wizard during checkout of an OSD task sequence catalog item. And if this option is selected on the **Choose Target** panel, App Portal will instruct SCCM to build an unknown computer and migrate the requester's data from their current machine to the new computer.
Show on support tools?	Choose whether this catalog item will be displayed on the **Support Tools** tab. This setting overrides globally visible settings and applies the visibility settings of the catalog item.
	If you wish to apply approval settings to the requests in **Support Tools**, select the **Require approval for support tools** option on the **Catalog Behavior** tab of the **Site Management > Settings > Web Site** view.
Show for Clone/Migrate	If this option is selected, then this application will be available on the **Clone/Migrate** view of the **Support Tools** tab. The **Clone/Migrate** feature is used to deliver applications from a source computer to a target computer. For more information, see Using Clone/Migrate to Migrate Applications to Another System.
Core application (not available for migration during task sequence deployment)	Every enterprise has a set of core applications that are included on all corporate images that are created, such as Microsoft Office, Chrome, etc. Because those applications are included in all OS images, there is no reason to ask an individual to select them during check out of an OSD task sequence catalog item.
	To prevent an application from being listed on the **Choose Existing Applications to Migrate** or **Additional Applications to Install During OS Deployment** panels of the Checkout Wizard, select this option.
	You can view a list of all catalog items that have been designated core applications on the **Catalog Management > Administration > Core Applications** view.
	📄❗
	Important • This option only applies to software catalog items, not general or task sequence, or cloud catalog items.
Define Installation Order?	Identify this catalog item is dependent on installation order. All catalog items with this tag can be globally ordered under the Deployment Management node > Install Sequence. This order will determine the order presented to the OSD Task Sequence when used as part of an OS Deployment.

Scheduling Options

The **Scheduling Options** area of the **General > Global** tab of the **Catalog Item Properties** dialog box includes the following options:

Table 4-20 • Scheduling Options

Property	Description
Allow scheduling immediately after approval?	Determines whether the requester can choose **Install immediately after approval** option during checkout. Disable this option when the application requires a reboot or otherwise interferes with the user's experience.
Allow user defined scheduling?	Determines whether the requester can select a specific date and time for installation scheduling for items that do not require approval. *Important •* *This option must be selected in order for you to specify software leasing. For more information. See Leasing Subtab.*
Allow ASAP scheduling?	Determines whether the requester can choose **Install ASAP** for items that do not require approval.
Initial schedule offset (hrs)	When ASAP scheduling is enabled, this value offsets the soonest time the requester can selected from the current time in hours.
Enable scheduling constraints?	Determines whether this catalog item is affected by scheduling constraints defined under Deployment Management. Select when you want the scheduling restricted based on scheduling constraints.
Require User Readiness record?	Determines whether a user readiness record is required to be present under Deployment Management for the requester to be able to request this catalog item.

Title & Description Subtab

On the **General > Title & Description** tab of the **Catalog Item Properties** dialog box, you enter a title to identify the item, enter a description of the item, and provide search keywords.

Figure 4-58: Catalog Item Properties Dialog Box / General > Title & Description Tab

The **General > Title & Description** tab of the **Catalog Item Properties** dialog box includes the following properties:

Table 4-21 • New Catalog Item / General > Title & Description Tab Properties

Property	Description
Language	Specify the language for the description. Additional languages can be added on the **Site Management > Communication > Languages** view.
Title	Enter a title to identify this catalog item.
Brief Description	Description of the catalog item that is displayed under the heading **Description** when catalog items are viewed in list view on the **Browse Catalog** tab.
Search Keywords	Define single words for searching accuracy.
Full Description	Enter a more detailed description of this catalog item. This text will be displayed when a catalog item is viewed in its detail view, which is opened by clicking on the catalog item name in either the list or card view.

Alert Subtab

You can use the **General > Alert** tab of the **Catalog Item Properties** dialog box to add additional information about the catalog item that you would like to be displayed to the user checking out the catalog item. This information will be presented to the user in a pop-up message when that catalog item is added to the cart.

Figure 4-59: Catalog Item Properties Dialog Box / General > Alert Tab

When a catalog item with an associated alert—and with the **Show alert message when adding to cart** option selected—is added to the cart on the **Browse Catalog** tab, the text of the alert message will appear in a pop-up dialog box.

Figure 4-60: Catalog Item Alert Message Pop-Up Dialog Box

Inventory Subtab

Note • Not available when creating a group catalog item.

App Portal allows tracking of software and computers in use in your company. App Portal will count and link license data directly to the organizational data to allow for detailed reporting on license usage.

You can use the **General > Inventory** tab of the **Catalog Item Properties** dialog box to link inventory Item to Catalog Items as part of a tracking and usage process. You can assign inventory items to computers that request this catalog item on installation or approval.

The **General > Inventory** tab has three subtabs:

● FlexNet Manager Suite Inventory Subtab

● SCCM Inventory Group Subtab

● Inventory Costs Subtab

FlexNet Manager Suite Inventory Subtab

If you have also purchased FlexNet Manager Suite and are connected to the Flexera Service Gateway, you can use App Portal to manage application licenses. On the **General > Inventory > FlexNet Manager Suite Inventory** tab, you specify inventory options.

Figure 4-61: Catalog Item Properties Dialog Box / General > Inventory > FlexNet Manager Suite Inventory

The **FlexNet Manager Suite Inventory** tab includes the following properties.

Table 4-22 • FlexNet Manager Suite Inventory Tab

Properties	Description
When inventory is exceeded	Select an option to specify what should occur when inventory is exceeded: ● **Disable request and approval** ● **Always require approval** ● **Do nothing**
Cost	Enter the cost of this catalog item.
Show inventory count to users	Select this option to display the inventory count of this catalog item on the **Browse Catalog** tab.

Table 4-22 • FlexNet Manager Suite Inventory Tab

Properties	Description
Show inventory cost to users	Select this option to display the cost of this catalog item on the **Browse Catalog** tab.

SCCM Inventory Group Subtab

Note • *This tab is not displayed if you are connected to FlexNet Manager Suite via the Flexera Service Gateway.*

You specify an inventory group for product licensing on the **SCCM Inventory Group** tab.

Figure 4-62: Catalog Item Properties Dialog Box / General > Inventory > SCCM Inventory Group Tab

The **SCCM Inventory Group** tab includes the following properties:

Table 4-23 • Catalog Item Properties Dialog Box / General > Inventory > SCCM Inventory Group Tab Properties

Property	Description
Select an inventory group for product licensing	Choose an inventory group to link to the request. Linking inventory groups to requests allows the request to become aware of inventory owned vs. used. The difference of which can affect how users request the application and the type of approval (if any) that is required.

Table 4-23 • Catalog Item Properties Dialog Box / General > Inventory > SCCM Inventory Group Tab Properties

Property	Description
When inventory is exceeded	Choose what to do when the inventory count is exceeded: • **Disable request and approval**—Will not allow clients to request or approvers to approve requests when the license count is exceeded • **Always require approval**—Will require approval regardless of other settings for the package. • **Do nothing**—Will take no action when the license count is exceeded.
Show inventory count to users	Whether the current count of available licenses should be displayed to the user.
Show inventory cost to users	Whether the current cost of available licenses should be displayed to the user.
Assign inventory on installation / approval	Assigns the request to the user upon approval and installation. Assigning the inventory allows for a purchase to be related to the request and assists in determining whether an installation is authorized.
Use the cost of the inventory group	Sometimes you may wish to display a different cost to the end user than is identified in the inventory group. Select this setting if you wish to use the cost of the inventory group or specify the new cost in the **Enter a custom cost** box.
Prevent reinstall / allow uninstall and repair only if installed	Only allow the install option if the software **is not** currently installed and only allow the uninstall option if the software **is** installed.
Select an inventory group for product installation detection	In the event you need to use two different inventory groups for licensing and detection, or wish to detect a product without making it licensed, specify the inventory group for product installation detection here.

Inventory Costs Subtab

On the **Inventory Costs** tab, you can specify different costs based on currency. Those currencies that have been enabled under **Site Management > Purchasing > Currency** will be displayed here to offer a specific cost based on the users default currency.

When specified at the catalog item level, the currency translation based on rate conversions is not used. The actual fixed value specified in the **Cost** column is displayed instead.

Figure 4-63: Catalog Item Properties Dialog Box / General > Inventory > Inventory Costs Tab

Upgrade/Replacement Subtab

On the **General > Upgrade/Replacement** tab, you can identify what catalog item to offer, or perform an upgrade to an existing catalog item.

Note • Upgrade/Replacement settings are only enforced when migrating existing applications or installing new applications as part of the deployment of an OSD task sequence catalog item or when using App Survey; they are not enforced when requesting an individual catalog item.

Figure 4-64: Catalog Item Properties Dialog Box / Upgrade/Replacement Tab

Search for the **Inventory Group** item in the left list and select a catalog item, then click the **Add** button to link the **Inventory Item** to the **Catalog Item**.

When finished, click the **Save** button to complete the process.

Alternates Subtab

You can use the **General > Alternates** tab to link catalog items to other catalog items to identify or offer other catalog items for deployment. For example, you can link applications that can replace existing items or new applications.

Figure 4-65: Catalog Item Properties Dialog Box / Alternates Tab

Catalog items are available as alternates if the **Allow switch to?** option is selected on the **General > Global** tab of the **Catalog Item Properties** dialog box.

Search for the **Catalog Item** in the left list and place a **Check** next to the item, then click the **Add** button to link the catalog item to the current catalog item.

When finished, click the **Save** button to complete the process.

Requirements Subtab

Note • Not available when creating a group catalog item.

You can use the **General > Requirements** tab to specify hardware that must be satisfied in order for the catalog item to be made available for check-out by the computer visiting the App Portal web site.

Figure 4-66: Catalog Item Properties Dialog Box / Requirements Tab

To enable this feature, select the **Enable hardware requirement verification** option, and select a metered application from the list.

Set the **When the computer does not meet the requirements** option to either **Do nothing**, **Prevent request**, or **Always require approval** to specify what you would like to take place when the computer does not meet this requirement.

To display a description of the requirements to the user visiting the App Portal web site, enter a description in the **Enter a message to display when requirements are not met** text box.

Reviews Subtab

📄

Note • Not available when creating a group catalog item.

On the **General > Reviews** tab, administrators can review surveys and ratings that have been submitted for the current catalog item.

Figure 4-67: Catalog Item Properties Dialog Box / General > Reviews Tab

Notes Tab

You may want to document a special issue or event associated with a particular catalog item. To do this, you can add notes to a catalog item on the **Notes** tab of the **Catalog Item Properties** dialog box.

To add a note, click **Add New Note** on the **Notes** tab of the **Catalog Item Properties** dialog box. A pop-up dialog box opens prompting you to enter the text of the note.

Figure 4-68: Adding a Note to the Notes Tab

After you enter the text of the note and click **Add Note**, the note is now listed on the **Notes** tab, along with the name of the person who added the note and the date and time.

Figure 4-69: Note Listed on the Notes Tab

To view and edit a note, click **Edit** next to the note text. A drop down editing area appears below the note name.

Figure 4-70: Editing a Note on the Notes Tab

Edit the text in the text box and click **Update** to save your edits.

Deployment Tab

Note • Not available when creating a group catalog item.

On the **Deployment** tab of the **Catalog Item Properties** dialog box, you specify deployment system options. The **Deployment** tab has the following subtabs:

- Global Subtab

- ConfigMgr / SCCM 2012 Subtab

- Altiris Subtab

- Casper Subtab

- AirWatch Subtab

- MobileIron Subtab

- Leasing Subtab

- Roles Subtab

The following dialog boxes are launched from the various subtabs of the **Deployment** tab.

- Collection Variables Dialog Box

- Computer Variables Dialog Box

- Add Package Dialog Box

- Add Program Dialog Box

- Add Software Product Dialog Box

- Altiris Software Product Deployment Dialog Box

- Add Existing Altiris Policy Dialog Box

- SCCM Deployment Dialog Box

Global Subtab

On the **Deployment > Global** tab, enter approval, installation, and notification options.

Figure 4-71: Catalog Item Properties Dialog Box / Deployment > Global Tab

The **Deployment > Global** tab of the **Catalog Item Properties** dialog box includes the following properties:

Table 4-24 • Catalog Item Properties Dialog Box / Deployment > Global Tab Properties

Property	Description
Require Approval for Install?	Determines whether the request requires approval for the install function. If an approval group is not specified, the default approver is specified in Email Settings.
Require Approval for Reinstall?	Allows a client to Rerun a program after it has been installed. This action will remove the previous execution flag from the client and force a machine policy cycle. The Service account will require local administrative permissions on the client.
Require Approval for Uninstall?	Determines whether the request requires approval for the uninstall function. If an approval group is not specified, the default approver is specified in Email Settings.

Table 4-24 • Catalog Item Properties Dialog Box / Deployment > Global Tab Properties

Property	Description
Require Approval for Clone/ Migrate?	Determines whether the request requires approval for the clone/migrate function from the Support Tools section in the storefront. If an approval group is not specified, the default approver specified in Email Settings.
Enable Reinstallation/Rerun?	Allows a client to Rerun a program after it has been installed. This action will remove the previous execution flag from the client and force a machine policy cycle. The Service account will require local administrative permissions on the client.
Enable Uninstallation (Remove from collection)?	Allows a client to uninstall a program after it has been installed or request uninstallation during checkout. If you select this option, an uninstall program must be linked to the catalog item on the **Deployment > ConfigMgr/CCM 2012** tab.
Enable Repair?	Allows a client to repair a program after it has been installed or request un installation during checkout. If you select this option, a repair program must be linked to the catalog item on the **Deployment > ConfigMgr/SCCM 2012** tab.
Apply Computer Variables (Task Sequence)?	Select this option to apply computer variables for task sequences. If this option is selected, the variable specified in the **Base Application Variable Name** field on the **Site Management > Settings > Deployment > ConfigMgr/ SCCM 2012** tab will be used to deploy applications as part of the Install Applications step in a SCCM OSD Task Sequence.
Remove Variables after successful OS Deployment?	Select this option to remove variables from the task sequence environment after successful OS deployment.
Remove from collection when complete?	Choose whether direct members of the SCCM collection should be removed once complete. Completion is determined using return values from SCCM specified in **Program Collection Cleanup Status IDs** and **Task Sequence Collection Cleanup Status IDs** fields on the **Site Management > Settings > Deployment > ConfigMgr/SCCM 2012** tab.
Start deployment using API?	When a request is submitted, if a catalog item does not require an approval, App Portal automatically triggers the deployment. However, if you have integrated App Portal with an ITSM system and you want to perform approvals using that system, you would not want the catalog item to be deployed until the external approval was performed. In this situation, you would select the **Start deployment using API?** option to delay deployment until a response from the ITSM system would trigger the deployment via App Portal's API.

Table 4-24 • Catalog Item Properties Dialog Box / Deployment > Global Tab Properties

Property	Description
Send failure email?	App Portal will send an email to the Site Administrator when the Advertisement fails on a client.
Send success email?	App Portal will send an email to the client when the Advertisement succeeds on a client.
Reboot required?	Visually indicated whether a reboot is required for this item.
Estimated run time	Textual display of the expected install time.
Automatically fail if final status is not received after *n* hours	To automatically fail the deployment of this catalog item if its final status is not received after a specified number of hours, enter a number in this text box.
Automatically fail if no status is received after *n* hours	To automatically fail the deployment of this catalog item if no status is received after a specified number of hours, enter a number in this text box.

ConfigMgr / SCCM 2012 Subtab

From the **ConfigMgr** or **SSCM 2012** subtab of the **Deployment** tab, you can add an application, package, or task sequence from System Center Configuration Manager to your catalog item and set its deployment settings.

If you have already added an application, package or task sequence to the catalog item, the **Deployment > ConfigMgr / SCCM 2012** tab lists the reference to that item, along with buttons that enable you to customize the deployment settings.

Figure 4-72: Deployment > ConfigMgr / SCCM 2012 Tab with a Linked Program

Before a package, application, or task sequence has been added to a catalog item, the **Deployment > ConfigMgr / SCCM 2012** tab is empty, and only includes one button: **Add Package**.

Figure 4-73: Deployment > ConfigMgr / SCCM 2012 Tab with No Linked Programs

The **ConfigMgr** / **SCCM 2012** subtab includes the following options:

Table 4-25 • Deployment > ConfigMgr / SCCM 2012 Subtab

Property	Description
Add Package	To add a package, application, or task sequence to this catalog item, click this button to open the Add Package Dialog Box. *Note • As soon as a package is added, the name of this button changes to **Change Package**.*
Change Package	To change packages, first delete existing packages, and then add a new package using the **Add Package** button. Clicking the **Change Package** button just displays a warning message stating that existing deployment(s) must be deleted in order to change the package. *Note • Only displayed after a package has been added.*
New Deployment	Click to add a new deployment. *Note • Only displayed for software catalog items.*
Delete Deployment	Click to delete the selected deployment. *Note • Only displayed for software catalog items.*
New Program	Click to add a new program. *Note • Only displayed for task sequence catalog items.*

Table 4-25 • Deployment > ConfigMgr / SCCM 2012 Subtab

Property	Description
Delete Program	Click to delete the selected program.
	📄
	Note • Only displayed for task sequence catalog items.
Get details	For verification of the listed program or application, select the check box next to an item and click **Get details** to verify the deployment of these new items created successfully in System Center Configuration Manager. After you click the **Get details** button, additional information is listed in the **Collection** column.
Collection Variables	To add variables to a collection, click this button to open the Collection Variables Dialog Box.
Computer Variables	To add variables to computers, click this button to open the Computer Variables Dialog Box.

Altiris Subtab

On the **Deployment > Altiris** subtab of the **Catalog Item Properties** dialog box, you add a software product or a policy on the Altiris Notification Server to the catalog item.

The information and buttons displayed on this tab depend upon whether a software product or policy has been added. Before a product or policy has been added, only the **Add Software Product** and **Add Existing Policy** buttons are displayed.

Figure 4-74: Catalog Properties Dialog Box / Deployment > Altiris Subtab (No Linked Programs)

After a policy or program has been added to the catalog item, buttons appear in the ribbon that enable you to change the product, add another policy/program, delete the program, and get additional details.

Figure 4-75: Catalog Properties Dialog Box / Deployment > Altiris Subtab (With Program Listed)

The **Deployment > Altiris** subtab includes the following properties:

Table 4-26 • Catalog Item Properties Dialog Box / Deployment > Altiris Subtab

Property	Description
Add Software Product	Click to open the Add Software Product Dialog Box followed by the Altiris Software Product Deployment Dialog Box, where you can select a package on the Altiris server to add to this catalog item.
Add Existing Policy	Click to open the Add Existing Altiris Policy Dialog Box, where you can select an existing policy on the Altiris server to add to this catalog item.
Change Software Product	To change a software product or policy, first delete existing policies/programs, and then add a new software product or policy using the **Add Software Product** or **Add Existing Policy** button. Clicking the **Change Software Product** button just displays a warning message stating that existing items must be deleted in order to change the software product. *Note • Only displayed after a software product or policy has been added.* *Note • This button is obsolete and will be removed in the next release.*
Delete Program	Select a software product or policy in the list and click this button to delete it from the catalog item.

Table 4-26 • Catalog Item Properties Dialog Box / Deployment > Altiris Subtab

Property	Description
Get details	Select a policy and then click this button to access the Altiris server and obtain additional information on the selected policy. *Tip • If you select a software item instead of a policy and then click this button, no additional information will be displayed. Additional information is only displayed for policies.*
Refresh	Click to contact the Altiris server and refresh the list.
List of products/policies	For each product or policy that is added to the catalog item, the following information is displayed in the list: • **Site**—Site server name. • **Server**—Site database server name. • **AdvertID**—Advertisement/policy ID created on the Altiris server. (Policy only) • **CollectionID**—Collection ID created by App Portal. • **Function**—Identifies the function of the program as either an Install, Uninstall, or Repair. • **Language**—Language of the program. • **Advertisement**—Name of advertisement defined on the Altiris server. (Policy only) • **Collection**—Name of collection defined on the Altiris server. (Policy only) • **Program**—Name of the program defined on the Altiris server. • **Package ID**—ID assigned to program by the Altiris server. (Policy only) • **Create Date**—Date and time program/policy was added to this catalog item. • **Error**—Displays an error message, if necessary.

Casper Subtab

From the **Casper** subtab of the **Deployment** tab, you can select a package from Casper to add to your catalog item and set its deployment settings. Existing macOS desktop applications are listed.

Figure 4-76: Catalog Properties Dialog Box / Deployment > Casper Subtab

AirWatch Subtab

From the **AirWatch** subtab of the **Deployment** tab, you can select a package from AirWatch to add to your catalog item and set its deployment settings. Existing mobile applications are listed.

Figure 4-77: Catalog Properties Dialog Box / Deployment > AirWatch Subtab

MobileIron Subtab

From the **MobileIron** subtab of the **Deployment** tab, you can select a package from MobileIron to add to your catalog item and set its deployment settings. Existing mobile applications are listed.

Figure 4-78: Catalog Properties Dialog Box / Deployment > MobileIron Subtab

Click **Delete** to remove a selected application from the catalog item.

If you click **Add Android Application** or **Add iOS Application**, a dialog box opens prompting you to select the desired application and then click **Add Application**.

Figure 4-79: Add Android Application Dialog Box

Leasing Subtab

On the **Deployment > Leasing** tab of the **Catalog Item Properties** dialog box, you can specify software leasing options.

*Important • To be able to specify software leasing options, you first need to select the **Allow user defined scheduling?** option in the Scheduling Options section of the **General > Global** tab of the **Catalog Item Properties** dialog box.*

Figure 4-80: Catalog Item Properties Dialog Box / Deployment > Leasing Tab

The **Deployment > Leasing** tab includes the following properties:

Table 4-27 • Deployment > Leasing Tab

Property	Description
Enable Leasing (Requires Uninstall Program)	Select to activate Software Leasing to show lease options on Checkout page.
Allow leasing up to X days	Determine the maximum number of days to allow a lease.
Default lease duration X days	Specify the default lease duration.
Notify users X day(s) before lease end	Determines when the notification email that the lease is expiring is sent to the user.
Disable Permanent Installation	Forces the requester to select a lease period and disables the **Permanent Installation** option during checkout.

Table 4-27 • Deployment > Leasing Tab

Property	Description
Allow user to extend lease when approval is not required	Allows the user to extend the lease of this catalog item without requiring any approval.
	If this option is selected for a catalog item, a user who has this catalog item installed would receive the following email shortly before the lease expiration date:
	Your lease for Orca 5.0.7069.0000 lease will expire on 4/9/2016 7:49:02 PM for User Don (UserDon) on AS2012R2-NB1.
	To extend the lease for Orca 5.0.7069.0000 lease, please visit This Link
	To extend the lease of this catalog item, the user must perform the following steps.
	To extend the lease of a catalog item:
	1. Click on **This Link** in the notification email you received. The **My Requests** page opens.
	2. Click on the catalog item with the expiring lease. The **Request Details** dialog box opens.
	3. Open the **Status** tab.
	4. Change the **Lease Expiration** date.
	5. Click **Save**.
Allow user to extend lease when approval is required	Allows the user to extend the lease when an approval is required for the catalog item to be requested.
Allow extension only up to maximum days allowed	If lease extension is enabled, this setting will allow a lease extension only up to the maximum number of days allowed to lease.

Roles Subtab

You can attach roles to Task Sequence catalog items to identify the applications that will be installed during an operating system deployment. You attach roles to a task sequence catalog item on the **Deployment > Roles** tab of the **Catalog Item Properties** dialog box.

Figure 4-81: Catalog Item Properties Dialog Box / Deployment > Roles Tab

You can use roles to specify applications, computer variables, and/or Microsoft User State Migration Tool (USMT) profiles that App Portal can apply conditionally during the imaging process.

Note • For more information on roles and how to create them, see Using Roles to Identify Applications to Deploy with a Task Sequence Catalog Item.

The **Deployment > Roles** tab of the **Catalog Item Properties** dialog box includes the following properties:

Table 4-28 • Deployment > Roles Tab / Catalog Item Properties Dialog Box

Property	Description
Allow user role selection	Select this option if you want the requester to be prompted to select roles.
	Also, make sure that the **Auto detect roles from role conditions** and **from inventory groups** options are not selected.
	Then, in the **Application Roles** list, select the role or roles that you would like to assign to this task sequence catalog item, as described in Application Roles.

Note • You can apply multiple roles to the same task sequence. The logic for each role will be applied and determined based on the criteria you specified.

Table 4-28 • Deployment > Roles Tab / Catalog Item Properties Dialog Box

Property	Description
Auto detect roles from role conditions	Select this option if you want to automatically add roles based on the conditions defined on the roles. You should also make sure that the **Allow user role selection** option is not selected. Also, do not select any roles. Roles will be detected during checkout based on the role conditions specified on the roles.
Auto detect installed apps	If this option is selected, along with the **Enable application migration and installation of additional applications** option on the **Site Management > Settings > Deployment > OS Deployment** tab, then the Choose Existing Applications to Migrate Panel will be displayed during OSD task sequence catalog item checkout. 📄 *Note • For more information, see Global vs. Catalog Item Level Settings for Migrating or Installing New Applications During OS Deployment.*
Application Roles	Existing roles are listed on the left side of this list. To add a role to the catalog item, select a role in this list and click the right arrow button. The selected role will then be displayed in the list on the right. • **Selecting all roles**—To select all roles, click the double-arrow button. • **Removing a role**—To remove a role from the catalog item, select the role name in the list on the right and click the delete icon. • **Reordering roles**—To reorder the selected roles, use the up and down arrow buttons. 📄 *Note • For information on how to create roles, see Creating Roles.*

Selecting Options on the Roles Tab

When attaching roles to task sequence catalog items to identify the applications that will be installed during an operating system deployment, the options that you select on the **Deployment > Roles** tab determine the requester's user experience during checkout.

Table 4-29 • Selecting Options on the Deployment > Roles Tab

Desired Action	Desired Checkout Panel to Display	Select roles?	Select these options	Do not select these options
Prompt the requester to select roles (groups of applications) to install on the target machine	Choose Roles Panel	Yes	Allow user role selection	Auto detect roles from role conditions Auto detect installed apps

Table 4-29 • Selecting Options on the Deployment > Roles Tab

Desired Action	Desired Checkout Panel to Display	Select roles?	Select these options	Do not select these options
Automatically add application roles based on the conditions defined on the roles	None	No	Auto detect roles from role conditions	Allow user role selection Auto detect installed apps
Prompt the requester to select which of their currently installed applications they want to install on the target machine	**Choose Existing Applications to Migrate Panel**	No	Auto detect installed apps	Auto detect roles from role conditions Allow user role selection

Collection Variables Dialog Box

📄

Note • *Displayed for System Center Configuration Manager deployment technology only.*

To add variables to a collection, open the **Collection Variables** dialog box by clicking the **Collection Variables** button on the **Deployment > ConfigMgr / SCCM 2012** tab of the **Catalog Item Properties** dialog box.

Figure 4-82: Collection Variables Dialog Box

Computer Variables Dialog Box

Note • Displayed for System Center Configuration Manager deployment technology only.

To add variables to computers, open the **Computer Variables** dialog box by clicking the **Computer Variables** button on the **Deployment > SCCM 2012** of the **Catalog Item Properties** dialog box.

Figure 4-83: Computer Variables Dialog Box

Add Package Dialog Box

On the **Add Package** dialog box, which opens when you click **Add Package** on the **Deployment > ConfigMgr, SCCM 2012** subtab of the **Catalog Item Properties** dialog box, you can select an application, package, task sequence, or virtual package on the SCCM server to add to a catalog item.

Figure 4-84: Add Package Dialog Box

The information displayed on the **Add Package** dialog box is similar for the **Applications**, **Packages**, **Task Sequences**, and **Virtual Applications** tabs.

All of the applications, packages, task sequences, or virtual applications in the connected SCCM server are listed on these tabs. To add an application, package, task sequence, or virtual application to this catalog item, select a list item on one of these tabs and then click **Add Program**. The SCCM Deployment Dialog Box will open, where you will then specify deployment settings.

The following information is displayed on the **Applications**, **Packages**, T**ask Sequence**s, and **Virtual Applications** tabs of the **Add Package** dialog box:

Property	Description
Select a site list	Select your SCCM server from this list. **Important •** *If there are no SCCM sites listed in this list, make sure that your SCCM connection settings are entered the **Site Management > Settings > Deployment** view.*
App ID / Package ID	Number that identifies that application or package in SCCM.
Manufacturer	Package or application manufacturer.
Name	Package or application name.
Version	Package or application version.

Add Program Dialog Box

You open the **Add Program** dialog box by first clicking **Add Package** on the **Deployment > ConfigMgr / SCCM 2012** tab to open the **Add Package** dialog box; selecting an application, package, or task sequence; and then clicking **Add Program**.

Adding a Program for an Application

The **Adding a Program for an Application** dialog box is opened by selecting an application on the **Add Package** dialog box and then clicking **Add Program**.

Adding a Program for a Package

The **Adding a Program for a Package** dialog box is opened by selecting a package on the **Add Package** dialog box and then clicking **Add Program**.

Adding a Program for a Task Sequence Catalog Item

You open the **Adding a Program for a Task Sequence Catalog Item** by opening the **Deployment > ConfigMgr / SCCM 2012** tab and clicking **Add Program** (after the task sequence catalog item already has an attached task sequence).

Add Software Product Dialog Box

📄

Note • *Displayed for Altiris Client Management Suite deployment technology only.*

On the **Add Software Product** dialog box, which opens when you click **Add Software Product** on the **Deployment >
Altiris** subtab of the **Catalog Item Properties** dialog box, you can select a package on the Altiris server to add to a catalog
item.

Figure 4-85: Add Software Product Dialog Box

The **Add Software Product** dialog box includes the following properties:

Table 4-30 • Add Software Product Dialog Box

Property	Description
Add Program	Click to add the selected software product to the App Portal catalog item. The Altiris Software Product Deployment Dialog Box opens.
Deployment Server	Name of Altiris server. [Read only]
Reload from Server	Click to connect to the Altiris server and refresh the list of products.

Table 4-30 • Add Software Product Dialog Box

Property	Description
Product List	List of products on the Altiris server. The following information is listed:

- Name

- Manufacturer

- Version

- Last Updated

Altiris Software Product Deployment Dialog Box

Note • *Displayed for Altiris Client Management Suite deployment technology only.*

On the **Altiris Software Product Deployment** dialog box, which opens when you click **Add Program** on the Altiris Add Software Product Dialog Box, you can specify Altiris deployment options for the software product that you are adding to this catalog item.

Figure 4-86: Altiris Software Product Deployment Dialog Box

The **Altiris Software Product Deployment** dialog box includes the following properties:

Table 4-31 • Altiris Software Product Deployment Dialog Box

Property	Description
Select deployment method	Select one of the following options: ● **Deploy to user** ● **Deploy to computer**
Show all languages	If you have multiple installation programs for different languages within a single request, select this option. 📄 *Note • If programs are specified for more than one language, the requester will select the language during the checkout process.*
Install, Uninstall, Repair	From the **Install**, **Uninstall**, and **Repair** lists, select the program name that you would like to add for each function. 📄 *Note • If you have selected the **Enable Uninstallation** and/or **Enable Repair** options on the **Deployment > Global** tab of the **Catalog Item Properties** dialog box, you are required to select a program from the **Uninstall** and/or **Repair** lists.* 📄 *Important • You are required to select a program from at least one of the **Install**, **Uninstall**, or **Repair** lists.*
Select sites to publish	[Read only] Lists the name of the Altiris server. An advertisement and collection for this software product will be created at this site.
Save	Click to save these deployment settings. The software product is now listed on the **Deployment > Altiris** subtab of the **Catalog Item Properties** dialog box. A entry appears for each of the programs (**Install**, **Uninstall**, **Repair**) that you selected.

Add Existing Altiris Policy Dialog Box

📄

Note • Displayed for Altiris Client Management Suite deployment technology only.

On the **Add Existing Policy** dialog box, which opens when you click **Add Existing Policy** on the **Deployment > Altiris** subtab of the **Catalog Item Properties** dialog box, you can select a policy on the Altiris server to add to a catalog item.

Figure 4-87: Add Existing Policy Dialog Box / Policy Tab

After you select a policy and click **Next**, the **Software Delivery Item** tab opens.

Figure 4-88: Add Existing Policy Dialog Box / Software Delivery Item Tab

SCCM Deployment Dialog Box

📄

Note • *Displayed for System Center Configuration Manager deployment technology only.*

You can add programs to deploy a catalog item to System Center Configuration Manager through App Portal. When you are creating a new task sequence catalog item using the **Catalog Item Properties** dialog box, you add programs on the **SCCM Deployment** dialog box.

📄

Note • *When creating a new catalog item using the **New Software Catalog Item Wizard**, you enter deployment settings on the ConfigMgr/SCCM 2012 Deployment Settings Panel or ConfigMgr/SCCM 2012 Package Deployment Settings Panel.*

When using the **Catalog Item Properties** dialog box to create a new catalog item, you open the **SCCM Deployment** dialog box by performing the following steps:

● **Step 1:** Open the **Deployment > SCCM 2012**, or **ConfigMgr** subtab.

● **Step 2:** Click **Add Package** to open the Add Package Dialog Box.

● **Step 3:** Select an application, package, or task sequence, and then click **Add Program**.

Figure 4-89: SCCM Deployment Dialog Box (Applications)

To open the **SCCM Deployment** dialog box for an existing catalog item, open the **Deployment > SCCM 2012** tab and click **New Deployment** (for applications) or **Add Program** (for packages).

The **SCCM Deployment** dialog box displays different options in the **SCCM Object** area, depending upon the type of **Software** catalog item you are creating:

Figure 4-90: SCCM Object ID Area

The **SCCM Deployment** dialog box includes the following properties:

Table 4-32 • SCCM Deployment Dialog Box

Property	Description
Select deployment method	(Applications only) Select one of the following options: ● **Deploy to user** ● **Deploy to computer**
Create Uninstall Collection	(Applications only) Select this option to create an uninstall collection.
Show all languages	(Packages only) Select this option if you have multiple installation programs for different languages within a single request. 📄 *Note •* *If programs are specified for more than one language, the requester will select the language during the checkout process.*
Select programs for functions	(Packages only) Select matching program name for each program function: **Install**, **Uninstall**, and **Repair**. ● If you have enabled **Uninstall** or **Repair** in the global settings, the uninstall and repair programs are required. ● You can have multiple installation programs for different languages within a single request. ● If programs are specified for more than one language, the requester will select the language during the checkout process.

Table 4-32 • SCCM Deployment Dialog Box

Property	Description
Program for OS Deployment Task Sequence	(Packages only) Select matching program name for the program function.
Select specific sites	Select the sites where this request will be available, the locations you wish to publish the catalog item to. An advertisement and collection will be created at the site(s) selected.
Make the advertisement mandatory	Determines whether the advertisement is created as a mandatory advertisement.
Mandatory over slow links?	Select this option to require that the installation is run even when a client has a slow connection. If this option is not selected, the SCCM client agent will not perform the installation if the client has a slow connection, but will perform the installation if the client is connected over a regular LAN connection.
Advertisement Priority	Specify the priority of the advertisement: **High**, **Medium**, or **Low**.
Ignore maintenance windows	Determines if the advertisement should ignore maintenance windows.
Allow system restart outside of maintenance windows	Select to allow the advertised program to restart the client even if the restart would occur outside a maintenance window.
Program rerun behavior	Specifies whether the advertised program will be rerun on the client computer if it has previously been run before the scheduled mandatory time. Select one of the following options: ● **Never rerun advertised program**—The program will not be rerun on the client if the program has previously been run on the client, even if the program originally failed or the program files have been changed. ● **Always rerun**—The program will always be rerun on the client when the advertisement is scheduled, even if the program has already been successfully run. ● **Rerun if failed previous attempt**—The program will be rerun when the advertisement is scheduled only if it failed on the previous run attempt. ● **Rerun if succeeded on previous attempt**—The program will be rerun only if it has previously run successfully on the client. *Important • This option is only enabled if **Make the advertisement mandatory** is also selected.*

Table 4-32 • SCCM Deployment Dialog Box

Property	Description
When a Distribution Point is available locally	Select one of the following options to specify how content will be downloaded from the distribution points when a distribution point is available locally: • **Run program from distribution point**—Run program directly from a distribution point. • **Download program from distribution point**—Download program from the distribution point to the client computer before attempting to run the program.
When no Distribution Point is available locally	Select one of the following options to specify how content will be downloaded from the distribution points when no distribution point is available locally: • **Do not run program**—Do not run program. • **Download program from remote distribution point**—Download the program from a remote distribution point to the client computer before attempting to run the program. • **Run program from a remote distribution point**—Run program directly from a remote distribution point.
When no protected distribution point is available, use an unprotected distribution point	Select this option to permit a client to use an unprotected distribution point if content is not immediately available on its protected distribution point. If this option is not selected, the client will not use unprotected distribution points.

Note • For more information, see Attaching a Program to Deploy a Catalog Item to System Center Configuration Manager.

AirWatch Tab

Note • Only available for AirWatch Mobile Application catalog items.

You are permitted to add multiple versions of a mobile application to the same catalog item in order to accommodate different operating systems (iOS, Android) and different (iPhone, iPad). When using the **New Catalog Item Wizard** to create the catalog item, you are restricted to adding just one iOS mobile application and one Android mobile application. However, on the **AirWatch** tab of the **Catalog Item Properties** dialog box you can add additional versions or delete existing ones.

Figure 4-91: AirWatch Tab / Catalog Item Properties Dialog Box (Mobile Application)

When adding additional versions of a mobile app, you are restricted to having a unique platform / device / Location Group ID combination. For example, a single catalog item could include the following versions of the XYZ mobile application because each one has a unique combination of platform / device / location:

- XYZ Application / Android / Chicago Location

- XYZ Application / Android / New York Location

- XYZ Application / iOS / iPad / Chicago Location

- XYZ Application / iOS / iPhone / Chicago Location

- XYZ Application / iOS / iPad / New York Location

- XYZ Application / iOS / iPhone / New York Location

You cannot add more than one version of a mobile application that has the same platform (iOS/Android), device (iPad/iPhone), and Location Group ID to the same catalog item.

Note • Android applications do not have any phone vs. tablet device distinction.

The **AirWatch** tab of the **Catalog Item Properties** dialog box includes the following properties:

Table 4-33 • AirWatch Tab / Catalog Item Properties Dialog Box

Property	Description
Add Android Application	Click to open the **Add Mobile Application** dialog box, where you are prompted to select an Android mobile application from the connected AirWatch instance.

Table 4-33 • AirWatch Tab / Catalog Item Properties Dialog Box

Property	Description
Add iOS Application	Click to open the **Add Mobile Application** dialog box, where you are prompted to select an iOS mobile application from the connected AirWatch instance.
Delete	Click to delete the selected
Send failure email? **Send success email?**	Select these options to send a notification email upon failure and/or success of deployment of this mobile application by AirWatch Server.
AirWatch Package Name	Name of package on the AirWatch instance.
Platform	Identifies the platform of the mobile application to be either **iOS** or **Android**.
AirWatch Supported Device	Identifies the supported device of the mobile application: either **iPad** or **iPhone** for iOS , or **Android** for Android .
AirWatch ID	Number identifying the application on the AirWatch server.
Location Group Id	Number identifying the Active Directory location group that was specified for this mobile application when it was added to AirWatch. Only users within the mobile application's same location group hierarchy will have access to that mobile application.

Link Desktop Catalog Tab

Note • *Only available for AirWatch mobile application catalog items.*

You can link a mobile application catalog item with its associated desktop catalog item so that when one of the linked applications is requested, the user will be informed that the other linked catalog item is also available.

- **Requesting a desktop catalog item**—If a user adds a desktop catalog item that is linked to a mobile catalog item to the cart, the user will be informed during checkout that they can optionally install the mobile catalog item onto their mobile device:

- **Requesting a mobile catalog item**—When a user clicks **Add** to add a mobile catalog item that is linked to a desktop catalog item to the cart, a message box will open asking the user whether they would like to also add the desktop catalog item to the cart.

You link a mobile application catalog item with a desktop catalog item on the **Link Desktop Catalog** tab of the mobile application's Catalog Item Properties dialog box.

Figure 4-92: Link Desktop Application / Catalog Item Properties Dialog Box (Mobile Application)

On the Link Desktop Catalog tab, use the **Search** field to locate the desktop catalog item that you want to link to, select it, and then click **Save**. Information about the linked catalog item will then be listed in the box.

To change the current mapping, perform another search.

FlexNet Manager Suite Tab

Note • *Not available when creating a group catalog item.*

On the two subtabs of the **FlexNet Manager Suite** tab of the **Catalog Item Properties** dialog box, you map the catalog item to a Flexera ID, and configure the catalog item's licensing.

● Mapping Tab

● License Reclamation Tab

● Alert Action Targets Tab

Mapping Tab

On the **FlexNet Manager Suite > Mapping** tab, you map the catalog item to a Flexera ID in FlexNet Manager Suite and specify licensing options.

- Mapping a Catalog Item to a Flexera ID

- Selecting the License Availability Scope

- Displaying Available Licenses During Checkout

- Performing an Advanced License Check During Checkout

Mapping a Catalog Item to a Flexera ID

You map a catalog item to its Flexera ID on the **FlexNet Manager Suite > Mapping** tab of the **Catalog Item Properties** dialog box.

Figure 4-93: Catalog Item Properties Dialog Box / FlexNet Manager Suite > Mapping Tab

Use the **Search** fields to locate a Flexera ID for this catalog item in the FlexNet Manager Suite database, select the appropriate item in the search results box, and then click **Save**.

When a catalog item is mapped, the **Flexera ID**—along with the **Product Name**, **Version**, **Edition**, and **Publisher**—are listed in the **FlexNet Manager Suite Mapping** area.

You follow the same procedure to map a catalog item to a Flexera ID for the first time and to change the mapping of that catalog item.

Selecting the License Availability Scope

To display a more accurate count of available licenses at the time a user requests an application from App Portal, you can use the Enterprise Group assignment data defined in FlexNet Manager Suite to determine a user's available license count.

You can specify that when determining available license count for a user, you want FlexNet Manager Suite to return the number of licenses that are available in the user's Enterprise Group rather than those available to the entire enterprise. This capability enables license reservation and consumption based on group ownership and permits the roll-up of license quantities for specific groups (cost centers, business units or locations).

Task   ***To select the license availability scope of an application:***

After the catalog item is mapped to a Flexera ID, you can specify how FlexNet Manager Suite will determine the available license count for this catalog item by making a selection from the **Select the licensing availability scope** list:

- **Global Only**—When determining available license count, FlexNet Manager Suite will return the number of licenses that are available to the entire enterprise.

- **Enterprise Groups Only**—When determining available license count, FlexNet Manager Suite will return only the number of licenses that are available to that user or computer.

- **Check Enterprise Groups and fallback to Global if not available**—When determining available license count, FlexNet Manager Suite will first check the number of licenses that are available to that user or computer; then, if no license is available, FlexNet Manager Suite will return the number of licenses that are available to the entire enterprise.

Note • In order to communicate with FlexNet Manager Suite, you need to be connected to the Flexera Service Gateway, as described in Connecting to the Flexera Service Gateway.

Displaying Available Licenses During Checkout

If you would like App Portal, during checkout, to display an icon that indicates whether there are licenses available for this product, select the **Check for license position during checkout** option. If this option is selected, one of the following will be displayed during checkout for this catalog item:

- **Licenses available**—If there are licenses available, the **License Available** icon is displayed along with the number of available licenses.

Figure 4-94: License Available Icon

- **No licenses available**—If no licenses are available, the **License Not Available** icon is displayed.

Figure 4-95: License Available Icon

Performing an Advanced License Check During Checkout

You can choose to have App Portal evaluate license entitlement by considering not only available licenses, but also second use rights, upgrade/downgrade rights, and exemption by device role rights (such as an MSDN subscription), all based upon information stored in FlexNet Manager Suite. This is referred to as an advanced license check. The following advanced license rights are evaluated:

- **Right of second use (also known as portable use)**—The right to use the software on both a desktop and a laptop with the same owner and only consume one license.

- **Upgrade rights**—The right to use the latest version of the software as soon as it becomes available.

- **Downgrade rights**—The right to use an older version of the software than the version purchased.

- **Exemption by device role rights**—The right to install software based upon a subscription role, such as an MSDN subscription.

These additional license rights are evaluated at checkout before a license is reserved. This solution helps ensure that your organization evaluates all key entitlement rights and does not mistakenly purchase more license entitlements that you actually require.

Advanced license check can be enabled globally and also on a catalog item basis:

- **Globally**—By default, advanced license check is not enabled. To enable it globally, select the **Enable Advanced License Check with FlexNet Manager Suite** option on the **Site Management > Settings >Flexera Integration** view. For more information, see Flexera Integration.

- **Per catalog item**—To control the advanced license check feature on a catalog item basis, select the **Check for advanced license during checkout** option on the **FlexNet Manager Suite > Mapping** tab of the **Catalog Item Properties** dialog box.

For more information, see Performing Advanced License Check.

License Reclamation Tab

On the **FlexNet Manager Suite > License Reclamation** tab, you configure the catalog item's licensing.

Figure 4-96: Catalog Item Properties Dialog Box / FlexNet Manager Suite > License Reclamation Tab

The **License Reclamation** tab includes the following properties:

Table 4-34 • FlexNet Manager Suite > License Reclamation Tab

Property	Description
Threshold To Detect Usage *nn* **Days of No Usage**	Determines whether the license will be submitted for reclamation automatically after the notification duration has exceeded and there is no response from the user.
Enable License Reclamation (Requires Uninstall Program)	Select to active License Reclamation. The request must be linked to an Inventory Group to enable License Reclamation. If the Inventory Groups does not include a Metering Rule, then the License reclamation will use all users who have the software installed regardless of usage.
Require manual approval for license reclamation actions	Determines whether manual approval is required for license reclamation.
Enable Email Notifications	Determines whether emails should be sent for this reclamation instance. Do not select this option if you want the un-installation to happen silently.
Notification frequency: x day(s)	Determines notification frequency.

Table 4-34 • FlexNet Manager Suite > License Reclamation Tab

Property	Description
Notification duration: x day(s)	Determines notification duration. The duration is the limit where the software will be uninstalled automatically if Auto-reclaim unanswered requests are selected.
Require explanation for keeping or removing license	Determines whether the user needs to enter an explanation on why they need to keep the software.
Send email notification to user	Determines whether the user should receive the email notification.
Send email notification to manager	Determines whether the user's manager (if specified in Active Directory) should receive the email notification.
On uninstall response	Select one of the following options: • **Review uninstall request**—When a user responds that they will allow the uninstall; this result will be stored in the license reclamation campaign for administrative review. No action will be taken to remove the software unless manually done by an administrator. • **Automatically submit uninstall request**—When a user responds that they will allow the uninstall, App Portal will create an uninstall request for that user's computer.
Auto-reclaim unanswered requests	Determines whether the software is submitted for un-installation automatically after the notification duration has exceeded and there is no response from the user.
Includes requests without an associated user	Determines if the license should be auto-reclaimed even if there is no user associated with the machine.
Enable Reclamation Archiving	Archiving allows a user to be considered a target for reclamation after a previous reclamation has completed. If a user responds with a "keep" response they will receive a notification again after the specified period of days elapses and they have still not used the software. If the user responds with an "uninstall" and later installs the program again and does not use it, they will receive a notification again after the specified period of days elapses and they have still not used the software.
Archive responses after x days	Determines the period of time that must elapse before reconsidering a previously completed reclamation action for reevaluation.

Alert Action Targets Tab

On the **FlexNet Manager Suite > Alert Action Targets** tab, you can specify the applications to target for the following types of Action Alert catalog items:

- **Proof of purchase Alert Action catalog items**—To generate a proof of purchase alert for an application, open the existing **Proof of purchase** Alert Action catalog item in the Catalog Item Properties dialog box, and then add that application to the list on the **FlexNet Manager Suite > Alert Action Targets** tab. Multiple applications can be targeted by adding more than one application to the list. For more information, see Triggering a Proof of Purchase Alert.

- **Custom Alert Action catalog items**— When you create a new custom Alert Action catalog item or want to convert an existing General catalog item to an Alert Action catalog item, you need to add at least one application to the list on the catalog item's **FlexNet Manager Suite > Alert Action Targets** tab.   For more information, see Creating a New Custom Alert Action Catalog Item and Creating a New Custom Alert Action Catalog Item.

Figure 4-97: Catalog Item Properties Dialog Box / FlexNet Manager Suite > Alert Action Targets Tab

The **Alert Action Targets** tab includes the following properties:

Table 4-35 • FlexNet Manager Suite > Alert Action Targets Tab

Property	Description
Filters	Use the filter fields in the columns to search the FlexNet Manager Suite database for the application that you want to target.
Add	Click to add selected applications to the list on the right.
"Selected" Applications List	Lists the applications that are targeted for this Proof-of-Purchase or Custom alert action catalog item.

Catalog Items Tab

📄

Note • *Only available when creating a group catalog item.*

On the **Catalog Items** tab, which appears when you are creating a group catalog item, you specify the catalog items that you want to include in the bundle.

Initially, catalog items are listed in the **Available Catalog Items to Group** list, and no catalog items are listed in the **Current Grouped Catalog Items** list.

Figure 4-98: Catalog Item Properties Dialog Box / Catalog Items Tab

In the **Available Items to Group** list, select the catalog items that you want to add to the group and then click **Group Programs**. The selected catalog items are now listed in the **Current Grouped Catalog Items** list.

Visibility Tab

Visibility controls whether a catalog item is visible for a user based on conditions. For each condition you can choose **Include** or **Exclude**. If a user matches an include condition, the item is visible. If the user matches an exclude condition, the item is not visible.

Exclude conditions are evaluated first. If a user matches an exclude condition, no further processing occurs and the item is not visible. If there are both exclude and include conditions specified, the user must not match exclude conditions and must match include conditions for the item to be visible.

Important • The creation of a condition based upon Active Directory device groups is not supported.

By default, all catalog items are visible when the **Is Enabled** Global option is specified. Use the **Visibility** tab of the **Catalog Item Properties** dialog box to further customize the visibility of items.

The **Visibility** tab includes two subtabs:

- Global Subtab

- Alternate Message Subtab

Global Subtab

The **Visibility > Global** subtab lists visibility conditions.

Figure 4-99: Catalog Item Properties Dialog Box / Visibility > Global Tab

On the **Global** tab, you can create conditions based on Active Directory Groups or OUs, Active Directory properties, and collections.

Important • *The creation of a condition based upon Active Directory device groups is not supported.*

After you use the Add Condition Dialog Box to add a condition to any of the three subtabs (**Group and OU**, **AD Property**, or **Collections**), that condition is listed on the **Visibility** tab.

After the condition is added, specify the **Enforcement** option you want to take effect: **Include** or **Exclude**.

Alternate Message Subtab

Instead of hiding a catalog item, you can specify a message to be displayed instead. You enter this message on the **Visibility > Alternate Message** tab.

Figure 4-100: Catalog Item Properties Dialog Box / Visibility > Alternate Message Tab

Add Condition Dialog Box

If you click **Add Condition** on the **Group and OU**, **AD Property**, or **Collections** subtabs of the **License Reclamation Campaign Conditions** dialog box or from the **Visibility** tab of the **Catalog Item Properties** dialog box, the **Add Condition** dialog box opens.

Figure 4-101: Add Condition Dialog Box

Search for the group or OU you want to add and place a check mark next to the item found.

Click the **Select** button to add the condition.

After you add a condition to any of the three subtabs (**Group and OU**, **AD Property**, or **Collections**), that condition is listed on one of the subtabs of the Standard Condition tab. After the condition is added, specify the **Enforcement** option you want to take effect: **Include** or **Exclude**.

Approval Tab

Note • *Not available when creating a group catalog item.*

Approval controls whether a catalog item requires approval (processes workflow) for a user based on conditions. For each condition, you can choose **Include** or **Exclude**.

- If the user matches an include condition, the item requires approval.

- If the user matches an exclude condition, the item does not require approval.

Exclude conditions are evaluated first. If a user matches an exclude condition, no further processing occurs and the item does not require approval. If there are both exclude and include conditions specified, the user must not match exclude conditions and must match include conditions for the item to require approval.

On the **Approval** tab, you specify the settings that determine who or what computer must apply to approval rules.

Figure 4-102: Catalog Item Properties Dialog Box / Approval Tab

The **Approval** tab includes the following properties:

Table 4-36 • Catalog Item Properties Dialog Box / Approval Tab

Property	Description
Require approval when assignment is present	Select to force a request for this catalog item to go through an approval process.
Disable approval for leased installations	Select to disable requests for this catalog item from using the approval process.
Disable questions when approval is not required	Select to disable the question template when approval is not required.
Group and OU, AD Property, and Collections tabs	Use to create conditions—based on Active Directory Groups or OUs, Active Directory properties, and collections—that will force requests for the catalog item to go through an approval process. See Add Condition Dialog Box.
Enforcement	After the condition is added, specify the **Enforcement** option you want to take effect: **Include** or **Exclude**.

Approval Process Tab

The properties on the **Approval Process** tab control how the request will be approved.

Workflow Subtab

The **Workflow** subtab shows the current approval workflows that are applied to the catalog item.

Figure 4-103: Catalog Item Properties Dialog Box / Approval Process > Workflow Tab

Click **Add Workflow** or **Remove Workflow** to add or remove approval workflows from this catalog item.

● If more than one workflow is specified, the conditions are evaluated to determine which workflow to use.

● If no workflow is defined or there are multiple workflows defined for which no condition could be matched, then the default workflow that is specified under the **Site Settings** is used.

Simulate Subtab

To view a simulation of the approval process for this catalog item, open the **Simulate** subtab.

Figure 4-104: Catalog Item Properties Dialog Box / Approval Process > Simulate Tab

In the **Enter a user ID in Domain\name format or a computer name** field, enter a domain and user name and then click **Show approval process**. The levels in the selected approval workflow are listed.

Custom Variables Tab

On the **Custom Variables** tab of the Catalog Item Properties dialog box, you can add custom variables to associate with a request.

A catalog item's associated custom variables will be available for use in external web actions or script commands. For example, you may want to use the same action for Standard, Professional, Enterprise editions of a catalog item and you could use a custom variable to differentiate the messages.

Figure 4-105: Custom Variables Tab of the Catalog Item Properties Dialog Box

---

*Note • To make a custom variable globally available, you can add it to the **Catalog Management > Catalog > Custom Variables** view. Variables defined there will be available on the **Custom Variables** tab of all future catalog items. See Custom Variables.*

On the **Custom Variables** tab, you can add new variables and edit existing variables**.**

Adding a New Variable

To add a new variable, click **Add New Variable**. A pop-up dialog opens where you can enter a **Variable Name**, **Value,** and **Description**. Click **Add Variable** to save the variable.

Figure 4-106: Add New Variable

Editing an Existing Variable

To edit a variable, lick **Edit** next to a variable name. An area drops down below the variable where you can edit and update the variable. Click **Update** to save your edits.

Figure 4-107: Variable Editing Area

Cloud Apps Tab

App Portal provides out-of-the-box support for three cloud applications—Box, Salesforce, and Microsoft Office 365—and automatically configures these catalog items with custom variables which are required for the account request to be completed. These variables can be viewed on the **Cloud Apps** tab of the **Catalog Item Properties** dialog box for Cloud catalog items.

Figure 4-108: Custom Variables on the Cloud Apps Tab of the Catalog Item Properties Dialog Box

On the **Cloud Apps** tab of a Cloud catalog item, you can view and edit existing variables, and create new variables.

Editing an Existing Variable

To edit a variable, lick **Edit** next to a variable name. An area drops down below the variable where you can edit and update the variable. Click **Update** to save your edits.

Figure 4-109: Variable Editing Area

Adding a New Variable

To add a new variable, click **Add New Variable**. A pop-up dialog opens where you can enter a **Variable Name**, **Value,** and **Description**. Click **Add Variable** to save the variable.

Figure 4-110: Add New Variable

Security Groups Tab

Note • *Not available when creating a group catalog item.*

By specifying security groups on the **Security Groups** tab, App Portal will add the user, machine or both to the specified security groups. The Service account will require modify permissions to the groups listed. The user will only be added to the group(s) if the installation process completes successfully.

In the event the program is uninstalled using SCCM App Portal, the user will be removed from the listed security groups.

Figure 4-111: Catalog Item Properties Dialog Box / Security Groups Tab

Actions Tab

Note • *Not available when creating a group catalog item.*

After you create actions, you can use the **Actions** tab to add them to the events during the request lifecycle.

Figure 4-112: Catalog Item Properties Dialog Box / Actions Tab

The **Actions** tab includes the following properties:

Table 4-37 • Catalog Item Properties Dialog Box / Actions Tab

Properties	Description
Current Events and Actions	Select an event that will trigger the action. The action will execute when the event completes.
Select a service	Select an action.
	If you select **Command Execution** from the **Select a service** list, a command previously created under **Site Management > Commands and Actions > New Command** is used. Those commands specified as **Execute from Server** are available. When the request stage is processed, the command will be invoked and passed the variables identified in the Command.
	If connected to Workflow Manager, you can select **Workflow Manager Action** from this list. See Connecting a Catalog Item to a Workflow Manager Workflow Request.
	If integrated with an ITSM system, you can select one of the ITSM system's services from the list. For more information, see Setting ITSM Actions on Catalog Items.
Select a method or command	Select a listed method or command.

Table 4-37 • Catalog Item Properties Dialog Box / Actions Tab

Properties	Description
Add a status	Select a status to identify what the catalog item's status will be when this action is executed.
Save	Click to add the action to the event tree on the left.

Note • For troubleshooting purposes, the log file for reference of actions is `WebServiceAction.log`.

Notifications Tab

Note • Not available when creating a group catalog item.

On the **Notifications** tab, you can specify custom notifications to replace the default notifications for different actions.

Figure 4-113: Catalog Item Properties Dialog Box / Notifications Tab

Select a custom notification message from the list provided and enter your custom message. The standard variables apply for custom messages.

For more information, see Editing Notification Email Templates and Messages.

Permissions Tab

You can assign additional permissions on a catalog item on the **Permissions** tab.

Figure 4-114: Catalog Item Properties Dialog Box / Permissions Tab

Available permissions are:

- Read

- Read / Write

- Read / Write / Delete

To add a user or group to the list, select **Add User/Group**.

Figure 4-115: Add Permission Dialog Box

Use the search box to locate the user or group that you want to add, select the permission level from the Assign rights list, and click **Assign Rights**.

Administration Node

The **Catalog Management > Administration** node consists of the following subviews:

- Core Applications

- Alternate Targets

- Alert Action Catalog Items

- Alert Action

- Catalog Templates

- Class Types

- Custom Variables

Core Applications

Every enterprise has a set of core applications that are included on all corporate images that are created, such as Microsoft Office, Chrome, etc. Because those applications are included in all OS images, there is no reason to ask an individual to select them during check out of a task sequence catalog item.

The **Core Applications** view, which is displayed by selecting **Catalog Management > Administration > Core Applications**, lists catalog items that have been designated as "core applications", meaning that they are not available for migration during task sequence deployment.

To add a catalog item to this list, select the **Core application** option on the **General > Global** tab of the catalog item's **Catalog Item Properties** dialog box.

Figure 4-116: Core Applications View

Alternate Targets

Sometimes when a user selects a catalog item and goes to check it out, they are prevented from doing so for various reasons. For example:

- **Machine is not found**—If the user's machine is not found by App Portal, they will be prevented from checking out.

- **Machine not on network**—If a user's machine is not on the network, it means that the standard method for installing software using System Center Configuration Manager or Altiris cannot be used.

- **Version user wants is not in the catalog**—If a user wants a more recent version of an application than the version that is in the catalog, they would not want to check out the older version; instead they would want to indicate that they would like the IT department to purchase the latest version.

To enable you to accommodate all of these types of situations using the current checkout structure available on the **Browse Catalog** tab (the App Portal storefront), you can create alternate targets that would be available for selection whenever a user attempts to check out a **Software** catalog item, as shown on the **Choose Target** panel of the Checkout Wizard.

Figure 4-117: Choose Target Panel of Checkout Wizard Displaying Alternate Targets

*Note • Alternate targets are only displayed for **Software** catalog items, not **General** catalog items.*

If a user selects an alternate target and then clicks **Next**, the original catalog item is replaced by the new alternate target, and checkout can proceed.

You create alternate targets on the **Alternate Targets** view.

Figure 4-118: Administration > Alternate Targets View

The **Alternate Targets** view includes the following properties:

Table 4-38 • Alternate Targets View Properties

Property	Description
Add New Alternate Target	Click to open the Create New Alternate Target Dialog Box.
ID	Number identifying the alternate target.
Alternate Target Text	Lists the name of the alternate target, which is the text that will be displayed on the **Choose Target** panel of the Checkout Wizard.
General Catalog Item	Lists the general catalog item that is associated with this alternate target.

Note • *If a user selects one of the alternate targets during checkout, the general catalog item associated with the selected alternate target will be checked out rather than the software catalog item that was originally selected.*

Create New Alternate Target Dialog Box

When you click **Add New Alternate Target** on the **Alternate Target** view, the **Create New Alternate Target** dialog box opens.

Figure 4-119: Create New Alternate Target Dialog Box

The Create New Alternate Target dialog box includes the following properties:

Table 4-39 • Create New Alternate Target Dialog Box

Property	Description
Alternate Target Text	Enter the name of this new alternate target, which is the text that will be displayed on the **Choose Target** panel of the Checkout Wizard.
General Catalog Item	Select the general catalog item that you would like to associate with this alternate target.

Alert Action Catalog Items

To instruct App Portal to generate alerts, you create and modify Alert Action catalog items, which are a specialized type of catalog item that uses FlexNet Manager Suite application recognition and licensing data to identify installed application/device combinations that need attention, such as unused applications, unlicensed applications, or applications targeted for another reason. App Portal then sends out alerts to the identified device owners to prompt them to take action to resolve the issues.

You create and modify Alert Action catalog items on the **Catalog Management > Catalog > Alert Action Catalog Items** view.

Figure 4-120: Alert Action Catalog Items View

To create a new Alert Action catalog item, open the **Alert Action Catalog Items** view and click **Add New Alert Action Catalog Item** to open the **New Alert Action Catalog Item Wizard**.

While Alert Action catalog items share the same **Catalog Item Properties** dialog box, they are not the same as standard App Portal catalog items:

● **Not listed on Browse Catalog tab**—Alert Action catalog items are not listed on the **Browse Catalog** tab.

● **Do not need to assign a category**—Because Alert Action catalog items are not listed on the **Browse Catalog** tab, you do not need to assign them to a category.

● **Can only be created on the Alert Action Catalog Items view**—You can only create new Alert Action catalog items on the **Catalog Management > Catalog > Alert Action Catalog Items** view.

- **Can be viewed and edited in two locations**—You can view and edit Alert Action catalog items in two locations in the App Portal interface: both on the **Alert Action Catalog Items** view and also on the **Catalog Management > Current Catalog Items > View All Items** view.

The **Alert Action Catalog Items** view includes the following properties:

Table 4-40 • Alert Action Catalog Items View

Properties	Description
ID	Number that uniquely identifies the Alert Action catalog item.
Alert Action	Title used to identify the Alert Action that is associated with this **Alert Action** catalog item.
Mapped General Catalog Name	Title used to identify this Alert Action catalog item.
Action Type	Type of the Alert Action that is associated with this Alert Action catalog item: **License Reclamation - Keep**—Predefined, system action type that is associated with the predefined, system Alert Action catalog item named **Keep**. The **Keep** Alert Action catalog item is associated with the automatic Unused Software alert, and gives users the choice to keep the unused software application. **License Reclamation - Uninstall**—Predefined, system action type that is associated with the predefined, system Alert Action catalog item named **Uninstall**. The **Uninstall** Alert Action catalog item is associated with the automatic Unused Software alert, and gives users the choice to uninstall the software application. **Alert Action**—Action type of the associated Alert Action that is used for all user-defined Alert Action catalog items. *Tip • All Alert Actions that you create will have the Action Type of Alert Action.*

Alert Action

To instruct App Portal to generate alerts, you create, and modify, *alert action catalog items*, which are a specialized type of catalog item that uses FlexNet Manager Suite application recognition and licensing data to identify installed application/device combinations that need attention, such as unused applications, unlicensed applications, or applications targeted for another reason. App Portal then sends out alerts to the identified device owners to prompt them to take action to resolve the issues.

Note • For more information on alert action catalog items, see Alert Action Catalog Items.

On the **Alert Action** view, you can convert a **General** catalog item to an **Alert Action** catalog item.

First you create a general catalog item and assign it an application to target on the **FlexNet Manager Suite > Alert Action Targets** tab of the Catalog Item Properties dialog box.

Then, to convert that general catalog item to an alert action catalog item, first open the **Alert Action** view:

Figure 4-121: Alert Action View

Next, double-click the alert action that you want to add to the general catalog item to open the **Alert Action Properties** dialog box.

Figure 4-122: Alert Action Properties Dialog Box

Then, select a general catalog item from the **General Catalog** list and click **Save**. That general catalog item would then be listed on the **Alert Action Catalog Items** view.

Catalog Templates

The **Catalog Templates** view lists the existing catalog items that have templates defined. Use this view to easily locate templates to change their settings.

Figure 4-123: Catalog Templates View

Class Types

Class types are a form of filtering catalog requests. Catalog items can be assigned to classes, and you use classes as a filter mechanism on the **My Requests** tab.

Table 4-41 • Class Types View

Create, Edit, and Delete Class Types	Assign Catalog Items to Classes	Filter Catalog Requests Using the Class Filter

Custom Variables

A catalog item's associated custom variables will be available for use in external web actions or script commands. For example, you may want to use the same action for Standard, Professional, Enterprise editions of a catalog item and you could use a custom variable to differentiate the messages.

You can add custom variables directly to a catalog item on the **Custom Variables** tab of the **Catalog Item Properties** dialog box, However, to make a custom variable globally available, you can add it to the **Catalog Management > Catalog > Custom Variables** view. Variables defined here will be available on the **Custom Variables** tab of all future catalog items.

Figure 4-124: Catalog Management > Catalog > Custom Variables View

*Note • This feature is not applicable to Cloud catalog items. There is no **Custom Variables** tab on the Catalog Item Properties dialog box for a Cloud catalog item, and variables defined on the **Catalog Management > Catalog > Custom Variables** view are not available to Cloud catalog items. See Defining Custom Variables for Cloud Catalog Items.*

On the **Catalog Management > Catalog > Custom Variables** view, you can add new variables and edit existing variables.

● Adding a New Variable

● Editing an Existing Variable

Adding a New Variable

To add a new variable, click **Add New Variable**. A pop-up dialog opens where you can enter a **Variable Name**, **Value,** and **Description**. Click **Add Variable** to save the variable.

Figure 4-125: Add New Variable

Editing an Existing Variable

To edit a variable, lick **Edit** next to a variable name. An area drops down below the variable where you can edit and update the variable. Click **Update** to save your edits.

Figure 4-126: Variable Editing Area

Expressions Node

Expressions control form validation. By linking expressions to form fields, you can assure that data entered into forms is in a consistent format and contains valid information.

By default, App Portal includes the following expressions, which are listed on the **Expressions View**:

Figure 4-127: Default Expressions on the Expressions View

Expressions are supported for the JavaScript language. For more information about JavaScript regular expressions, visit:

http://www.regular-expressions.info/javascript.html

Expressions are defined and listed on the **Expressions** subview of the **Admin > Site Management** view.

- Expressions View
- Expression Properties Dialog Box

Expressions View

You create and edit expressions on the **Expressions View**, which is opened by selecting **Expressions** under **Site Management** on the **Admin** tab.

Figure 4-128: Expressions View

The **Expressions View** includes the following properties:

Table 4-42 • Expressions View

Property	Description
Name	Lists the name of the expression.
Expression	Lists the expression that will perform the form validation.
Sample Format	Lists the format that the expression validates. This value will be displayed under the form field requiring validation.

Expression Properties Dialog Box

To add a new expression, click **Add New Expression** on the **Expressions View** to open the **Expression Properties** dialog box.

Figure 4-129: Expression Properties Dialog Box

The **Expression Properties** dialog box includes the following properties:

Table 4-43 • Add New Expression Dialog Box

Property	Description
Name	Enter a descriptive name for the expression.

Table 4-43 • Add New Expression Dialog Box

Property	Description
Expression	Enter the expression that will perform the form validation. Expressions are supported for the JavaScript language. For more information about JavaScript regular expressions, visit: http://www.regular-expressions.info/javascript.html
Sample Format	Enter the format that the expression validates. This value will be displayed under the form field requiring validation to inform the user of the correct format to enter.

Workflows Node

Approval workflows define how a request should be routed for review. Workflows consist of workflow steps. Each step is a group or user that reviews the request. Approval workflows can be dynamic or static, and can have conditions applied to them.

Approval workflows are defined and listed on the **Workflows View**, which is opened by selecting **Workflows** under **Site Management** on the **Admin** tab.

Figure 4-130: Workflows View

Dynamic vs. Static Workflow Steps

Each workflow step (also referred to as a level) can be either dynamic or static:

- **Dynamic** steps are evaluated based on user and computer conditions. For example, if the workflow step is defined as **Manager**, the end user's manager will be required to approve the request.

- **Static** steps are the same regardless of who requests it or where it goes. For example, if the workflow step is assigned to a specific user, that same user will be required to approve all requests for this catalog item, no matter which end user requests it.

Using Conditions

Workflows and workflow steps can have conditions applied to them. Conditions determine whether the workflow and / or workflow step should be applied to the given situation.

- **Single workflow applied to catalog item**—When you assign a single workflow to a catalog item, the conditions of the *workflow* are not evaluated; only the *workflow step* conditions are evaluated.

- **Multiple workflows applied to catalog item**—When you apply more than one workflow to a catalog item, the conditions of the workflow as well as the steps within that workflow are evaluated.

Conditions can be based on user attributes including group and OU membership, AD property value, deployment system collection membership for both users and computers, and catalog item properties such as cost and inventory availability.

Creating and Editing Workflows

You create and edit workflows on the Workflow Properties Dialog Box, which is opened from the **Workflows** view by clicking **New Workflow** or by double-clicking on an existing workflow.

Workflow Properties Dialog Box

On the **Workflow Properties** dialog box, which is opened by clicking **New Workflow** on the **Workflows** view, you specify the properties of an approval workflow.

Figure 4-131: General Tab of Workflow Properties Dialog Box

To create a workflow, enter the properties on the following tabs:

- General Tab

- Workflow Steps Tab

- Conditions Tab

- Applies To Tab

- Simulate Tab

You can also have a workflow step execute a custom action on the Workflow Step Properties Dialog Box, as described in Configuring a Workflow Step to Execute a Custom Action.

General Tab

On the **General** tab of the **Workflow Properties** dialog box, you specify a workflow name and description and identify the process type.

Figure 4-132: Workflow Properties Dialog Box / General Tab

The **General** tab of the **Workflow Properties** dialog box includes the following properties:

Table 4-44 • Workflow Properties Dialog Box / General Tab

Property	Description
Workflow Name	Friendly name of the workflow (e.g. Finance Workflow, Engineering Application workflow, Expensive Software workflow).
Workflow Description	Provide details about the workflow and its use.

Table 4-44 • Workflow Properties Dialog Box / General Tab

Property	Description
Process Type	Select one of the following: • **Linear**—The approval process functions in a linear fashion. Each approver must approve the request in order as defined in each workflow step. • **Pool**—Anyone in any workflow step can approve the request. It takes only one approver to approve the request. All approvers will be notified of the request. • **Pool within Group**—This option will allow anyone within a workflow to approve the request before it is forwarded to the next workflow step.
Allow requester to define workflow	Enables the requester to change who the members of the workflow step are.

Workflow Steps Tab

Workflow steps of an approval workflow are defined and edited on the **Workflow Steps** tab of the **Workflow Properties** dialog box.

Figure 4-133: Workflow Properties Dialog Box / Workflow Steps Tab

Note the following regarding workflow steps:

• Workflow steps are executed from top to bottom.

• Each step can be configured with conditions to determine whether the step will be used.

• Steps can contain direct members, static approval groups, and dynamic approval groups.

- Steps can also execute custom actions when that step is processed.

Add New Level Dialog Box

Existing workflow steps are listed on the **Workflow Steps** tab. To add a new workflow step, click **Add New Level** to open the **Add New Level** dialog box.

Figure 4-134: Adding a New Level on the Workflow Steps Tab

On the **Add New Level** dialog box, you are prompted to select one of the following groups:

Table 4-45 • Groups Listed on the Add New Level Dialog Box

Group	Description
User Approval Group (Static)	Uses the approvers listed in the specified User Approval Group. Approvers within this type of group are static, they do not change based on user conditions.
Property Approval Group (Static)	Uses the approvers listed in the specified Property Approval Group. Approvers within this type of group are static, they do not change based on user conditions.
OU Approval Group (Static)	Uses the approvers listed in the specified OU Approval Group. Approvers within this type of group are static, they do not change based on user conditions.
Collection Approval Group (Static)	Uses the approvers listed in the specified Collection Approval Group. Approvers within this type of group are static, they do not change based on user / computer conditions.

Table 4-45 • Groups Listed on the Add New Level Dialog Box

Group	Description
Dynamic Approval Groups 	Dynamic approval groups display properties, not actual groups. When you create a dynamic approval group for at least one property (department, OU, collection, etc.) that property is exposed here. ● **Manager**—Uses the Manager attribute from Active Directory. ● **Computer - Managed By**—Uses the Managed By attributes of the computer object in Active Directory. ● **<Property Defined Group>**—Uses the approvers specified for the property defined. Example, you create a property based approval group for the IT Department. You specify the group to use the department attribute and the values include IT Department, Info Tech, and Information Technology values from the department attribute in Active Directory. This action exposes the "Department" attribute under the Dynamic Approval Group. Adding the Department as a workflow step will cause the workflow to look at the requesting users department, search for a value that matches IT Department, Info Tech, or Information Technology and use the corresponding approvers identified for that group. 📄 *Note • In order to effectively use dynamic approval groups, you should have approval groups created for every value of the property you choose to use.*

📄

*Note • To create a new approval group, select **Approval Groups** under **Site Management**.*

After you select a group on the **Add New Level** dialog box and click **Add Selected Group**, the new workflow step is listed on the **Workflow Steps** tab. The workflow steps in the following image are read as "First use the user's Active Directory Manager as the first level of approval, and then send the request to the Directors user approval group".

Figure 4-135: Workflow Steps Tab

Workflow Step Properties Dialog Box

Each workflow step can have properties defined. Double click the workflow step to open the **Workflow Step Properties** dialog box.

Figure 4-136: Options Tab of Workflow Step Properties Dialog Box

Options Tab

The **Options** tab of the **Workflow Step Properties** dialog box includes the following properties:

Table 4-46 • Workflow Step Properties

Property	Description
Approver Type	Select the approver type as either **Reviewer** or **Purchaser**
Set Status	Select a custom status for this workflow step. Workflow status is created and managed under Settings > Workflow Status. Setting a status other than Default Status will set the request with the identified status when that workflow step is in progress.
Set Action	Software installations are typically triggered and allowed for installation after all workflow steps have occurred. If you wish to have this action occur earlier in the workflow process, identify the step in which you want the software install action to occur.
Question template	Select a question template to link to the specified workflow step. When a question template is linked to a workflow step the approvers at that step will be presented with those questions. If there are required questions within the question template the request cannot move to the next workflow step until all required questions have been answered.
Allow Approval Level User Edit	Select this option if you wish to allow this specific approval step to be identified by the requester. With this option enabled the requester will be able to change the users within this step.
Force Approval Level User Edit	Select this option if you wish to require that this specific approval step must be identified by the requester.

Conditions Tab

The **Conditions** tab of the **Workflow Step Properties** dialog box lists any conditions that are applied to the workflow step.

Figure 4-137: Conditions Tab of New Level Dialog Box

The conditions that you apply to a workflow step determine when the step should apply.

- Conditions can be defined using **Group and OU** membership, **AD Property** value, **Collection** membership, answers to **Questions**, or based on the license availability and cost of a catalog item (on the **Catalog Item** subtab).

- Conditions specified here can be specified to enforced as either **Include** or **Exclude** by making a selection in the **Enforcement** column.

For more information on creating conditions, see Add Condition Dialog Box.

External Actions Tab

On the **External Actions** tab of the **Workflow Step Properties** dialog box, you can configure a workflow step to execute a custom action, as described in Configuring a Workflow Step to Execute a Custom Action.

Figure 4-138: External Actions Tab of Workflow Step Properties Dialog Box

To configure a workflow step to execute a custom action, first create a script, web service, or request command, as described in the following three topics:

- Script Commands

- Web Service Commands

- Request Commands

Then open the **External Actions** tab, and from the **Select a service** list and the **Select a method or command** lists, select the appropriate service and command, and then click **Save**.

Conditions Tab

The **Conditions** tab of the **Workflow Properties** dialog box lists the conditions that apply to this approval workflow. Conditions can be based on user attributes displayed on the following tabs:

- **Group and OU**—User's Group and OU membership.

- **AD Property**—Active Directory property value.

- **Collections**—Deployment system collection membership for both users and computers.

- **Question Condition**—Answer that a user gives to a question when submitting the request.

- **Catalog Item**—Catalog item properties, such as cost and inventory availability.

Figure 4-139: Conditions Tab of Workflow Properties Dialog Box

The conditions that you apply to a workflow step determine when the step should apply:

- Conditions specified here are limited to **Include**, meaning you define conditions when you want the item to apply.

- Adding a **Question Condition** enables you to base the condition on an answer that an end user gives when submitting the request.

- An additional condition, **Catalog Item**, offers the ability to include a step based on the license availability and cost of a catalog item.

Both workflows and workflow steps can have conditions applied to them. Conditions determine whether the workflow and / or workflow step should be applied to the given situation:

- **Single workflow applied to catalog item**—When you assign a single workflow to a catalog item, the conditions of the *workflow* are not evaluated; only the *workflow step* conditions are evaluated.

- **Multiple workflows applied to catalog item**—When you apply more than one workflow to a catalog item, the conditions of the workflow as well as the steps within that workflow are evaluated.

Note • For more information on creating conditions, see Creating a New Approval Workflow and Add Condition Dialog Box.

Applies To Tab

The **Applies To** tab of the **Workflow Properties** dialog box identifies the catalog items that the workflow applies to.

Figure 4-140: Applies To Tab of Workflow Properties Dialog Box

If more than one workflow is applied to a single catalog item, the conditions on the workflow will be evaluated to determine which one to use. If more than one workflow applies to a given catalog item, the first workflow identified will be used.

Tip • Be cautious not to create conditions that overlap.

Simulate Tab

On the **Simulate** tab, you enter a user ID or a computer name so that you can simulate the approval process for that user or computer.

Figure 4-141: Simulate Tab of Workflow Properties Dialog Box

Enter the user ID or computer name and click **Show approval process**.

Approval Groups Node

Approval groups are used to group users or groups together to identify a group of approvers. Approval groups are then linked to catalog items indicating that the catalog item should go through the workflow process.

Figure 4-142: Approval Groups > User Groups View

Existing approval groups are listed when you select the **Families**, **User Group**, **Property Groups**, **OU Groups**, or **Collection Groups** subnodes of the **Approval Groups** node.

There should also be a **Default Workflow** identified and configured on the **General** tab of the **Site Management > Settings > Web Site** view. There are two settings for default workflows:

- General requests

- Procurement requests

Both can be set with the same workflow or different ones. This is the "catch all" in the event approval is specified and no approvers are defined or you are using a dynamic approval process and the approvers could not be determined (such as you specified manager approval and the user does not have a manager defined.)

Approval Group Properties Dialog Box

When you create a new approval group by selecting the **Approval Groups > New Group** node under **Site Management**, or when you edit an existing approval group, the **Approval Group Properties** dialog box opens, which consists of three tabs:

- Workflow Type Tab

- Workflow Properties Tab

- Workflow Members Tab

Workflow Type Tab

On the **Workflow Type** tab, you specify a group name, group type, and workflow family.

Figure 4-143: Approval Group Properties Dialog Box / Workflow Type Tab

The **Workflow Type** tab includes the following properties:

Table 4-47 • Approval Group Properties Dialog Box / Workflow Type Tab

Property	Description
Group Name	Enter a name to identify this group.

Table 4-47 • Approval Group Properties Dialog Box / Workflow Type Tab

Property	Description
Group type	Select one of the following group types: • **User group**—Users organized in a specific order. You apply user groups directly to a workflow step. User groups are used when the approvers do not change. • **Active Directory Property Group**—These groups allow you to relate users to AD properties like departments and offices. Create these groups when you want to route requests based on these attributes, such as marketing approvers or Chicago office approvers. • **Organizational Unit**—These groups allow you to relate users to AD OUs. Create these groups when you want to route requests based on user or computer location within the AD OU hierarchy. • **User Collection**—Enables you to relate users to collections on your deployment system. Create these groups when you want to route requests based on user collection membership within your deployment system. • **Computer Collection**—Enables you to relate users to collections on your deployment system. Create these groups when you want to route requests based on computer collection membership within your deployment system.
Workflow family	Select an approval workflow family from the list. Approval workflow families are created and managed on the **Approval Groups > Families** view under **Site Management**.

Workflow Properties Tab

On the **Workflow Properties** tab, you group the properties for the group type selected.

Figure 4-144: Approval Group Properties Dialog Box / Workflow Properties Tab

📄

*Note • The **Workflow Properties** tab is not displayed if you are creating a approval group with a **group type** of **User group**.*

The **Workflow Properties** tab includes the following properties:

Table 4-48 • Approval Group Properties Dialog Box / Workflow Properties Tab

Tab	Description
Search box	Use to search for active directory properties. 📄 *Note • Only displayed when **Group type** of **Active Directory Property Group** is selected.*
Available	This box lists all available properties. To group the properties, follow the instructions to move the properties from the **Available** box to the **Current** box.
Current	Selected properties are listed in this box.
Apply to user or computer objects?	Select one of the following options: ● **Apply process to user objects in specified OUs** ● **Apply process to computer objects in OUs** 📄 *Note • Only displayed when **Group type** of **Organizational Unit** is selected.*
Include child OUs?	Select one of the following options: ● **Apply process to specified OUs and child OUs** ● **Apply process only to the specified OUs** 📄 *Note • Only displayed when **Group type** of **Organizational Unit** is selected.*

Workflow Members Tab

On this tab, you specify the people that you want to receive the request as part of a workflow step.

Figure 4-145: Approval Group Properties Dialog Box / Workflow Members Tab

The **Workflow Members** tab includes the following options:

Table 4-49 • Approval Group Properties Dialog Box / Workflow Members Tab

Property	Description
Search fields	Use to search for users or groups.
Search results	This box lists users and groups that match the search criteria. To select a user or group to receive the request as part of a workflow step, select a user or group and click the arrow to move it to the **Selected** list.
Current	Selected users or groups are listed in this box.

Workflow Status Node

Workflow steps allow the customization of the status regarding the workflow process. You customize status on the **Site Management > Workflow Status** view.

Figure 4-146: Workflow Status

You can create your own workflow status to convey the progress, state, or otherwise identify what is happening at the particular workflow step.

Create New Status Dialog Box

To add a new status click **Add Status**. The **Create New Status** dialog box opens.

Figure 4-147: Create New Status Dialog Box

The **Create New Status** dialog box includes the following properties:

Table 4-50 • Create New Status Dialog Box

Property	Description
Status Name	Enter a name to identify this new status.
Status Description	Enter a description of the meaning of this status.
Status Icon	Select an icon that will indicate this new status in the App Portal user interface.

Questions Node

When submitting a software request, sometimes the end user needs to answer a set of questions that will give App Portal the information it needs in order to fulfill that software request.

For example, in order to approve a software request, a manager may want to know the name of the project that the end user is working on that requires this application. Or, in order to determine licensing requirements, the manager may want to know how frequently the end user will use this application or the time of day that it would be used.

In App Portal, you use the **Question Manager** to create questions, then group those questions into question templates using the **Template Manager**.

After you have created a Question Template, you can then attach it to a catalog item, as described in Attaching a Question Template.

The **Site Management > Questions** node has two views:

- Question Manager
- Template Manager

Question Manager

In App Portal, you use the **Question Manager** to create questions, then group those questions into question templates using the **Template Manager**. Asking the appropriate questions for a request allows you to gather the appropriate data to make informed approval decisions.

Figure 4-148: Question Manager View

Questions are defined on the Question Properties Dialog Box. To add a question, click **Add Question**. To edit an existing question, double-click on it.

Question Properties Dialog Box

Questions are defined on the **Question Properties** dialog box, which is opened by clicking **Add Question** or double-clicking on an existing question on the **Question Manager** view.

The **Question Properties** dialog box includes the following tabs:

- Question Tab
- Answers Tab
- Question Condition Tab
- Standard Condition Tab

Question Tab

On the **Question** tab of the **Question Properties** dialog box, you specify general properties of the question.

Figure 4-149: Question Properties Dialog Box / Question Tab

The **Question** tab of the **Question Properties** dialog box includes the following properties:

Table 4-51 • Question Properties Dialog Box / Question Tab

Property	Description
Question Title	Enter a name for this question.
Question to be asked	Enter the actual question to be asked to the requester or approver.
Question details (pop-up information)	Enter any further descriptive text. This information when present shows as a pop-up dialog when the control is focused or the mouse hovers over it.
Apply response to computer variable	Choose whether the response to the question should be written to the computer variable of the targeted and/or source machine.
Apply variable to	Select **Source**, **Target**, or **Source and Target** to apply the variable to the respective computer objects when being used as part of an OSD Task Sequence Catalog Item.
Apply to build type	Choose **Bare Metal**, **In-Place Migration**, **Side-by-Side Migration**, or **Not Specified** to apply the variable to the respective scenario when being used as part of an OSD Task Sequence Catalog Item.
Mask Variable	When a variable value is applied to a computer object, the value of the variable can be masked, just like when you type in a password. To mask the variable, select the **Mask Variable** option. There are cases where you would not want the response to the question to be visible in the user interface, such as when it is a password.
Target	Select whether the question is to be answered by the **Requester**, **Approver**, or **Either** one.
Required	Select this option to require the user to answer this question before proceeding.
Focus	Select one of the following options: • **Request Specific**—Select this option to indicate that the question is related to the entire request (such as asking for the end user's cost center). When this option is selected, the question will only be asked once per request, and the question will be displayed at the top of the **Respond to Questionnaire** panel of the checkout procedure. • **Item Specific**—Select this option to indicate that the question is related to an individual catalog item. When this option is selected, the question will be displayed on the lower portion of the **Respond to Questionnaire** panel. in the table next to the catalog item. 📄 *Note • Even if more than one catalog item in the cart has an associated question template that contains the same **Request-Specific** question, the question is not repeated. It is only asked once per request.*

Table 4-51 • Question Properties Dialog Box / Question Tab

Property	Description
Question Format	Select the format of the question: • **Single Line**—Input will allow for a single line of data. • **Multiline / Rich Text Box**—Input will allow for multiple lines of text. • **Checkbox List / Dropdown List / Radio Button List**—Input will allow for multiple selections. If you select one of these options, you will also need to open the **Answer** tab of the **Question Properties** dialog box and enter the possible answers for this multiple selection question, • **Date / Time / Date and time**—Input will allow for a date / time entry.
Mask Input	Select to prevent the characters of the user's entry to be displayed.
Answer Format	The input of this question must match the format that is selected from this list (such as **Alphabetic**, **Alphanumeric**, **Phone Number**, etc.). *Note • Multiple choices and multiple selections do not require an accepted answer type.*
Control Width **Control Dropdown Width** **Control Height**	Customize the appearance of the control by sizing it to meet your needs.

Answers Tab

If you created a question with a format of **Checkbox List**, **Dropdown List**, or **Radio Button List**, the **Answer** tab of the **Question Properties** dialog box is enabled and you are prompted to enter the possible answers to these questions.

You can select **Manual Entry** to specify the values for items such as drop down lists and radio buttons. You also have the option of selecting **From Web Service** so that this list can be linked to a web service that returns a list of values.

Figure 4-150: Question Properties Dialog Box / Answers Tab - List

When you click **Add New Record**, additional fields are displayed:

Figure 4-151: Question Properties Dialog Box / Answers Tab - New Record

When defining a new answer, enter the following information:

Table 4-52 • Question Properties Dialog Box / Answers Tab

Property	Description
Manual Entry	Select this option to manually enter possible answers for this question.
From Web Service	Select this option to obtain possible answers for this question from a web service which you specify. You can write the web service using the sample file found in the following location: [*AppPortalInstallationDirectory*]\Web\WS\SampleQuestionAnswers.asmx For more information, see Providing Answers Using a Web Service.
Answer Text	Enter the value that will be displayed in the drop down list, such as `Engineering`.
Answer Value	Enter the value that will be recorded for this selection, such as `ENG`.
Apply Role	Select a role.
Message	Enter additional information.

Providing Answers Using a Web Service

If you want to provide answers to a question using a web service, select the **From Web Service** option on the **Answers** tab of the **Question Properties** dialog box.

Figure 4-152: Selecting the "From Web Service" Option on the Answers Tab

When creating the web service, use the provided sample file, `SampleQuestionAnswers.asmx`, that is installed in the following location:

[*AppPortalInstallationDirectory*]\Web\WS\SampleQuestionAnswers.asmx

Question Condition Tab

On the **Question Condition** tab, you define a condition which is based upon the answer to another single-selection question (which must be in the format of **Dropdown List** or **Radio Button List**).

Figure 4-153: Question Condition Tab

The **Question Condition** tab includes the following properties:

Table 4-53 • Question Condition Tab

Property	Description
Please select the Question Condition	From the **Please select the Question Condition** list, select a question. *Note • Only existing questions with the **Question Format** of **Radio Button List** or **Dropdown List** will populate this list. If you do not have single-selection questions defined, this list will not be populated.*
Please select the Question Condition Value	Select the answer to the selected question that the end user will have to select in order for this question to be displayed.

Standard Condition Tab

On the **Standard Condition** tab, you can create conditions based on user attributes including group and OU membership, Active Directory property values, and deployment system collection membership for both users and computers.

Figure 4-154: Standard Condition Tab

Click **Add Condition** to open the **Condition Properties** dialog box and add a **Group and OU**, **AD Property**, or **Collections** condition, as described in Add Condition Dialog Box.

Add Condition Dialog Box

If you click **Add Condition** on the **Group and OU**, **AD Property**, or **Collections** tabs of several dialog boxes, the **Add Condition** dialog box opens.

Figure 4-155: Add Condition Dialog Box

On the **Add Condition** dialog box, do the following:

- Use the search box to search for the group, OU, property, or collection that you want to add, and select the checkbox next to the item in the search results list.

- Click the **Select** button to add the condition. After you add a condition to any of the three subtabs (**Group and OU**, **AD Property**, or **Collections**), that condition is listed on that subtab.

- After the condition is added, specify the **Enforcement** option you want to take effect: **Include** or **Exclude**.

Figure 4-156: Selecting the Enforcement Option

Template Manager

Question templates allow you to group questions together and apply to requests. You can add questions to a template and then select the template in the **General** settings of the request.

Figure 4-157: Template Manager View

To create a new question template, click **Add Template** to open the **Question Template Properties** dialog box.

Question Template Properties Dialog Box

Question templates are created on the **Questions > Template Manager** view.

Figure 4-158: Question Template Properties Dialog Box

The **Question Template Properties** dialog box includes the following properties:

Table 4-54 • Question Template Properties Dialog Box

Property	Description
Template Name	Enter a name to identify the question template.
Available questions list	List of all defined questions. To add a question to the template, select a question in this list and use the arrow keys to move it to the **Current Questions** list.
Current Questions list	List of the questions that are in this question template.

Click **Save** to save your selections.

5

Using App Broker for ServiceNow

Note • *For App Broker for ServiceNow's out-of-the-box workflow to function, you are required to be connected to an instance of FlexNet Manager Suite.*

You can use App Broker for ServiceNow to extend the power of your ServiceNow service catalog, enable software license governance and on-going optimization, and automate and accelerate the fulfillment of software requests to any device. Using App Broker for ServiceNow enables you to provide your employees with a single service portal for all request types: software, hardware, and other IT services.

Like App Portal, App Broker for ServiceNow is a universal enterprise app store for desktop, mobile, and cloud applications that enables IT to maintain license compliance while providing automated software delivery. But with App Broker for ServiceNow, instead of using the App Portal end user interface, employees request software directly in the ServiceNow self-service portal. You publish App Broker catalog items as service items within ServiceNow.

With App Broker for ServiceNow, not only can your employees request software catalog items directly from the ServiceNow self-service portal, they can also submit OS deployment/application migration requests using a custom App Portal Employee App Provision Request wizard from within the ServiceNow interface.

Note • *App Portal Enterprise Edition also offers standard integration with ServiceNow, as described in Configuring ITSM Integration. However, this feature is limited to automatically creating or updating ServiceNow incidents or requests whenever a specified action occurs in App Portal (such as when a request is submitted). There is no integration with App Portal catalog items or app store features.*

The following topics explain how to set up and use App Broker for ServiceNow:

- About App Broker for ServiceNow

- Integrating App Broker with ServiceNow

- Managing App Portal Catalog Items in ServiceNow

- Requesting App Portal Catalog Items Using the ServiceNow Interface

- Using the Employee App Provision Request Wizard to Request Task Sequence Catalog Items

- App Broker for ServiceNow Reference

About App Broker for ServiceNow

Like App Portal, App Broker for ServiceNow is a universal enterprise app store for desktop, mobile, and cloud applications that enables IT to maintain license compliance while providing automated software delivery. But with App Broker for ServiceNow, instead of using the App Portal end user interface, employees request software directly in the ServiceNow self-service portal. In other words, you manage your application catalog using App Portal, but users request software catalog items using the ServiceNow interface.

Using App Broker for ServiceNow enables you to provide your employees with a single service portal for all request types: software, hardware, and other IT services, while also enabling you to optimize software license use and enable automated software delivery through System Center Configuration Manager, Symantec Altiris, VMware AirWatch, and/or JAMF Casper.

Figure 5-1: App Portal Catalog Items Displayed in ServiceNow Service Catalog Interface

Additional information about App Broker for ServiceNow is provided in the following sections:

- App Broker for ServiceNow Integration Overview

- App Broker for ServiceNow Features

- Supported ServiceNow Interfaces

- App Portal Software Request Workflow

App Broker for ServiceNow Integration Overview

You can use App Broker for ServiceNow to extend the power of your ServiceNow service catalog, enable software license governance and on-going optimization, and automate and accelerate the fulfillment of software requests to any device. Using App Broker for ServiceNow enables you to provide your employees with a single service portal for all request types: software, hardware, and other IT services. App Broker for ServiceNow provides two levels of integration with ServiceNow:

- **Integration with ServiceNow self-service portal**—With App Broker for ServiceNow, instead of using the App Portal end user interface to request catalog items, employees are able to request software directly in the ServiceNow self-service portal. See Integration with ServiceNow Self-Service Portal

- **Employee App Provision Request wizard in ServiceNow**—Employee are also able to submit OS deployment/ application migration requests using a custom App Portal Employee App Provision Request wizard from within the ServiceNow interface. See Employee App Provision Request Wizard in ServiceNow to Request Task Sequence Catalog Items.

Integration with ServiceNow Self-Service Portal

App Broker for ServiceNow enables organizations to provide intelligent license checking and reclamation as well as the automated deployment of applications to improve efficiency, reduce costs, and maintain continual license compliance.

The following diagram provides an overview of how App Broker interacts with ServiceNow and FlexNet Manager Suite to complete a software request.

Figure 5-2: App Broker / ServiceNow Integration Overview

As illustrated in this diagram, the following steps take place when an employee requests software in ServiceNow.

- **Employee requests software in ServiceNow**—An employee submits a software request from either the service portal or service catalog interface of ServiceNow.

- **ServiceNow sends request to App Broker**—ServiceNow sends the request to App Broker.

- **App Broker obtains license information**—App Broker obtains license information from FlexNet Manager Suite, which can include performing an advanced license check (considering second use rights, upgrade/downgrade rights, and exceptions).

- **License and cost information is sent to ServiceNow**—The license information obtained from FlexNet Manager Suite, along with cost information, is displayed in ServiceNow, where the approver can review the cost that will be incurred and decide whether to approve the request.

- **Request is sent through approval process, if required**—If the requested catalog item requires approval, the request is sent through the ServiceNow approval process.

- **License is reserved**—If a license is required and the request is approved, App Broker reserves a license.

- **App Broker deploys software via deployment system**—App Broker automatically deploys the software to the specified device using the appropriate deployment system.

- **Status information displayed in ServiceNow**—The status of the software deployment is displayed in ServiceNow. During the delivery stage, App Broker continually monitors the status of requests, updates the status in ServiceNow.

Each of these steps are incorporated into the App Portal Software Request Workflow, which uses App Broker REST API to perform these tasks in App Portal.

For more information, see Requesting App Portal Catalog Items Using the ServiceNow Interface.

Employee App Provision Request Wizard in ServiceNow to Request Task Sequence Catalog Items

Employees can use App Broker's **Employee App Provision Request** wizard within the ServiceNow interface to submit requests for OS deployment and/or application migration. Each request generates a the checkout of a task sequence catalog item in App Portal, which is deployed by System Center Configuration Manager.

Figure 5-3: Employee App Provision Request Wizard in the ServiceNow

The Employee App Provision Request wizard was designed to automate the provisioning tasks that are required when a new employee joins an organization or an existing employee changes roles. A service catalog request can be submitted from ServiceNow and the entire workflow will be taken care of by App Portal, including creating and importing a new machine, and installing all of the software applications that the employee needs. While the requests are submitted in ServiceNow, the deployment tasks are perform by App Portal using App Broker's REST API.

For more information, see Using the Employee App Provision Request Wizard to Request Task Sequence Catalog Items.

App Broker for ServiceNow Features

All of the governance, compliance, and automation features that App Portal with FlexNet Manager Suite provides are also available in App Broker for ServiceNow.

- **Out-of-the-box ServiceNow workflow for advanced license check and deployment**—App Broker for ServiceNow includes a ServiceNow workflow which displays the flow of how advanced license check and deployment is performed (which is triggered when user submits a ServiceNow software request). This workflow is available as an update set that can be applied to any ServiceNow instance. For more information, see App Portal Software Request Workflow.

- **Automatic import of App Portal catalog items into ServiceNow**—A background task runs periodically to sync the App Portal catalog with ServiceNow and add catalog items to the ServiceNow service catalog. For more information, see Importing Catalog Items into ServiceNow.

- **License compliance**—App Broker for ServiceNow leverages asset management data from FlexNet Manager, including product use rights and license entitlement data, to ensure proper governance and compliance over the request and installation of software. Licenses are reserved during the request process. For more information on product use rights, see Performing Advanced License Check.

- **Uses ServiceNow approval and notification features**—When a ServiceNow user submits a software request, all notifications and approvals will be performed by ServiceNow; App Portal is just responsible for performing the license check and deployment.

- **Reclamation of unused software**—To further optimize software license consumption and reduce spending on new software licenses, App Broker (like App Portal) enables the automation of software reclamation to uninstall applications that are not used or rarely used. For more information, see Configuring the My Apps Feature to Perform Compliance Management.

- **Automatic software deployment**—App Broker automates the deployment of software through popular systems management and mobility management solutions that manage the growing diversity of today's endpoint , including Microsoft System Center Configuration Manager, Symantec Altiris, JAMF Casper, and VMware AirWatch.

- **Provision cloud services**—In addition to performing automatic software deployment, you can use App Broker for ServiceNow to provision cloud services like Office 365, Salesforce, and Box. For more information, see Configuring Cloud Application Integration.

- **Ability to view deployment status in ServiceNow**—App Broker passes deployment status information (deployment complete, pending, or failed) back to ServiceNow.

Supported ServiceNow Interfaces

With App Broker for ServiceNow, employees can request catalog items using the same interface they are accustomed to using to request hardware or other IT services.

App Broker supports the Jakarta, Kingston, and London releases of ServiceNow.

ServiceNow Service Catalog Interface

The following is an example of an App Portal catalog item displayed in the ServiceNow service catalog interface.

Figure 5-4: App Portal Catalog Items Displayed in ServiceNow Service Catalog Interface

ServiceNow Service Portal Interface

The following is an example of the new ServiceNow service portal interface.

Figure 5-5: ServiceNow Service Portal Interface

App Broker ServiceNow Workflows

When you integrate App Broker with ServiceNow, two ServiceNow workflows are created: one to perform catalog item requests using the ServiceNow interface, and the other to request OSD task sequence catalog items using the Employee App Provision Request wizard.

- App Portal Task Sequence Request Workflow

- App Portal Software Request Workflow

App Portal Task Sequence Request Workflow

This **Flexera Software - App Portal Task Sequence Request** workflow is used when a request is submitted using the Employee App Provision Request wizard.

Figure 5-6: Flexera Software - App Portal Task Sequence Request Workflow

Each step in the workflow is associated with an API REST Message, as described in API REST Messages Used By App Portal Workflows. This workflow includes the following steps.

Table 5-1 • Workflow Steps in Flexera Software - App Portal Task Sequence RequestWorkflow

Steps	Description
Read Task Sequence Request Data	Extracts request data required by App Portal.
	After user clicks on the **Submit Request** button, the data for that request will get inserted into the x_fls_appportal_task_sequence_requests table. As soon as the data gets inserted into this table, the workflow will be triggered, and this activity will extract the request data required by App Portal for that request.
Submit Task Sequence Request Data	Submits task sequence request data required by App Portal.
	Uses the App Portal - Submit Order REST message.
Notification	Notifies administrator of exceptions in App Portal workflow.

After a request has been completed, ServiceNow administrators can view that request's completed workflow, which includes a blue line that indicates the path that was taken.

Figure 5-7: Flexera Software - App Portal Task Sequence Request Workflow / Completed

App Portal Software Request Workflow

App Broker for ServiceNow includes a custom ServiceNow workflow—implemented using a new set of App Broker REST API endpoints—which is used to integrate App Portal and ServiceNow. This workflow is based on industry best practices for software license governance and software delivery.

This **Flexera Software - App Portal Software Request** workflow enables ServiceNow to perform advanced license checks, reserve available licenses, and perform automated software delivery to multiple device types.

Figure 5-8: Flexera Software - App Portal Software Request Workflow

Each step in the workflow is associated with an API REST Message, as described in API REST Messages Used By App Portal Workflows. This workflow includes the following steps.

Table 5-2 • Workflow Steps in Flexera Software - App Portal Software Request Workflow

Steps	Description
Read Request Data	Extracts request data required by App Portal.
Validate Request	Validates request data required by App Portal and returns one of the following responses: ● **Not Found**—User does not exist ● **Invalid Response**—Did not receive a 200 HTTP response ● **Invalid User**—User record does not contain a valid AD Guid (identifier) ● **Invalid Computer**—Computer is not a client of deployment technology ● **Valid Data**—The data is valid. Uses the App Portal - Validate Request Data REST message.

Table 5-2 • Workflow Steps in Flexera Software - App Portal Software Request Workflow

Steps	Description
Check If Licensable	Checks App Portal to determine if software is licensable and returns one of the following responses: • **Not Found**—Requested catalog item does not exist • **Invalid Response**—Did not receive a 200 HTTP response • **Licensable**—The software is licensable • **Not Licensable**—The software is not licensable. Uses the App Portal - Check If Licensable REST message.
License Reservation Check	Checks App Portal for software license reservation requirement and returns one of the following responses: • **Not Found**—Requested catalog item does not exist • **Invalid Response**—Did not receive a 200 HTTP response • **Reservation Not Required**—Software license reservation is not required • **Reservation Required**—Software license reservation is required. Uses the App Portal - License Reservation Check REST message.
License Availability Check	Checks App Portal for software license availability and returns one of the following responses: • **Not Found**—Requested catalog item does not exist • **Invalid Response**—Did not receive a 200 HTTP response • **License Available**—Software license is available • **License Not Available**—Software license is not available. Uses the App Portal - License Availability Check REST message.
Reserve License	Instructs App Portal to reserve software license and returns one of the following responses: • **Not Found**—Requested catalog item does not exist • **Invalid Response**—Did not receive a 200 HTTP response • **License Reserved**—Software license is reserved • **License Not Reserved**—Software license is not reserved. Uses the App Portal - Reserve License REST message.

Table 5-2 • Workflow Steps in Flexera Software - App Portal Software Request Workflow

Steps	Description
Submit Order	Submits software order without reservation OR submits software order. One of the following responses is returned: ● **Not Found**—Unexpected 404 HTTP response received ● **Invalid Response**—Did not receive a 200 HTTP response ● **Order Submitted**—The software order has been submitted. Uses the App Portal - Submit Order REST message.
Notification	Notifies administrator of exceptions in App Portal workflow.

After a catalog item request has been completed, ServiceNow administrators can view that catalog item's completed workflow, which includes a blue line that indicates the path that was taken.

Figure 5-9: Flexera Software - App Portal Software Request / Completed

Integrating App Broker with ServiceNow

To set up App Broker for ServiceNow, you need to perform the following steps:

Table 5-3 • Integrating App Broker with ServiceNow

Task	Description
Step #1: Download update set files	Open the Flexera Software Product & License Center and download the Flexera Software update set file: `Flexera Software App Broker Update Set for ServiceNow (Kingston and London).xml`
Step #2: Import and configure update set in ServiceNow	In ServiceNow, import the update set and then edit some of the default parameters to customize it to your organization. For instructions, see: • About the App Portal ServiceNow Update Set • Importing and Configuring the Flexera Software App Portal Update Set in ServiceNow
Step #3: Create and correctly configure user account in ServiceNow	In ServiceNow, you need to create a user account with the correct roles assigned. This account is used for integration between Service Now and App Broker. For instructions, see: Creating a ServiceNow Integration User.
Step #4: Connect App Portal to ServiceNow	Enter ServiceNow connection information on the **Site Management > Settings > ServiceNow Integration** view of App Portal. For instructions, see: • Connecting App Broker with ServiceNow • Viewing ServiceNow Web Services in App Portal

About the App Portal ServiceNow Update Set

A ServiceNow update set is a group of customizations, in an XML file, that can be moved from one ServiceNow instance to another. App Broker for ServiceNow includes an update set that, when imported into ServiceNow, will create all of the ServiceNow entities that are required for ServiceNow to work with App Portal.

Figure 5-10: App Portal ServiceNow Update Set

When you import the App Portal ServiceNow update set XML file into ServiceNow, a custom ServiceNow application named **Flexera Software App Portal** is created, which contains all of the following ServiceNow entities:

- **Workflows**—Workflows named **Flexera Software - App Portal Software Request** and **Flexera Software - App Portal Task Sequence Request** are created. For more information, see App Broker ServiceNow Workflows.

- **REST messages**—All of the ServiceNow REST messages used to communicate with App Portal to perform the steps in these workflows. For more information, see API REST Messages Used By App Portal Workflows.

- **Table schemas**—Custom tables are created to contain the imported App Portal catalog item data:

  - App Portal Catalog Items (x_fls_appportal_catalog_items)

  - App Portal Catalog Import Service (x_fls_appportal_import_service)

  - App Portal Task Sequence Requests (x_fls_appportal_task_sequence_requests)

Note • For more information on update sets and how to import them, see Saving Customizations in a Single XML File:

http://wiki.servicenow.com/index.php?title=Saving_Customizations_in_a_Single_XML_File

Importing and Configuring the Flexera Software App Portal Update Set in ServiceNow

To import the App Portal update set into ServiceNow and to customize its settings for your organization, perform the following steps.

Task   ***To import and configure the App Portal - ServiceNow Update Set:***

1. Download the Flexera Software App Portal update set file (`Flexera Software AppBroker 2017 R1 Update Set.xml`) from the Flexera Software Product and License Center.

2. Open your ServiceNow instance.

3. In the search box, enter **Retrieved Update Sets**.

4. In the search results, click **Retrieved Update Sets**. The **Retrieved Update Sets** page opens.

5. Under **Related Links**, click **Import Update Set from XML**. The I**mport XML** page opens.

6. Click **Choose File**, select the Flexera Software App Portal update set `.xml` file and click **Upload**. When the upload is complete, the file will be listed on the **Retrieved Update Sets** page.

7. Click the name of the update set to open the detailed view.

8.   Click **Preview Update Set**. After previewing the update set, if there are any errors, they will be listed at the bottom of the screen on the **Update Set Preview Problems** tab.

9.   To resolve an error, select it, open the **Actions on selected rows...** menu at the bottom of the screen, and click **Accept remote update**.

Repeat this procedure until all errors are resolved. You may select multiple errors at a time. When all errors are resolved, the **Commit Update Set** button is enabled.

10. Click **Commit Update Set**. As soon as the update set is committed, if you enter **Flexera** in the ServiceNow search box, and you will see the following new items listed in the menu:

*Note • You will be using the **Employee App Provision Request** option to submit an App Portal request, and use **Employee App Provision Requests Status** to view the status of those requests.*

11. In the top toolbar of ServiceNow, click on the **Settings** icon:

The **System Settings** view opens.

12. Select the **Developer** tab. The **Developer** tab opens.

13. Change the value of the **Application** field from **Global** to **Flexera Software App Portal** and close the view.

14. Under **Flexera Software App Portal** in the menu, click on **Properties**. The **Properties** view opens.

15. To connect ServiceNow to your instance of App Portal, click on `x_fls_appportal.AppBrokerUrl`. The **System Property** view for that property opens.

16. In the **Value** field, enter the URL to your App Portal server using the following format:

    ```
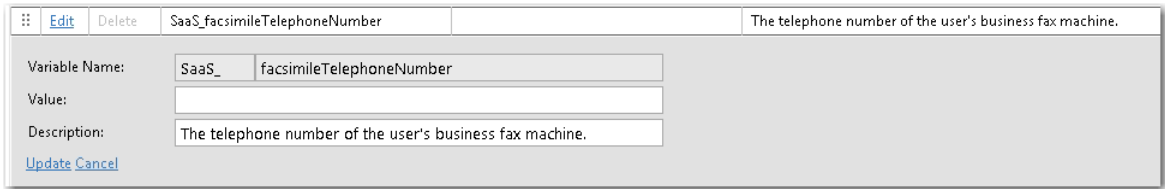    http://APPPORTAL_LOCATION/ESD/api
    ```

17. Click **Update**.

18. Under **Flexera Software App Portal** in the menu, click on **Rest Messages**. The **Rest Messages** view opens.

19. For each REST message, perform the following steps:

a. Click on the REST message name to open the detailed view.

b. Click on the method at the bottom of the screen (**get** or **post**).

c. On the **HTTP Request** tab, select the name of your ServiceNow MID server that has access to App Portal from the **Use MID Server** list.

Note • A ServiceNow MID server is a Windows service running in your environment which enables ServiceNow, a cloud application, to communicate with App Portal, an on-premises application.

d. On the **Authentication** tab, set **Authentication type** as desired for your organization. By default, **None** will be selected. Select the authentication type that the selected ServiceNow MID server should use to access the App Portal REST API.

e. To edit a selected **Basic auth profile**, click the ⓘ icon to open the **Basic Auth Configurations** dialog box, where you can edit the password.

f. Click on the name of the configuration that you want to edit.

Creating a ServiceNow Integration User

This simple process sets up the user account used for integration between Service Now and App Broker, and assigns the user to the appropriate roles that represent the minimum permission required for end user of ServiceNow for successful integration with App Broker. Complete this task while you are still logged into ServiceNow as an administrator.

Task   **To create the user account in ServiceNow with the correct roles assigned:**

1. In ServiceNow, go to **User Administration > Users**.

2. Click **New**, complete the properties for your new user, and click **Submit**.

   Tip • Take note of the user ID and password, as it is used again in the set-up process in section Connecting App Broker with ServiceNow.

3. Once the creation process finishes, click the hyperlinked **User ID** for this user, and scroll down to **Roles**.

4. Click **Edit**, and select the following from the collection, and add them to the **Roles List**.

   ● `x_fls_appportal.user`

   ● `catalog_admin`

- `mid_server`

- `web_service_admin`

- `pa_admin`

- `import_transformer`

Note • *These roles are the minimum permission required for end user of ServiceNow for successful integration with App Portal / App Broker.*

5. Click **Save**.

Connecting App Broker with ServiceNow

After you have imported the App Portal update set, as described in Importing and Configuring the Flexera Software App Portal Update Set in ServiceNow, you need to connect App Broker with that instance of ServiceNow.

Task   **To connect App Broker with ServiceNow:**

1. Launch App Broker.

Tip • *Make sure that you have already uploaded the App Broker license file and added connection information for all desired deployment systems.*

2. Open the Site Management > Settings > ServiceNow Integration view. The **ServiceNow Integration** view opens.

3. Under ServiceNow Integration, enter the following:

- ● **ServiceNow Instance URL**—Enter the URL of your ServiceNow instance in the following format:

  `https://yourinstance.service-now.com`

- ● **ServiceNow User Name**—Enter your ServiceNow user account name (see Creating a ServiceNow Integration User).

- ● **ServiceNow Password**—Enter your ServiceNow password (see Creating a ServiceNow Integration User).

> **Important** • *Do not use any special characters in the URL field. The only special character that is permitted is _ (underscore). Dashes (-) and other special characters are not permitted.*

> **Important** • *The account used to connect must have access to invoke web methods in ServiceNow.*

4. Under **ServiceNow Integration**, click **Test**. App Broker will connect to that instance of ServiceNow and will obtain integration settings.

5. Under **ServiceNow Integration**, click **Create Default ITSM Operations** to create the ITSM operations in App Portal for the Incident Management and Request Management features in ServiceNow.

6. In in the **ServiceNow State Mapping** area, you can map request status values to ServiceNow request state values. App Portal / App Broker can only return three different statuses to ServiceNow: **Pending**, **Success**, or **Failure**. You can manually map those App Portal request statuses to ServiceNow request states by entering values in the **ServiceNow Status** fields. To discover the valid values for ServiceNow request states that you can enter in the **ServiceNow Status** fields, perform the following steps:

   a. Login to ServiceNow and search for "choice" in the navigation panel, and then select **System Definition > Choice Lists**.

   The **Choice Lists** page is displayed.

   b. Use the **Element** column filter to filter down to ***request_state** to display the valid choices in the **Value** column that map to the desired statuses in App Portal / App Broker.

   c. Copy the value from the **Value** column in ServiceNow, return to App Portal / App Broker, and then paste the copied value into a **ServiceNow Status** field under **ServiceNow Request State Mapping** on the **ServiceNow Integration** view.

   d. Click **Test** to test the configuration of the **ServiceNow Request State Mapping**.

   Note • Whenever you get updates from System Center Configuration Manager (such as a successful or failed deployment), the request state will be updated in ServiceNow.

7. Under **ServiceNow Employee App Provisioning**, perform the following steps:

   a. Enter `x_fls_appportal_task_sequence_requests` in the **ServiceNow Employee App Requests data table** field.

   b. Click **Test** to test the connection to the table.

   c. Click **Create Employee App Provision Operations** to create operations in App Portal for this ServiceNow table.

8. Under **ServiceNow Catalog Item Integration**, perform the following steps:

   a. Select the **Sync catalog items with ServiceNow** to automatically sync all new catalog items to the connected ServiceNow catalog.

   b. In the **ServiceNow Variable Set Name** field, enter `App Portal Variable Set`.

   c. In the **ServiceNow Import Set table for saving App Portal catalog details**, enter:

      `x_fls_appportal_import_service`

   d. Click **Test** to validate the entries.

   e. Click **Create Catalog Operations** to create ServiceNow catalog operations.

   f. If you are an existing App Portal customer who has already defined catalog items, you have to click the **Enable** button next to **Enable all software catalog items to sync with ServiceNow** to sync existing catalog items with ServiceNow. If you do not click this button, only new and updated catalog items will be synced with ServiceNow.

9. After you click the **Create Catalog Operations** button under **ServiceNow Catalog Item Integration**, the **ServiceNow Catalog Operations** area is displayed. Enter the following names of the ServiceNow operations that create, update, and delete a ServiceNow import set, which are:

   - **Import Set create operation**—By default, this is set to `Create ServiceNow Import Set Record`.

   - **Import Set update operation**—By default, this is set to `Update ServiceNow Import Set Record`.

   - **Import Set delete operation**—By default, this is set to `Delete ServiceNow Import Set Record`.

   Click **Sync Catalog Now** to sync ServiceNow with the App Portal catalog.

10. Click **Save** to save your settings.

Viewing ServiceNow Web Services in App Portal

App Portal and App Broker for ServiceNow include web services to integrate with ServiceNow, which are listed on the **Site Management > ITSM Integration** view. The number of systems listed depends upon which ServiceNow integration features that you have configured.

Table 5-4 • App Portal / App Broker for ServiceNow Web Services

System Name	Feature	Description
ServiceNow - Create Incident Management Service	Standard App Portal Integration with ServiceNow	Use to create a ServiceNow incident.
ServiceNow - Create Request Management Service	Standard App Portal Integration with ServiceNow	Use to generate a request in ServiceNow for account creation in Box, Office 365, or Salesforce.
ServiceNow - Catalog Import Set Management Service	App Broker for ServiceNow	Use to request catalog items in ServiceNow using the ServiceNow interface.

Table 5-4 • App Portal / App Broker for ServiceNow Web Services

System Name	Feature	Description
ServiceNow - Update Task Sequence Request Management Service	App Broker for ServiceNow	This operation is used to push the status of Employee App Provision Requests from App Portal to ServiceNow.

Viewing App Portal / App Broker for ServiceNow Web Services

After you have connected to ServiceNow, as described in Connecting App Broker with ServiceNow, two new web services will be listed on the **ITSM Integration** view named **ServiceNow - Catalog Import Set Management Service** and **ServiceNow - Update Task Sequence Request Management Service**.

To view and modify these web services, perform the following steps.

Task   ***To view and modify the ServiceNow web services:***

1.   On the Admin tab, select **Site Management - ITSM Integration**. The **ITSM Integration** view opens, listing the available services of the connected systems

2.   Click on one of the services. A list of the operations included in the selected service opens:

3.   Click on one of the operations. The **Configure Operation** view opens.

4.   In the top part of this screen, review and edit the operation settings, as described in About the Operation Settings.

5.   In the **Configure Fields** table, note that App Portal variables are used the following parameters, and those variables will be replaced with catalog-item-specific values at run time. The following table lists typical parameters used in operations:

Parameter	Description
ap_category	The default value is ##Category##.
ap_flexeraid	The default value is ##FlexeraID##.
ap_packageid	The default value is ##PackageID##.
cost	The default value is ##CatalogCost##.
description	The default value is ##PackageDesc##.
name	The default value is ##PackageTitle##.
short_description	The default value is ##BriefDescription##.

Note • The workflow parameter should be empty.

6. You can choose to edit these parameters, as described in About the Parameter Settings.

7. Click **Save** to save your edits.

Managing App Portal Catalog Items in ServiceNow

This section explains the options you have for syncing App Portal catalog items with ServiceNow, and how to activate imported catalog items in the ServiceNow service catalog.

- Importing Catalog Items into ServiceNow

- Activating Catalog Items in the ServiceNow Service Catalog

Importing Catalog Items into ServiceNow

You can specify that you want App Broker automatically sync App Portal's new and updated catalog items to ServiceNow. You can also choose to sync existing catalog items.

To set catalog item sync options, perform the following steps.

Task   ***To import catalog items into ServiceNow:***

1. Open the Site Management > Settings > ServiceNow Integration view.

2. Enter all the **ServiceNow Integration** details. For more information, see Connecting App Broker with ServiceNow.

3. Select the **Sync catalog items with ServiceNow** option and click **Save**. This will start the automatic sync of all of App Portal's new and updated catalog items to ServiceNow.

4. If you are an existing App Portal customer who has already defined catalog items that you want to import into ServiceNow, click the **Enable** button next to **Enable all software catalog items to sync with ServiceNow**. If you do not click this button, only new and updated catalog items will be synced with ServiceNow.

Activating Catalog Items in the ServiceNow Service Catalog

When the **Sync catalog items with ServiceNow** option on the ServiceNow Integration view is selected, a background task runs periodically to trigger the import of new and updated catalog items and to perform deletions. If you click the **Enable** button next to **Enable all software catalog items to sync with ServiceNow**, all existing catalog items are imported.

In both of these instances, catalog items are added to the ServiceNow service catalog but are not automatically activated. A ServiceNow administrator is then required to select which items to activate in the ServiceNow catalog. The ServiceNow administrator can also choose to deactivate catalog items.

Task   ***To activate or deactivate catalog items in the ServiceNow service catalog:***

1. In the ServiceNow search box, enter **Maintain Items** and click **Maintain Items** in the search results. The **Catalog Items** view opens.

2. Click on the name of the catalog item that you want to edit. The edit view of the catalog item opens.

3. To activate or deactivate a catalog item, select its check box in the list and then click the **Activate** or **Deactivate** button at the bottom of the list.

Requesting App Portal Catalog Items Using the ServiceNow Interface

When an end user requests an App Portal catalog item from the ServiceNow interface, they have the following user experience.

Task   ***To request an App Portal catalog item in ServiceNow:***

1. In the search box, enter **Service Catalog** and click **Service Catalog** in the search results. The **Service Catalog** home
    page opens.

2. Click **Software**. The **Service Catalog > Software** page opens.

3. Click on the catalog item you wish to obtain. The detailed view of that catalog item opens.

4. From the **Select device to install software on** list, select a device.

5. Click **Order Now**. The order is submitted and a confirmation message is displayed.

6. To view all requests for App Portal catalog items via ServiceNow, do the following:

   a. Enter **tables** in the search box and press Enter.

   b. Under **System Definition**, click **Tables.**

   c. In the right side under the **Name** column, search for **sc_request**.

   d. Right click **sc_request** and then click **Show List**.

   This displays all the requests placed for App Portal catalog items via ServiceNow. Their status can be seen under the **Request state**. column.

Clicking one of the requests (**REQ0010002**) displays the request details. If the status is **Success** in App Portal, the **Request State** displays as **Closed Complete**.

7. Click on the **Number** of the request you just submitted. The **Order Status** page is displayed.

Using the Employee App Provision Request Wizard to Request Task Sequence Catalog Items

You can submit App Portal OSD task sequence catalog items using custom App Portal pages displayed within the ServiceNow interface in a wizard named **Employee App Provision Request**.

Figure 5-11: Employee App Provision Request Wizard in ServiceNow

The Employee App Provision Request wizard was designed to automate the provisioning tasks that are required when a new employee joins an organization or an existing employee changes roles. A service catalog request can be submitted from ServiceNow and the entire workflow will be taken care of by App Portal, including creating and importing a new machine, and installing all of the software applications that the employee needs. While the requests are submitted in ServiceNow, the deployment tasks are perform by App Portal using App Broker's REST API.

After you perform the steps in Importing and Configuring the Flexera Software App Portal Update Set in ServiceNow, the Employee App Provision Request wizard will be available in your ServiceNow instance.

Using this self-service wizard, the following tasks can be performed:

- **Add new computer**—You can add a new computer to System Center Configuration Manager and provision it with your corporate OS image and applications suitable to the specified user's role.

- **Upgrade existing computer**—You can upgrade the OS of an existing computer, with the option of adding additional applications. You can also choose to just add additional applications to an existing computer without upgrading the OS.

- **Perform side-by-side migration**—Perform a side-by-side migration of applications from an existing system to a replacement system, which will be imaged with the selected corporate OS.

For instructions on how to use the Employee App Provision Request Wizard, see the following topics:

- Importing a New Computer

- Updating an Existing Computer

- Viewing Request Status

Importing a New Computer

To use the Employee App Provision Request wizard to add a new computer to System Center Configuration Manager and deploy an operating system and applications, perform the following steps.

Task   ***To import a new computer:***

1. Click on **Employee App Provision Request** in the ServiceNow menu. The **User Information and Request Type** panel of the wizard opens.

2. Enter the **Domain** and **User name** that this computer will be assigned to.

3. Under **Request Type**, select **New computer**.

4. Click **Next**. The **Select OSD Task Sequence** panel opens.

5. From the **Task sequence** list, select the task sequence corresponding to the OS you want to deploy, and then click **Next**. The **Create New Computer** panel opens.

6. In the **New computer name** field, enter name for the new computer which you are adding to System Center Configuration Manager.

7. Enter either the **MAC address** or **SMBIOS GUID** of the new computer. Only one value is required.

8. To associate the computer in System Center Configuration Manager with the user you entered on the **User Information and Request Type** panel, select the **Do you want to associate the user: NAME?** option.

9. Click **Create Computer**. The computer is created in System Center Configuration Manager. When creation is complete, the computer's resource ID is displayed.

10. Click **Next**. The **Role Applications** panel opens, listing the applications that are associated with the selected employee's roles, which will be installed on the target computer.

11. Click **Next**. The **Application Migration** panel opens.

12. If you want to migrate applications from an existing computer to the target computer, select the **Migrate applications from existing computer** option. If you select this option, the **Select computer** field is displayed, where you are prompted to search for the existing computer.

13. Search for an existing computer (if desired), and then click **Next**. The **Choose Existing Applications to Migrate** panel opens, listing the applications installed on the specified existing computer.

Choose Existing Applications to Migrate

The listed applications are deployed on the selected user's current operating system. Select the applications that you want to migrate to the new operating system as part of this OS deployment.

Items per page: [10 ▼]

	🔍	Name ⌄	Description	Cost	Recommendation	Information
☐		Acrobat® XI Standard 11.0	Get what you need to get the job done right.	$250.00	👎	Usage Pattern: Infrequently Used.
☐		CTSC v1.0	Catalog item and attach a worflow to test the test Approval conditions, when there is condition for AD Property with "Include" condition.	$0.00	👎	Usage Pattern: Infrequently Used.
☐		Dreamweaver CC	Website and mobile app design.	$0.00	👎	Usage Pattern: Infrequently Used.

« ‹ **1** › »   3 items in 1 pages

[Back]   [Next]

*Note • If a catalog item has been designated as a **Core application**, then it will not be displayed on this panel, even if it is installed on the selected computer.*

14. Select the applications that you want to migrate and then click **Next**. The **Choose Additional Applications to Install During OS Deployment** panel opens. Applications that have already been selected in previous panels are already selected and cannot be unselected.

15. Select the additional applications that you want to migrate and then click **Add Applications**. The applications are added to the **Additional Applications Selected for Deployment** table at the bottom of the panel.

16. Click **Next**. The **Summary** panel opens.

Summary

Review your selections and click **Submit Request**. To edit your selections, click **Back**.

Target computer: ABCComputer

Task sequence: Task Sequence_1_OSD_Sh_Jul1

Selected Applications for Deployment

Name	Description
Role Applications	
Acrobat® XI Pro 11.0	Experience the full power of PDF with Acrobat XI.
Adobe Captivate 8	Create a wide range of eLearning and HTML5 based content without programming.
Adobe Connect™	Get a complete web conferencing solution for the enterprise.
Existing Applications to Migrate	
Acrobat® XI Standard 11.0	
Dreamweaver CC	
CTSC v1.0	
Additional Applications to Install	
AIM Keys 3.0	Simple, timesaving macro utility - Now even better!
AdobeReader V6.0	Install Fail with Workflow step level condition
After Effects CC	Cinematic visual effects and motion graphics.

Back   Submit Request

17. Click **Submit Request**. The request is submitted and the **Request Complete** panel opens.

Request Complete

Request was completed successfully!
To check the status of the request, click View Status.

To submit another request, click New Request.

New Request   View Status

18. Click **View Status** to open the **Request Status** page, which lists the status for all submitted requests. For more information, see Viewing Request Status.

Updating an Existing Computer

To use the Employee App Provision Request wizard to update the operating system and/or applications on an existing computer, perform the following steps.

Task   ***To update an existing computer:***

1. Click on **Employee App Provision Request** in the ServiceNow menu. The **User Information and Request Type** panel of the wizard opens.

2. Enter the **Domain** and **User name** that the computer you will be updating is assigned to.

3. Under **Request Type**, select **Existing computer**.

4. Click **Next**. The **Upgrade Operating System** panel opens.

5. Select one of the following options:

    ● If you want to upgrade the OS of the existing computer, select **Upgrade OS**.

    ● If you only want to migrate applications or add additional applications to the existing computer but do not do not want to upgrade its OS, select **Do not upgrade OS**.

6. Click **Next**. The **Select the Target Computer** panel opens.

7. Do one of the following:

   - To select one of the computers associated with the specified user to update, select the **Select a computer associated to use: USERNAME**, and select a computer name from the **Select computer** list.

   - To search for an existing computer to update, select the **Search for a computer** option and search for a computer in the **Select computer** box.

8. After you select a computer to update, click **Next**. The **Select OSD Task Sequence** or **Select Non-OSD Task Sequence** panel opens, listing the name of the selected computer and its current operating system.

📄

*Note • If selected **Do not upgrade OS** on a previous panel, the **Select Non-OSD Task Sequence** panel will be displayed.*

9. From the **Task sequence** list, select the task sequence corresponding to the action you want to take, and then click **Next**. The **Role Applications** panel opens, listing the applications that are associated with the selected employee's roles, which will be installed on the target computer.

10. Click **Next**. The **Application Migration** panel opens.

11. If you want to migrate applications from an existing computer to the target computer, select the **Migrate applications from existing computer** option. If you select this option, the **Select computer** field is displayed, where you are prompted to search for the existing computer.

12. Search for an existing computer (if desired), and then click **Next**. The **Choose Existing Applications to Migrate** panel opens, listing the applications installed on the specified existing computer.

Note • *If a catalog item has been designated as a **Core application**, then it will not be displayed on this panel, even if it is installed on the selected computer.*

13. Select the applications that you want to migrate and then click **Next**. The **Choose Additional Applications to Install During OS Deployment** panel opens. Applications that have already been selected in previous panels are already selected and cannot be unselected.

14. Select the additional applications that you want to migrate and then click **Add Applications**. The applications are added to the **Additional Applications Selected for Deployment** table at the bottom of the panel.

15. Click **Next**. The **Summary** panel opens.

Summary

Review your selections and click **Submit Request**. To edit your selections, click **Back**.

Target computer: ABCComputer

Task sequence: Task Sequence_1_OSD_Sh_Jul1

Selected Applications for Deployment

Name	Description
Role Applications	
Acrobat® XI Pro 11.0	Experience the full power of PDF with Acrobat XI.
Adobe Captivate 8	Create a wide range of eLearning and HTML5 based content without programming.
Adobe Connect™	Get a complete web conferencing solution for the enterprise.
Existing Applications to Migrate	
Acrobat® XI Standard 11.0	
Dreamweaver CC	
CTSC v1.0	
Additional Applications to Install	
AIM Keys 3.0	Simple, timesaving macro utility - Now even better!
AdobeReader V6.0	Install Fail with Workflow step level condition
After Effects CC	Cinematic visual effects and motion graphics.

Back   Submit Request

16. Click **Submit Request**. The request is submitted and the **Request Complete** panel opens.

Request Complete

Request was completed successfully!
To check the status of the request, click View Status.

To submit another request, click New Request.

New Request   View Status

17. Click **View Status** to open the **Request Status** page, which lists the status for all submitted requests. For more information, see Viewing Request Status.

Viewing Request Status

You can view the request status for submitted requests on the E**mployee App Provision Requests Status** page, which is opened by clicking **View Status** on the **Summary** panel of the wizard, or by selecting **Employee App Provision Requests Status** in the ServiceNow menu.

The **Employee App Provision Requests Status** page has two views:

- Request Status View

- Details of the Request View

Request Status View

On the **Request Status** view, a list of all submitted requests is displayed, along with a icon to indicate the request status.

Figure 5-12: Employee App Provision Requests Status / Request Status View

On the **Request Status** view of the Employee App Provision Requests Status page, the following information is displayed:

Table 5-5 • Employee App Provision Requests Status / Request Status View

Property	Description
Request ID	Number identifying the request in App Portal.

Table 5-5 • Employee App Provision Requests Status / Request Status View

Property	Description
Catalog ID	Number identifying the task sequence catalog item in App Portal.
Created	Date and time request was submitted.
UserName Domain	Identifies the user assigned to the target computer.
Target Computer	Identifies the target computer.
Status	Icon indicating the status of the request as one of the following:
	In Progress
	Completed
	Pending
	Failed
View Details	Click to open the Details of the Request View.
Refresh Data	Click the refresh the data in the list.
Create New Request	Click to create a new request.

Details of the Request View

If you click on the View Details button on the Request Status View, details on the selected request are displayed on the **Details of the Request** view.

Figure 5-13: Employee App Provision Requests Status / Details of the Request View

App Broker for ServiceNow Reference

This section includes information on the App Broker REST API endpoints and REST messages, and also includes information on extracting a ServiceNow custom application as an update set.

- App Portal / App Broker ServiceNow Web Services

- App Broker REST API Endpoints

- API REST Messages Used By App Portal Workflows

- Extracting Custom Application as an Update Set

App Portal / App Broker ServiceNow Web Services

App Portal and App Broker for ServiceNow include web services to integrate with ServiceNow, which are listed on the **Site Management > ITSM Integration** view. The number of systems listed depends upon which ServiceNow integration features that you have configured.

Table 5-6 • App Portal / App Broker for ServiceNow Web Services

System Name	Feature	Description
ServiceNow - Create Incident Management Service	Standard App Portal Integration with ServiceNow	Use to create a ServiceNow incident.
ServiceNow - Create Request Management Service	Standard App Portal Integration with ServiceNow	Use to generate a request in ServiceNow for account creation in Box, Office 365, or Salesforce.
ServiceNow - Catalog Import Set Management Service	App Broker for ServiceNow	Use to request catalog items in ServiceNow using the ServiceNow interface.
ServiceNow - Update Task Sequence Request Management Service	App Broker for ServiceNow	This operation is used to push the status of Employee App Provision Requests from App Portal to ServiceNow.

For more information, see Configuring ITSM Integration.

App Broker REST API Endpoints

The App Broker REST API, which powers the App Portal ServiceNow Request workflow, is hosted in the ESD virtual directory, the same directory where the App Portal / App Broker administrator and end user website exists. The API endpoints are accessible through the following URL domain and path:

```
http://APPPORTALSERVERNAME/esd/api
```

The following API endpoints are used to perform this ServiceNow integration:

- Getting Additional Applications for OSD Checkout

- Getting Applications Associated to User and Machine Based on Conditional Roles

- Importing New Computer in System Center Configuration Manager and Associating a User

- Returning All Available System Center Configuration Manager Sites

- Getting Task Sequence Catalog Items

- Getting Status of Task Sequence / OSD Requests

- Getting Installed OS Information for a Machine

- Getting the Deployment Technology Details for a Machine

- Getting the Settings Related to Task Sequences

- Getting the Applications That Can Be Migrated

- Getting the Roles Applicable to a User

- Getting the Machines Associated to a User

- Submitting a Task Sequence / OSD Request

- Getting Additional Apps for Employee App Provisioning

For detailed information on the App Broker REST API endpoints, see App Broker REST API Reference.

API REST Messages Used By App Portal Workflows

Each step in the **Flexera Software - App Portal Task Sequence Request Workflow** and **Flexera Software - App Portal Software Request Workflow** is associated with an API REST message, which are used to communicate with App Portal to perform the steps in the workflow, as described in App Broker ServiceNow Workflows.

The App Portal REST messages are displayed on the **REST Messages** view.

Figure 5-14: REST Messages View

Click on a REST message to view its details.

Figure 5-15: REST Message / App Portal - Reserve License

The Flexera Software App Portal custom application includes the following REST messages.

Table 5-7 • Flexera Software App Portal / REST Messages

REST Message	Method	Endpoint
App Portal - Check If Licensable	Get	`http://APSERVER/ESD/api/catalogs/${catalogId}`
App Portal - Get Additional Applications	Get	`http://APSERVER/ESD/apps?osdCompatible=true&searchText=${searchText}`
App Portal - Get Applications for Role	Get	`http://APSERVER/ESD/Roles/domain=${domain}/user=${username}/` `    machine=${machinename}/apps`

Table 5-7 • Flexera Software App Portal / REST Messages

REST Message	Method	Endpoint

App Portal - Get Migratable Applications	Get	`http://APSERVER/ESD/`
		`apps?targetmachinename=${machinename}&machineDomain=${domain}&sourcema`
		`chinename=${machinename}&migratable=true`

App Portal - Get Requests Status	Get	`http://APSERVER/ESD/requests/${requestId}`

App Portal - Get Role Details	Get	`http://APSERVER/ESD/`
		`roles?domain=${domain}&username=${username}&machinename=${machinename}`
		`&getRoles=true`

App Portal - Get Task Sequence Settings	Get	`http://APSERVER/ESD/admin/TaskSequenceSettings`
App Portal - Get Task Sequences	Get	`http://APSERVER/ESD/catalogs/` `tasksequence?isOsDeployment=${isOSDeployment}`
App Portal - Is Computer Exists	Get	`http://APSERVER/ESD/computers/ComputerName=${machinename}/` `DeploymentMapping`
App Portal - License Availability Check	Get	`http://APSERVER/ESD/api/catalogs/${catalogId}/licenses/` `availability?dn=${domain}&un=${username}&dev=${machineName}`
App Portal - License Reservation Check	Get	`http://APSERVER/ESD/api/catalogs/${catalogId}/licenses/` `necessity?dn=${domain}&un=${username}&dev=${machineName}`
App Portal - Reserve License	Post	`http://APSERVER/esd/api/catalogs/${catalogId}/` `licenses?dn=${domain}&un=${username}&dev=${machineName}`
App Portal - Submit Order	Post	`http://APSERVER/esd/api/servicenow/requests/${serviceNowId}?` `dn=${domain}&un=${username}&dev=${machineName}`
App Portal - Validate Request Data	Get	`http://APSERVER/ESD/api/users?filter=email%3D%3D%22${userEmail}` `%22&machineName=${computerName}`
App Portal - Import New Computer	Post	`http://APSERVER/ESD/computers`
App Portal Get OperatingSystem Info	Get	`http://APSERVER/ESD/computers/ComputerName=${machinename}/` `OperatingSystemInfo`

Table 5-7 • Flexera Software App Portal / REST Messages

REST Message	Method	Endpoint
App Protal - Get Machines For User	Get	`http://APSERVER/ESD/users/domain=${domain}/user=${username}/machines`

API REST Messages Used by the Flexera Software - App Portal Software Request Workflow

Each step in the **Flexera Software - App Portal Software Request Workflow** is associated with an API REST message, which are used to communicate with App Portal to perform the steps in the workflow, as described in App Portal Software Request Workflow.

The six App Portal REST messages are displayed on the **REST Messages** view.

Figure 5-16: REST Messages View

Click on a REST message to view its details.

Figure 5-17: REST Message / App Portal - Reserve License

The Flexera Software App Portal custom application includes the following REST messages.

Table 5-8 • Flexera Software App Portal / REST Messages

REST Message	Method	Endpoint
App Portal - Check If Licensable	Get	`http://APSERVER/ESD/api/catalogs/${catalogId}`
App Portal - License Availability Check	Get	`http://APSERVER/ESD/api/catalogs/${catalogId}/licenses/` `    availability?dn=${domain}&un=${username}&dev=${machineName}`
App Portal - License Reservation Check	Get	`http://APSERVER/ESD/api/catalogs/${catalogId}/licenses/` `    necessity?dn=${domain}&un=${username}&dev=${machineName}`
App Portal - Reserve License	Post	`http://APSERVER/esd/api/catalogs/${catalogId}/` `    licenses?dn=${domain}&un=${username}&dev=${machineName}`

Table 5-8 • Flexera Software App Portal / REST Messages

REST Message	Method	Endpoint
App Portal - Submit Order	Post	`http://APSERVER/esd/api/servicenow/requests/${serviceNowId}?dn=${domain}&un=${username}&dev=${machineName}`
App Portal - Validate Request Data	Get	`http://APSERVER/ESD/api/users?filter=email%3D%3D%22${userEmail}%22&machineName=${computerName}`

Extracting Custom Application as an Update Set

If you decide to modify the **Flexera Software App Portal** custom application in ServiceNow, you can extract that custom application as an update set XML file so that you can make it available on other instances of ServiceNow.

Task ***To extract a custom application as an update set:***

1. Enter **System Applications** in the search box and click on **Applications** in the search results. The **Applications** view opens.

2. Click on **Flexera Software App Portal**. The **Custom Application - Flexera Software App Portal** view opens.

3. Make any desired changes.

4. Under **Related Links**, click **Publish to Update Set**.

The **Publish to Update Set** dialog box opens.

5. Enter a name and click **Publish**.

6

Using App Broker for BMC

> 📄
>
> **Note •** *For App Broker for BMC's out-of-the-box workflow to function, you are required to be connected to an instance of FlexNet Manager Suite.*

App Broker 2017 includes integration with BMC MyIT, which enables you to use MyIT as your front end app store, while App Portal performs the behind-the-scenes fulfillment of software requests, including automatically reserving licenses.

You can use App Broker for BMC to extend the power of your MyIT service catalog, enable software license governance and on-going optimization, and automate and accelerate the fulfillment of software requests to any device. Using App Broker for BMC enables you to provide your employees with a single service portal for all request types: software, hardware, and other IT services.

> 📄
>
> **Note •** *App Portal Enterprise Edition also offers standard out-of-the-box integration with BMC Remedy, but integration is limited to automatically creating or updating BMC Remedy tickets whenever specified actions occur in App Portal (such as when a request is submitted or completed).*

The following topics explain how to set up and use App Broker for BMC:

- About App Broker for BMC

- Configuring App Broker for BMC

- Using App Broker for BMC

About App Broker for BMC

Like App Portal, App Broker for BMC is a universal enterprise app store for desktop, mobile, and cloud applications that enables IT to maintain license compliance while providing automated software delivery. But with App Broker for BMC, instead of using the App Portal end user interface, employees request software directly in the MyIT self-service portal. In other words, you manage your application catalog using App Portal, but users request software catalog items using the MyIT interface.

Using App Broker for BMC enables you to provide your employees with a single service portal for all request types: software, hardware, and other IT services, while also enabling you to optimize software license use and enable automated software delivery through System Center Configuration Manager, Symantec Altiris, VMware AirWatch, and/or JAMF Casper.

Figure 6-1: Catalog Items Displayed in MyIT Service Catalog Interface

Additional information about App Broker for BMC is provided in the following sections:

- App Broker for BMC Integration Overview
- App Broker for BMC Features

App Broker for BMC Integration Overview

App Broker for BMC enables organizations to provide intelligent license checking and reclamation as well as the automated deployment of applications to improve efficiency, reduce costs, and maintain continual license compliance.

The following diagram provides an overview of how App Broker interacts with MyIT and FlexNet Manager Suite to complete a software request.

Figure 6-2: App Broker / MyIT Integration Overview

As illustrated in this diagram, the following steps take place when an employee requests software in MyIT.

● **Employee requests software in MyIT**—An employee submits a software request from either the service portal or service catalog interface of MyIT.

● **MyIT sends request to App Broker**—MyIT sends the request to App Broker.

● **App Broker obtains license information**—App Broker obtains license information from FlexNet Manager Suite, which can include performing an advanced license check (considering second use rights, upgrade/downgrade rights, and exceptions).

● **License and cost information is sent to MyIT**—The license information obtained from FlexNet Manager Suite, along with cost information, is displayed in MyIT, where the approver can review the cost that will be incurred and decide whether to approve the request.

● **Request is sent through approval process, if required**—If the requested catalog item requires approval, the request is sent through the MyIT approval process.

● **License is reserved**—If a license is required and the request is approved, App Broker reserves a license.

● **App Broker deploys software via deployment system**—App Broker automatically deploys the software to the specified device using the appropriate deployment system.

● **Status information displayed in MyIT**—The status of the software deployment is displayed in MyIT. During the delivery stage, App Broker continually monitors the status of requests, updates the status in MyIT.

App Broker for BMC Features

All of the governance, compliance, and automation features that App Portal with FlexNet Manager Suite provides are also available in App Broker for BMC.

- **Out-of-the-box MyIT workflow for advanced license check and deployment**—App Broker for BMC includes a MyIT workflow performs advanced license check and deployment, which is triggered when user submits a MyIT software request. This workflow is available as an update set that can be applied to any MyIT instance.

- **Automatic import of App Portal catalog items into MyIT**—A background task runs periodically to sync the App Portal catalog with MyIT and add catalog items to the MyIT service catalog.

- **License compliance**—App Broker for BMC leverages asset management data from FlexNet Manager, including product use rights and license entitlement data, to ensure proper governance and compliance over the request and installation of software. Licenses are reserved during the request process.

- **Uses MyIT approval and notification features**—When a MyIT user submits a software request, all notifications and approvals will be performed by MyIT; App Portal is just responsible for performing the license check and deployment.

- **Reclamation of unused software**—To further optimize software license consumption and reduce spending on new software licenses, App Broker (like App Portal) enables the automation of software reclamation to uninstall applications that are not used or rarely used.

- **Automatic software deployment**—App Broker automates the deployment of software through popular systems management and mobility management solutions that manage the growing diversity of today's endpoint , including Microsoft System Center Configuration Manager, Symantec Altiris, JAMF Casper, and VMware AirWatch.

- **Provision cloud services**—In addition to performing automatic software deployment, you can use App Broker for BMC to provision cloud services like Office 365, Salesforce, and Box.

- **Ability to view deployment status in MyIT**—App Broker passes deployment status information (deployment complete, pending, or failed) back to MyIT.

Configuring App Broker for BMC

To configure using App Broker for BMC, perform the tasks.

- Validating the Connection Between App Portal and MyIT

- Integrating App Portal with BMC MyIT

- Opening the MyIT End User Interface

- Launch App Portal in BMC Cloud Environment

Validating the Connection Between App Portal and MyIT

Flexera Software has a partnership with BMC, and therefore BMC MyIT offers a Flexera Connector option in its user interface.

Figure 6-3: Flexera Connector in MyIT Service Broker Interface

To validate the connection of your installation of App Portal with BMC MyIT, perform the following steps.

Task   ***To validate the connection of App Portal with BMC MyIT:***

1. Launch BMC MyIT Service Broker and login using administrative credentials.

2. Open the **Import** tab.

3. Double click on **Flexera**. A list of all of the catalog items in App Portal opens.

Integrating App Portal with BMC MyIT

To connect BMC MyIT with App Portal, perform the following steps.

Task   **To integrate BMC MyIT Service Broker with App Portal:**

1.   Launch BMC MyIT Service Broker and login using administrative credentials. The MyIT Service Broker **Dashboard** opens.

2.   Open the **Import** tab.

3. Select the name of your App Portal catalog (such as Flexera) and click the **Catalog Import Options** button. The **Entire Catalog** tab of the selected catalog page is displayed.

4. Select a catalog item that has not yet been configured, such as **Adobe Reader**, and click the **Configure** button. The **Configuration Options** view opens.

Configuration Options

1 service

Software Request

Profile Details *

Workflow

Queue for Import   Close

5. Click **Workflow**. The **Select Workflow** view opens.

6. Select a workflow, such as **Flexera TYPICAL SCENARIO**, and click **Save**.

Note • The Flexera TYPICAL SCENARIO workflow was created as part of the Flexera Integration and is listed on the Workflow tab. Once the workflow is created it will get listed under Workflows.

7. Back on the **Configuration Options** view, click **Profile Details**. The **Profile Details** view opens.

8. From the **Service Excerpt** list, select **excerpt**. This is equivalent to the **Short description** field in App Portal.

9. From the **Service Description** list, select **description**, which is equivalent to the **Full description** field in App Portal.

10. Click **Save** to save changes and close the **Profile Details** view. The **Configuration Options** view opens.

11. Click **Queue for Import** and observe that the status of the selected catalog item will be updated to **Queued**. Catalog items are imported from App Portal into BMC MyIT. Queue for import means that the catalog items are ready to be imported into BMC.

12. Click the **Import 1 Item** button. The item is imported from App Portal to BMC MyIT, and the **Catalog Queue** page opens.

13. Double click on **Flexera**. The **Entire Catalog** tab of the **Flexera** page opens, and the **Last Import** column of the catalog item lists the time period since the import (such as 5 minutes) and the **Status** column is changed to **Configured**.

14. Click on the **Close** button to close the **Flexera** page, and then click on **Services** to open the **Services** tab of MyIT.

15. Double-click on a catalog item, such as **Adobe Reader v8.0**. The **Service Options** view opens.

16. Expand the **Pending** status.

17. Click on the arrow next to **Questions**. The **Service Questions** page opens.

18. Drag and drop the machine name from left pane to the right pane. The **Question Settings** view opens. On this view, you need to select the questions that will be asked during checkout.

19. From the **Form Element Type** list, select the type of the machine name field, such as **Text Field**.

20. Click **Save** to close the **Question Settings** view. The **Service Questions** view opens, displaying the **machine name** field.

21. Click **Close**. The **Service Options** view opens.

22. From the **Actions** menu, select **Approve & Publish**. The **Status** for **Approved** and **Published** is updated to **Just now**.

23. Click **Close**.

Opening the MyIT End User Interface

To open the BMC MyIT end user interface, perform the following steps.

Task   ***To open the MyIT user interface:***

1. Login to MyIT using an end-user login.

2. Search for the published services (catalog items) by entering text in the **Search** text box. A list of search results appears in a pop-up dialog box:

3. Click on the catalog item that you want to request. Detailed information about that catalog item is listed.

4. Click on the **Request Now** or **Add to Cart** button. If you click **Request Now**, The **Required Information** tab of the **Checkout** process opens.

5. Enter the **Machine Name** and click on the **Complete request** button. The **Confirmation** tab of the **Checkout** process opens and the **Request Submitted** message is displayed.

6. Click the **I'm done** button.

7. Click on **My Activity > All activity**. The request that you just completed is listed.

Launch App Portal in BMC Cloud Environment

Once the request is placed in BMC MyIT, the same request can be seen in App Portal on the **My Request** tab, where you can monitor the deployment status.

Note • *There are no settings required in App Portal for BMC MyIT integration to work. The installation of App Portal is already present in the Cloud instance of BMC.*

Using App Broker for BMC

- Making a Software Request in BMC MyIT

- Checking on the App Portal Status of a Request Submitted in BMC MyIT

Making a Software Request in BMC MyIT

Task

To make a software request in BMC MyIT:

1. Launch BMC MyIT and log in. The BMC MyIT **Home** page opens.

2. Search for **Adobe Reader v8.0**. It will be returned in the search results.

3. Click on **Adobe Reader v8.0**. The detail information for that catalog item is displayed.

4. Click **Request Now**. The **Checkout** view opens and you are prompted to specify the machine name.

5. Enter a machine name and click **Complete request**. The **Request Submitted** page opens.

6. Click **I'm done**.

7. Select **My Activity > All Activity**. My activity page opens, and **Adobe Reader v8.0** is listed.

Checking on the App Portal Status of a Request Submitted in BMC MyIT

To check on the App Portal status of a request submitted in BMC MyIT, perform the following steps.

Task   ***To check on the status of a request that was submitted in BMC MyIT:***

1. Launch App Portal and open the **My Requests** page. The request for **Adobe Reader v8.0** is listed.

2. Once the collection icon appears in App Portal, then open the BMC MyIT end user page and look for the catalog item **Adobe Reader 8.0**.

3. Open the **My Stuff** tab and observe that **Adobe Reader v8.0** will have a status of **Installation Pending**.

4. Open App Portal again, open the **My Requests** page, and click on the **Refresh** button after about 15-20 minutes. The deployment icon should be updated to **Success**.

5. Open BMC MyIT again, open the **My Stuff** tab, and search for **Adobe Reader v8.0**. Its status should have been updated to **Installation Complete**.

Note • *Similarly the catalog items which have a status of **Failed** are updated to the status of **Installation Failure** in BMC MyIT.*

7

Using Compliance Management Features to Track Software Licensing and Usage

📄

*Note • Starting with App Portal 7.5, licensing and inventory can be managed by FlexNet Manager Suite, replacing the functionality previously available on the **Inventory Management** and **Purchase Management** views. If your organization has purchased FlexNet Manager Suite and registered it with the Flexera Service Gateway, the **Inventory Management** views will not be displayed.*

App Portal allows tracking of software and computers in use in your company. App Portal will count and link license data directly to the organizational data to allow for detailed reporting on license usage.

In App Portal, there are two methods you can use to perform compliance management: the **My Apps** feature, which requires integration with FlexNet Manager Suite, and the **Inventory** feature. The items displayed under **Compliance Management** on the **Admin** tab depend upon which method you are using.

Figure 7-1: Comparison of Compliance Management Menu Items

This chapter describes both methods that App Portal can use to perform compliance management, and also explains how to set up upgrade and retire campaigns to enforce compliance management.

- Configuring the My Apps Feature to Perform Compliance Management

- Using the Inventory Feature to Perform Compliance Management

- Using Retire and Upgrade Campaigns to Enforce Compliance Management

● Compliance Management Reference

Configuring the My Apps Feature to Perform Compliance Management

Note • *This feature requires that App Portal is connected to FlexNet Manager Suite via the Flexera Service Gateway.*

On the App Portal **My Apps** tab, users can view a list of applications installed on their devices, and address automatic and administrator-defined alerts to ensure that those applications comply with corporate software policies. This assists IT administrators in driving continual software license reclamation and optimization.

Figure 7-2: My Apps Tab

On the App Portal **My Apps** tab, users will see the Software Policy Score™ that reports on the usage of the applications installed on their device.

To target an application for license reclamation, administrators need to add that application to the **My Apps License Reclamation Policies** list, which is opened by selecting **Compliance Management > My Apps**.

This section explains how to enable the **My Apps** tab, how to specify target applications, how to set global options, and how to manage alert action catalog items.

- Enabling the My Apps Tab

- Specifying the License Reclamation Target Applications

- Setting My Apps Tab Options

- Configuring SmartUninstall in Your System Center Configuration Manager Environment

- Creating Views to Include or Exclude Machines from My Apps

- Managing Alert Action Catalog Items

Important • *To use the My Apps feature, the App Portal system account must have read access to the FlexNet Manager Suite database, which is specified on the* **FlexNet Manager Suite Database Connection Settings** *area of the* **Site Management > Settings > Flexera Integration** *view on the* **Admin** *tab.*

Enabling the My Apps Tab

To enable the **My Apps** tab, App Portal must be integrated with FlexNet Manager Suite and the **Enable the My Apps Feature** option on the **Site Management > Settings > Flexera Integration** view must be selected.

Important • *In order for the* **My Apps** *tab to be displayed to a user, the user must be the primary user of the machine upon which they are viewing App Portal. Even if the* **My Apps** *tab is enabled, if a user is viewing the App Portal site from a machine that they are not the primary user of, the* **My Apps** *tab will be hidden.*

Task   ***To enable the My Apps tab:***

1. App Portal communicates with FlexNet Manager Suite via the Flexera Service Gateway component. Connect App Portal to the Flexera Service Gateway as described in Connecting to the Flexera Service Gateway.

    You may also need to enter additional FlexNet Manager Suite On Premises or FlexNet Manager Suite Cloud credentials on the **Site Management > Settings > Flexera Integration** view, as described in Entering FlexNet Manager Suite Settings.

2. Open the **Site Management > Settings > Flexera Integration** view and locate the **My Apps Options** area.

3. Select the **Enable My Apps Feature?** option.

4. Continue with the steps in Setting My Apps Tab Options.

Specifying the License Reclamation Target Applications

To specify which applications in your enterprise will be subject to license reclamation (uninstallation), you need to specifically add those applications to the **My Apps License Reclamation Policies** list, which is opened by selecting **Compliance Management > My Apps** on the **Admin** tab.

You have several options when adding applications to the **My Apps License Reclamation Policies** view.

Task   ***To specify applications to be reclaimed:***

1. On the **Admin** tab, select **Compliance Management > My Apps**. The **My Apps License Reclamation Policies** list opens and lists those applications that are already targeted for reclamation.

2. To add an application to the list, click one of the following buttons:

   - **Add Discovered Flexera IDs**—Click to view a list of all applications in the enterprise that have a Flexera ID identified.

   - **Add Flexera ID From Licenses**—Click to view a list of all applications in the enterprise that have a license created in FlexNet Manager Suite.

   - **Search Flexera ID**—Click to search all applications in the FlexNet Manager Suite Application Recognition Library.

   A list of applications opens.

3. Use the column filters to locate the application you want to add and select its check box.

Note • Hold down the Ctrl button to select more than one application at a time.

Note • If there is no check box next to an application's name, it means that the item has already been added to the reclamation list.

4. Click the **Add** button. The application is added to the **My Apps License Reclamation Policies** list.

5. Optionally, click **Configure Policy** in the **License Reclamation Policy** column to set policy options for this application such as the license reclamation threshold and whether to automatically uninstall this application. See Configure License Reclamation Policy for more information.

6. Optionally, click **View Devices** in the **Devices** column to view a list of devices where this application is installed. See Devices (My Apps) for more information.

7. Optionally, click **View Alerts** in the **Alerts column** to view a list of alerts that have already been generated for this application, if any. See Alerts (My Apps) for more information.

Setting My Apps Tab Options

By setting **My Apps** options, you can specify the number of days in the license reclamation threshold, the FlexNet Manager Suite classification of applications to list on the **My Apps** tab, and whether to also send out email notifications to a user when an alert on the **My Apps** tab is generated for that user.

Task   **To set My Apps options:**

1. Perform the steps in Enabling the My Apps Tab.

2. Locate the **My Apps Options** on the **Site Management > Settings > Flexera Integration** view.

3. If you want App Portal to automatically send out an email notification to users each time an alert is generated for one of their installed applications, select the **Enable My Apps Email Notifications?** option.

4. If you want to deploy the Smart Uninstaller client tool (`AppPortal.SmartUinstall.exe`) with distributed Windows Installer packages to enable automatic license reclamation (even if an uninstallation program was not defined in the deployment technology for that application), select the **Smart Uninstaller is deployed for License Reclamation?** option.

   Note • Valid option for Windows Installer packages only.

   Note • For more information, see Configuring SmartUninstall in Your System Center Configuration Manager Environment.

5. If you want to use a custom number of days as the threshold for reclaiming a software license, select the number of days from the **License Reclamation Threshold** list. The default value is 30.

   Note • To proceed with configuring which applications are subject to license reclamation/uninstallation, continue with the steps in Specifying the License Reclamation Target Applications.

6. Select the **Bypass Question for uninstall checkout** option to specify that if a user is submitting a request for the uninstall of a catalog item, they will not be prompted to answer the catalog item's associated questions.

Configuring SmartUninstall in Your System Center Configuration Manager Environment

If you want to deploy the Smart Uninstaller client tool (`AppPortal.SmartUinstall.exe`) with distributed Windows Installer packages to enable automatic license reclamation (even if an uninstallation program was not defined in the deployment technology for that application), select the **Smart Uninstaller is deployed for License Reclamation?** option under **My Apps Options** on the **Site Management > Settings > Flexera Integration** page.

> **Note •** *Valid option for Windows Installer packages only.*

In addition to selecting this option, you also need to configure SmartUninstall in your System Center Configuration Manager environment.

Task   **To configure SmartUninstall in your System Center Configuration Manager environment:**

1. Locate the `AppPortal.SmartUninstall.exe` file in the following directory:

   `C:\Program Files (x86)\Flexera Software\App Portal\Utilities`

2. Open System Center Configuration Manager and add the `AppPortal.SmartUinstall.exe` file as a package.

3. To that package, add a program with the following command-line.

   ```
   AppPortal.SmartUninstall.exe http://<AppPortalServer>/ESD/WS/Integration.asmx
       "Data Source=[FNMS_DBSERVER];Initial Catalog=[FNMS_DB_NAME];Integrated Security=True"
   ```

4. Add scheduling options for the package as needed.

5. In your production environment, deploy this package to all machines and execute this EXE in the required intervals.

> **Note •** *You can try to manually run this EXE, as an administrator, on a client machine to see how it works. It logs whatever is done on the client machine under %TEMP%AppPortal.SmartUninstall.log.*

Creating Views to Include or Exclude Machines from My Apps

You can create views, named `vMyAppsInclude` and `vMyAppsExclude`, that contain a list of machines that can be included or excluded from the **My Apps** tab.

Task   **To create views to include or exclude machines on the My Apps tab:**

- **Include view**—To define your own data source of machines for license reclamation using **My Apps**, create a view named `vMyAppsInclude`. The following is sample code:

  ```
  CREATE VIEW [dbo].[vMyAppsInclude]
  AS
  SELECT MachineName, UniqueName
  FROM vUserComputerMap
  WHERE [YOUR INCLUDE CONDITION]
  ```

```
GO
```

- **Exclude view**—To exclude machines for license reclamation using **My Apps**, create a view named vMyAppsExclude. The following is sample code:

```
CREATE VIEW [dbo].[vMyAppsExclude]
AS
SELECT MachineName, UniqueName
FROM vUserComputerMap
WHERE [YOUR EXCLUDE CONDITION]
GO
```

Important • *If you define a vMyAppsInclude view, then do not also define a vMyAppsExclude view. The vMyAppsInclude view is the exclusive data source of machines for license reclamation; you can define a condition that specifies which machines to exclude within the WHERE clause of this view.*

Managing Alert Action Catalog Items

Rather than sending out repeated email notifications to users regarding expired licenses or unused software, administrators can instruct App Portal to generate license reclamation, proof of purchase, and custom alert actions to prompt end users to address compliance issues. Users resolve these issues on the **My Current Alerts** subtab of the **My Apps** tab.

Figure 7-3: My Current Alerts Subtab of My Apps Tab

To instruct App Portal to generate alerts, you create, and modify, *Alert Action catalog items*, which are a specialized type of catalog item that uses FlexNet Manager Suite application recognition and licensing data to identify installed application/device combinations that need attention, such as unused applications, unlicensed applications, or applications targeted for another reason. App Portal then sends out alerts to the identified device owners to prompt them to take action to resolve the issues.

You create and modify Alert Action catalog items on the **Catalog Management > Catalog > Alert Action Catalog Items** view.

ID	Alert Action	Mapped General Catalog Name	Action Type
1	Proof of purchase	Proof of purchase	Compliance
2	Uninstall	Uninstall	Uninstall
3	Keep	Keep	Keep
6	Outdated Browser Detected	Outdated Browser Detected	Compliance
1006	Unapproved Software Detected	Unapproved Software Detected	Compliance
1007	Old App Version Detected	Old App Version	Compliance
1008	Deprecated Software	Deprecated Software	Compliance

Figure 7-4: Alert Action Catalog Items View

While Alert Action catalog items share the same catalog item properties dialog box, they are not the same as standard App Portal catalog items:

- **Not listed on Browse Catalog tab**—Alert Action catalog items are not listed on the **Browse Catalog** tab.

- **Do not need to select a category**—When creating Alert Action catalog items, you do not need to specify a category.

- **Can only be created on the Alert Action Catalog Items view**—You can only create new Alert Action catalog items on the **Catalog Management > Catalog > Alert Action Catalog Items** view.

- **Can be viewed and edited in two locations**—You can view and edit Alert Action catalog items in two locations in the App Portal interface: both on the **Alert Action Catalog Items** view and also on the **Catalog Management > Current Catalog Items > View All Items** view.

The following topics explain the types of Alert Action catalog item, and how to create, modify, and target them:

- Types of Alert Action Catalog Items

- Triggering a Proof of Purchase Alert

- Creating a New Custom Alert Action Catalog Item

- Customizing an Unused Software Alert

- Converting a General Catalog Item to an Alert Action Catalog Item

- Deleting an Alert Action

- Scheduling My Apps Background Processes

Types of Alert Action Catalog Items

You can create and enable several types of Alert Action catalog items:

- Predefined Alert Action Catalog Items

- Unused Software Alert

- Proof of Purchase Action Alert

- Administrator-Created Custom Action Alert

Predefined Alert Action Catalog Items

App Portal is shipped with the following pre-defined Alert Action catalog items (which correspond to pre-defined Alert Actions and templates of the same name):

Table 7-1 • Types of Pre-Defined Alert Action Catalog Items

Alert Action Catalog Item / Alert Action	Question Template	Description
Proof of purchase	ProofOfPurchaseTemplate	Administrators can prompt this Alert Action catalog item to generate alerts by targeting it to a specific application in the FlexNet Manager Suite database.
Keep	KeepTemplate	These are used as part of the automatically-generated unused software alert. Users are prompted to either **Keep** or **Uninstall** the unused application.
Uninstall	UninstallationWithNoProgramTemplate	

You can also create your own custom Alert Action catalog items, as described in Administrator-Created Custom Action Alert.

Unused Software Alert

As soon as the **My Apps** feature is enabled, App Portal will automatically send alerts to end users for each installed application that they have not used for a specified number of days. The end user must then choose to either complete a business justification survey to keep the seldom-used software or uninstall that application.

If a user selects **Uninstall**, the application will be uninstalled in one of two ways:

- **Application has an associated uninstall action**—If the application has an associated App Portal catalog item with an uninstall program, App Portal will submit a uninstall message to System Center Configuration Manager or Altiris, which will in turn uninstall the application. The amount of time that this takes depends upon the deployment technology.

- **Application does not have an associated uninstall action**—If application does not have an associated App Portal catalog item with an uninstall program, a General catalog item is checked out, which only registers the user's intent but does not actually trigger the uninstall.

Unused software alerts are only sent for applications belonging to the FlexNet Manager Suite application classifications (such as **Commercial**) that are selected in the App Portal **My Apps Options** settings. If no classifications are selected, then unused software alerts will be sent for applications in all classifications.

For more information, see Customizing an Unused Software Alert.

Proof of Purchase Action Alert

When informed by FlexNet Manager Suite that there are no remaining licenses for an application, administrators can choose to trigger a proof of purchase alert be sent to unlicensed users of that application by modifying the existing **Proof of purchase** Alert Action catalog item to target the identified application. See Triggering a Proof of Purchase Alert.

Administrator-Created Custom Action Alert

An administrator can create a custom alert and attach a question template to it to gather information. This alert can be targeted to specific users. This information is delivered to the administrator via the standard checkout process. See Creating a New Custom Alert Action Catalog Item

📄

Note • *App Portal's extensible application programming interface (API) gives administrators the ability to define and enforce additional policies.*

Triggering a Proof of Purchase Alert

When informed by FlexNet Manager Suite that there are no remaining licenses for an application, administrators can choose to trigger a proof of purchase alert by modifying the existing **Proof of purchase** Alert Action catalog item to target the identified application.

📋

Task   ***To trigger a proof of purchase alert for an application:***

1. On the **Admin** tab, open the **Catalog Management > Catalog > Alert Action Catalog Items** view.

2. In the catalog item list, double-click on **Proof of purchase**. The **Catalog Item Properties** dialog box for the **Proof of purchase** Alert Action catalog item opens.

3. Open the **FlexNet Manager Suite > Alert Action Targets** tab.

4. Use the filter fields in the columns to search the FlexNet Manager Suite database for the application that you want to target.

5.   Select an application and click **Add**. The application is now listed in the **Application** list on the right.

6.   Optionally, set visibility options, as described in Controlling Visibility of a Catalog Item by Adding Conditions.

7.   Save the **Proof of purchase** Alert Action catalog item. App Portal would then generate proof of purchase alerts to be sent to all unlicensed users who have that application installed. To resolve the alert, the user would need provide proof of purchase for the unlicensed software.

Creating a New Custom Alert Action Catalog Item

You can create custom Alert Action catalog items, which can have an attached question template, along with possible visibility and other custom options. When the alert is responded to, that information is delivered to the App Portal administrator via the standard checkout process.

Note • *App Portal's extensible application programming interface (API) gives administrators the ability to define and enforce additional policies.*

Task   **To create a new custom Alert Action catalog item:**

1.   Create questions and a question template to associate with this custom Alert Action catalog item, as described in Managing Questions and Question Templates.

2.   On the **Admin** tab, open **Catalog Management > Catalog > Alert Action Catalog Items** view.

3.   Click **Add New Alert Action Catalog Item**. The **New Catalog Item Wizard** opens.

4. Select **Alert Action Catalog Item** and click **Next**. The **Catalog Item Title and Category** panel opens.

5. Enter a **Title** to identify this Alert Action catalog item.

6. In the **Alert Action Name** field, enter the name of the new alert action that you are creating that will be associated with this Alert Action catalog item. Usually you would enter the same name as the **Title**.

7. Optionally, enter a **Brief Description** of this Alert Action catalog item.

8. Click **Next**. The **Ready to Create** panel opens and lists a summary of the settings you have chosen.

9. Select the **Load advanced view after creating the catalog item** option and then click **Create**. A confirmation message opens stating that catalog item creation was successful.

10. Click **OK**. The **Catalog Item Properties** dialog box for the new action alert catalog item opens.

11. On the **General > Global** tab, select the question template that you prepared from the **Question Template** list.

12. If you want to target this alert to owners of a specific application, open the **FlexNet Manager Suite > Alert Action Targets** tab and perform the following steps:

    a. Use the filter fields in the columns to search the FlexNet Manager Suite database for the application that you want to target.

    b. Select an application and click **Add**. The application is now listed in the **Application** list on the right.

13. Optionally, set visibility options, as described in Controlling Visibility of a Catalog Item by Adding Conditions.

14. Make any additional customizations that you would like to make on the following tabs of the **Catalog Item Properties** dialog box:

    ● Approval Tab

    ● Approval Process Tab

    ● Security Groups Tab

    ● Actions Tab

    ● Notifications Tab

    ● Permissions Tab

15. Save this new Alert Action catalog item. App Portal would then send alerts to the appropriate users.

Customizing an Unused Software Alert

When the **My Apps** feature is enabled, App Portal automatically sends alerts to users for each installed application that they have not used for the number of days specified by the App Portal administrator as the license reclamation threshold. This is an automated process, and there is no associated Alert Action catalog item to generate unused software alerts.

However, to customize unused software alerts, you can make the following modifications:

- **Edit the Keep and Uninstall question templates**—You can change the questions that are asked when the user clicks **Keep** or **Uninstall** by editing the following question templates:

Alert Action Catalog Item	Associated Question Template
Keep	KeepTemplate
Uninstall	UninstallationWithNoProgramTemplate

  For more information, see Managing Questions and Question Templates

- **Change the License Reclamation Threshold property**—To adjust the time period that determine which applications are considered unused, you can change the number of days in the **License Reclamation Threshold**. For more information, see Setting My Apps Tab Options.

- **Modify the classification of applications that are included in unused software alerts**—To control which applications are displayed on the **My Apps** tab—and also which applications receive automatically-generated unused software alerts, you can change the which FlexNet Manager Suite application classifications are displayed. For more information, see Setting My Apps Tab Options.

Converting a General Catalog Item to an Alert Action Catalog Item

You can convert a **General** catalog item to an **Alert Action** catalog item on the **Catalog Management > Catalog > Alert Action** view.

Task ***To convert a General Catalog item to an Alert Action catalog item.***

1. Create a General catalog item, as described in Creating a New Catalog Item Using the Wizard.

2. Open the **General** catalog item in the **Catalog Item Properties** dialog box and open the **FlexNet Manager Suite > Alert Action Targets** tab.

3. Use the filter fields in the columns to search the FlexNet Manager Suite database for the application(s) that you want to target.

4. Select an application and click **Add**. The application is now listed in the **Application** list on the right.

5. Save the **General** catalog item and close the **Catalog Item Properties** dialog box.

6. Open the **Catalog Management > Catalog > Alert Action** view.

7. Double-click the alert action that you want to add to the **General** catalog item. The **Alert Action Properties** dialog box opens.

8. Select the General catalog item from the **General Catalog** list and click **Save**. The General catalog item is now listed on the **Alert Action Catalog Items** view.

Deleting an Alert Action

On the **Catalog Management > Catalog > Alert Action** view, you can delete an alert action and, simultaneously, its associated Alert Action catalog item (if no alerts exist for that Alert Action catalog item).

Task   ***To delete an alert action:***

1. Open the **Catalog Management > Catalog > Alert Action** view.

2. Double-click the alert action that you want to delete. The **Alert Action Properties** dialog box opens.

3.   Click **Delete**. The alert action and its mapped Alert Action catalog item are deleted.

Scheduling My Apps Background Processes

App Portal periodically initiates processes to detect unused software and to send out email notifications. These background processes are scheduled to run using Microsoft Task Scheduler.

Figure 7-5: Microsoft Task Scheduler Listing App Portal Processes

By default the following processes are scheduled to run at 12:00 a.m. each Sunday:

- `App Portal - Process Computers for My Apps Alerts`

- `App Portal - Send out My Apps Email Notifications`

You can adjust when and how often these processes are run using the Microsoft Task Scheduler on your App Portal web server.

Using the Inventory Feature to Perform Compliance Management

App Portal allows tracking of software and computers in use in your company. App Portal will count and link license data directly to the organizational data to allow for detailed reporting on license usage.

This section describes using the App Portal **Inventory** feature to perform compliance management. This feature does not require integration with FlexNet Manager Suite.

- Creating a New Inventory Category

- Adding an Inventory Class

- Adding an Inventory Record

- Configuring an Inventory Item

- License Reclamation Using Inventory Features

Note • If App Portal is connected to FlexNet Manager Suite, these inventory management features will not be displayed.

Creating a New Inventory Category

In the event that your App Portal environment does not have FlexNet Manager Suite, then inventory records can be created in App Portal for each application needing to be discovered for the OSD process.

The following instructions provide the steps to create a new inventory category.

Task   **To create a new inventory category:**

1. On the **Admin** tab, select **Compliance Management** > **Inventory Categories**.

2. Select one of the folders in the tree and then click **Add Category**. You are prompted to enter a category name.

3. In the **New Category Name** box, enter a category name. For example, you could enter the name of a vendor such as `Adobe` or `Microsoft`.

4. Click **Add**. The new inventory category is now listed in the tree.

Adding an Inventory Class

By default, App Portal ships with three standard inventory classes, which are those that are typically expected to be seen and inventoried in a System Center Configuration Manager environment:

●   **Add Remove Programs**

●   **Computer System**

●   **Installed Software**

If you would like to add an inventory class, perform the following steps.

Task   **To add an inventory class:**

1. On the **Admin** tab, select **Compliance Management** > **Inventory Attributes**.

2. In the **Select an inventory class** list, select a new class, such as **Add Remove Programs (64)**. Attributes of that class are listed.

3. Under **Select the attributes you wish to track**, select the desired attributes.

4. Click **Save**. The new inventory class is now available for selection.

Adding an Inventory Record

In the event that your App Portal environment is not integrated with FlexNet Manager Suite, then inventory records can be created in App Portal for each application needing to be discovered for the OSD process.

Note • *If your environment is integrated with FlexNet Manager Suite, you will not be able to create an inventory record in App Portal.*

To add a new inventory record, perform the following steps.

Task   ***To add an inventory item:***

1. On the **Admin** tab, select **Compliance Management > Add Inventory**. The **Add New Inventory** dialog box opens.

2. In the **Logical inventory group name** field, enter a name that will represent the inventory record. The name can be general if you will track multiple versions of a program, or very specific if you are tracking a single instance of a program.

   For example, to track all versions of Visio, use a group name of `Microsoft Visio`. To track a single version, use a name of `Microsoft Visio 2013`.

3. In the **Category** field, select the category of the new inventory item.

   Note • For information on creating an inventory category, see Creating a New Inventory Category.

4. From the **Notification Threshold** list, select the percentage of total inventory that the available count has to drop below before you are alerted. If you only wish to be alerted when there is no more inventory, select **0%**.

5. Select the **Show visual indication of inventory status** option if you wish to see a visual alert of the inventory status: **OK**, **Warning**, or **Critical**.

6. Select the **Send daily inventory summary notifications** option if you wish to include this inventory item in the daily license summary report that is emailed to the License Administrator.

7. Specify an update interval in the **Update Frequency** section. This will set an interval time for when to update the inventory collection in System Center Configuration Manager.

8. Click **Save** when you have completed configured the initial available settings for a new inventory item. After you click **Save**, additional tabs will appear at the top of the Inventory Item Properties dialog box.

9. Continue with the steps in Configuring an Inventory Item.

Configuring an Inventory Item

After a new inventory item is created and saved, three configuration tabs appear at the top of the Inventory Item Properties dialog box: **General**, **Usage**, **Usage Report**.

Figure 7-6: Inventory Item Properties Dialog Box Tabs

To configure an inventory item, perform the following steps.

Task   **To configure an inventory item:**

1. Open the **General > General** tab of an inventory item's **Inventory Item Properties** dialog box.

2. In the **Category** field, specify the category of the inventory item.

> **Note •** *For information on creating an inventory category, see* Creating a New Inventory Category.

3. From the **Notification Threshold** list, select the percentage of total inventory that the available count has to drop below before you are alerted. If you only wish to be alerted when there is no more inventory, select **0%**.

4. Select the **Show visual indication of inventory status** option if you wish to see a visual alert of the inventory status: **OK**, **Warning**, or **Critical**.

5. Select the **Send daily inventory summary notifications** option if you wish to include this inventory item in the daily license summary report that is emailed to the License Administrator.

6. You can optionally use the **Inventory Cost** and **Inventory Count** fields to manually set the cost and license count for an inventory item. Or, if you leave in place the default settings, the cost and license count from purchasing information will automatically be used.

> **Tip •** *To display the cost of an item to the requester on the Browse Catalog tab, you would need to select the* **Show inventory cost to users** *option on the* **General > Inventory** *subtab of the catalog item's Catalog Item Properties dialog box.*

7. Specify an update interval in the **Update Frequency** section to specify how frequently to update the inventory collection in System Center Configuration Manager. You can specify **Manually**, **Monthly**, **Weekly**, **Daily**, or **Every x Hours** (8, 4, 2, or 1). You can also specify the start date and time of the first update.

8. To optionally enter associated information about what the inventory item will be used for, open the **General > Notes** tab and enter a note.

9. Continue with the steps in Specifying Usage Information for an Inventory Item.

Specifying Usage Information for an Inventory Item

The settings that you make on the **Usage** tab of the **Inventory Item Properties** dialog box defines how App Portal determines whether inventory is in use. Installed software is considered in use software. Having the program installed and appearing in Add/Remove Programs for most cases is considered used.

Usage information is read from the System Center Configuration Manager database and updated in the App Portal database.

Important • To determine if the user is actually using the software, you must have a Software Metering rule defined in System Center Configuration Manager.

You configure usage for an inventory item on the **Usage** tab of the **Inventory Item Properties** dialog box. The **Usage** tab includes three subtabs:

● Specifying Inventory Class Information

- Specifying Usage Count Information

- Selecting a Software Metering Rule to Determine Usage

Specifying Inventory Class Information

There are two types of inventory classes the system starts with.

- **Add Remove Program Data**—Uses data reported in Add Remove Programs to determine usage.

- **Hardware Inventory Class Data**—Uses Computer System data to determine usage based on hardware inventory data.

On the **Usage** > **Inventory Class** tab, you can specify what **Inventory Class** of information App Portal will use.

Figure 7-7: Inventory Item Properties Dialog Box / Usage > Inventory Class Tab

The **Usage > Inventory Class** tab includes the following properties:

Table 7-2 • Usage > Inventory Class Tab

Property	Description
Calculation method	Select one of the following options:
	- **Calculate Per Computer**
	- **Calculate Per User**
	- **Manual Entry**

Table 7-2 • Usage > Inventory Class Tab

Property	Description
Class Type	Select one of the following options: • **Use a SCCM Inventory Class** • **Use SCCM Query**
Match method	Select one of the following options: • **Match any item** • **Match all items**
Collection Limiting	You can specify what collection to run this inventory data for.

Specifying Usage Count Information

On the **Usage > Count** tab of the **Inventory Item Properties** dialog box, you can populate the current inventory grid with programs from the **Available Inventory** list. Sort and search the list as necessary to locate all the programs representing the Inventory Group.

Task   ***To add an inventory item attribute:***

1. On the **Inventory Item Properties** dialog box, open the **Usage > Count > Include Rules** tab.

2. Click the **New Inventory Attribute** button. A dialog box opens prompting you to select an **Inventory Class** to search for attributes.

3. Select an item from the drop down list of available **Inventory Classes**:

- **Add Remove Programs**
- **Add Remove Programs (64)**
- **Computer System**
- **Installed Executable**
- **Installed Software**

4. Use the filter boxes to search for an item, select one of the found items, and then click the **Add To Include** button.

📄

---

*Note • In some cases, there could be hundreds of discovered inventory properties or versions of an application. If your criterion returns multiple pages of results, select all on the current page, click **Add to Include**, and then continue to the next page and repeat.*

You will notice the attributes of the item are added to the grid.

5. You can **modify** the inventory attributes by **Clicking Edit** at the end of each attribute.

6. You can also add attributes by adding information from a MSI installation file by clicking the **Add New MSI** button.

7. Enter a UNC path to the MSI file and click **Select**.

Selecting a Software Metering Rule to Determine Usage

On the **Usage > Metering** tab of the Inventory Item Properties dialog box, you can select the software metering rule to determine actual user usage of the program.

Figure 7-8: Inventory Item Properties Dialog Box / Usage > Metering Tab

On the **Metering** tab, you specify the conditions that qualify as NOT being used using a combination of days used, frequency of use, and duration of use.

Task   ***To specify metering conditions:***

1. Select either **Metering Rule** or **Asset Intelligence**.

2. From the **Software Metering** list, select a metering rule that you want to configure.

3. Specify conditions.

4. Once settings are confirmed, click the **Save** button to complete the process.

Viewing a Usage Report for an Inventory Item

You can use the **Usage Report** tab to get a quick glance at the information related to an inventory item. The **Usage Report** tab lists all the systems that the inventory item is detected on. It is a good tool to use to validate if you have configured inventory information and rules correctly.

Figure 7-9: Inventory Item View / Usage Report Tab

License Reclamation Using Inventory Features

*Note • License reclamation can also be performed using App Portal's **My Apps** feature, which requires integration with FlexNet Manager Suite. For more information, see Configuring the My Apps Feature to Perform Compliance Management.*

License reclamation utilizes the ability of System Center Configuration Manager to track and meter program usage data to create an email based campaign to encourage the user to uninstall the software. Using License Reclamation can greatly reduce the license usage of an application by removing the installations, and therefore reclaiming licenses, and saving costs.

The requirements for automatic license reclamation are:

● A System Center Configuration Manager program that uninstalls the software

● A System Center Configuration Manager Software metering rule that tracks the usage data for the program.

When a request is enabled for reclamation, the computers and their associated users are loaded into a database table. The license reclamation process will use this data to track the notification frequency and user response. This data is periodically refreshed to add new records as they fall into scope of the license reclamation settings.

- Viewing Requests Enabled for License Reclamation

- Authorizing Reclamation

Viewing Requests Enabled for License Reclamation

To view requests enabled for license reclamation, perform the following steps:

Task   **To view requests enabled for license reclamation:**

1. On the **Admin** tab, select **Compliance Management > License Reclamation**.

2. Double-click on one of the listed **Catalog Items**. The License Reclamation dialog box for that catalog item opens:

3. View the statistics summary at the top of the dialog box, which indicates the current activity of the license reclamation records.

Item	Description
Total	The total targets in scope for the reclamation.
Active	The count of in progress reclamation actions. Records that have not been responded to and have not expired.
Responded	The count of reclamation actions that have been responded to.
Auto-Reclaimed	The count of reclamation actions that did not receive a response by the end of the reclamation campaign and that were automatically submitted for reclamation (uninstall software).

Item	Description
Inactive	The count of records that are in scope with the reclamation rules but have not been activated for reclamation. This occurs when you choose to verify the reclamation action before beginning the process (Default).
Succeeded	The count of records where the reclamation was initiated and where the uninstall process completed successfully.
Owned	If the request is linked to an inventory group the current owned inventory count is displayed.
Used	If the request is linked to an inventory group the current usage inventory count is displayed.
Owed	If the request is linked to an inventory group and the current license usage is negative, the current cost of the license multiplied by the count of negative licenses is displayed. As the license reclamation process continues, this value ideally will go to zero.

4. View the items in the license reclamation grid, which is where the records and responses to the campaign are tracked.

Item	Description
	The first column allows the selection of the row for an action. The email alert icon denotes that the machine identified for reclamation does not have an associated user and will be unable to send email notifying of the action.
User Columns	Identifies properties of the user and computer
Authorized	Authorized indicates whether the record is authorized to begin sending email notifications. When the license reclamation settings indicate that approval should be given before reclaiming, all records are added as unauthorized.
State	State indicates one of two possible states of a record: ● **Active**—The request is actively pursuing reclamation against the target ● **Paused**—The request is not pursuing reclamation against the target
Email Enabled	Email Enabled indicates whether emails are being sent either to the user or manager
Last Sent	The day and time a reclamation request was last sent to the user
Next Notify	Determines the next date and time that the user will be sent a reclamation email as defined in the request settings.
Response	Indicates whether the user has responded to the reclamation mail
Responded On	The date and time that the user responded to the reclamation mail
Expires	The date and time that the reclamation expires (Duration)

Authorizing Reclamation

Once a record is authorized, the reclamation process begins. The user will begin receiving a template email according to the interval and duration specified in the request. The email is completely customizable under **Site Management > Communication > Notifications > License Reclamation** tab.

Figure 7-10: License Reclamation Tab of Site Management > Communication > Notifications

Within the email template are links that the user can select to complete the request for reclamation.

Figure 7-11: License Reclamation Notification Email

Selecting either the **Uninstall** link or **Keep** link directs the user to the App Portal website. The message displayed is customizable by editing the **License Reclamation - Uninstall Program** notification.

Figure 7-12: Uninstall Confirmation Message

After submitting the request, a final message appears, customizable by editing the **License Reclamation - Uninstall Program - after submit** notification.

Figure 7-13: Final Uninstall Action Message

A new request is created under the My Requests for the uninstall action.

Using Retire and Upgrade Campaigns to Enforce Compliance Management

Note • This feature requires that App Portal is connected to FlexNet Manager Suite via the Flexera Service Gateway.

You can create Upgrade and Retire campaigns that will automatically retire a specified application or upgrade it to a newer version throughout your enterprise. You can use this feature in conjunction with the **My Apps** feature to ensure license compliance.

You configure retire and upgrade campaigns on the new **Retire Campaign** and **Upgrade Campaign** views under **Compliance Management**.

● Using Retire Campaigns to Remove Applications from Your Enterprise

● Using Upgrade Campaigns to Upgrade Applications Throughout Your Enterprise

● Creating Views to Include or Exclude Machines from Upgrade or Retire Campaigns

Using Retire Campaigns to Remove Applications from Your Enterprise

📄

Note • *This feature requires that App Portal is connected to FlexNet Manager Suite via the Flexera Service Gateway.*

You can create a campaign to automatically retire (uninstall) an application that is installed in your enterprise or an application that could be installed in the future. You create retire campaigns on the **Retire Campaign Policies** view, which is opened by selecting **Compliance Management > Retire Campaign**.

To create a retire campaign, perform the following steps.

Task   **To create a retire campaign:**

1. Select **Compliance Management > Retire Campaign**. The **Retire Campaign Policies** view opens.

2. Do one of the following:

    - **To retire an application installed in your enterprise**—To create a campaign to retire an application that is installed in your enterprise, click **Add Discovered Flexera IDs**. The **Add FlexeraID From Applications Discovered in FNMS** view opens, listing all of the applications that have been discovered by FlexNet Manager Suite as being installed in your enterprise.

    - **To retire an application that could be installed in the future**—To create a campaign to retire an application that could be installed in your enterprise in the future, click **Search Flexera ID**. The **Search for FlexeraID** view opens, listing all of the existing applications/versions in the FlexNet Manager Suite database.

3. Locate and select the application(s) that you want to create a retire campaign for and click **Add**. An individual retire campaign is created for each selected application.

4. Click **Back to Campaign** to return to the **Retire Campaign Policies** view. The application that you added is now listed.

5. Click **Configure Policy** in the **Retire Campaign Policy** column of the application. The **Configure Retire Campaign Policy** view opens.

6. On this view, select the **Enable retire campaign** option to enable the retire campaign for this application, which will start the uninstallation process.

7. If you want to notify the user when the uninstallation of the retired software is complete, select the **Notify user** option.

8. Click **Save** to return to the **Retire Campaign Policies** view.

9. To view a list of devices where the selected application is currently installed, click **View Devices**. The Devices view for retire campaigns opens.

All of the devices where this application is installed are listed, along with the **Computer Name**, `Assigned User`, **Last Used Date**, **Discovery Date**, and **Status**.

10. Click **Back to Retire Campaign** to return to the **Retire Campaign Policies** view.

11. To view a list of alerts that have been generated as part of a retire campaign, click **View Alerts**. The **Alerts** view for retire campaigns opens.

The **Computer Name**, **Notification Date**, **Last Used Date**, **Alert Type**, **Is Expired**, **Is Uninstalled**, `Uninstall Message`, and **Uninstall Date** are listed for each alert.

How Uninstallation is Triggered in a Retire Campaign

Once a retire campaign is enabled, the uninstallation process will begin. What happens next depends upon the whether or not the application has an uninstall program associated with it in its deployment technology:

- **With associated uninstall program**—If an uninstall program has been associated with this application in its deployment technology, App Portal will send an uninstall request to the deployment technology.

- **Without associated uninstall program**—If an uninstall program has not been associated with this application in its deployment technology, App Portal will submit a request for that machine for a general catalog item named **Uninstall**, which is available out-of-the-box with App Portal.

Using Upgrade Campaigns to Upgrade Applications Throughout Your Enterprise

Note • This feature requires that App Portal is connected to FlexNet Manager Suite via the Flexera Service Gateway.

You can create a campaign to automatically upgrade an application that is installed in your enterprise or an application that could be installed in the future to an application/version you specify. You create retire campaigns on the **Upgrade Campaign Policies** view, which is opened by selecting **Compliance Management > Upgrade Campaign**.

To create an upgrade campaign, perform the following steps.

Task   *To create an upgrade campaign:*

1. Select **Compliance Management > Upgrade Campaign**. The **Upgrade Campaign Policies** view opens.

2. Do one of the following:

    ● **To upgrade an application installed in your enterprise**—To create a campaign to upgrade an application that is installed in your enterprise, click **Add Discovered Flexera IDs**. The **Add FlexeraID From Applications Discovered in FNMS** view opens, listing all of the applications that have been discovered by FlexNet Manager Suite as being installed in your enterprise.

    ● **To upgrade an application that could be installed in the future**—To create a campaign to upgrade an application that could be installed in your enterprise in the future, click **Search Flexera ID**. The **Search for FlexeraID** view opens, listing all of the existing applications/versions in the FlexNet Manager Suite database.

3. Locate and select the application(s) that you want to create an upgrade campaign for and click **Add**. An individual upgrade campaign is created for each selected application.

4. Click **Back to Campaign** to return to the **Upgrade Campaign Policies** view. The application that you added is now listed.

5. Click **Configure Policy** in the **Upgrade Campaign Policy** column of the application. The **Configure Upgrade Campaign Policy** view opens.

6. Perform a search in the **Applications** list and select an application that users will be upgraded to.

7. Select the **Enable upgrade campaign** option to enforce the campaign.

8. If you want to notify the user when the software upgrade is complete, select the **Notify user** option.

9. Click **Save** to return to the **Upgrade Campaign Policies** view. The application that you selected as the replacement will be listed in the **Upgrade To** column.

10. To view a list of devices where a selected application is currently installed, click **View Devices**. The **Devices** view opens.

All of the devices where this application is installed are listed, along with the **Computer Name**, `Assigned User`, **Last Used Date**, **Discovery Date**, and **Status**.

11. Click **Back to Upgrade Campaign** to return to the **Upgrade Campaign Policies** view.

12. To view a list of alerts that have been generated as part of an upgrade campaign, click **View Alerts**. The **Alerts** view for upgrade campaigns opens.

The **Computer Name**, **Notification Date**, **Last Used Date**, **Alert Type**, **Is Expired**, **Is Installed**, `Install Message`, and **Install Date** are listed for each alert.

About Uninstalling the Original Version of the Application

When an upgrade campaign is enforced, the original application is **not** automatically uninstalled unless:

● The installer of the upgraded version automatically uninstalls the older version, OR

● A supersedence relationship for the application has been configured in System Center Configuration Manager.

Creating Views to Include or Exclude Machines from Upgrade or Retire Campaigns

You can create views that contain a list of machines that can be included or excluded from upgrade or retire campaigns.

Creating Views to Include or Exclude Machines from Upgrade Campaigns

To create views to include or exclude machines from upgrade campaigns, perform the following steps.

Task   ***To create views to include or exclude machines from upgrade campaigns:***

● **Include view**—To define your own data source of machines for upgrade campaigns, create a view named vUpgradeInclude. The following is sample code:

```
CREATE VIEW [dbo].[vUpgradeInclude]
AS
SELECT MachineName, UniqueName
FROM vUserComputerMap
WHERE [condition]
GO
```

● **Exclude view**—To exclude machines for upgrade campaigns, create a view named vUpgradeExclude. The following is sample code:

```
CREATE VIEW [dbo].[vUpgradeExclude]
AS
SELECT MachineName, UniqueName
```

```
FROM vUserComputerMap
WHERE [condition]
GO
```

Important • *If you define a* vUpgradeInclude *view, then do not also define a* vUpgradeExclude *view. The* vUpgradeInclude *view is the exclusive data source of machines for upgrade campaigns; you can define a condition that specifies which machines to exclude within the WHERE clause of this view.*

Creating Views to Include or Exclude Machines from Retire Campaigns

To create views to include or exclude machines from retire campaigns, perform the following steps.

Task ***To create views to include or exclude machines from retire campaigns:***

- **Include view**—To define your own data source of machines for retire campaigns, create a view named vRetireInclude. The following is sample code:

  ```
  CREATE VIEW [dbo].[vRetireInclude]
  AS
  SELECT MachineName, UniqueName
  FROM vUserComputerMap
  WHERE [condition]
  GO
  ```

- **Exclude view**—To exclude machines for retire campaigns, create a view named vRetireExclude. The following is sample code:

  ```
  CREATE VIEW [dbo].[vRetireExclude]
  AS
  SELECT MachineName, UniqueName
  FROM vUserComputerMap
  WHERE [condition]
  GO
  ```

Important • *If you define a* vRetireInclude *view, then do not also define a* vRetireExclude *view. The* vRetireInclude *view is the exclusive data source of machines for retire campaigns; you can define a condition that specifies which machines to exclude within the WHERE clause of this view.*

Compliance Management Reference

You configure App Portal's compliance and license reclamation features on the **Compliance Management** views, which are opened by selecting one of the nodes under **Compliance Management** on the **Admin** tab.

Under **Compliance Management**, the following nodes are listed:

- My Apps

- Retire Campaign

- Upgrade Campaign

My Apps

On the App Portal **My Apps** tab, users can view a list of applications installed on their devices, and address automatic and administrator-defined alerts to ensure that those applications comply with corporate software policies. This assists IT administrators in driving continual software license reclamation and optimization.

To specify which applications in your enterprise will be subject to license reclamation (uninstallation), you need to add those applications to the My Apps License Reclamation Policies list, which is opened by selecting **Compliance Management > My Apps**.

When adding applications to the **My Apps License Reclamation Policies** list, you can add applications based upon those applications discovered in FlexNet Manager Suite, based upon licenses in FlexNet Manager Suite, or by searching for a specific Flexera ID.

- My Apps License Reclamation Policies

- Add Flexera ID Lists

*Important • To use the My Apps feature, the App Portal system account must have read access to the FlexNet Manager Suite database, which is specified on the **FlexNet Manager Suite Database Connection Settings** area of the **Site Management > Settings > Flexera Integration** view.*

My Apps License Reclamation Policies

On the App Portal **My Apps** tab, users can view a list of applications installed on their devices, and address automatic and administrator-defined alerts to ensure that those applications comply with corporate software policies. This assists IT administrators in driving continual software license reclamation and optimization.

To specify which applications in your enterprise you want to target for license reclamation (uninstallation), you need to add those applications to the **My Apps License Reclamation Policies** list, which is opened by selecting **Compliance Management > My Apps**.

When adding applications to this list, you can select from a list of applications with identified Flexera IDs or those that have a license created in FlexNet Manager Suite. You can also choose to search the entire Application Recognition Library for an application to add.

Figure 7-14: My Apps License Reclamation Policies

The **My Apps License Reclamation Policies** view includes the following properties:

Table 7-3 • My Apps License Reclamation Policies View

Property	Description
Product	Name of application.
Classification	Identifies application as belonging to one of the following FlexNet Manager Suite classifications:

* **Beta**—Pre-release application (such as beta releases, alpha releases, or release candidates).

* **Component**—Item is used/installed as a component of another application or suite, and is not licensed as a standalone item.

* **Commercial**—Requires a license to be purchased for use in a commercial setting.

* **Freeware**—Licensed for use in a commercial setting free of charge.

* **Malware**—Application is considered to be potentially harmful (such as a virus or a Trojan horse).

* **Shareware**—Application is available for download from Internet shareware sites, and typically uses a "try-before-you-buy" licensing model.

* **Update**—Application represents an update (such as a service pack) to another application, issued free to all customers regardless of purchasing agreements or support contracts (a "minor" update).

* **X Rated**—Application potentially contains objectionable or sexually explicit material.

Property	Description
Version	Version number of application.

Table 7-3 • My Apps License Reclamation Policies View

Property	Description
Flexera ID	A unique code assigned to applications by FlexNet Manager Suite that is used to link application information from FlexNet Manager Suite with application information in App Portal, and with other Flexera Software applications.
Publisher	Manufacturer of application.
Edition	Edition description of application, if any.
Threshold	Number of days the application has to be unused before an unused software alert is triggered.
Has Uninstall Program	If an uninstall program has been associated with this application in its deployment technology, **Yes** will be listed. If it does not have an associated uninstall program, **No** will be listed.
Enabled?	
Per License Cost ($)	
Policy	License Reclamation Policy. Click **Configure** to open the Configure License Reclamation Policy view for that application, where you can set license reclamation policy options.
Exclusion Conditions	Clicking the **Edit** link to view a list of all license reclamation campaign conditions which have been sent out for this application or click **Add** to add a new campaign condition. The **License Reclamation Campaign Conditions** pop-up appears. See License Reclamation Campaign Conditions.
Targeted Devices	Click **View** to view the Devices (My Apps) view, a list of the devices where this application is currently installed.
Alerts	Click **View Alerts** to view the Devices (My Apps) view, a list of alerts that have been generated for this application.
Add Discovered Flexera IDs	Click to view a list of all applications in the enterprise that have a Flexera ID identified.
Add Flexera ID from Licenses	Click to view a list of all applications in the enterprise that have a license created in FlexNet Manager Suite.
Search Flexera ID	Click to search all applications in the FlexNet Manager Suite Application Recognition Library.

Configure License Reclamation Policy

After you add an application to the **My Apps License Reclamation Policies** list, which means that the application is targeted for reclamation, you have the option of setting configuration options by clicking the **Configure Policy** link in the **License Reclamation Policy** column for that application.

Figure 7-15: Configure License Reclamation Policy View

The **Configure License Reclamation Policy** view includes the following properties:

Table 7-4 • Configure License Reclamation Policy View

Properties	Description
Application	Name of application.
Flexera ID	Flexera ID of application.
Enable License Reclamation Policy	Select this option to enable license reclamation for this application. Clear the selection to disable the license reclamation policy.
License Reclamation Threshold	Specify the number of days that this application has to be unused to trigger a reclamation action. This can be set to 0 or any other positive integer number. When the value is set to 0, the Global threshold value is used.

Table 7-4 • Configure License Reclamation Policy View

Properties	Description
Allow users to uninstall unused software	If you want to prompt users to uninstall their unused software by displaying an unused software alert message on their **My Apps** tab, select this option. If this option is selected, you have three additional options: ● **Automatically uninstall software if the user has not responded to the notification within *n* days**—If the user does not respond to the unused software alert within the number of days you specify, the application will be automatically uninstalled. ● **Uninstall unused software even when there is no associated user for the device**—If App Portal detects unused software on a device that does not have an associated user (meaning that there is no one to respond to an unused software alert message), uninstall the application. ● **Automatically expire notification if the unused software at time of notification is later reported as used**—If this option is selected, and the user uses the software that they have an unused software alert message about, cancel the unused software alert message. If this option is not selected, the alert message would still be in effect even if a user uses software that was reported as unused.
Automatically uninstall unused software without any user intervention	If you want to automatically uninstall unused software without any user intervention, select this option. As soon as the license reclamation threshold is reached, this application will be automatically uninstalled without prompting the user. If you select this option, you have one additional option: ● **Notify user once the uninstallation of unused software is complete**—If you select this option, users will receive a notification email when one of their unused applications is automatically uninstalled. If this option is not selected, the user will not be notified.

Devices (My Apps)

After you add an application to the **My Apps License Reclamation Target Policies** list, which means that the application is targeted for reclamation, you have the option of viewing a list of all devices where this application is installed by clicking the **View Devices** link in the **Devices** column for that application.

Figure 7-16: Devices View

All of the devices where this application is installed are listed, along with the **Computer Name**, `Assigned User`, **Last Used Date**, **Discovery Date**, **Status, Processed, Uninstalled,** and **Is eligible for Alerts?**.

Note the following:

- The **Processed** column indicates whether the device is already processed or not.

- The **Uninstalled** column indicates whether the particular software is uninstalled from the device or not. This value depends on the Processed column: if the device is already processed then the value of this column will be either True or False. Otherwise it will not be applicable.

- The **Is eligible for Alerts?** column provides a link with **Yes/No** values and indicates whether the device is eligible for processing the alerts or not based on the conditions defined for that campaign. Clicking this link opens an Evaluating condition for <application name> on <device> pop-up with detailed information on eligibility as shown following:

Alerts (My Apps)

After you add an application to the **My Apps License Reclamation Policies** list, which means that the application is targeted for reclamation, you can view a list of all alerts which have been sent out for this application by clicking the **View Alerts** link in the **Alerts** column for that application.

Figure 7-17: Alerts View

Add Flexera ID Lists

To specify which applications in your enterprise will be subject to license reclamation (uninstallation), you need to specifically add those applications to the **My Apps License Reclamation Policies** list, which is opened by selecting **Compliance Management > My Apps** on the **Admin** tab. To add an application to this list, click one of the buttons in the toolbar:

Figure 7-18: Buttons to Add Applications to Reclamation Target List

You have several options when adding applications to the **My Apps License Reclamation Policies** view, depending upon which button you click:

- **Add Discovered Flexera IDs**—Click to view a list of all applications in the enterprise that have a Flexera ID identified. A list entitled *Add Flexera ID From Applications Discovered in FNMS* opens.

- **Add Flexera ID From Licenses**—Click to view a list of all applications in the enterprise that have a license created in FlexNet Manager Suite. A list entitled *Add Flexera ID From Licenses in FNMS* opens.

- **Search Flexera ID**—Click to search all applications in the FlexNet Manager Suite Application Recognition Library. A list entitled *Search for Flexera ID* opens.

All of these lists of applications have the same information displayed; they just are listing a different set of applications.

Figure 7-19: Add Flexera ID From Applications Discovered in FNMS

The application lists that open when adding applications to the **My Apps License Reclamation Policies** view include the following properties:

Table 7-5 • Add Flexera IDs Lists

Property	Description
Product	Name of application.
Version	Version number of application.
Classification	Identifies application as belonging to one of the following FlexNet Manager Suite classifications: • **Beta**—Pre-release application (such as beta releases, alpha releases, or release candidates). • **Component**—Item is used/installed as a component of another application or suite, and is not licensed as a standalone item. • **Commercial**—Requires a license to be purchased for use in a commercial setting. • **Freeware**—Licensed for use in a commercial setting free of charge. • **Malware**—Application is considered to be potentially harmful (such as a virus or a Trojan horse). • **Shareware**—Application is available for download from Internet shareware sites, and typically uses a "try-before-you-buy" licensing model. • **Update**—Application represents an update (such as a service pack) to another application, issued free to all customers regardless of purchasing agreements or support contracts (a "minor" update). • **X Rated**—Application potentially contains objectionable or sexually explicit material.
Flexera ID	A unique code assigned to applications by FlexNet Manager Suite that is used to link application information from FlexNet Manager Suite with application information in App Portal, and with other Flexera Software applications.
Edition	Edition description of application, if any.
Publisher	Manufacturer of application.

To add an application to the **My Apps License Reclamation Policies** list, use the column filters to locate the application you want to add and select its check box, and then click the **Add** button. The application is added to the **My Apps License Reclamation Policies** list.

Note • If there is no check box next to an application's name, it means that the item has already been added to the reclamation list.

Note • Hold down the Ctrl button to select more than one application at a time.

License Reclamation Campaign Conditions

After you add an application to the **My Apps License Reclamation Policies** list, which means that the application is targeted for reclamation, you can view a list of all license reclamation campaign conditions which have been sent out for this application by clicking the **Edit** link in the **Exclusion Conditions** column for that application or you can add a new campaign condition by clicking the **Add** link.

Figure 7-20: License Reclamation Campaign Conditions

The fields are described:

Property/Tabs	Description
Group and OU, AD Property, and Collections tabs	Use to create conditions—based on Active Directory Groups or OUs, Active Directory properties, and collections—that will force the **MyApps** process to evaluate user/device eligibility to process reclamation. See Add Condition Dialog Box.
Add Condition	If you click **Add Condition** on the **Group and OU**, **AD Property**, or **Collections** subtabs of the **License Reclamation Campaign Conditions** dialog box the **Add Condition** dialog box opens. See Add Condition Dialog Box.
Remove Condition	Select the checkbox of a condition and then click **Remove Condition** to remove that condition from the campaign.
Save	Saves the current pop-up settings.
Apply to OU and child OUs	Select this check box to apply this condition to all of the OU's child OUs. If this option is not selected, this condition is not applied to the selected OU's child OUs.

Retire Campaign

You can create a campaign to automatically retire (uninstall) an application that is installed in your enterprise or an application that could be installed in the future. You create retire campaigns on the **Retire Campaign Policies** view, which is opened by selecting **Compliance Management > Retire Campaign**.

When configuring a retire campaign, you use the following views:

- Retire Campaign Policies

- Add FlexeraID From Applications Discovered in FNMS

- Search for Flexera ID

- Configure Retire Campaign Policy

- Devices (Retire Campaign)

- Alerts (Retire Campaign)

Retire Campaign Policies

Existing retire campaigns are listed on the **Retire Campaign Policies** view. From this view, you can create a new retire campaign, configure a retire campaign, view the devices associated with a retire campaign, and view alerts associated with a retire campaign.

Figure 7-21: Retire Campaign Policies

The Retire Campaign Policies view includes the following properties.

Table 7-6 • Retire Campaign Policies View

Property	Description
Product	Name of selected application.
Classification	Category of selected application in FlexNet Manager Suite as being: Freeware, Component, etc.
Version	Version of selected application.
Flexera ID	Flexera ID of selected application.
Publisher	Publisher of selected application.

Table 7-6 • Retire Campaign Policies View

Property	Description
Edition	Edition of selected application.
Has Uninstall Program	Identifies whether or not a uninstallation program is associated with the application in its deployment technology.
Enabled?	Indicates whether or not the campaign has been enabled (by selecting the **Enable retire campaign** option on the Configure Retire Campaign Policy view).
Policy	Click **Configure** to open the Configure Retire Campaign Policy view for the application.
Exclusion Condition	Clicking the **Edit** link to view a list of all retire campaign conditions which have been sent out for this application or click **Add** to add a new retire campaign condition. The Retire Campaign Conditions pop-up appears.
Targeted Devices	Click **Devices** to open the Devices (Retire Campaign) view for the application.
Alerts	Click **Alerts** to open the Alerts (Retire Campaign) view for the application.
Add Discovered Flexera IDs	Click to create a campaign to retire an application that is installed in your enterprise. The Add FlexeraID From Applications Discovered in FNMS view opens, listing all of the applications that have been discovered by FlexNet Manager Suite as being installed in your enterprise.
Search Flexera IDs	Click to create a campaign to retire an application that could be installed in your enterprise in the future. The Search for Flexera ID view opens, listing listing all of the existing applications/versions in the FlexNet Manager Suite database.
Delete	Click to delete the selected application's retire campaign.

Add FlexeraID From Applications Discovered in FNMS

To create a campaign to retire an application that is installed in your enterprise, click **Add Discovered Flexera IDs**. on the Retire Campaign Policies view. The **Add FlexeraID From Applications Discovered in FNMS** view opens, listing all of the applications that have been discovered by FlexNet Manager Suite as being installed in your enterprise.

Figure 7-22: Add FlexeraID From Applications Discovered in FNMS View

For each application, the **Product**, **Version**, **Classification**, **FlexeraID**, **Edition**, and **Publisher** are listed. Use the filters to locate the application that you want to add to the retire campaign and then click **Add**.

Click **Back to Campaign** to return to the Retire Campaign Policies view.

Search for Flexera ID

To create a campaign to retire an application that could be installed in your enterprise in the future, click **Search Flexera ID**. The **Search for FlexeraID** view opens, listing all of the existing applications/versions in the FlexNet Manager Suite database.

Figure 7-23: Add FlexeraID From Applications Discovered in FNMS View

For each application, the **Product**, **Version**, **Classification**, **FlexeraID**, **Edition**, and **Publisher** are listed. Use the filters to locate the application that you want to add to the retire campaign and then click **Add**.

Click `Back to Campaign` to return to the Retire Campaign Policies view.

Configure Retire Campaign Policy

You can configure retire campaign policies on the **Configure Retire Campaign Policy** view, which is opened by clicking **Configure Policy** in the **Retire Campaign Policy** column on the Retire Campaign Policies view.

Figure 7-24: Configure Retire Campaign Policy View

On the **Configure Retire Campaign Policy** view, select the **Enable retire campaign** option to enable the retire campaign for this application, which will start the uninstallation process.

If you want to notify the user when the uninstallation of the retired software is complete, select the **Notify user** option.

Click **Save** to return to the **Retire Campaign Policies** view.

Devices (Retire Campaign)

The **Devices** view lists all devices where the selected application is currently installed. You open the **Devices** view by clicking **View Devices** on the Retire Campaign Policies view.

Figure 7-25: Devices View for Retire Campaign

All of the devices where this application is installed are listed, along with the **Computer Name**, `Assigned User`, **Last Used Date**, **Discovery Date**, **Status, Processed, Uninstalled,** and **Is eligible for Alerts?**.

Note the following:

● The **Processed** column indicates whether the device is already processed or not.

● The **Uninstalled** column indicates whether the particular software is uninstalled from the device or not. This value depends on the Processed column: if the device is already processed then the value of this column will be either True or False. Otherwise it will not be applicable.

- The **Is eligible for Alerts?** column provides a link with **Yes/No** values and indicates whether the device is eligible for processing the alerts or not based on the conditions defined for that campaign. Clicking this link opens an Evaluating condition for <application name> on <device> pop-up with detailed information on eligibility as shown following:

Alerts (Retire Campaign)

The **Alerts** view lists all alerts that have been generated as part of the selected retire campaign. You open the **Alerts** view by clicking **View Alerts** on the Retire Campaign Policies view.

Figure 7-26: Alerts View for Retire Campaign

For each alert, the **Computer Name**, **Notification Date**, **Last Used Date**, **Alert Type**, **Is Expired**, **Is Unisntalled**, **Uninstall Message**, and **Uninstall Date** are listed.

Retire Campaign Conditions

After you add an application to the **Retire Campaign Policies** list, which means that the application is targeted for retiring, you can view a list of all retire campaign conditions which have been sent out for this application by clicking the **Edit** link in the **Exclusion Conditions** column for that application or you can add a new campaign condition by clicking the **Add** link. The **Retire Campaign Conditions** pop-up appears.

Figure 7-27: Retire Campaign Conditions

The following table describes the properties and tabs:

Property/Tabs	Description
Group and OU, AD Property, and Collections tabs	Use to create conditions—based on Active Directory Groups or OUs, Active Directory properties, and collections—that will force requests for the catalog item to go through an approval process. See Add Condition Dialog Box.
Add Condition	If you click **Add Condition** on the **Group and OU**, **AD Property**, or **Collections** subtabs of the **License Reclamation Campaign Conditions** dialog box the **Add Condition** dialog box opens. For more information see Add Condition Dialog Box.
Remove Condition	Select the checkbox of a condition and then click **Remove Condition** to remove that condition from the campaign.
Save	Saves the current pop-up settings.
Apply to OU and child OUs	Select this check box to apply this condition to all of the OU's child OUs. If this option is not selected, this condition is not applied to the selected OU's child OUs.

Upgrade Campaign

You can create a campaign to automatically upgrade an application that is installed in your enterprise or an application that could be installed in the future to an application/version you specify. You create retire campaigns on the **Upgrade Campaign Policies** view, which is opened by selecting **Compliance Management > Upgrade Campaign**.

When configuring an upgrade campaign, you use the following views:

● Upgrade Campaign Policies

- Add FlexeraID From Applications Discovered in FNMS

- Search for Flexera ID

- Configure Upgrade Campaign Policy

- Devices (Upgrade Campaign)

- Alerts (Upgrade Campaign)

Upgrade Campaign Policies

Existing upgrade campaigns are listed on the **Upgrade Campaign Policies** view. From this view, you can create a new upgrade campaign, configure an upgrade campaign, view the devices associated with an upgrade campaign, and view alerts associated with an upgrade campaign.

Figure 7-28: Upgrade Campaign Policies

The **Upgrade Campaign Policies** view includes the following properties.

Table 7-7 • Upgrade Campaign Policies View

Property	Description
Product	Name of selected application.
Classification	Category of selected application in FlexNet Manager Suite as being: Freeware, Component, etc.
Version	Version of selected application.
Flexera ID	Flexera ID of selected application.
Publisher	Publisher of selected application.
Edition	Edition of selected application.
Upgrade To	Lists the application that this application will be upgraded to.
Enabled?	Indicates whether or not the campaign has been enabled (by selecting the **Enable upgrade campaign** option on the Configure Upgrade Campaign Policy view).
Policy	Click **Configure** to open the Configure Upgrade Campaign Policy view for the application.

Table 7-7 • Upgrade Campaign Policies View

Property	Description
Exclusion Condition	Clicking the **Edit** link to view a list of all upgrade campaign conditions which have been sent out for this application or click **Add** to add a new upgrade campaign condition. The **Upgrade Campaign Conditions** pop-up appears.
Targeted Devices	Click **Devices** to open the Devices (Upgrade Campaign) view for the application.
Alerts	Click **Alerts** to open the Alerts (Upgrade Campaign) view for the application.
Add Discovered Flexera IDs	Click to create a campaign to upgrade an application that is installed in your enterprise. The Add FlexeraID From Applications Discovered in FNMS view opens, listing all of the applications that have been discovered by FlexNet Manager Suite as being installed in your enterprise.
Search Flexera IDs	Click to create a campaign to upgrade an application that could be installed in your enterprise in the future. The Search for Flexera ID view opens, listing all of the existing applications/versions in the FlexNet Manager Suite database.
Delete	Click to delete the selected application's upgrade campaign.

Add FlexeraID From Applications Discovered in FNMS

To create a campaign to upgrade an application that is installed in your enterprise, click **Add Discovered Flexera IDs**. on the Upgrade Campaign Policies view. The **Add FlexeraID From Applications Discovered in FNMS** view opens, listing all of the applications that have been discovered by FlexNet Manager Suite as being installed in your enterprise.

Figure 7-29: Add FlexeraID From Applications Discovered in FNMS View

For each application, the **Product**, **Version**, **Classification**, **FlexeraID**, **Edition**, and **Publisher** are listed. Use the filters to locate the application that you want to add to the upgrade campaign and then click **Add**.

Click `Back to Campaign` to return to the Upgrade Campaign Policies view.

Search for Flexera ID

To create a campaign to upgrade an application that could be installed in your enterprise in the future, click **Search Flexera ID** on the Upgrade Campaign Policies view. The **Search for FlexeraID** view opens, listing all of the existing applications/versions in the FlexNet Manager Suite database.

Figure 7-30: Add FlexeraID From Applications Discovered in FNMS View

For each application, the **Product**, **Version**, **Classification**, **FlexeraID**, **Edition**, and **Publisher** are listed. Use the filters to locate the application that you want to add to the upgrade campaign and then click **Add**.

Click `Back to Campaign` to return to the Upgrade Campaign Policies view.

Configure Upgrade Campaign Policy

You can configure upgrade campaign policies on the **Configure Upgrade Campaign Policy** view, which is opened by clicking **Configure Policy** in the **Upgrade Campaign Policy** column on the Upgrade Campaign Policies view.

Figure 7-31: Configure Upgrade Policy View

On the **Configure Upgrade Campaign Policy** view, perform a search in the **Applications** list and select an application that users will be upgraded to.

Select the **Enable upgrade campaign** option to enforce the campaign.

If you want to notify the user when the software upgrade is complete, select the **Notify user** option.

Click **Save** to return to the Upgrade Campaign Policies view. The application that you selected as the replacement will be listed in the **Upgrade To** column.

Devices (Upgrade Campaign)

The **Devices** view lists all devices where the selected application is currently installed. You open the **Devices** view by clicking **View Devices** on the Upgrade Campaign Policies view.

Figure 7-32: Devices View for Upgrade Campaign

All of the devices where this application is installed are listed, along with the **Computer Name**, `Assigned User`, **Last Used Date**, **Discovery Date**, **Status, Processed, Uninstalled,** and **Is eligible for Alerts?**.

Note the following:

- The **Processed** column indicates whether the device is already processed or not.

- The **Uninstalled** column indicates whether the particular software is uninstalled from the device or not. This value depends on the Processed column: if the device is already processed then the value of this column will be either True or False. Otherwise it will not be applicable.

- The **Is eligible for Alerts?** column provides a link with **Yes/No** values and indicates whether the device is eligible for processing the alerts or not based on the conditions defined for that campaign. Clicking this link opens an Evaluating condition for <application name> on <device> pop-up with detailed information on eligibility as shown following:

Alerts (Upgrade Campaign)

The **Alerts** view lists all alerts that have been generated as part of the selected upgrade campaign. You open the **Alerts** view by clicking **View Alerts** on the Upgrade Campaign Policies view.

Figure 7-33: Alerts View for Retire Campaign

For each alert, the **Computer Name**, **Notification Date**, **Last Used Date**, **Alert Type**, **Is Expired**, **Is Installed**, **Install Message**, and **Install Date** are listed.

Upgrade Campaign Conditions

After you add an application to the **Upgrade Campaign Policies** list, which means that the application is targeted for an upgrade, you can view a list of all upgrade campaign conditions which have been sent out for this application by clicking the **Edit** link in the **Exclusion Conditions** column for that application or you can add a new upgrade campaign condition by clicking the **Add** link. The **Upgrade Campaign Conditions** pop-up appears.

Figure 7-34: Retire Campaign Conditions

The following table describes the properties and tabs:

Property/Tabs	Description
Group and OU, AD Property, and Collections tabs	Use to create conditions—based on Active Directory Groups or OUs, Active Directory properties, and collections—that will force requests for the catalog item to go through an approval process. See Add Condition Dialog Box.
Add Condition	If you click **Add Condition** on the **Group and OU**, **AD Property**, or **Collections** subtabs of the **Upgrade Campaign Conditions** dialog box the **Add Condition** dialog box opens. For more information see Add Condition Dialog Box.
Remove Condition	Select the checkbox of a condition and then click **Remove Condition** to remove that condition from the campaign.
Save	Saves the current pop-up settings.
Apply to OU and child OUs	Select this check box to apply this condition to all of the OU's child OUs. If this option is not selected, this condition is not applied to the selected OU's child OUs.

8

Using Task Sequence Catalog Items to Perform OS and Application Deployment

App Portal provides solutions to greatly reduce the operational overhead experienced by traditional OS deployment solutions and to enhance the end-user experience, making OS deployments self-service instead of administrator-driven.

With App Portal you can deliver new computer imaging, existing computer re-imaging, and replacement of computers through your enterprise app store by leveraging core OSD functionality in Microsoft System Center Configuration Manager. Users initiate the migration/deployment by requesting a catalog item in the enterprise app store, scheduling the deployment around a time that is convenient for them. Users can easily migrate existing applications to the new system, and also have the option of installing additional applications during OS deployment. Users can also request task sequence catalog items to migrate existing applications and/or install additional applications to a computer, without performing an OS deployment or upgrade.

Information about performing operating system deployment by offering task sequence catalog items in the App Portal storefront is presented in the following sections:

Table 8-1 • Using App Portal to Perform Operating System Deployments

Section	Description
Overview of App Portal Support for Operating System Deployment	Explains how App Portal can manage typical components of OS deployments and enhance Microsoft's OS deployment solution.
Configuring App Portal Global Settings for OS Deployment	Lists the global settings you have to configure in App Portal to perform catalog item OS deployment using your App Portal storefront.
Configuring System Center Configuration Manager Task Sequences	Describes the two additional steps, Install Packages and Install Applications, that need to be included in a System Center Configuration Manager task sequence in order to support App Portal OS imaging.
Creating OSD Task Sequence Catalog Items	Takes you step-by-step through the creation of an App Portal OSD task sequence catalog item, including describing all available options.
Using Roles to Identify Applications to Deploy with a Task Sequence Catalog Item	Explains how to use roles (which can be applied conditionally) to identify groups of applications that can be deployed with OSD task sequence catalog items.

Table 8-1 • Using App Portal to Perform Operating System Deployments (cont.)

Section	Description
Configuring the Migration/ Installation of Applications During OS Deployment	Explains how to enable application options, designate applications as "core", making them ineligible for migration, and how to specify upgraded or replacement applications.
Using User Readiness and Constraints to Schedule OS Deployments	Explains how to use user readiness records to schedule an OS deployment with a user, and how to use constraints to limit scheduling possibilities for catalog items.
Requesting an OSD Task Sequence Catalog Item	Explains how to request an OSD task sequence catalog item to perform the following types of OS deployments: ● Deploying an OS on a new computer. ● Upgrading the OS of an existing computer. ● Installing an OS on a new computer and migrating applications from an existing computer (side-by-side migration).
OS Deployment Reference	This section contains information on the views and dialog boxes under the **Deployment Management** node that are used to perform operating system deployment by offering task sequence catalog items in the App Portal storefront: **Roles**, **Constraints**, **User Readiness**, and **Install Sequence**.

📄

Note • *For information about performing OS and application deployment using methods other than by offering OSD task sequence catalog items in the App Portal storefront, see Using App Survey, Clone/Migrate, and Support Tools to Perform Advanced Deployment Tasks.*

Overview of App Portal Support for Operating System Deployment

You can use System Center Configuration Manager's operating system deployment feature to create operating system images, and then use App Portal to perform self-service deployment of those images to target computers.

The following topics provide an overview of App Portal's support for performing operating system deployments.

● Types of OS Deployments Supported by App Portal

● Overview of Steps to Take to Set Up OS Deployment

Types of OS Deployments Supported by App Portal

App Portal enables you to make OS deployments self-service instead of administrator-driven. App Portal end users can initiate an OS deployment by checking out a catalog item in the App Portal storefront. App Portal supports the following OS deployment types:

Table 8-2 • Types of OS Deployments Supported by App Portal

OS Deployment Type	Description
Deploy OS on New Computer (Bare-Metal Install)	In this scenario, your OS corporate image is deployed for the first time to a new computer. Since this machine is new to your organization, no user data or applications need to be captured or migrated. For more information, see Deploying an OS on a New Computer.
Upgrade OS of Existing Computer (In-Place Migration)	In this scenario, the operating system of an existing computer in your organization is upgraded. The existing user data and applications are captured prior to the OS upgrade, and then later restored to the machine after the OS upgrade has been completed. For more information, see Upgrading the OS of an Existing Computer.
Replace Computer (Side-by-Side Migration)	In this scenario, user data and applications are migrated from an existing system to the replacement system, which will be imaged with the selected operating system. For more information, see Performing a Side-By-Side Migration from a Source to a Target Computer.

In all of these scenarios, if the installation of additional applications is enabled, you also have the option of selecting additional applications to install during deployment. All software catalog items that are available for installation on the target system would be listed on the **Choose Additional Applications to Install During an OS Deployment** panel of the Checkout Wizard. For more information, see Global vs. Catalog Item Level Settings for Migrating or Installing New Applications During OS Deployment.

Overview of Steps to Take to Set Up OS Deployment

To get started using App Portal to perform automated OS deployments via the App Portal storefront, you need to perform the following steps.

Table 8-3 • Steps to Configure OS Deployment in App Portal

Step	Description
Step 1: **Configuring App Portal Global Settings for OS Deployment**	First, specify which of the multiple deployment technologies that App Portal is connected to contains your task sequences, and then specify global OSD settings for that selected deployment technology.

Table 8-3 • Steps to Configure OS Deployment in App Portal

Step	Description
Step 2: **Configuring System Center Configuration Manager Task Sequences**	To support App Portal OS imaging, System Center Configuration Manager task sequences must exist and they must includes these two steps: Install Packages and Install Applications.
Step 3: **Creating OSD Task Sequence Catalog Items**	Once System Center Configuration Manager task sequences exist, you are ready to create OSD task sequence catalog items that will appear in your App Portal storefront.
Step 4: **Using Roles to Identify Applications to Deploy with a Task Sequence Catalog Item**	You can, optionally, create roles (which can be applied conditionally) to define groups of applications. If you then associate a role with a task sequence catalog item, it will be used to determine which applications will be deployed with OSD task sequence catalog items.
Step 5: **Configuring the Migration/Installation of Applications During OS Deployment**	You may want to use these various features to specify which applications are migrated/installed during the deployment of an OS task sequence catalog item: • Identifying Existing Applications to Include in OS Deployment • Prevent a Catalog Item from Being Included in OS Deployment By Designating it as Core Application • Specifying the Sequence of Catalog Item Installation During OS Deployment • Using Upgrade/Replacement to Identify New/Replacement Versions
Step 6: **Using User Readiness and Constraints to Schedule OS Deployments**	You can use App Portal's **User Readiness** and **Constraints** features to schedule users for OS deployment and to limit the number of users that can request and schedule an OS deployment at the same time.

Configuring App Portal Global Settings for OS Deployment

Before you can use App Portal OSD task sequence catalog items to perform OS deployment, the App Portal site must be configured to support OS deployment.

• Specifying the Default OS Deployment Technology

• Specifying Global OS Deployment Settings

Specifying the Default OS Deployment Technology

App Portal supports connections to multiple deployment technologies simultaneously, including Microsoft System Center Configuration Manager (ConfigMgr), and Microsoft System Center 2012 Configuration Manager.

However, before you can use OSD task sequence catalog items to perform OS deployment, you need to specify which of these deployment technologies contains your task sequences.

Task   ***To specify the default OS deployment technology:***

1.   On the **Admin** tab, open the **Common** tab of the **Site Management > Settings > Deployment** view.

2.   From the **Inventory / OS Deployment** list, select the deployment technology that you want App Portal to use to perform OS deployments and to read inventory data.

Specifying Global OS Deployment Settings

After you have specified a default OS deployment technology, as described in Specifying the Default OS Deployment Technology, you need to also specify global OS deployment settings for that deployment technology on the **OS Deployment** tab of the **Site Management > Settings > Deployment** view.

Figure 8-1: OS Deployment Tab of Site Management > Settings > Deployment View

On the **OS Deployment** tab, you can specify the following types of global settings:

- **Application migration**—You can enable the migration of existing installed applications from the source machine to the target machine (when performing either a computer upgrade or when performing a side-by-side migration). You can also specify whether to enable the requester to either migrate all existing applications or only those that they select during checkout.

- **Installation of additional applications**—You can select an option to enable the requester to select additional applications to install during OS deployment.

- **OSD site server settings**—You need to provide settings specific to the default OS deployment technology that you selected, as described in Specifying the Default OS Deployment Technology.

To specify global App Portal site settings for OS deployment, perform the following steps.

Task   ***To specify global App Portal site settings for OS deployment:***

1. On the **Admin** tab, open the **OS Deployment** tab of the **Site Management > Settings > Deployment** view.

2. If you want to give requesters the ability to migrate existing applications from the source computer to the target computer during OS deployment, select the **Enable application migration and installation of additional applications** option. If this option is selected, the Choose Existing Applications to Migrate Panel will be displayed during the checkout of an OSD task sequence catalog item (if the **Auto detect installed apps** option on the **Deployment > Roles** tab of the **Catalog Item Properties** dialog box of the task sequence catalog item is also selected).

   Also, when the **Enable application migration and installation of additional applications** option is selected, the following suboptions are enabled:

   ● **Enable requester to specify which existing applications to migrate**

   ● **Prompt requester to select additional applications to install**

   Important • *This feature requires either a connection to FlexNet Manager Suite or the creation of App Portal inventory records for each application needing to be discovered for the OSD process and then associating that inventory record with its associated software catalog item. For more information, see Identifying Existing Applications Using FlexNet Manager Suite or Identifying Existing Applications by Creating App Portal Application Inventory Records.*

3. If you want to give requesters the ability to specify which existing applications to migrate by making selections on the **Choose Existing Applications to Migrate** panel of the Checkout Wizard, select the **Enable requester to specify which existing applications to migrate** option.

- **If this option is selected**, when the **Choose Existing Applications to Migrate** panel of the Checkout Wizard is displayed, the requester will be able to select which of the applications on the existing computer will be migrated to the target computer.

- **If this option is not selected**, all applications on the existing computer will automatically be selected and the requester will be unable to deselect them.

> *Note • To enable this option, you must first select the **Enable application migration and installation of additional applications** option.*

> *Note • You can prevent an application from being listed on the **Choose Existing Applications to Migrate** panel. See Prevent a Catalog Item from Being Included in OS Deployment By Designating it as Core Application.*

4. If you wish to give requesters the ability to select additional applications to install during OS deployment, select the **Prompt requester to select additional applications to install** option.

If this option is selected, the Choose Additional Applications to Install During OS Deployment Panel of the Checkout Wizard will be displayed during the checkout of an OSD task sequence catalog item.

> *Note • To enable this option, you must first select the **Enable application migration and installation of additional applications** option.*

> *Note • You can prevent an application from being listed on the **Choose Additional Applications to Install During OS Deployment** panel. See Prevent a Catalog Item from Being Included in OS Deployment By Designating it as Core Application.*

5.   Specify the following the settings specific to the default OS deployment technology that you selected in Specifying the
     Default OS Deployment Technology.

Property	Description
Path to inboxes	Specify the path to the System Center Configuration Manager In Boxes, such as: `\\FLEXDCCM\sms_flx\inboxes\` This path is used to transfer the Discovery Data Record (DDR) for user and computer discovery, when the new computer is created during a "bare metal" scenario. **Important •** *Specify the path to the same System Center Configuration Manager technology you selected in the* **Inventory / OS Deployment** *field on the* **Site Management > Settings > Deployment > Common** *tab.* **Note •** *When System Center Configuration Manager runs a discovery, it creates DDRs. The information contained in a DDR varies depending upon the discovered resource. For example, it can include the NetBIOS name of a computer, the IP address and IP subnet of a computer or device, and the computer operating system name.*
Default OSD site server	Choose the System Center Configuration Manager site where new computer objects will be imported when using bare metal OS deployment.
Default OSD time zone	Enter the default time zone for new computers imported into System Center Configuration Manager as a part of an OS deployment. For example, enter **-6** to indicate that the time zone is 6 hours behind Coordinated Universal Time (UTC), the world's time standard.
Store OSD packages as computer variables	If you select this option, when applications are targeted to an OS deployment, the applications will be stored on the computer object as variables. This allows for the MDT process to automatically install the applications without any further customizations. If you do not select this option, you will need to obtain the applications using SQL or web service calls.
Base application variable name	This base variable will be used to deploy applications as part of the **Install Applications** step in a System Center Configuration Manager OSD task sequences. It should match the value specified in the **Install Applications** task sequence step exactly. The variable name and value will be appended to the variables list of the System Center Configuration Manager object. The default value is `COALESCEDAPPS`.
Base package variable name	This base variable will be used to deploy packages as part of the **Install Software** step in a System Center Configuration Manager OSD task sequence. It should match the value specified in the **Install Software** task sequence step exactly. The variable name and value will be appended to the variables list of the System Center Configuration Manager Computer object. The default value is `PACKAGES`.

Property	Description
Coalesce digits for OSD variable (applications)	This setting, which works in conjunction with the **Base application variable name** COALESCEDAPPS, is used during OS deployment when App Portal writes applications that need to be migrated as computer variables. This value sets the number of digits used in variable names. For example: • If this field is set to **2** and App Portal has to write three applications, then the variables App Portal would write would be COALESCEDAPPS01, COALESCEDAPPS02, COALESCEDAPPS03. • If this field is set to **3** and App Portal has to write three applications, then the variables App Portal would write would be COALESCEDAPPS001, COALESCEDAPPS002, COALESCEDAPPS003. ...and so forth.
Coalesce digits for OSD variable (packages)	This setting, which works in conjunction with the **Base package variable name** PACKAGES, is used during OS deployment when App Portal writes packages that need to be migrated as computer variables. This value sets the number of digits used in variable names. For example: • If this field is set to **2** and App Portal has to write three packages, then the variables App Portal would write would be PACKAGES01, PACKAGES02, PACKAGES03. • If this field is set to **3** and App Portal has to write three packages, then the variables App Portal would write would be PACKAGES001, PACKAGES002, PACKAGES003. ...and so forth.
Use single task sequence for capture and deployment	Determines whether both the source and target computers are inserted into the same collection for side-by-side migrations. *Important • If this option is used, you must properly configure your task sequence to perform only specific steps based on computer variable values. Failure to do so can result in the source computer being reimaged!*
Overwrite existing resources for computer import	You could select this option to overwrite existing resources for computer import. However, for operating system deployments, leave this option unselected.
Task sequence collection cleanup status IDs	Identifies the status IDs that would cause the removal of a computer from the task sequence collections. The use case is that the computer is not removed from the collection at an early enough stage to prevent the task sequence from rerunning after the computer is rebooted. *Note • You also need to select the **Remove from collection when complete?** option on the **Deployment > Global** tab of the Catalog Properties dialog box.*

6. Click **Save**.

Configuring System Center Configuration Manager Task Sequences

A task sequence is a mechanism used in System Center Configuration Manager for performing multiple steps or tasks on a client computer at the command-line level without requiring user intervention. Task sequences are used by System Center Configuration Manager to deploy operating systems.

A System Center Configuration Manager task sequence manages the following key components of a typical OS deployment:

- **Base image**—The base image, or WIM (Windows Imaging Format), is the base operating system image that will be used for deployment.

- **Device drivers**—Most enterprises support more than one hardware type. Device drivers are typically included in a task sequence to apply the correct drivers for each supported hardware type.

- **Base configuration**—The base configuration refers to basic settings, or configurations, applied during the task sequence process. An example would be enabling Microsoft BitLocker to the device receiving the image.

- **Standard applications**—Standard applications are applications that are applied to every OS build. These can be configured as part of the task sequence.

To support App Portal OS imaging, the task sequence must includes these two additional steps:

- **Install Packages**

- **Install Applications**

Both the **Install Packages** and **Install Applications** steps should be configured to install according to a dynamic list. The base variable name used should match the base variable names set on the App Portal site settings.

To add a step to an existing System Center Configuration Manager task sequence, perform the following steps.

Task

To add a step to a System Center Configuration Manager task sequence:

1. In the System Center Configuration Manager console, click **Software Library**.

2. In the **Software Library** workspace, expand **Operating Systems**, and then click **Task Sequences**.

3. Either open an existing task sequence for editing or click **Create Task Sequence** to open the **Create Task Sequence Wizard**.

4. Follow the steps in the *How to Create Task Sequences* topic on the Microsoft TechNet site to add both an **Install Packages** and **Install Applications** step to the task sequence:

   https://technet.microsoft.com/en-us/library/hh273490.aspx#BKMK_CreateTaskSequence

Creating OSD Task Sequence Catalog Items

After you have created task sequences in System Center Configuration Manager and have specified global App Portal OSD settings, as described in Configuring App Portal Global Settings for OS Deployment, you are ready to create OSD task sequence catalog items.

To create an App Portal task sequence catalog item to be used to request an operating system deployment, perform the following steps.

Task   ***To create a task sequence catalog item:***

1. Under **Catalog Management**, select **New Catalog Item Wizard**. The **Catalog Item Type** panel of the **New Catalog Item Wizard** opens.

2. Select **Task Sequence** and click **Next**. The **SCCM 2012 / ConfigMgr Task Sequences** panel opens.

3. Select the System Center Configuration Manager task sequence that you want to associate with this catalog item.

4. Select the **Is OS Deployment?** option below the list.

5. Click **Next**. The **Catalog Item Title and Category** panel opens.

6. In the **Title** field, enter a title to identify this catalog item in your App Portal storefront. By default, the name of the task sequence that you selected is listed in this field.

7. From the **Category** field, select a category to specify this catalog item's location in the App Portal catalog. You are required to select at least one category, but you may select more than one.

8. In the **Brief Description** field, enter the text that you want to display under the catalog item **Title** in the App Portal storefront.

9. By default, a generic icon is associated with this catalog item. To associate a custom icon to this catalog item, click **Change** to open the **Image Selection** dialog box and select a `.gif`, `.jpg`, or `.png` icon file.

Tip • *For best results, the uploaded image should be 80 px by 80 px or larger.*

10. Optionally, from the **Template** list, select an existing template to apply advanced settings to this catalog item.

11. When you are finished editing the fields on the **Catalog Item Title and Category** panel, click **Next**. The **SCCM 2012/ConfigMgr Task Sequence Deployment Settings** dialog box opens.

12. Specify the following deployment settings:

Property	Description
Make the advertisement mandatory	Select this option to make this task sequence a mandatory installation for all clients of the associated advertised group.
Mandatory over slow links?	Select this option to require that the installation is run even when a client has a slow connection. If this option is not selected, the SCCM client agent will not perform the installation if the client has a slow connection, but will perform the installation if the client is connected over a regular LAN connection.
Advertisement Priority	Specify the priority of the advertisement: **High**, **Medium**, or **Low**.
Ignore maintenance windows	Select to have the advertised program ignore maintenance windows while the program is running.
Allow system restart outside of maintenance windows	Select to allow the advertised program to restart the client even if the restart would occur outside of a maintenance window.
Show the task sequence progress	Select to make the task sequence progress bar visible to users.
Make this task sequence available to boot media and PXE	Select to make the advertisement available to boot media and PXE clients.

Property	Description
Program rerun behavior	Specifies whether the advertised program will be rerun on the client computer if it has previously been run before the scheduled mandatory time. Select one of the following options: ● **Never rerun advertised program**—The program will not be rerun on the client if the program has previously been run on the client, even if the program originally failed or the program files have been changed. ● **Always rerun**—The program will always be rerun on the client when the advertisement is scheduled, even if the program has already been successfully run. ● **Rerun if failed previous attempt**—The program will be rerun when the advertisement is scheduled only if it failed on the previous run attempt. ● **Rerun if succeeded on previous attempt**—The program will be rerun only if it has previously run successfully on the client. *Important • This option is only enabled if **Make the advertisement mandatory** is also selected.*
Download options	Select one of the following options to specify how content will be downloaded from the distribution points when a distribution point is available locally: ● **Download content locally when needed by running task sequence** ● **Download all contents locally before starting task sequence** ● **Access content directly from a distribution point when needed by the running task sequence**
When no local distribution point is available, use a remote distribution point	Select this option to specify that when no distribution point is available locally, run the program directly from a remote distribution point.
When no protected distribution point is available, use an unprotected distribution point	Select this option to permit a client to use an unprotected distribution point if content is not immediately available on its protected distribution point. If this option is not selected, the client will not use unprotected distribution points.

13. Click **Next**. The **Ready to Create** panel opens.

14. Select the **Load advanced view after creating the catalog item** option.

15. Review the summary information and then click **Create** to create this new catalog item. The **General > Global** tab of the **Catalog Item Properties** dialog box opens.

16. In the **Request options** area, select the **Enable request on behalf?** option so that a requester (who has the **Request on Behalf** permission) can request this task sequence catalog item for another person or device.

17. In the **Request options** area, select the **Enable unknown computer deployment (OSD only)?** option to enable deployment of this task sequence catalog item to unknown computers.

18. If you want to control which users are permitted to request this OSD catalog item, select the **Require User Readiness record?** option, and define user readiness records as described in Using User Readiness Records to Schedule Users for OS Deployment.

*Note • User Readiness is only applicable if the requester selects the **Reimage my computer (MACHINENAME) with a new Operating System** or **Build an unknown computer and migrate my data from MACHINENAME to the new computer** options on the **Choose Target** panel of the Checkout Wizard. User Readiness is not applicable if the requester selects the **Image a new computer or existing computer** option.*

19. If you want to use constraints to limit the scheduling possibilities for this catalog item, select the **Enable scheduling constraints?** option, and define those constraints as described in Using Constraints to Limit Scheduling Possibilities for Catalog Items.

20. Open the **Deployment > Global** tab.

21. On the **Deployment > Global** tab, select the following options:

- **Apply Computer Variables (Task Sequence)?**—Select this option so that the variable specified in the **Base application variable name** field on the **Site Management > Settings > Deployment > OS Deployment** tab will be used to deploy applications as part of the **Install Applications** step in an SCCM OSD Task Sequence.

- **Remove Variables after successful OS Deployment?**—Select this option to remove variables from the task sequence environment after a successful OS deployment.

22. Open the **Deployment > Roles** tab and specify roles, as described in Using Roles to Identify Applications to Deploy with a Task Sequence Catalog Item.

23. Specify any other catalog item properties that you desire, as described in Creating Catalog Items.

24. Click **Save**.

Using Roles to Identify Applications to Deploy with a Task Sequence Catalog Item

You can use roles to manage software deployments. Roles are a grouping of applications, computer variables, and/ or User State Migration Tool (USMT) profiles that App Portal can apply conditionally during the imaging process.

- **Role types**—Roles can contain applications (such as System Center Configuration Manager applications or packages), System Center Configuration Manager task sequence variables, or Microsoft User State Migration Tool (USMT) profiles that are used to transfer data and settings. You can use roles to sort applications in an organized manner, such as by business unit, during the imaging process.

- **Conditions**—You can apply roles conditionally using an Active Directory (AD) security group or Organizational Unit (OU), AD property, or System Center Configuration Manager Collection.

If a role is associated with a task sequence catalog item, when a requester checks out that catalog item, they will be prompted to select a role to specify the applications that will be installed along with the new operating system. For example, you could create roles to identify the applications used by members of each of your departments (Sales, Marketing, Engineering, Finance, etc.). Then when that catalog item is checked out, the requester will be prompted to select the role of the department that they belong to.

- About Roles and Conditions

- Role Based Scenarios

- Creating Roles

- Associating a Role with a Task Sequence Catalog Item

Note • Roles are used exclusively for the OS deployment (OSD) process in System Center Configuration Manager. The App Portal's Roles feature is not available for Symantec Endpoint Management (Altiris). For grouping applications together in an organized fashion outside of the System Center Configuration Manager OSD process, see Creating a Group Catalog Item.

About Roles and Conditions

You can use roles to manage software deployments. A role is a logical container that you can use to apply and or group software applications, tasks, settings and/or functions. In a role, you can assign dynamic conditions directly to a catalog item that will enable that role to detect its deployment target.

- Role Types

- Role Conditions

- How Roles Work

Role Types

There are three role types:

- **Applications**—On the **Applications** tab of the **Role Properties** dialog box, you can apply a single or grouped and sorted lists of software applications to roles.

- **Computer variables**—On the **Variables** tab of the **Role Properties** dialog box, you can apply standard OSD/MDT variables and the population of those values—either hard set or passed as tokens from SS native data—to a role. You can also apply custom variables and the population of those values—either hard set or passed as tokens from SS native data—to a role.

- **USMT profiles**—On the **USMT Profiles** tab of the **Role Properties** dialog box, you can apply USMT profiles. Using user profile migration integration with USMT (Microsoft User State Migration Tool) enables both admin and user-controlled Scan State and Load State configuration profiles to be applied to roles, which are then passed to computer variables for use by a task sequence.

The three role types can be used in combination or separately in any way you choose on the same role or multiple roles that might apply to the same conditional criteria. For instance, you might have a separate role for each type to be applied based on the same or different conditions.

Role Conditions

On the **Conditions** tab of the **Role Properties** dialog box, you can define role conditions to enable roles to be applied to a user or computer automatically based on the criteria of the condition.

For example, if a user is a member of the Active Directory OU "HR", or if a user or their system is a member of a collection, you might have a role that automatically targets a set of applications to them that you have defined in the role.

There are three condition types:

- Active Directory Groups and OUs

- Active Directory Properties

- SCCM Collections

How Roles Work

Roles do not rely on identifying applications present on a source or destination computer. Instead, applications and packages are written to the destination computer object on the **Variables** tab. These variables are used during the System Center Configuration Manager task sequence process for the **Install Package** and **Install Application** steps.

The following are the steps explaining how roles are detected and assigned during the imaging process:

- **Create role**—You create a role in App Portal.

- **Enable role for catalog item**—You enable a role for an App Portal task sequence catalog item.

- **Role is evaluated during checkout**—During the App Portal checkout process, the role is evaluated.

- **Roles are applied to the computer object as variables**—Any roles that are detected for the user or computer are applied to the computer object within System Center Configuration Manager as variables.

- **Variables are evaluated by task sequence**—The variables are evaluated by the task sequence and used where defined within the task sequence process.

Role Based Scenarios

You can get very creative using role based task management and the scenarios mentioned in this section are just a few of the many ways to use them.

The following table lists some role-based scenarios applied to various deployment types.

Table 8-4 • Role-Based Scenarios

Scenario	Description
Scenario #1 **OS and Application Deployment**	A role has three application packages assigned to it and the role is assigned to a Windows 7 OS deployment task sequence package catalog item in App Portal. The applications assigned to the role will be applied as part of the OS deployment.
Scenario #2 **Application Deployment Only – Assigned Direct**	A role has three application packages assigned to it. That role is then assigned to a generic task-sequence-based catalog item and will apply those applications to the system.
Scenario #3 **Application Deployment Only – Assigned by Condition**	A role has three application packages assigned to it. That role is assigned to a task-sequence-based catalog item, but only applies if a condition is met such as the user is a member of a certain AD OU.

Table 8-4 • Role-Based Scenarios (cont.)

Scenario	Description
Scenario #4 **Profile Migration**	A role is configured for profile migration with USMT. You can configure a role to migrate user profiles with USMT by intelligently detecting the user details to migrate based on role conditions.
Scenario #5 **Two-Step System Migration**	**Step 1: Deploy OS First** Role 1 applies computer variables as part of OS imaging deployment and is deployed first. **Step 2: Migrate User Applications Second** Role 2 migrates a user's applications, and installs a role-based set of department applications to the system. This is a very handy scenario in large enterprise sites, where they may purchase hundreds of new computers at a time. ● **Step 1**—The systems go to a depot where they are pre-built and have the company image deployed to them. ● **Step 2**—Next, a system is allocated to a user at a location and delivered with a base build. The user logs in and visits App Portal and requests to be provisioned. ● **Step 3**—The user's prior software applications and department applications (role based), plus their profiles get provisioned and migrated to their new system.
Scenario #6 **OS Deployment, Application Deployment and User Profile Migration All in One**	You have flexibility to use role types and conditions in virtually any combination, as well as configure multiple roles that apply to the same user or system based on the condition configured.

Creating Roles

You can use roles to manage software deployments. A role is a logical container that you can use to apply and or group software applications, tasks, settings and/or functions. In a role, you can assign dynamic conditions directly to a catalog item that will enable that role to detect its deployment target.

The following topics explain how to create roles in App Portal.

● Creating a New Role

● Adding Role Conditions

● Specifying Computer Variables

● Setting USMT Profiles

Creating a New Role

You can use roles to manage software deployments. A role is a logical container that you can use to apply and or group software applications, tasks, settings and/or functions. In a role, you can assign dynamic conditions directly to a catalog item that will enable that role to detect its deployment target.

Perform the following steps to create a new role.

Task   ***To create a new role based on OU membership:***

1. On the **Admin** menu, expand the **Deployment Management** node and select **Roles**. You should see a listing of existing roles, if there are any defined.

Role	Condition Count	Variable Count	Application Count	USMT Configured
Enginering	0	0	3	No
Sales Department	0	0	2	No
Service Desk	2	0	1	No

2. Click the **New Role** button. The **Create New Role** dialog box opens.

3. On the **General** tab, enter a name in the **Application Role Name** field, to describe this role.

4. In the **Application Role Description** field, enter a description for the role.

5. Click the **Save Role** button.

6. Open the **Applications** tab.

📄

Note • If a catalog item has been designated as a core application, as described in Prevent a Catalog Item from Being Included in OS Deployment By Designating it as Core Application, *that catalog item will not be returned in search results when performing a search on the* **Applications** *tab.*

7. Use the **Search Catalog Items** box to locate catalog items to add to the role. Select a catalog item and then click the right arrow button to move it from the **Available Catalog Items** list to the **Current Catalog Items** list, adding the catalog item to the role.

8. Click **Save Role** to create the new role. You will notice the following tabs become available for you to further configure the role properties: **Conditions**, **Variables**, and **USMT Profiles**.

9. Proceed with the following steps to perform additional configuration of this role:

   - Adding Role Conditions

   - Specifying Computer Variables

   - Setting USMT Profiles

Adding Role Conditions

You can apply roles conditionally using Active Directory (AD) security group or Organizational Unit (OU), Active Directory property, or System Center Configuration Manager collection. Roles can also be configured to be selected rather than be applied conditionally.

The following topics explain how to add role conditions to OSD task sequence catalog items.

- Adding Role Conditions Based on Security Group Membership

- Adding Role Conditions Based on an Active Directory Property

- Adding Role Conditions Based on Collections

Adding Role Conditions Based on Security Group Membership

You can apply role conditions to apply include or exclude conditions to a role based on security group membership (AD group membership or OU container).

Task   ***To add role conditions based on security group membership:***

1. Perform the steps in Creating a New Role.

2. Open the **Conditions** tab of the **Role Properties** dialog box. The **Group and OU** subtab opens.

3. Click **Add Condition**. The **Add Condition** dialog box opens.

4. Set the search focus to one of the following:

   - **To search for AD groups**, leave the search focus set to **Search Groups**.

- **To search for OUs**, set the search focus to **Search OUs**.

5. In the condition search box, enter the name of the group, such as **Admin**.

6. Click **Search**. Search results are listed.

7. Select the desired OU, such as **Administrators**.

8. Click the **Select** button.

9. Close the search window. On the **Conditions > Group and OU** tab, you now have an entry for a security group.

10. From the **Enforcement** list, select **Include** or **Exclude**.

11. If desired, select the **Apply to OU and child OUs** option.

12. Click **Save Role**.

Adding Role Conditions Based on an Active Directory Property

You can add an include or exclude role condition based on an Active Directory property.

Task   ***To create a new role based on Active Directory property:***

1. Perform the steps in Creating a New Role.

2. Open the **Conditions** tab of the **Role Properties** dialog box. The **Group and OU** subtab opens.

3. Open the **AD Property** tab.

4. Click **Add Condition**. The **Conditions** dialog box opens.

5. Select an AD property from the first list, such as **Department**.

6. In the **Search** field, enter a search term, such as **Sales**.

7. Click **Search**.

8. Select item(s) in the search results list,

9. Select either **Include Properties** or **Exclude Properties**.

10. Click **Select**.

11. Close the **Add Conditions** dialog box. On the **Conditions > AD Property** tab, the selected properties are listed.

12. In the **Operator** column, select one of the following options to configure this condition:

- **Equal To**
- **Greater Than**
- **Less Than**
- **Contains**
- **Starts With**
- **Ends With**

13. In the **Enforcement** column, select either **Include Property** or **Exclude Property**.

14. If desired, select the **Apply to OU and child OUs** option.

15. Click **Save Role**.

Adding Role Conditions Based on Collections

You can add an include or exclude role condition based on System Center Configuration Manager collections.

Task   ***To create a new role based on collections:***

1. Perform the steps in Creating a New Role.

2. Open the **Conditions** tab of the **Role Properties** dialog box. The **Group and OU** subtab opens.

3. Open the **Collections** tab.

Note • *You can create two types of "collection" conditions: user collections and machine collections. However, when defining a condition on a role, App Portal only supports user collection conditions. This is because roles are associated with the users, not with machines.*

4. Click **Add Condition**. The **Add Condition** dialog box for collections opens.

5. In the **Enter a collection name** search box, enter a word or phrase.

6.   Click **Search**. Search results are displayed.

7.   Select item(s) in the search results list.

8.   Select either **Include Collections** or **Exclude Collections** from the list.

9.   Click **Select**.

10.   Close the **Add Condition** dialog box. On the **Collections** tab, the selected collection names are now listed.

11.   In the **Enforcement** column, select either **Include Property** or **Exclude Property**.

12.   Click **Save Role**.

Specifying Computer Variables

On the **Variables** tab of the **Role Properties** dialog box, you can specify variables that can be used by the task sequence process that delivers the applications specified in this role.

Task   ***To specify computer variables for a role:***

1.   Perform the steps in Creating a New Role.

2.   Open the **Variables** tab of the **Role Properties** dialog box.

3. Click the **Add Variable** button. The **Variable Properties** dialog box opens, prompting you to do one of the following:

- Select or enter an MDT variable value from the **Select or enter a variable name** list:

- Select or enter an App Portal variable value from the **Select or enter the variables Value** list:

4. You also have the option to select to mask a variable's value by selecting the **Mask variable value** option.

5.   From the **Apply these variables** list, select whether to apply the variable to the **Source**, **Target**, or **Both**.

6.   Use the **Apply to build type** list to specify under which conditions you apply the variable: **Not Specified**, **Bare Metal Build**, **In-Place Migration**, or **Side-by-Side Migration**.

7.   Click **Add Variable**. A message appears stating that the variable was updated successfully.

8.   Close the **Variable Properties** dialog box. The new variable is now listed on the **Variables** tab.

Setting USMT Profiles

User state migration refers to the process of transferring user persona information and settings between using the Microsoft User State Migration Tool (USMT), a command line utility program. You can configure a role in App Portal to migrate user profiles with USMT by intelligently detecting the user details to migrate based on role conditions.

On the **USMT Profiles** tab of the **Role Properties** dialog box, you can define the USMT parameters to be used during the scan state tasks on the source computer and load state tasks on the destination computer during the System Center Configuration Manager OSD process.

To create a new role for managing USMT settings, perform the following steps.

Task   ***To create a new role for managing USMT settings:***

1.   Perform the steps in Creating a New Role.

2.   Open the **USMT Profiles** tab. The **Scan State** subtab of the **User Profiles** tab opens.

3. For **Scan State Options**, select one of the following options:

    ● **Migrate All Profiles**—Select this option to migrate all USMT profiles to target machine. If you select this option, you can also enter **Additional Scan State Arguments** that will be used during the scan state step in the System Center Configuration Manager task sequence. If you select this option, skip to Step 10.

    ● **Identify Profiles for Migration**—Select this option if you want to specify the USMT profiles that you want to migrate to the target machine. If you select this option, continue with Step 4.

4. If **Identify Profiles for Migration** is selected, the following additional fields are displayed:

5. Select one of the following options to identify the profiles:

- **Migrate any users who are currently logged on and any users whose profiles have been loaded**—Pass to the System Center Configuration Manager task sequence scan state step the options to capture the users who are currently logged on, as well as any users whose profiles have been loaded.

- **Migrate last logon / top console user**—Pass to the System Center Configuration Manager task sequence scan state step the options to capture only the last logon and top console (primary console) user.

- **Migrate users whom logged in within the last x days**—Pass to the System Center Configuration Manager task sequence the options to capture the user state for users who have logged in during the last (x) days during the scan state step. Enabling this option displays the **Select num** text box, where you can supply the number of days to be used for the calculation.

- **Migrate users whom logged in since [specified date]**—Pass to the System Center Configuration Manager task sequence scan state step the options to capture the user state for users who have logged in since a specified date. Enabling this option adds a date field that you can use to select the date to be used for the calculation.

6. If you want to exclude local profiles from the scan state step in the System Center Configuration Manager task sequence, select the **Exclude Local Profiles** option.

7. If you want to exclude user persona information from identified domains during the scan state step in the System Center Configuration Manager task sequence, enter domain names in the **Exclude profiles from the following domains** box.

8. If you want scan state arguments to be used during the scan state step in the System Center Configuration Manager task sequence, enter those arguments in the **Dynamic Scan State Arguments** field.

9. If you want additional scan state arguments to be used during the scan state step in the System Center Configuration Manager task sequence, enter those arguments in the **Additional Scan State Arguments** field.

10. Click **Save Role**.

11. Open the **Load State** subtab.

12. Select one of the following options:

- **Restore All Profiles**—Select this option to restore all USMT profiles to the destination computer. If you select this option, you can also enter **Additional Load State Arguments** that will be used during the load state step in the System Center Configuration Manager task sequence. If you select this option, skip to Step 20.

- **Identify Profiles for Restore**—Select this option if you want to specify the USMT profiles that you want to restore to the destination computer. If you select this option, continue with Step 13.

13. If the **Identify Profiles for Restore** option is selected, additional fields are displayed.

14. Select one of the following options to identify the profiles:

- **Restore any users who are currently logged on and any users whose profiles have been loaded**—Pass to the System Center Configuration Manager task sequence load state step the options to capture the users who are currently logged on, as well as any users whose profiles have been loaded.

- **Restore last logon / top console user**—Pass to the System Center Configuration Manager task sequence load state step the options to capture only the last logon and top console (primary console) user.

- **Restore users who logged in within the last x days**—Pass to the System Center Configuration Manager task sequence the options to capture the user state for users who have logged in during the last (x) days during the load state step. Enabling this option displays the **Select num** text box, where you can supply the number of days to be used for the calculation.

- **Restore users who logged in since [specified date]**—Pass to the System Center Configuration Manager task sequence load state step the options to capture the user state for users who have logged in since a specified date. Enabling this option adds a date field that you can use to select the date to be used for the calculation**.**

15. If you want to exclude local profiles from the load state step in the System Center Configuration Manager task sequence, select the **Exclude Local Profiles** option.

16. If you want to exclude user persona information from identified domains during the load state step in the System Center Configuration Manager task sequence, enter domain names in the **Exclude profiles from the following domains** box.

17. If you want to move profiles from one domain to another during the load state process, select the **Move Domains** option, and then enter both the **Old Domain** name and **New Domain** name.

18. If you want load state arguments to be used during the load state step in the System Center Configuration Manager task sequence, enter those arguments in the **Dynamic Load State Arguments** field.

19. If you want additional load state arguments to be used during the load state step in the System Center Configuration Manager task sequence, enter those arguments in the **Additional Load State Arguments** field.

20. Click **Save Role**.

Associating a Role with a Task Sequence Catalog Item

To associate a role with a **Task Sequence** catalog item, perform the following steps:

Task   ***To associate a role with a task sequence catalog item:***

1. Create roles, as described in Using Roles to Identify Applications to Deploy with a Task Sequence Catalog Item.

2. Open the **Deployment > Roles** tab of the **Catalog Item Properties** dialog box for the task sequence catalog item.

On the left pane of the **Application Roles** list, all available roles that are not currently assigned to the task sequence are listed.

> **Note •** *If you are editing a **Software** or **General** catalog item (instead of a **Task Sequence** catalog item), the **Deployment > Roles** tab will not appear.*

3. Do one of the following:

- **If you want to automatically add roles based on the conditions defined on the roles**—Clear the selection of the **Allow user role selection** option, and select the **Auto detect roles from role conditions** and **from inventory groups** options.

   Note • Do not select any roles. Roles will be detected during checkout based on the role conditions specified on the **Conditions** *tab of the* **Role Properties** *dialog box.*

- **If you want the requester to be prompted to select roles**—Select the **Allow user role selection** option and make sure that the **Auto detect roles from role conditions** and **from inventory groups** options are not selected. Then select the role or roles that you would like to assign to this task sequence catalog item and use the arrow button to move them into the right pane.

   If you select a role here, whenever a catalog item is selected that has a linked role for checkout, during the checkout process the role, this role (in this case the **Engineering Role**) will apply and install any accompanying applications assigned in the role as part of the initial request.

   Note • You can apply multiple roles to the same task sequence. The logic for each role will be applied and determined based on the criteria you specified.

4. Click **Save**

Configuring the Migration/Installation of Applications During OS Deployment

The following topics explain how to configure the migration/installation of applications during the deployment of an OSD task sequence catalog item:

Table 8-5 • Configuring the Migration/Installation of Applications During OS Deployment

Topic	Description
Global vs. Catalog Item Level Settings for Migrating or Installing New Applications During OS Deployment	Explains how to specify whether or not a requester is prompted to select existing applications to migrate and/or new applications to install during the checkout of an OS deployment task sequence catalog item by setting both global and catalog item settings.

Table 8-5 • Configuring the Migration/Installation of Applications During OS Deployment

Topic	Description
Identifying Existing Applications to Include in OS Deployment	In order to migrate applications from an existing user's computer to a target computer, you need App Portal to determine which applications are installed on the user's current system. This requires using either a connection to FlexNet Manager Suite or the creation of App Portal Inventory records.
Prevent a Catalog Item from Being Included in OS Deployment By Designating it as Core Application	This section explains how to prevent an application from being available for migration/installation during the deployment of an OSD task sequence catalog item.
Specifying the Sequence of Catalog Item Installation During OS Deployment	This section explains how to specify the order that applications are installed during OS deployment.
Using Upgrade/Replacement to Identify New/Replacement Versions	Instead of migrating an application during OSD task sequence catalog item deployment, you can specify that an application be upgraded to a new or different application.

Global vs. Catalog Item Level Settings for Migrating or Installing New Applications During OS Deployment

To determine whether or not a requester is prompted to select existing applications to migrate and/or new applications to install during the checkout of an OS deployment task sequence catalog item, you must specify both global settings and settings on the individual task sequence catalog item.

- Global OS Deployment Settings

- OSD Task Sequence Catalog Item Settings

- Configuring the Display of Application Migration/Installation Panels

Global OS Deployment Settings

The global settings pertaining to application migration and installation of additional applications during an OS deployment that was initiated by checking out a task sequence catalog item are set on the **Site Management > Settings > Deployment > OS Deployment** tab.

Figure 8-2: Application Migration / Installation of Additional Application Settings for OS Deployment

The following table describes the global settings that pertain to application migration and installation of additional applications during OS deployment.

Table 8-6 • OS Deployment Application Migration / Installation of New Applications Global Settings

Property	Description
Enable application migration and installation of additional applications	Select this option to enable a requester to select existing applications to migrate and additional applications to install during the checkout of an OSD task sequence catalog item.
	If this option is selected, the Choose Existing Applications to Migrate Panel of the Checkout Wizard will be displayed during the checkout of an OSD task sequence catalog item.
	Also, if this option is selected, applications will be listed in the **Applications Included** column of the roles table on the **Choose Roles** panel. If this option is not selected, this column will be empty; only the names of the roles will be listed.
	*Note • In order for the **Choose Existing Applications to Migrate** panel of the Checkout Wizard to be displayed, the **Auto detect installed apps** option on the **Deployment > Roles** tab of the **Catalog Item Properties** dialog box of the task sequence catalog item must also be selected.*

Table 8-6 • OS Deployment Application Migration / Installation of New Applications Global Settings

Property	Description
Enable requester to specify which existing applications to migrate	This option is enabled if you select the **Enable application migration and installation of additional applications** option. • **If this option is selected**, when the **Choose Existing Applications to Migrate** panel of the Checkout Wizard is displayed, the requester will be able to select which of the applications on the existing computer will be migrated to the target computer. • **If this option is not selected**, all applications on the existing computer will automatically be selected and you will be unable to deselect them. *Note • To prevent an application from being listed on the Choose Existing Applications to Migrate panel, select the Core application option on the General > Global tab of the catalog item's Catalog Item Properties dialog box.*
Prompt requester to select additional applications to install	If this option is selected, the Choose Additional Applications to Install During OS Deployment Panel will be displayed in the Checkout Wizard, prompting the requester of an OSD task sequence catalog item to select additional applications to install on the target computer. *Note • This option is enabled if you select the Enable application migration and installation of additional applications option.* *Note • To prevent an application from being listed on the Choose Additional Applications to Install During OS Deployment panel, select the Core application option on the General > Global tab of the catalog item's Catalog Item Properties dialog box.*

OSD Task Sequence Catalog Item Settings

Whether or not some of the settings selected on the **Site Management > Settings > Deployment > OS Deployment** tab apply to an individual OSD task sequence catalog item depends upon the selection of the **Auto detect installed apps** option on the **Deployment > Roles** tab of the catalog item's **Catalog Item Properties** dialog box.

Figure 8-3: Auto Detect Installed Apps Option on Deployment > Roles Tab

If the **Auto detect installed apps** option is selected, along with the global **Enable application migration and installation of additional applications** option, then the Choose Existing Applications to Migrate panel will be displayed during OSD task sequence catalog item checkout.

Configuring the Display of Application Migration/Installation Panels

The following table lists the combinations of options you need to select to configure which of application migration and installation panels will appear in the Checkout Wizard when checking out an OSD task sequence catalog item:

Table 8-7 • Configuring the Display of Application Migration/Installation Panels

If you want to display this checkout panel …	Select these global options …	Select this catalog item option …
Choose Existing Applications to Migrate (Without ability to select applications)		
Choose Existing Applications to Migrate (With ability to select applications)		
Choose Additional Applications to Install During OS Deployment		Does not matter if **Auto detect installed apps** is selected or not selected.

Table 8-7 • Configuring the Display of Application Migration/Installation Panels

If you want to display this checkout panel …	Select these global options …	Select this catalog item option …
Choose Roles (Without listing the applications included in each role) 📄 ___ **Note •** *Also, roles must be associated with the OSD task sequence catalog item.*	Enable application migration and installation of additional applications ☐ Enable requester to specify which existing applications to migrate ☐ Prompt requester to select additional applications to install ☐	Does not matter if **Auto detect installed apps** is selected or not selected.
Choose Roles (Listing the applications included in each role) 📄 ___ **Note •** *Also, roles must be associated with the OSD task sequence catalog item.*	Enable application migration and installation of additional applications ☑ Enable requester to specify which existing applications to migrate ☐ Prompt requester to select additional applications to install ☐	Does not matter if **Auto detect installed apps** is selected or not selected.

Identifying Existing Applications to Include in OS Deployment

File and usage evidence becomes important during an OS imaging process since it can be used to identify applications that are on an existing system and provide usage information so that the user or administrator is able to make a decision on whether that application should be included on a new or reimaged device.

File and usage evidence is available through integration with FlexNet Manager Suite (FNMS). In the event that an environment does not have FlexNet Manager Suite, then inventory records can be created in App Portal for each application needing to be discovered for the OSD process.

- Identifying Existing Applications Using FlexNet Manager Suite

- Identifying Existing Applications by Creating App Portal Application Inventory Records

Identifying Existing Applications Using FlexNet Manager Suite

📄

___

Note • *This feature requires a connection with FlexNet Manager Suite.*

File and usage evidence becomes important during an OS imaging process since it can be used to identify applications that are on an existing system and provide usage information so that the user or administrator are able to make a decision on whether that application should be included on a new or reimaged device.

App Portal is capable of leveraging application inventory and usage data from Microsoft System Center Configuration Manager. This application inventory and usage evidence is available through integrating App Portal with FlexNet Manager Suite (FNMS).

To connect App Portal to the Flexera Service Gateway and FlexNet Manager Suite, perform the following tasks:

- Connecting to the Flexera Service Gateway

●   Entering FlexNet Manager Suite Settings

Identifying Existing Applications by Creating App Portal Application Inventory Records

File and usage evidence becomes important during an OS imaging process since it can be used to identify applications that are on an existing system and provide usage information so that the user or administrator are able to make a decision on whether that application should be included on a new or reimaged device.

App Portal is capable of leveraging application inventory and usage data from Microsoft System Center Configuration Manager. This application inventory and usage evidence is available through integrating App Portal with FlexNet Manager Suite (FNMS).

However, in the event that an environment is not integrated with FlexNet Manager Suite, you need to create App Portal inventory records for each application needing to be discovered for the OSD process, and then associate each inventory record with its associated software catalog item.

●   Creating a New Inventory Record

●   Associating an Inventory Record with a Catalog Item

Note • *System Center Configuration Manager inventory must be collected and available prior to creating inventory records in App Portal or the information necessary to create an inventory record will not be present. If this is the case, simply enable hardware inventory and allow at least one inventory cycle to complete on the System Center Configuration Manager clients.*

Creating a New Inventory Record

For each application that you want to include in OS deployment, you need to create an inventory record. To create an inventory record in App Portal, perform the following steps.

Task   *To create an inventory record:*

1. On the **Admin** tab, expand the **Compliance Management** section and click **Add Inventory**.

The **Add New Inventory** wizard opens.

2. In the **Logical inventory group name** field, enter a name that will represent the inventory record.

   This name can be general, if you want to track multiple versions of a program, or very specific, if you want to track a single instance of a program. For example, to track all versions of Visio, enter `Microsoft Visio`. To track a single version, enter `Microsoft Visio 2017`.

3. Select the inventory **Category** for this new inventory item.

   Note • For information on creating an inventory category, see Creating a New Inventory Category.

4. Set any additional parameters, as described in Configuring an Inventory Item.

5. Click **Save**. Additional tabs are displayed.

6.   Open the **Usage > Count > Include Rules** tab. On this tab, you need to locate and select the versions of this application in System Center Configuration Manager that you want to include in this inventory record.

7. Click **New Inventory Attribute**. The New Inventory Attribute dialog box opens, prompting you to select an **Inventory Class** to search for attributes.

8. From the **Select an Inventory Class** list, select one of the following to use to determine application usage:

   ● **Add Remove Programs**

- **Computer System**

- **Installed Software**

Tip • *Typically, you would select* **Add Remove Programs** *or, for 64-bit programs,* **Add Remove Programs 64***.*

Note • *For information on creating an inventory category, see* Creating a New Inventory Category*.*

9. Use the filter boxes to search for an item.

Note • *In some cases, there could be hundreds of discovered inventory properties or versions of an application. If this occurs, select* **20** *or* **50** *from the* **Page size** *list to see more entries per page. If your criterion returns multiple pages, you will need to select all of the items listed on that page, click* **Add to Include***, and then proceed to the next page and repeat the steps to add all of the listed items. This should be a very rare occurrence, and may be due to the installation behavior of some applications.*

10. Select one or more of the found items, then click the **Add To Include** button.

11. Close the **New Inventory Attribute** screen. At least one **Inventory Attribute Group**, with one to three properties per version/group will be listed in the grid. In some cases, there may be no version number, or no publisher, leaving the **DisplayName** as the only populated attribute.

12. Click **Save**.

13. Open the **Usage > Metering** tab.

14. Select the **Metering Rule** or **Asset Intelligence** rule that you want to use to identify usage for the application.

15. Click the **Save** button and close the Inventory settings window.

Associating an Inventory Record with a Catalog Item

For each application that needs to be discovered during the OS deployment process, you need to create an inventory record, as described in Creating a New Inventory Record, and then associate that inventory record with the application's catalog item.

Task   *To associate an inventory record with a catalog item:*

1. Open the **Catalog Item Properties** dialog box of the catalog item that you want to associate with an inventory item.

2. Open the **General > Inventory > SCCM Inventory Group** tab.

3. Under **Select an inventory group for product installation detection**, select the appropriate inventory record you created, as described in Creating a New Inventory Record.

4. Click **Save**.

5. Repeat these steps for all applications that need to be discovered during the OS deployment process.

Prevent a Catalog Item from Being Included in OS Deployment By Designating it as Core Application

Every enterprise has a set of core applications that are included on all corporate images that are created, such as Microsoft Office, Chrome, etc. Because those applications are included in all OS images, there is no reason to ask an individual to select them during check out of an OSD task sequence catalog item.

You can prevent a specific application from being listed on the **Choose Existing Applications to Migrate** or **Additional Applications to Install During OS Deployment** panels of the Checkout Wizard by designating it as a core application.

- Designating a Catalog Item as a Core Application

- Viewing All Core Applications

Designating a Catalog Item as a Core Application

To specify a catalog item as a core application, perform the following steps.

Task   **To designate a catalog item as a core application:**

1. Open the **General > Global** tab of a catalog item's **Catalog Item Properties** dialog box.

2. Under **Request options**, select **Core application**.

Note • *The Core application option only applies to Software catalog items, not General or Task Sequence, or Cloud catalog items.*

3. Click **Save**.

Viewing All Core Applications

To view a list of all catalog items that have been designated core applications, perform the following steps.

Task   **To view all core applications:**

1. On the **Admin** tab, expand the **Catalog Management** section.

2. Click **Administration > Core Applications**. All catalog items that have been designated as core applications are listed.

Specifying the Sequence of Catalog Item Installation During OS Deployment

When migrating multiple applications onto the same machine during an OSD deployment, it is possible that you would need to specify the order in which catalog items are installed. For example, some software packages cannot be installed until prerequisite packages are first installed.

You can specify the order that applications are installed on the **Deployment Management > Install Sequence** view.

Task   **To specify the sequence of catalog item installation:**

1. For each catalog item that you want to specify the installation sequence of, perform the following steps:

   a. Open the **General > Global** tab of the catalog item's **Catalog Item Properties** dialog box.

   b. In the **Request options** section, select the **Define Installation Order?** option.

      c.   Click **Save**.

2.   To specify the sequence of catalog item installation for the specified catalog items, perform the following steps:

      a.   Open the **Deployment Management > Install Sequence** view. All of the catalog items that have the **Define Installation Order?** option selected will be listed.

      b.   Edit the numbers in the **Order** column until the catalog items are in the correct installation order.

      c.   Click **Save Order**.

Using Upgrade/Replacement to Identify New/Replacement Versions

Note • Upgrade/Replacement settings are only enforced when migrating existing applications or installing new applications as part of the deployment of an OSD task sequence catalog item or when using App Survey; they are not enforced when requesting individual catalog items.

Note • Upgrade/replacement requires installation evidence provided by either FlexNet Manager Suite or App Portal inventory records, as described in Identifying Existing Applications to Include in OS Deployment.

The **Upgrade/Replacement** feature makes it easy for you to update or replace applications at the same time you upgrade a user's operating system or migrate them to a new computer. The **Upgrade/Replacement** feature enables you to specify that if a mapped application is selected for migration/installation during the checkout of an OSD task sequence catalog item, that application will be replaced by the specified replacement catalog item (either a newer version or a replacement catalog item).

The Upgrade/Replacement feature is enforced when an existing user is checking out an OSD task sequence catalog item, and they are prompted to select existing applications to migrate. The existing applications which have been designated as due to be upgraded or replaced are listed in the table on the **Choose Existing Applications to Migrate** panel of the Checkout wizard, with their upgrade/replacement catalog item listed in the **Information** column of the table.

Figure 8-4: Upgrade/Replacement Items on Choose Existing Applications to Migrate Panel of Checkout Wizard

Note • *Upgrade/Replacement is also enforced when migrating applications using the App Survey feature, as described in Using App Survey to Deploy Applications.*

To specify that a catalog item should be upgraded or replaced with a different catalog item during the checkout of an OSD task sequence catalog item, perform the following steps.

Task   *To designate that a catalog item should be upgraded or replaced by another catalog item:*

1. Open the **General > Upgrade/Replacement** tab of the **Catalog Item Properties** dialog box of the "replacement" catalog item (the catalog item that you want to designate as a replacement for the original catalog item).

   Important • *Make sure that you are editing the properties of the catalog item that you want to replace the original catalog item, not the original catalog item.*

2. Use the search boxes to locate the original catalog item that you want this catalog item to replace

3. Select the original catalog item and then click **Add**. The original catalog item is now listed in the **Application** list on the right side of the dialog box.

4. Click **Save**.

Using User Readiness and Constraints to Schedule OS Deployments

You can use App Portal's **User Readiness** and **Constraints** features to schedule users for OS deployment and to limit the number of users that can request and schedule an OS deployment at the same time.

- **User readiness**—App Portal's **User Readiness** feature can be used to control which users are permitted to select an OSD catalog item, and to specify when they can schedule a deployment. You can set a start and end date to establish a deployment window for each user, including recommended blackout dates, and notify the users of these constraints via email.

- **Constraints**—Constraints are used to limit the scheduling possibilities for catalog items. For example you could use constraints to prevent all of your users from requesting and scheduling a software installation at the same time. You

would also use constraints if you wanted to perform a deployment in a controlled manner over a period of time, but you still want to allow the users to initiate the installation.

For information on these scheduling options, see the following topics:

- Using User Readiness Records to Schedule Users for OS Deployment

- Using Constraints to Limit Scheduling Possibilities for Catalog Items

Using User Readiness Records to Schedule Users for OS Deployment

App Portal's **User Readiness** feature can be used to extend user self-service functionality of operating system images, as well as required applications. It can be used to control which users are permitted to select an OSD catalog item, and to specify when they can schedule a deployment. You can set a start and end date to establish a deployment window for each user, including recommended blackout dates, and notify the users of these constraints via email.

For example, you could use these user readiness constraints to prevent all enterprise users from requesting and scheduling an OS deployment at the same time. You could also use these constraints if you wanted to perform an OS deployment in a controlled manner over a period of time, but you still wanted to allow the users to initiate the installation.

*Note • User Readiness is only applicable if the requester selects the **Reimage my computer (MACHINENAME) with a new Operating System** or **Build an unknown computer and migrate my data from MACHINENAME to the new computer** options on the **Choose Target** panel of the Checkout Wizard. User Readiness is not applicable if the requester selects the **Image a new computer or existing computer** option.*

To learn more about App Portal's **User Readiness** feature, see the following topics:

- About User Readiness

- Creating a User Readiness Record

- Modifying a Task Sequence Catalog Item to Require a User Readiness Record

- Bulk Import of User Readiness Data

About User Readiness

When using the User Readiness feature, you create records that define a requester as "ready" for either a regular catalog item or a task sequence catalog item. Those users are informed, usually via email, that they are scheduled to have a catalog item or task sequence (OS deployment) installed on their device, and are prompted to select an installation date within the range of available dates.

- **Typically used for OS deployment**—User readiness records are typically used for operating system deployment, but can also be used to install or upgrade a software application that is used by the entire corporation (such as Microsoft Office).

- **Use to target sets of users**—Using user readiness records enable you to target specific sets of users at a time.

- **Use to prevent installation of catalog items**—User readiness can also restrict or prevent installation of a catalog item if a readiness record is required, but not yet present.

- **Deployment window can expire, providing enhanced security**—If a user has not scheduled a deployment within the deployment window, and the deployment window expires, the deployment is no longer able to be scheduled. This gives you an extra layer of security for sensitive catalog items such as OS deployments.

- **Specifying that a catalog item requires a user readiness record**—You specify that a catalog item requires a user readiness record by selecting the **Require User Readiness record?** option on the **General** tab of the **Catalog Item Properties** dialog box. Only those catalog items that have this option selected will be available for selection on the **User Readiness** view.

Delivery of a Catalog Item That Requires a User Readiness Record

If a catalog item requires a user readiness record, two actions must occur before the item can be delivered to the user:

- **User must be added to user readiness record**—For the catalog item in question, the user must have been added to the list of users for which readiness records are required.

- **User must respond to notification**—The user must have responded to the readiness record request notification.

Important Considerations About User Readiness

Note the following regarding the use of user readiness records:

- **Adding users**—You can associate a user with a user readiness record by manually searching for and adding the user, or by importing an Excel file containing a list of users. But you cannot associate users with a user readiness record by selecting an Active Directory group or a collection of users. You can only add users individually, or by importing an Excel file containing a list of users.

- **Cannot target machines**—You cannot use user readiness records to push a deployment to specific machines. User readiness targets the user, not the machine.

- **No forced deployment**—If a "ready" user does not schedule an installation date, the catalog item will not be installed. Even though a user readiness record for a catalog item with a start and end date has been associated with a user, there is no forced deployment if that person fails to select a date.

- **User readiness record settings overwrite constraint settings**—Each user readiness record has settings similar to those of a constraint, defining the start date, end date, and blackout dates for deployment. However, the start date, end date, and blackout date settings of a user readiness record overwrite those of a constraint.

Creating a User Readiness Record

Creating a user readiness record involves specifying a catalog item, adding users, and specifying a date range for deployment. To create a user readiness record, perform the following steps.

Task   **To create a user readiness record:**

1. On the **Admin** tab, select **Deployment Management > User Readiness**. The **User Readiness** view opens.

2. To add a record and specify a catalog item, click **Add Users**. The following dialog box opens.

3. Select a catalog item from the **Select a catalog item** list and click **Continue**. The **User Readiness** dialog box opens displaying a list of users.

4. Select users and then click **Add Selected Results**. You are prompted to confirm that you want to import records.

*Note • You can also click **Show filter** to filter the user list.*

5. Click **OK**. The calendar portion of the **User Readiness** dialog box opens.

6. Select the start and end dates of the deployment period, recommended schedule date (optional), and any blackout dates. This information will be communicated to the user if the **Send notification emails** is checked.

*Note • You can edit and customize the notification email template on the **Site Management > Communication > Notifications** view.*

7. Click **Add**.

8. Close the **User Readiness** dialog box.

9. On the **User Readiness** view, select the catalog item from the **Select a catalog item** list. The readiness records are now listed in the grid.

When the user schedules the install, the **Is Scheduled** column will read "**Yes**" and the actual scheduled date will appear. Once the installation begins, the status of the installation will be visible in the status column.

10. To make changes to readiness records individually, double-click the row.

11. To make bulk changes, select the records and choose the desired action from the **Bulk Actions** toolbar item.

Important • When using constraints to manage a deployment, as described in Using Constraints to Limit Scheduling Possibilities for Catalog Items, *you can also specify start date, end date, and blackout dates. If a constraint with specified blackout dates also applies to a software deployment that is managed by a user readiness record with specified blackout dates, the blackout dates will be combined. However, the start date, end date, and blackout date settings of a user readiness record overwrite those of a constraint.*

Modifying a Task Sequence Catalog Item to Require a User Readiness Record

The following instructions provide the steps to modify a task sequence catalog item to require a user readiness record. To complete this task, perform the following steps:

Task   ***To modify a task sequence catalog item to require a readiness record:***

1. Open the **Catalog Item Properties** dialog box of a task sequence catalog item.

2. On the **General > Global** tab under the **Scheduling Options** section, select the **Enable user defined scheduling?** and **Require User Readiness record?** options.

3. Click **Save**.

Checkout Experience When User Readiness Record is Required

If a task sequence catalog item requires a user readiness record, when a user requests that catalog item, one of the following will occur during checkout:

- **User readiness record for this user does not exist**—If no user readiness record for this user exists, the following message will be displayed:

- **User readiness record for this user exists**—If a user readiness record for this user exists, the user will be prompted to select an installation date on the **Choose Scheduling Options** panel of the checkout wizard, but they will only be permitted to select dates within the date range specified in the user readiness record. It will be impossible for the user to schedule installation at a time outside of that date range.

Bulk Import of User Readiness Data

When using the App Portal **User Readiness** feature, you can import user data from a Microsoft Excel Workbook rather than having to select a user individually. A sample workbook is available within the User Readiness view of App Portal.

The following figure details the bulk import area of User Readiness.

Figure 8-5: Bulk Import Area of User Readiness

After you import user data, you can perform bulk actions on those imported users.

Figure 8-6: Bulk Actions on User Readiness View

For these imported users, you can **Set Initial Schedule**, which includes setting a start date, end date, and suggested scheduled date. You can also use **Mark as Ready** to specify that the users are ready for deployment. All users who are marked as ready will receive the deployment at the scheduled time (whether they selected it or it was the default selection).

📄

Note • *The bulk import function of User Readiness requires that Microsoft Access Database Engine 2016 Redistributable be installed on the App Portal web server. The Microsoft Access Database Engine 2016 Redistributable is a free download available at the following URL:*

https://www.microsoft.com/en-us/download/details.aspx?id=54920

Using Constraints to Limit Scheduling Possibilities for Catalog Items

Constraints are used to limit the scheduling possibilities for catalog items. For example you could use constraints to prevent all of your users from requesting and scheduling a software installation at the same time. You would also use constraints if you wanted to perform a deployment in a controlled manner over a period of time, but you still want to allow the users to initiate the installation.

While constraints are most useful for OSD deployments, they can be used for any catalog item.

- About Constraints

- Configuring Constraints

About Constraints

Constraints are used to limit the scheduling possibilities for catalog items. For example you could use constraints to prevent all of your users from requesting and scheduling a software installation at the same time. You would also use constraints if you wanted to perform a deployment in a controlled manner over a period of time, but you still want to allow the users to initiate the installation.

While constraints are most useful for OSD deployments, they can be used for any catalog item.

There are three types of constraints:

- **Global constraint**—A global constraint is evaluated after all other constraints have been assessed. You use the global constraint to limit at a top level the volume of requests that can be submitted on a daily basis.

  For example, you could use the global constraint to limit the volume based on what the help desk could support on a daily basis. Once the global limit has been reached for that day, no more scheduling can occur.

  You configure a global constraint by clicking **Edit Global Constraint** on the **Deployment Management > Constraints** view.

- **Default constraint**—The default constraint, when configured, applies in the event no conditional constraint could be found. Because conditional constraints apply based on conditions, it is possible that a user or computer may not qualify for any constraints. In this event, you still may want a constraint applied, hence the presence of the default constraint.

  You configure a default constraint by clicking **Edit Default Constraint** on the **Deployment Management > Constraints** view.

- **Conditional constraint**—Conditions can be set on constraints to determine whether a constraint should be applied. The same conditions found elsewhere apply here: **OU**, **Group**, **Property**, and **Collection**. When a user matches a condition for a constraint, no further evaluation is performed on other constraints and the settings for the constraint are applied.

  You configure a conditional constraint by clicking **Add Constraint** on the **Deployment Management > Constraints** view, and then specifying conditions on the **Conditions** tab of the **Create Constraints** dialog box.

For more information, see Configuring Constraints.

Configuring Constraints

As described in About Constraints, there are three types of constraints: global, default, and conditional. The procedure for configuring all three types of constraints is similar, except that you add conditions to a conditional constraint.

To configure a conditional constraint, perform the following steps:

Task   ***To configure a conditional constraint:***

1. On the **Admin** tab, select **Deployment Management > Constraints**.

2. Click **Add Constraint**. The **Create Constraints** dialog box opens.

3. On the **General** tab, define the parameters for the constraint:

Property	Description
Constraint Name	Enter a name to identify the constraint.
Start After / End By	Use to set the time range for the selected days that are available for the schedule. • **Start After**—Opening date of deployment, • **End By**—Date when the deployment will no longer be available
Start Time / End Time	To limit installation to a specific time range for a day of the week, specify the **Start Time** and **End Time** for that day. If no start or end time is specified, then any time is available. In this example, the requester would only be able to select a time range for installation between 8:00 a.m. and 5:00 p.m. on Monday through Friday. Saturday and Sunday would have any time available.
Limits Content Size	To limit the scheduling based on the total content size for items being delivered for others that meet the same constraint, enter a limit (in KB, MB, or GB). This limit is calculated by totaling the SCCM package size for the requested items for that day. In this example, if 10 users scheduled Microsoft Office (a 1 GB package) from the IT Department on Tuesday, the next user would hit the content size limit for that day and would not be able to schedule their installation for Tuesday. If the requester selects Wednesday, the same evaluation will occur for that day.
Type Limits: Software, OSD, Virtual, and General	Use to limit the volume of the specific class of catalog item (software, OS deployment, virtual package, or general) that can be requested. This allows you to limit by the type instead of limiting the time or data size.

4. Open the **Conditions** tab. Conditions are what determine the application of a constraint.

5. Choose the conditions that will qualify a user or computer. When a condition match is found, that constraint will be used and no further evaluations will occur.

*Tip • You can use the **AD Property** subtab to allow for custom values of a variable type (starts with, contains, etc.).*

6. Open the **Blackout Dates** tab. Use blackout dates to limit scheduling options such as holidays. The requester will not be able to select a date from the scheduler if it is blacked out.

Note • *When using a user readiness record to manage a deployment, as described in Using User Readiness Records to Schedule Users for OS Deployment, you can also specify blackout dates. If a constraint with specified blackout dates also applies to a software deployment that is managed by a user readiness record with specified blackout dates, the blackout dates will be combined.*

7. Click **Save**. The constraint is now listed on the **Constraints** view.

Requesting an OSD Task Sequence Catalog Item

You can request an OSD task sequence catalog item using the Checkout Wizard. After you add the OSD task sequence catalog item to the cart, the selection you make on the **Choose Target** panel of the Checkout Wizard will determine the deployment type of the selected task sequence.

Figure 8-7: Options on the Choose Target Panel

The following table lists the option you should pick on the **Choose Target** panel of the Checkout Wizard for each deployment type and requester type.

Table 8-8 • Types of OSD Task Sequence Deployments

Deployment Type	Description	Requester	Select This Option on Choose Target Panel
New Install (Bare-Metal)	**The OS corporate image is deployed for the first time to a new computer. Since this machine is new to your organization, no user data or applications need to be captured or migrated.** See Deploying an OS on a New Computer.	Request on Behalf	**Image a new computer or existing computer**
Refresh (In-Place Migration)	**The OS of an existing computer in your organization is upgraded. The existing user data and applications are captured prior to the OS upgrade, and then later restored to the machine after the OS upgrade has been completed.** See **Upgrading the OS of an Existing Computer.**	Self	**Reimage my computer (DEVICE_NAME) with a new Operating System**
		Request on Behalf	**Image a new computer or existing computer**
Replace (Side-by-Side Migration)	**User data and applications are migrated from an existing system to a replacement system.** See **Performing a Side-By-Side Migration from a Source to a Target Computer.**	Self	**Build an unknown computer and migrate my data from DEVICE NAME to the new computer**
		Request on Behalf	**Image a new computer or existing computer**

Deploying an OS on a New Computer

In a bare-metal installation scenario, your OS corporate image is deployed for the first time to a new computer. Since this machine is new to your organization, no user data or applications need to be captured or migrated.

To deploy an OS on a new computer, perform the following steps.

Task   ***To deploy an OS on a new computer:***

1.   On the **Browse Catalog** tab, locate an OS deployment task sequence catalog item for the operating system you desire, and click **Add** to add it to your cart. The **Choose Target** panel of the Checkout Wizard opens.

2.   Select **Image a new computer or existing computer** and click **Next**. The **Import New Computer** panel opens.

Note • *If a questionnaire template was associated with this catalog item, the* Respond to Questionnaire Panel *would be displayed prior to the* **Import New Computer** *panel.*

3.   From the **New computer name** list, specify a name for the new computer. Because it is a new computer, additional fields are displayed to enable you to identify it in System Center Configuration Manager:

4. Enter the following information to configure the new computer with System Center Configuration Manager:

Field	Description
Time Zone	Select the time zone for the System Center Configuration Manager site.
SCCM Site	Select the System Center Configuration Manager site where you want to create a new computer object.
MAC Address **SMBIOS GUID**	Enter either the MAC address or the SMBIOS GUID the computer you are importing. *Note* • *You are only required to enter one of these values.*

5. Under **Build Type**, select **New Computer (No data migration)**.

6. Under **User**, enter the **Domain**, **User ID**, **Full Name** and **Email Address** of the user that will be assigned to this new computer.

7. Click **Import Computer**, and then verify that the old machine, new machine, and user information have been added to the table at the bottom of the page.

8. At the top of the page, click **Next**. If roles were associated with this catalog item, the **Choose Roles** panel opens.

Whether or not the requester is permitted to select roles on this panel depends upon whether the **Allow user role selection** option is selected on the **Deployment > Roles** subtab of this catalog item's Catalog Item Properties dialog box:

- **Selected**—The requester is able to select roles that will determine which applications will be installed on the target computer.

- **Not selected**—The roles will be listed on this panel, but they will automatically be selected and the requester will be unable to clear the selection.

9. Click **Next**. If the **Prompt requester to select additional applications to install** option is selected on the **Site Management > Settings > Deployment > OS Deployment** tab, the **Choose Additional Applications to Install During OS Deployment** panel opens.

10. Select any additional applications that you want to install during OS deployment, and then click **Add Applications** to add them to the selection list.

11. Click **Next**. If the **Enable user defined scheduling?** option is selected on the **General > Global** tab of the Catalog Item Properties dialog box for this catalog item, the **Choose Scheduling Options** panel is displayed during checkout, which prompts the requester to choose when the request should be fulfilled.

12. Specify scheduling options, as described in Choose Scheduling Options Panel and click **Next**. The **Submit Request** panel opens.

13. Click **Submit** to submit the request.

Upgrading the OS of an Existing Computer

In an upgrade or "in-place migration" scenario, an existing computer, which includes a corporate operating system, is upgraded. The existing user data and applications are captured prior to the OS upgrade, and then later restored to the machine after the OS upgrade has been completed.

To perform an in-place migration, perform the following steps.

Task   ***To upgrade the OS of an existing computer:***

1. On the **Browse Catalog** tab, locate an OS deployment task sequence catalog item, and click **Add** to add it to your cart. The **Choose Target** panel of the Checkout Wizard opens.

2. Select **Reimage my computer (COMPUTER_NAME) with a new Operating System** and click **Next**. If roles were associated with this catalog item, the **Choose Roles** panel opens.

Whether or not the requester is permitted to select roles on this panel depends upon whether the **Allow user role selection** option is selected on the **Deployment > Roles** subtab of this catalog item's Catalog Item Properties dialog box:

- **Selected**—The requester is able to select roles that will determine which applications will be installed on the target computer.

- **Not selected**—The roles will be listed on this panel, but they will automatically be selected and the requester will be unable to clear the selection.

📄

Note • *If a questionnaire template was associated with this catalog item, the Respond to Questionnaire Panel would be displayed prior to the **Import New Computer** panel.*

3. Click **Next**. If the **Enable application migration and installation of additional applications** option is selected on the **Site Management > Settings > Deployment > OS Deployment** tab, the **Choose Existing Applications to Migrate** panel opens, listing the applications currently installed on the requester's computer.

📄

Note • *If the **Enable requester to specify which existing applications to migrate** option is also selected on the **Site Management > Settings > Deployment > OS Deployment** tab, then the requester will be able to specify which of the existing applications to migrate. If this option is not selected, all applications are automatically selected and cannot be unselected.*

4.   Select the applications that you want to migrate and click **Next**. If the **Prompt requester to select additional applications to install** option is selected on the **Site Management > Settings > Deployment > OS Deployment** tab, the **Choose Additional Applications to Install During OS Deployment** panel opens.

Note • *Applications that were selected on the previous panel are already selected on this panel and cannot be unselected.*

5.   Select any additional applications that you want to install during OS deployment, and then click **Add Applications** to add them to the selection list.

6.   Click **Next**. If the **Enable user defined scheduling?** option is selected on the **General > Global** tab of the Catalog Item Properties dialog box for this catalog item, the **Choose Scheduling Options** panel is displayed during checkout, which prompts the requester to choose when the request should be fulfilled.

7. Specify scheduling options, as described in Choose Scheduling Options Panel and click **Next**. The **Submit Request** panel opens.

8. Click **Submit** to submit the request.

Performing a Side-By-Side Migration from a Source to a Target Computer

In a side-by-side migration scenario, user data and applications are migrated from an existing system to the replacement system, which will be imaged with the selected operating system.

With a side-by-side migration, App Portal creates a computer association during checkout so that the Microsoft User State Migration Tool (USMT) is able to detect where to perform the scan state and restore state activities.

When using computer association to perform a side-by-side migration, the following occurs:

- **Replacing existing computer with new computer**—You are replacing an existing computer with another corporate imaged device.

- **User persona information is migrated**—User persona Information from the existing is migrated to the replacement computer

- **Application estate is migrated**—The application estate from the existing system is migrated to the replacement computer

- **Can migrate to a different OS version**—This migration can be to a different version of an operating system.

- **Computer association is created**—App Portal creates a computer association in System Center Configuration Manager.

Task   ***To perform a side-by-side migration:***

1.   On the **Browse Catalog** tab, locate an OS deployment task sequence catalog item, and click **Add** to add it to your cart.
The **Choose Target** panel of the Checkout Wizard opens.

2.   Select **Image a new computer or existing computer** and click **Next**. The **Import New Computer** panel opens.

Note • *If a questionnaire template was associated with this catalog item, the Respond to Questionnaire Panel would be displayed prior to the* **Import New Computer** *panel.*

3. From the **New computer name** list, specify the name of the computer you are migrating to.

4. From the **Old computer** name list, select the name of the existing computer (which you are migrating data from).

5. Under **Build Type**, select **Side-by-Side Migration**.

6. Under **User**, enter the **Domain**, **User ID**, **Full Name** and **Email Address** of the user that will be assigned to the target computer.

7. Click **Import Computer**, and then verify that the old machine, new machine, and user information have been added to the table at the bottom of the page.

8. At the top of the page, click **Next**. If roles were associated with this catalog item, the **Choose Roles** panel opens.

Whether or not the requester is permitted to select roles on this panel depends upon whether the **Allow user role selection** option is selected on the **Deployment > Roles** subtab of this catalog item's Catalog Item Properties dialog box:

- **Selected**—The requester is able to select roles that will determine which applications will be installed on the target computer.

- **Not selected**—The roles will be listed on this panel, but they will automatically be selected and the requester will be unable to clear the selection.

9. Click **Next**. If the **Enable application migration and installation of additional applications** option is selected on the **Site Management > Settings > Deployment > OS Deployment** tab, the **Choose Existing Applications to Migrate** panel opens, listing the applications currently installed on the **Old computer** that was selected.

Note • *If the* **Enable requester to specify which existing applications to migrate** *option is also selected on the* **Site Management > Settings > Deployment > OS Deployment** *tab, then the requester will be able to specify which of the existing applications to migrate. If this option is not selected, all applications are automatically selected and cannot be unselected.*

10. Select the applications that you want to migrate and click **Next**. If the **Prompt requester to select additional applications to install** option is selected on the **Site Management > Settings > Deployment > OS Deployment** tab, the **Choose Additional Applications to Install During OS Deployment** panel opens.

Note • *Applications that were selected on the previous panel are already selected on this panel and cannot be unselected.*

11. Select any additional applications that you want to install during OS deployment, and then click **Add Applications** to add them to the selection list.

12. Click **Next**. If the **Enable user defined scheduling?** option is selected on the **General > Global** tab of the Catalog Item Properties dialog box for this catalog item, the **Choose Scheduling Options** panel is displayed during checkout, which prompts the requester to choose when the request should be fulfilled.

13. Specify scheduling options, as described in Choose Scheduling Options Panel and click **Next**. The **Submit Request** panel opens.

14. Click **Submit** to submit the request.

OS Deployment Reference

This section contains information on the views and dialog boxes under the **Deployment Management** node that are used to perform operating system deployment by offering task sequence catalog items in the App Portal storefront: **Roles**, **Constraints**, and **User Readiness**.

- Roles

- Constraints

- Install Sequence

- User Readiness

*Note • For reference information on **App Survey**, **Support Tools**, and **Clone/Migrate**, see Using App Survey, Clone/Migrate, and Support Tools to Perform Advanced Deployment Tasks.*

Roles

On the **Roles** view, which is opened by selecting **Deployment Management > Roles**, all roles that have been created are listed.

Figure 8-8: Roles View

The **Roles** view includes the following properties and buttons.

Table 8-9 • Roles View Properties

Property	Description
Role	Name of role. Double-click on this role name to edit its properties on the **Role Properties** dialog box. On the **Role Properties** dialog box, you can also delete the role.
Condition Count	Number of conditions defined on the **Conditions** tab of the **Role Properties** dialog box for this role. Conditions are used to determine which users the role applies to.
Variable Count	Number of variables defined on the **Variables** tab of the **Role Properties** dialog box for this role. The **Variables** tab is used to define System Center Configuration Manager task sequence variables that would be assigned to the source, destination, or both computers as part of the System Center Configuration Manager OSD process.
Application Count	Number of applications selected on the **Applications** tab of the **Role Properties** dialog box for this role.
USMT Configured	Whether or not a USMT profile has been configured on the **USMT Profiles** tab of the Role Properties dialog box for this role. The **USMT Profiles** tab is used to define parameters to be used during the System Center Configuration Manager OSD process when performed with USMT (Microsoft User State Migration Tool). These parameters will be passed to the System Center Configuration Manager task sequence.
Description	Description of the role.
New Role	Click to open the **Create New Role** dialog box and create a new role.

Role Properties / Create New Role Dialog Box

When you are defining or editing a role on the **Role Properties / Create New Role** dialog box, you can set properties on the following tabs:

- General Tab

- Applications Tab

- Conditions Tab

- Variables Tab

- USMT Profiles Tab

General Tab

The **General** tab of the **Create New Role** dialog box contains the title and description information for the role.

Figure 8-9: Create New Role Dialog Box / General Tab

The **General** tab of the **Create New Role** dialog box includes the following properties:

Table 8-10 • General Tab Properties / Create New Role Dialog Box

Property	Description
Application Role Name	Used to define the title of the role.
Application Role Description	Used to define the description of the role.
Delete Role	Click to delete the role.
Save Role	Click to save any changes to the role.

Applications Tab

The **Applications** tab of the **Create New Role** dialog box provides the area to add applications to the role. This tab also provides a list of the applications currently assigned to the role.

Figure 8-10: Create New Role Dialog Box / Applications Tab

The **Applications** tab of the **Create New Role** dialog box includes the following properties:

Table 8-11 • Applications Tab Properties / Create New Role Dialog Box

Element	Details
Search Catalog Items	Used to define application title search criteria to locate applications to include in the role.

Table 8-11 • Applications Tab Properties / Create New Role Dialog Box

Element	Details
Available Catalog Items	Lists result from the search criteria defined in the **Search Catalog Items** field. Applications can be selected from this section and be added to be included in the role. 📄 *Note •* If a catalog item has been designated as a core application, as described in *Prevent a Catalog Item from Being Included in OS Deployment By Designating it as Core Application,* that catalog item will not be returned in search results when performing a search on the **Applications** tab.
Current Catalog Items	List of the applications that are currently assigned to the role.

Conditions Tab

The **Conditions** tab is used to define who the role applies to.

Figure 8-11: Create New Role Dialog Box / Conditions Tab

The **Conditions** tab includes three subtabs:

- Group and OU

- AD Property

- Collections

Group and OU

On the **Group and OU** tab, you can add role conditions used to apply **Include** or **Exclude** conditions to a role based on security group membership (AD group membership or OU container).

Figure 8-12: Conditions > Group and OU Tab / Role Properties Dialog Box

The **Conditions > Group and OU** tab of the **Create New Role** dialog box includes the following properties and buttons:

Table 8-12 • Conditions > Group and OU Tab Properties / Role Properties Dialog Box

Property / Tabs	Details
Add Condition	Click to open the **Add Condition** dialog box, where you can add a condition to the role.
Remove Condition	Click to delete the selected condition from the role.
Name	Name of selected Group/OU.
Value	Value of Group/OU.
Enforcement	Select **Include** or **Exclude** to specify the type of condition that you are adding.
Apply to OU and child OUs	Select this option to apply this condition to all of the OU's child OUs. If this option is not selected, this condition is not applied to the selected OU's child OUs.

AD Property

On the **AD Property** tab, you can add role conditions used to apply **Include** or **Exclude** conditions to a role based on an AD property.

Figure 8-13: Conditions > AD Property Tab / Role Properties Dialog Box

The **Conditions > AD Property** tab of the **Role Properties** dialog box includes the following properties and buttons:

Table 8-13 • Conditions > AD Property Tab Properties / Role Properties Dialog Box

Property / Tabs	Details
Add Condition	Click to open the **Add Condition** dialog box, where you can add a condition to the role.
Remove Condition	Click to delete the selected condition from the role.
Name	Name of selected AD property.
Value	Value of AD property.
Operator	Operator used in the AD property condition.
Enforcement	Select **Include Property** or **Exclude Property** to specify the type of condition that you are adding.
Apply to OU and child OUs	Select this option to apply this condition to all of the OU's child OUs. If this option is not selected, this condition is not applied to the selected OU's child OUs.

Collections

On the **Collections** tab, you can add role conditions used to apply **Include** or **Exclude** conditions to a role based on System Center Configuration Manager collection membership.

Figure 8-14: Conditions > Collections Tab / Role Properties Dialog Box

The **Conditions > Collections** tab of the **Role Properties** dialog box includes the following properties and buttons:

Table 8-14 • Conditions > AD Property Tab Properties / Role Properties Dialog Box

Property / Tabs	Details
Add Condition	Click to open the **Add Condition** dialog box, where you can add a condition to the role.
Remove Condition	Click to delete the selected condition from the role.
Value	Value of System Center Configuration Manager collection.
Enforcement	Select **Include Collection** or **Exclude Collection** to specify the type of condition that you are adding.
Deployment Technology	Deployment technology containing the selected collection.

📄

Note • You can create two types of "collection" conditions: user collections and machine collections. However, when defining a condition on a role, App Portal only supports user collection conditions. This is because roles are associated with the users, not with machines.

Add Condition Dialog Box

The fields on the **Add Condition** dialog box depend upon the type of condition you are adding:

- Add Condition Dialog Box / Group and OU Condition

- Add Condition Dialog Box / AD Property Condition

- Add Condition Dialog Box / Collection Condition

Add Condition Dialog Box / Group and OU Condition

When you are creating a condition to apply include or exclude conditions to a role based on security group membership (AD group membership or OU container), the **Add Condition** dialog box has the following configuration:

Figure 8-15: Add Condition Dialog Box / Group and OU

The **Add Condition / Group and OU** dialog box includes the following properties:

Table 8-15 • Add Condition Dialog Box / Group and OU

Property	Description
Domain List	Select the domain that you want to search.
Search Groups / Search OUs	Set the search focus to one of the following: • **To search for AD groups**, leave the search focus set to **Search Groups**. • **To search for OUs**, set the search focus to **Search OUs**.
Search	In the condition search box, enter the name of the group, such as **Admin**.
Include Groups / Exclude Groups	Select one of these options to determine whether to add an include or exclude condition.
Search Results	Lists the results of the search for AD groups or OUs.
Select	Click to add the selected security groups to the condition.

Add Condition Dialog Box / AD Property Condition

When you are creating a condition to apply include or exclude conditions to a role based on AD properties, the **Add Condition** dialog box has the following configuration:

Figure 8-16: Add Condition Dialog Box / AD Property

The **Add Condition / AD Property** dialog box includes the following properties:

Table 8-16 • Add Condition Dialog Box / AD Property

Property	Description
AD Property	Select the AD Property that you want to search.
Search	In the condition search box, search for the desired value of the AD property.
Include Properties / Exclude Properties	Select one of these options to determine whether to add an include properties or exclude properties condition.
Search Results	Lists the results of the search for AD properties.
Select	Click to add the selected AD property values to the condition.

Add Condition Dialog Box / Collection Condition

When you are creating a condition to apply include or exclude conditions to a role based on System Center Configuration Manager collections, the **Add Condition** dialog box has the following configuration:

Figure 8-17: Add Condition Dialog Box / Collection

The **Add Condition / Collection** dialog box includes the following properties:

Table 8-17 • Add Condition Dialog Box / Collection

Property	Description
Search	In the condition search box, search for the desired System Center Configuration Manager collection.
Include Collections / Exclude Collections	Select one of these options to determine whether to add an include collections or exclude collections condition.
Search Results	Lists the results of the search for collections.
Select	Click to add the selected collections to the condition.

Variables Tab

The **Variables** tab of the **Create New Role** dialog box is used to define System Center Configuration Manager task sequence variables that would be assigned to the source, destination, or both computers as part of the System Center Configuration Manager OSD process.

Figure 8-18: Create New Role Dialog Box / Variables Tab

The **Variables** tab of the **Create New Role** dialog box includes the following properties:

Table 8-18 • Variable Tab Properties / Create New Role Dialog Box

Property	Description
Add Variable	Click to open the **New Variable** dialog box, where you can add a System Center Configuration Manager task sequence variable to the role.
Delete Variable	Click to delete the selected System Center Configuration Manager task sequence variable from the role.
Variable Name	Lists the name of the variable.
Variable Value	Contains the value for the variable name.
Apply To Computer	Used to identify if the variable should be applied to the **Source**, **Target**, or **Source and Target** computers.
Apply To Build Type	Used to specify if the variable applies to a particular build. The available options are: • **Not Specified**—Applies to all builds. • **Bare Metal Build**—Applies only to a bare metal build. • **In-Place Migration**—Applies only to in-place migrations. • **Side-by-Side Migration**—Applies only to side-by-side migrations.

Add Variable Dialog Box

You can use the **Add Variables** dialog box to specify variables that can be used by the task sequence process that delivers the applications specified in a role. You open the **Add Variables** dialog box by clicking **Add Variable** on the **Variables** tab of the **Role Properties** dialog box,

Figure 8-19: Add Variables Dialog Box

On the **Add Variables** dialog box, you can either select an MDT variable from the **Select or enter a variable name** list, or select an App Portal variable value from the **Select or enter the variables Value** list.

The **Add Variables** dialog box has the following properties.

Table 8-19 • Add Variables Dialog Box

Property	Description
Select or enter a variable name	Select or enter an MDT variable from this list.
Select or enter a variable value	Select or enter an App Portal variable value from this list.
Mask variables name	To mask a variable's value, select the **Mask variable value** option.
Apply these variables to	Select whether to apply the variable to the **Source**, **Target**, or **Both**.
Apply to build type	Specify under which conditions you apply the variable: **Not Specified**, **Bare Metal Build**, **In-Place Migration**, or **Side-by-Side Migration**.
Add Variable	Click to add the variable to the condition.

USMT Profiles Tab

The **USMT Profiles** tab is used to define parameters to be used during the System Center Configuration Manager OSD process when performed with USMT (Microsoft User State Migration Tool). These parameters will be passed to the System Center Configuration Manager task sequence.

Scan State Subtab

On the **Scan State** tab, you first need to specify a **Scan State Option** to define the USMT parameters that will be used during scan state task on the source computer during the System Center Configuration Manager OSD process.

The other options displayed on the **Scan State** subtab depend upon which of the **Scan State Options** is selected.

Figure 8-20: Role Properties Dialog Box / USMT Profiles / Scan State / Identify Profiles for Migration

The **USMT Profiles > Scan State** subtab of the **Role Properties** dialog box includes the following properties:

Table 8-20 • USMT Profiles > Scan State Tab of Role Properties Dialog Box

Subtab / Property	Description
Scan State Options / Not Configured	Select this option if you do not want any settings or arguments passed to the System Center Configuration Manager task sequence for the scan state step.
Scan State Options / Migrate All Profiles	Select this option to migrate all USMT profiles to target machine. If you select this option, you can also enter **Additional Scan State Arguments** to be used during the scan state step in the System Center Configuration Manager task sequence.

Table 8-20 • USMT Profiles > Scan State Tab of Role Properties Dialog Box

Subtab / Property	Description
Scan State Options / Identify Profiles for Migration	Select this option to specify the USMT profiles that you want to migrate to the target machine. If you select this option, you also need to select one of the following options to identify the profiles: • **Migrate any users who are currently logged on and any users whose profiles have been loaded**—Pass to the System Center Configuration Manager task sequence scan state step the options to capture the users who are currently logged on, as well as any users whose profiles have been loaded. • **Migrate last logon / top console user**—Pass to the System Center Configuration Manager task sequence scan state step the options to capture only the last logon and top console (primary console) user. • **Migrate users whom logged in within the last x days**—Pass to the System Center Configuration Manager task sequence the options to capture the user state for users who have logged in during the last (x) days during the scan state step. Enabling this option displays the **Select num** text box, where you can supply the number of days to be used for the calculation. • **Migrate users whom logged in since [specified date]**—Pass to the System Center Configuration Manager task sequence scan state step the options to capture the user state for users who have logged in since a specified date. Enabling this option adds a date field that you can use to select the date to be used for the calculation**.**
Exclude Local Profiles	Select this option to exclude local profiles from the scan state step in the System Center Configuration Manager task sequence.
Exclude profiles from the following domains	Enter domain names in this text box to exclude user persona information from identified domains during the scan state step in the System Center Configuration Manager task sequence.
Dynamic Scan State Arguments	Enter scan state arguments to be used during the scan state step in the System Center Configuration Manager task sequence.
Additional Scan State Arguments	Enter additional scan state arguments to be used during the scan state step in the System Center Configuration Manager task sequence.

Load State Subtab

On the **Load State** tab, you first need to specify a **Load State Option** to define the USMT parameters to be used during the load state task on the destination computer during the System Center Configuration Manager OSD process.

The other options displayed on the **Load State** subtab depend upon which of the **Load State Options** is selected.

Figure 8-21: Role Properties Dialog Box / USMT Profiles / Load State / Identify Profiles for Restore

The **USMT Profiles > Load State** subtab of the **Role Properties** dialog box includes the following properties:

Table 8-21 • USMT Profiles > Load State Tab of Role Properties Dialog Box

Subtab / Property	Description
Load State Options / Not Configured	Select this option if you do not want any settings or arguments passed to the System Center Configuration Manager task sequence for the load state step.
Load State Options / Restore All Profiles	Select this option to restore all USMT profiles to the destination computer. If you select this option, you can also enter **Additional Load State Arguments** to be used during the load state step in the System Center Configuration Manager task sequence.

Table 8-21 • USMT Profiles > Load State Tab of Role Properties Dialog Box

Subtab / Property	Description
Load State Options / Identify Profiles for Restore	Select this option to specify the USMT profiles that you want to restore to the target machine. If you select this option, you also need to select one of the following options to identify the profiles:
	• **Restore any users who are currently logged on and any users whose profiles have been loaded**—Pass to the System Center Configuration Manager task sequence load state step the options to capture the users who are currently logged on, as well as any users whose profiles have been loaded.
	• **Restore last logon / top console user**—Pass to the System Center Configuration Manager task sequence load state step the options to capture only the last logon and top console (primary console) user.
	• **Restore users who logged in within the last x days**—Pass to the System Center Configuration Manager task sequence the options to capture the user state for users who have logged in during the last (x) days during the load state step. Enabling this option displays the **Select num** text box, where you can supply the number of days to be used for the calculation.
	• **Restore users who logged in since [specified date]**—Pass to the System Center Configuration Manager task sequence load state step the options to capture the user state for users who have logged in since a specified date. Enabling this option adds a date field that you can use to select the date to be used for the calculation**.**
Exclude Local Profiles	Select this option to exclude local profiles from the load state step in the System Center Configuration Manager task sequence.
Exclude profiles from the following domains	Enter domain names in this text box to exclude user persona information from identified domains during the load state step in the System Center Configuration Manager task sequence.
Move Domains	Select this option to move profiles from one domain to another during the load state process. You also need to enter both the **Old Domain** name and **New Domain** name.
Dynamic Load State Arguments	Enter load state arguments to be used during the load state step in the System Center Configuration Manager task sequence.
Additional Load State Arguments	Enter load state arguments to be used during the load state step in the System Center Configuration Manager task sequence.

User Readiness

App Portal's **User Readiness** feature can be used to control which users are permitted to select an OSD catalog item, and to specify when they can schedule a deployment. You can set a start and end date to establish a deployment window for each user, including recommended blackout dates, and notify the users of these constraints via email.

Figure 8-22: Deployment Management > User Readiness View

The **User Readiness** view includes the following properties and buttons:

Table 8-22 • User Readiness View

Property	Description
Select a catalog item	Select a catalog item to view the user readiness records that have been defined for it.
User ID	ID of selected user.
Name	Name of selected user.
Is Ready	Indicates whether or not the user is designated as ready.
Office	Location of user.
Department	Department of user.
Suggested Date	Suggested install date for catalog item.
Start Date	Start date for beginning of eligible installation period.
End Date	End date for end of eligible installation period.
Is Scheduled	Indicates whether or not the user has scheduled the installation of the catalog item.
Schedule Date	Date that the user has scheduled the installation of the catalog item.
Status	Installation status.
Show filter	Click to show the **Filter Builder** dialog box, where you can use expressions to build a filter.
Add Users	Click to add a user readiness record for a user.
Import / Update Users	Click to perform a bulk import of user readiness data. See Bulk Import of User Readiness Data.

Table 8-22 • User Readiness View

Property	Description
Bulk Actions	Select one of the following options from the list to perform a bulk action to the selected user readiness records: • Mark as ready • Mark as not ready • Set blackout dates • Set initial schedule • Delete
Refresh	Click to refresh the data on the view.
Save View	Click to save the view so that the next time the **User Readiness** view is opened, the currently selected catalog item is selected.

Add Users Wizard

You use the **Add Users Wizard** to add a user readiness record. You open the **Add Users Wizard** by clicking **Add Users** on the **User Readiness** view.

The Add Users Wizard consists of the following panels:

• Select Catalog Item Panel

• User Readiness Panel

• Calendar Panel

Select Catalog Item Panel

On the **Select Catalog Item** panel of the **Add Users Wizard**, you select the catalog item to which you are adding a user readiness record.

Figure 8-23: Add Users Wizard / Select a Catalog Item Panel

Select a catalog item from the **Select a catalog item** list and click **Continue**.

User Readiness Panel

On the **User Readiness** panel of the **Add Users Wizard**, you select the users to which you are adding a user readiness record.

Figure 8-24: Add Users Wizard / User Readiness Panel

Select the desired users and then click **Add Selected Results**. You are prompted to confirm that you want to import records.

*Note • You can also click **Show filter** to filter the user list using expressions on the **Filter Builder** dialog box.*

Calendar Panel

After you have added users to a user readiness record on the User Readiness panel of the Add Users Wizard, the Calendar panel opens.

Figure 8-25: Add Users Wizard / Calendar Panel

Select a date in the **Select a start date** and **Select an end date** fields to define the deployment period. You can also select a recommended **Schedule Date** (optional), and select any desired **Blackout Dates** within this deployment period during which deployment would not be permitted.

If you want to communicate this information to the specified users, select the **Send notification emails** option.

Note • *You can edit and customize the notification email template on the* **Site Management > Communication > Notifications** *view.*

When you have finished defining the deployment period, click **Add**. The **User Readiness** panel is displayed. Next, close the **User Readiness** dialog box to return to the **User Readiness** view.

Constraints

Constraints are used to limit the scheduling possibilities for catalog items. For example you could use constraints to prevent all of your users from requesting and scheduling a software installation at the same time. You would also use constraints if you wanted to perform a deployment in a controlled manner over a period of time, but you still want to allow the users to initiate the installation.

While constraints are most useful for OSD deployments, they can be used for any catalog item.

Existing constraints are listed on the **Deployment Management > Constraints** view.

Figure 8-26: Constraints View

The Constraints view includes the following properties and buttons:

Table 8-23 • Constraints View

Property	Description
Constraint Name	Name of defined constraint.
Starts After	Start date of constraint, if any.
Ends By	End date of constraint, if any.
Add Constraint	Click to open the **Create Constraints** dialog box and add a new constraint.
Edit Global Constraint	Click to open the **Global Constraint** dialog box, where you can edit an existing global constraint.
Edit Default Constraint	Click to open the **Default Constraint** dialog box, where you can edit the default constraint.

Create Constraints / Global Constraint / Default Constraint Dialog Box

There are three types of constraints:

- **Global constraint**—A global constraint is evaluated after all other constraints have been assessed. You use the global constraint to limit at a top level the volume of requests that can be submitted on a daily basis. For example, you could use the global constraint to limit the volume based on what the help desk could support on a daily basis. Once the global limit has been reached for that day, no more scheduling can occur. You configure a global constraint by clicking **Edit Global Constraint** on the **Constraints** view.

- **Default constraint**—The default constraint, when configured, applies in the event no conditional constraint could be found. Because conditional constraints apply based on conditions, it is possible that a user or computer may not qualify for any constraints. In this event, you still may want a constraint applied, hence the presence of the default constraint. You configure a default constraint by clicking **Edit Default Constraint** on **Constraints** view.

- **Conditional constraint**—Conditions can be set on constraints to determine whether a constraint should be applied. The same conditions found elsewhere apply here: **OU**, **Group**, **Property**, and **Collection**. When a user matches a condition for a constraint, no further evaluation is performed on other constraints and the settings for the constraint are applied. You configure a conditional constraint by clicking **Add Constraint** on the **Constraints** view, and then specifying conditions on the **Conditions** tab of the **Create Constraints** dialog box.

The procedure for configuring all three types of constraints is similar, except that you add conditions to a conditional constraint.

The **Constraints** dialog boxes include the following tabs:

- General Tab

- Conditions Tab

- Blackout Dates Tab

General Tab

On the General tab of the Constraints dialog boxes, you specify the name of the constraint and define the time constraints.

Figure 8-27: General Tab of Create Constraints / Global Constraint / Default Constraint Dialog Box

The **General** tab includes the following properties:

Table 8-24 • General Tab of Create Constraints / Global Constraint / Default Constraint Dialog Box

Property	Description
Constraint Name	Enter a name to identify the constraint.
Start After / End By	Use to set the time range for the selected days that are available for the schedule. • **Start After**—Opening date of deployment, • **End By**—Date when the deployment will no longer be available
Start Time / End Time	To limit installation to a specific time range for a day of the week, specify the **Start Time** and **End Time** for that day. If no start or end time is specified, then any time is available. In this example, the requester would only be able to select a time range for installation between 8:00 a.m. and 5:00 p.m. on Monday through Friday. Saturday and Sunday would have any time available.
Limits Content Size	To limit the scheduling based on the total content size for items being delivered for others that meet the same constraint, enter a limit (in KB, MB, or GB). This limit is calculated by totaling the SCCM package size for the requested items for that day. In this example, if 10 users scheduled Microsoft Office (a 1 GB package) from the IT Department on Tuesday, the next user would hit the content size limit for that day and would not be able to schedule their installation for Tuesday. If the requester selects Wednesday, the same evaluation will occur for that day.
Type Limits: Software, OSD, Virtual, and General	Use to limit the volume of the specific class of catalog item (software, OS deployment, virtual package, or general) that can be requested. This allows you to limit by the type instead of limiting the time or data size.

Conditions Tab

*Note • This tab only appears on the **Create Constraints** dialog box.*

On the **Conditions** tab of the **Create Constraints** dialog box, you enter conditions to determine the application of a constraint.

Figure 8-28: Conditions Tab of Create Constraints Dialog Box

On the **Conditions** tab, specify the conditions to qualify a user or computer. When a condition match is found, that constraint will be used and no further evaluations will occur.

For detailed information on creating conditions, see the information on the Conditions Tab of the **Role Properties** dialog box.

*Note • You can use the **AD Property** subtab to allow for custom values of a variable type (starts with, contains, etc.).*

Blackout Dates Tab

On the **Blackout Dates** tab, specify blackout dates to limit scheduling options such as holidays. The requester will not be able to select a date from the scheduler if it is blacked out.

Figure 8-29: Blackout Dates Tab of Create Constraints / Global Constraint / Default Constraint Dialog Box

Note • When using a user readiness record to manage a deployment, as described in Using User Readiness Records to Schedule Users for OS Deployment, you can also specify blackout dates. If a constraint with specified blackout dates also applies to a software deployment that is managed by a user readiness record with specified blackout dates, the blackout dates will be combined.

Install Sequence

When migrating multiple applications onto the same machine during an OSD deployment, it is possible that you would need to specify the order in which catalog items are installed. For example, some software packages cannot be installed until prerequisite packages are first installed.

You can specify the order that applications are installed on the **Deployment Management > Install Sequence** view, which lists all of the catalog items that have the **Define Installation Order?** option selected on the **General > Global** tab of the **Catalog Item Properties** dialog box.

Figure 8-30: Install Sequence View

On the Install Sequence View, edit the numbers in the **Order** column until the catalog items are in the correct installation order, and then click **Save Order**.

9

Using App Survey, Clone/Migrate, and Support Tools to Perform Advanced Deployment Tasks

This section explains advanced deployment tasks that you can perform using App Portal that do not involve the checkout of an OSD task sequence catalog item in the App Portal storefront.

You can use **App Survey** to identify the installed applications on a source computer so that they can be selected, and then installed, onto a target computer. You can use **Clone/Migrate** to deliver the known application estate from a source computer to a target computer (outside of the realm of task sequence OS deployment). You can also execute custom commands/action on a selected resource on the **Support Tools** view.

📄

Note • *This section explains how to use App Survey, Clone/Migrate, and Support Tools to perform deployment tasks. For information on performing OS deployment using OSD task sequence catalog items (including migrating existing applications), see Using Task Sequence Catalog Items to Perform OS and Application Deployment.*

Information about using **App Survey**, **Clone/Migrate**, and **Support Tools** is presented in the following sections.

Table 9-1 • App Portal's App Survey and Clone/Migrate Features

Topic	Description
Using App Survey to Deploy Applications	Explains how to use **App Survey** to identify the installed applications on a source computer so that they can be selected, and then installed, onto a target computer.
Using Clone/Migrate to Migrate Applications to Another System	Explains how to use **Clone/Migrate** to deliver the known application estate from a source computer to a target computer (outside of the realm of task sequence OS deployment). This is commonly known as a "break/fix" scenario.
Reviewing Resource Information and Executing Commands/Actions on the Support Tools View	Describes how to select a user or computer on the **Support Tools** view and then execute a custom command that you have created.

Using App Survey to Deploy Applications

Important • App Survey is dependent upon having either a connection to FlexNet Manager Suite or the creation of App Portal inventory records for each application needing to be discovered for the migration process and then associating that inventory record with its associated software catalog item. For more information, see Identifying Existing Applications Using FlexNet Manager Suite or Identifying Existing Applications by Creating App Portal Application Inventory Records.

App Survey is a feature within App Portal that is used to identify the installed applications on a source computer so that they can be selected, and then installed, onto a target computer. It automates the procedure of migrating existing user applications to a new operating system/device.

The App Survey feature uses installation evidence and usage data to detect the installed applications that are installed on a user's system, and lists the discovered applications on the **App Survey** tab. After a user selects the applications that they want to migrate on the **App Survey** tab, the App Portal administrator can automatically migrate those selected applications to the user's new device.

The App Survey feature does not involve checking out a task sequence catalog item, or any catalog item, on the **Browse Catalog** tab using the Checkout Wizard. Instead individual catalog item requests are generated from the **Deployment Management > App Survey Results** view by the App Portal administrator.

Information about using the App Survey feature is presented in the following sections:

- Enabling the App Survey Tab

- Enabling Inventory Detection for App Survey

- Identifying Applications to Migrate on the App Survey Tab

- Viewing App Survey Results and Migrating Applications

- Performing Upgrade/Replacement via App Survey Deployment

Enabling the App Survey Tab

On the **App Survey** tab, users can identify which applications they want to have redeployed onto a new computer. In order for the **App Survey** tab to be displayed to users, it must be enabled. To enable the **App Survey** tab, perform the following steps.

Task   *To enable the App Survey tab:*

1. On the **Admin** tab, select **Site Management > Settings > Web Site**.

2. Open the **Catalog Appearance** tab.

3. Under **Catalog Tab Strip**, select **Display Application Survey Tab**.

4. Click **Save**.

Enabling Inventory Detection for App Survey

Important • App Survey is dependent upon having either a connection to FlexNet Manager Suite or the creation of App Portal inventory records for each application needing to be discovered for the migration process and then associating that inventory record with its associated software catalog item. For more information, see Identifying Existing Applications Using FlexNet Manager Suite or Identifying Existing Applications by Creating App Portal Application Inventory Records.

To enable inventory detection of catalog items so that App Portal can identify the catalog items installed on a user's existing , perform the following steps.

Task   **To enable inventory detection for App Survey:**

1. On the **Admin** tab, open the **OS Deployment** tab of the **Site Management > Settings > Deployment** view.

2. To enable users to select existing applications to migrate on the **App Survey** tab, select the **Enable application migration and installation of additional applications** option.

3. Click **Save**.

Identifying Applications to Migrate on the App Survey Tab

On the **App Survey** tab, users are prompted to identify which applications they want to have redeployed onto a new computer during OS deployment.

After users have selected applications on the **App Survey** tab, App Portal administrators can then review the results of this survey on the **Deployment > AppSurvey Results** view, and can then approve applications for redeployment.

To identify applications to migrate on the App Survey tab, perform the following steps.

Task   ***To identify applications to migrate on the App Survey tab:***

1. Open the **App Survey** tab. Applications that are installed on the user's connected device are listed.

2. Select all of the applications that you would like to be deployed on your new target system.

3. Click **Next**. The questions in the question template identified in the **Application Survey Question Template ID** field
    on the **Site Management > Settings > Web Site > Catalog Behavior** tab are listed.

4. Answer the displayed questions and click **Save Survey**. The survey responses are saved and the **Review Selections** panel opens, listing the user's selections.

Specifying a Question Template for App Survey

To specify which questions are displayed on the **Step 2: Answer Questions** step of an App Survey, perform the following steps.

Task   ***To specify a question template for App Survey:***

1. Create a question template containing questions that you want to ask during App Survey, as described in Creating a Question Template, and note the ID of that template.

2. Open the **Catalog Behavior** tab under **Site Management > Settings > Web Site**, and scroll down to the **Behaviors** area.

3. In the **Application Survey Question Template ID** field, enter the ID of the question template that you want to use, and click **Save**.

Viewing App Survey Results and Migrating Applications

As described in Identifying Applications to Migrate on the App Survey Tab, users can identify applications that they want to have migrated onto a new computer. The results of these surveys are listed on the **AppSurvey Results** view, where administrators can review the surveys and migrate the selected applications to the new computer.

Figure 9-1: App Survey Results View

To review the App Survey results and migrate applications, perform the following steps:

Task   **To review App Survey results:**

1. On the **Admin** tab, select **Deployment Management** > **AppSurvey Results**. The App Survey Results view opens.

2. Locate and double-click the survey of the user that you want to review. The **General** tab of the **App Survey Properties** dialog box opens.

3. Enter the **Target Machine Name** to which you want to migrate the selected applications and click **Set Name**.

4. Open the **Selected Applications** tab. The applications the user selected on the **App Survey** tab are listed.

5. Review the listed applications. To prevent an application from being deployed, select it and then click **Remove from deployment**.

6. Open the **Installed Applications** tab.

7. If any applications are listed here that you want to add to the deployment, select the application and click **Add to deployment**.

8. Open the **Questions** tab.

9. Review the answers to the questions provided by the users.

10. When you are done reviewing the survey, click **Validate**.

11. Close the **App Survey Properties** dialog box.

12. To initiate migration of the applications specified in the survey, select the survey on the **App Survey Results** view and click **Migrate Selected**. A catalog item request is automatically submitted for each of the applications specified in the survey to migrate them to the **Target Machine** that was specified on the **General** tab of the **App Survey Properties** dialog box. After the survey has been submitted, you can expand the survey to see a list of the applications and their install status:

Submitted catalog item requests are displayed on the **My Requests** tab.

> **Note** • You can also use the User Readiness feature in conjunction with **App Survey**. You could define a User Readiness record for a user/device that would result in an email notification being sent to a user to prompt them to perform an App Survey. For more information, see Using User Readiness Records to Schedule Users for OS Deployment.

Performing Upgrade/Replacement via App Survey Deployment

> **Note** • Upgrade/replacement requires installation evidence provided by either FlexNet Manager Suite or App Portal inventory records, as described in Identifying Existing Applications to Include in OS Deployment.

The **Upgrade/Replacement** feature in conjunction with **App Survey** makes it easy for you to update or replace applications at the same time you migrate them to a new computer. The **Upgrade/Replacement** feature enables you to specify that if a mapped application is selected for migration via App Survey, that application will be replaced by the specified replacement catalog item (either a newer version or a replacement catalog item).

If you have designated that a catalog item should be upgraded or replaced by another catalog item, as described in Using Upgrade/Replacement to Identify New/Replacement Versions, the replacement catalog item will be migrated via App Survey instead of the original catalog item.

If a catalog item that has been designated as one that will be upgraded/replaced, when you hover over the box icon in the **Recommendation** column of the **App Survey** tab, the name of the application that it will be upgraded to is listed.

Figure 9-2: Upgrade/Replace Message on the App Survey Results Tab

Using Clone/Migrate to Migrate Applications to Another System

You can use the App Portal **Clone/Migrate** feature deliver the known application estate from a source computer to a target computer (outside of the realm of task sequence OS deployment). This is commonly known as a "break/fix" scenario.

The **Clone / Migrate** feature, found on the **Support Tools** tab, provides administrators an avenue to use App Portal to deliver the operating system and applications while limiting access to the System Center Configuration Manager console.

Figure 9-3: Clone/Migrate View on the Support Tools Tab

One unique thing about using App Portal's Clone/Migrate feature, instead of the other OS deployment features, is that you can use Clone/Migrate with Symantec Altiris Client Management Suite, not just System Center Configuration Manager. This is because, unlike App Survey, Clone/Migrate places the target machine into the appropriate collection or filter depending upon the deployment technology. In other words, Clone/Migrate works outside of the Microsoft System Center Configuration Manger task sequence process.

The following sections provide additional details about the App Portal Clone/Migrate feature:

- How Clone/Migrate Works

- Enabling a Catalog Item for Clone/Migrate

- Performing a Clone/Migrate Operation

How Clone/Migrate Works

Clone/Migrate relies on mapping installation and usage evidence to a catalog item, which is then associated to a deliverable product in the deployment system.

The following figure provides a visualization on the mapping of application data using Clone/Migrate.

Figure 9-4: Clone/Migrate Overview Diagram

Clone/Migrate leverages a combination of inventory and usage evidence.

- **Inventory evidence is collected**—System Center Configuration Manager hardware inventory collects the inventory evidence that is consumed by both FlexNet Manager and App Portal.

- **Usage evidence is collected**—System Center Configuration Manager software metering or asset intelligence collects the usage evidence that is consumed by both FlexNet Manager and App Portal.

- **Catalog item is associated with application in System Center Configuration Manager**—The catalog item is associated to the application or package in System Center Configuration Manager. The catalog item is also associated with the software inventory and usage evidence as outlined above.

- **Clone/Migrate identifies applications to include**—Clone/Migrate uses the software inventory evidence that is associated to the catalog item to identify which application or package to include in the Clone/Migrate process. Clone/Migrate displays usage information based on the software usage evidence that is associated to the catalog item.

- **Software is deployed**—The software titles which are selected during the clone/migrate process are then inserted into each of the associated install collections with System Center Configuration Manager for deployment. System Center Configuration Manager completes the deployment as designed.

Enabling a Catalog Item for Clone/Migrate

Clone/Migrate requires that application detection is enabled on each catalog item that is expected to participate in Clone/Migrate, just as App Survey does. To review the steps to take in order to enable a catalog item for application detection, review the Enabling Inventory Detection for App Survey section provided above.

Also, for each software catalog item which will participate in the OS deployment build process, you need to set several properties on that catalog item's **Catalog Item Properties** dialog box.

Task **To configure catalog item settings for Clone/Migrate deployment:**

1. Open the **General > Global** tab of the **Catalog Item Properties** dialog box for the software catalog item.

2. Under **Request options**, select **Show for Clone/Migrate?**

3. Click **Save**.

Performing a Clone/Migrate Operation

Before beginning a Clone/Migrate operation, first identify the source destination computers.

To perform a Clone/Migrate operation, perform the following steps.

Task   ***To perform a Clone/Migrate operation:***

1. On the **Support Tools** tab, click **Clone/Migrate**. The **Clone/Migrate** view opens.

2. From the **Select source computer** list, select or enter the name of the source computer that will have installed applications evaluated for migration to the destination computer.

3. From the **Select destination computer** list, select or enter the name of the destination computer where the selected applications will be installed.

4. The **Associated user** field displays the name of the owner of the destination computer, based on the user-to-computer relationship mapping setting that is configured for the environment. If necessary, use the **Change User** button to update the user association for the destination computer.

5. Optionally, select the following options:

    •   After you migrate the applications, if you want them to be uninstalled from the source computer, select the **Uninstall from source computer when possible** option. When this option is selected, App Portal will schedule the uninstallation of any application that App Portal has an uninstall package for assigned in the catalog item associated with that application.

    •   If you want the target user to be able to see the request listed on the **My Requests** page (when the user selects the **Clone/Migrate** filter under **Advanced** search), select the **Make request visible to target** users option. The user will be able to view the status and progress of the request.

    •   If you want any pending requests that are currently assigned to the source computer to be changed to the target, or destination computer, select the **Update pending requests to target new machine** option.

6. Click the **Compare Computers** button to evaluate the installed applications on the source and destination computers, and display the details available for this Clone/Migrate transaction. In the Clone/Migrate details pane, the following information is listed for each application:

Column	Details
Applications available migration	Lists the catalog item title for the application discovered on the source computer.

Column	Details
Cost	Lists any cost associated with the discovered application.
Recommendation	Lists icons that provide a recommendation on whether or not the discovered application should be included in the Clone/Migrate process. There are three possible recommendations icons listed:
	• **Thumbs up**—Listed for any application that has usage information and that is used within the usage threshold set for the environment or user. It is also listed for applications which have no usage information.
	• **Thumbs down**—Listed for any application that has usage information and the usage details exceed the usage threshold set for the environment or user.
	• **Already installed**—Listed in the event that the application already exists on the destination computer.
Information	Includes additional details regarding the discovered application. This may include general installation or usage information.

7. In the Clone/Migrate details pane, select the applications that should be included in the Clone/Migrate process.

8. Review additional configuration items and set them as desired.

9. When ready to initiate the migration, click the **Migrate Programs** button. A message appears when the migration has been successfully initiated.

Reviewing Resource Information and Executing Commands/Actions on the Support Tools View

The **Support Tools** view, which is opened by selecting **Support Tools** on the **Support Tools** tab, can be used to search for users and computers, and then select a support action on a selected user or computer.

Figure 9-5: Support Tools View of Support Tools Tab

On the **Support Tools** view, you can select a user or computer and then execute a custom command that you have created using the **Commands and Action** function under **Site Management**.

Figure 9-6: Site Management > Commands and Actions > Script Commands

- Viewing Resource Details on the Support Tools View

- Creating Commands/Actions to Execute on Support Tools View

- Executing Commands/Actions on the Support Tools View

Viewing Resource Details on the Support Tools View

On the **Support Tools** view, you can search for a user or computer and then view details of that resource on its **Software Catalog Details** dialog box.

To view resource details, perform the following steps.

Task   **To view resource details:**

1. On the **Support Tools** tab, click **Support Tools**. The **Support Tools** view opens.

2. Enter search terms in the filter boxes to locate a user or computer. Matching resources are listed.

3.   Double click a resource. The **Software Catalog Details** dialog box for that resource opens, displaying information on four tabs: **Assigned Software**, **Installed Software (ARP)**, **Installed Software (AI)**, and **Deploy Software**.

4.   On the three subtabs of the **Assigned Software** tab, view information regarding installed software, computer assignments, and user assignments. This information is obtained from SCCM Inventory.

5.   On the **Installed Software (ARP)** tab, view a list of software that was installed manually. This information is obtained from SCCM Inventory.

6. On the **Installed Software (AI)** tab, view a list of software that was installed automatically. This information is obtained from SCCM Inventory.

7. On the **Deploy Software** tab, all catalog items that have the **Show on support tools?** option selected on the **General > Global** tab of the **Catalog Item Properties** dialog box will be displayed. From the Deploy Software tab, catalog item requests can be submitted by clicking **Deploy Software**.

Creating Commands/Actions to Execute on Support Tools View

On the **Support Tools** view, you can select a user or computer and then execute a custom command that you have created using the **Commands and Action** function under **Site Management**.

Commands allow arbitrary commands to be executed against a selected machine from the **Support Tools** tab in the software store or as part of a request at one or more stages during the request life cycle.

- Client commands and server commands that are executed run under the context of the visiting user and are invoked using JavaScript.

- Server commands run under the context of the App Portal account specified during setup.

- Use of commands executed from the client requires modification of browser security settings to allow Active X content.

Commands and actions are defined on the **Site Management > Commands and Actions** view. For information on creating custom commands and actions, see the following topics:

- Script Commands

- Web Service Commands

- Request Commands

Executing Commands/Actions on the Support Tools View

On the **Support Tools** view, you can select a user or computer and then execute a custom command that you have created using the **Commands and Action** function under **Site Management**.

To execute a command/action on a selected user or computer on the **Support Tools** view, perform the following steps.

Task **To execute a command/action on a user or computer:**

1. On the **Support Tools** tab, click **Support Tools**. The **Support Tools** view opens.

2. Enter search terms in the filter boxes to locate a user or computer. Matching resources are listed.

3. Click the gear icon in the **Action** column next to a resource listing. A menu of available commands/actions are listed.

4. Select an command/action from the list. The command/action is executed.

10

Variables Reference

App Portal uses the following variables:

Table 10-1 • App Portal Variables

Variable	Description
`##Action##`	Install, uninstall, repair.
`##ApprovalHistory##`	All approval history (who has approved).
`##Approver##`	Shows the current approver.
`##APPROVALKEYWORDS##`	Keywords that the approver then enters on the reply of the email in order to approve the request.
`##ApproveRequest##`	A URL link directly to the My Requests tab selecting and showing only that single request and opens the approval pop-up asking for approval reason. This variable is only valid if there are no pending approval questions.
`##AUTOAPPROVEREASON##`	Used in the Flexible Approval process, this displays comments relating to the approve or reject reason if the approver has added any comments.
`##AutoApproveRequest##`	Auto approves the request without asking for approval reason and no confirmation. This variable is only valid if there are no pending approval questions
`##EMAILAPPROVALMAILTOLINKS##`	Used in Flexible Approval, this provides the content and links for MailTo links.
`##EMAILAPPROVALPLACEHOLDER##`	Used in Flexible Approval, this provides the content for the Flexible Approval details.

Table 10-1 • App Portal Variables

Variable	Description
`##InstallBegin##`	When the installation should begin (maximum SCCM polling interval configuration setting plus insert date).
`##InstallDate##`	Scheduled install date in client time.
`##LastApprover##`	Shows last approver, if any.
`##LastApproverNotes##`	Notes of the last approver.

`##Leased##`	Outputs the following:
	
	`The lease for this software will expire " &`
	`    Request_Data.TotalDaysLeased & " days after the install`
	`    completes."`

`##LicenseData##`	Output of the license data related to a request (inventory group, cost, owned, remaining, used).
`##manager##`	Manager of the requester.
`##manager## (##Requester_ manager##)`	Manager of the requester, target user, current user.
`##QuestionID:XX:Message##`	Shows the message for the associated question response.
`##QuestionID:XX##`	Where XX is the question ID number; we will put the response to the question in this variable.
`##Questions_CSV##`	All questions and responses in CSV format. (Used import into other data sources using email.)
`##REJECTKEYWORDS##`	Keywords that the approver of a software catalog request item then enters as first word in the reply of the email in order to reject the request.
`##RejectRequest##`	A URL link directly to the My Requests tab selecting and showing only that single request and opens the rejection pop-up asking for rejection reason. This variable is only valid if there are no pending approval questions.
`(RequestID:##REQUESTID##)`	Used in Flexible Approval, this provides the ID of the catalog request.
`##ReviewQuestions##`	A URL link directly to the Unanswered Question tab of the Details view of an order.
`##UserReadinessXX##`	All columns from the `WD_UserReadiness` table where XX is the column name.

Table 10-1 • App Portal Variables

Variable	Description
##ViewApprovers##	A URL link directly to the Approvers tab of the Details view of an order
##ViewDetails##	A URL link directly to the Details tab of the Details view of an order
##ViewInventory##	A URL link directly to the Inventory tab of the Details view of an order.
##ViewQuestions##	A URL link directly to the Questions tab of the Details view of an order.
##ViewRequest##	A URL link directly to the My Requests tab selecting and showing only that single request.
##WS_XX##	Where XX is the web service ID used to pass the result of a web service call (if any WS actions associated with the request).

11

App Portal API Reference

This section describes App Portal's legacy API web methods and integration API web methods. Using web services allows for cross platform support from a variety of development languages.

- App Portal Integration API Web Methods

- Legacy API Web Methods

- VBScript Examples

- PowerShell Example

Note • App Portal also has a set of API web methods, but they are SOAP based, while App Broker's API is REST and SOAP based. For more information, see App Broker REST API Reference.

App Portal Integration API Web Methods

The App Portal integration API is exposed as a Web Service, located at the following URL:

```
http://[AppPortalServer]/ESD/ws/integration.asmx
```

Visit this page to see detailed examples of these web methods in SOAP 1.1, SOAP 1.2, HTTP GET, and HTTP POST format.

Syntax

These web methods use the following syntax:

```
webMethodName (parameter1value, parameter2value, parameter3value, ...)
```

Parameter values must be listed in the order in which they appear in the **Parameters** tables provided in this section, separated by commas. Strings must be enclosed in double quotes. Here is an example of a web method with multiple parameters, some of which are strings:

```
ExpireAlertsForAppByComputer ("MGS-APP-00000140330", "DT-ITA-080950", 1)
```

Web Methods

The following App Portal integration API web methods are documented in this section:

- AddAltirisPackageOrPolicy

- AddAltirisPolicy

- AddCasperPackage

- AddCM12App

- AddCM12Package

- AddCMPackage

- AddCMTaskSequence

- AddConfigMgrApp

- AddConfigMgrPackage

- AddFlexeraIdForMyAppsLicenseReclamation

- AddUsertoCatalogSecurity

- AddWorkflowToCatalogItem

- AttachCM12ApplicationDeployment

- AttachCM12PackageDeployment

- AttachCM12TaskSequenceDeployment

- AttachConfigMgrApplicationDeployment

- AttachConfigMgrPackageDeployment

- AttachConfigMgrTaskSequenceDeployment

- CancelRequest

- CreateAirWatchDeploymentForCatalogItem

- CreateCategory

- CreateDefaultData

- CreateGeneralCatalogItem

- CreateGroupCatalog

- CreateManagerWorkflow

- CreateNewCatalogItem

- CreateQuestionTemplate

- CreateSubCategory

- CreateWorkflow

- CreateWorkflowGroup

- DeleteAlertsForApp

- DeleteAlertsForAppByComputer

- DeleteAlertsForAppByUser

- DeleteAlertsForComputer

- DeleteAlertsForUser

- EnableAllSoftwareCatalogSyncInToServiceNow

- EnableSoftwareCatalogSyncInToServiceNow

- ExpireAlertsForApp

- ExpireAlertsForAppByComputer

- ExpireAlertsForAppByUser

- ExpireAlertsForComputer

- ExpireAlertsForUser

- GetAlertsForAlertAction

- GetAlertsForLicenseReclamation

- GetCatalogItemTemplates

- GetCategories

- GetCategoryByID

- GetCategoryByName

- GetDataForUninstallRequestWithNoAlert

- GetLicenseDetails

- GetProduceCodeForUninstall

- GetResolvedRequestVariables

- GetSoftwaresToUninstallFromDevice

- GetVersion

- InsertAlertAction

- InsertLicenseReclamationAlert

- PublishAltirisCatalogItemEx

- PublishCatalogItem

- PublishCatalogItemEx

- PublishCatalogItemForPackage

- ReadDB

- RemoveAltirisPolicy

- SetAlternateApproverAndOutOfOffice

- SetInstallStatus

- SetInstallStatusWithLease

- StartDeployment

- SynchCurrentForest

- SyncSingleUserComputer

- UpdateCatalogLicenseInfo

- UpdateCatalogLicensePosition

- UpdateCatalogLicenseScope

- UpdateDB

- UpdateMyAppsLicenseReclamationPolicyForFlexeraID

- UpdateUninstallStatusForDevice

AddAltirisPackageOrPolicy

You can use the AddAltirisPackageOrPolicy web method to add an Altiris package or policy to a catalog item.

Parameters

The AddAltirisPackageOrPolicy web method includes the following parameters:

Table 11-1 • AddAltirisPackageOrPolicy Parameters

#	Parameters	Data Type	Description
1.	**catalogItemID**	Integer	ID of the catalog item.
2.	**packageOrPolicyID**	String (GUID)	GUID of policy or package.
3.	**programData**	String	String of the format InstallType(Integer)| programID where InstallType may be one of the following: • **0**—Install • **1**—Uninstall • **2**—Repair The programID is a string. For example: 0|programID
4.	**deploymentTarget**	Enum Value	Use one of the following values: • **0**—DeployToUser • **1**—DeployToComputer

Return Value

Returns one of the following values:

- Returns TRUE for success
- Returns FALSE for failure

AddAltirisPolicy

You can use the `AddAltirisPolicy` web method to add an Altiris policy to a catalog item.

Parameters

The `AddAltirisPolicy` web method includes the following parameters:

Table 11-2 • AddAltirisPolicy Parameters

#	Parameters	Data Type	Description
1.	**catalogItemID**	Integer	ID of the catalog item.
2.	**packageGuid**	String	GUID of the Altiris policy.
3.	**programGuid**	String	GUID of the Altiris program.
4.	**programType**	String	Enter one of the following values to identify the purpose of this Altiris policy: • **Install** • **Uninstall** • **Repair**
5.	**deploymentTarget**	Enum value	Use one of the following values: • **0**—DeployToUser • **1**—DeployToComputer

Return Value

Returns one of the following values:

- Returns TRUE for success.
- Returns FALSE for failure.

AddCasperPackage

You can use the `AddCasperPackage` web method to add a Casper package to a catalog item.

Parameters

The AddCasperPackage web method includes the following parameters:

Table 11-3 • AddCasperPackage Parameters

#	Parameters	Data Type	Description
1.	catalogItemId	Integer	ID of the catalog item.
2.	deploymentPackageId	Integer	ID the package in Casper.
3.	distributionPoint	String	Casper distribution point.
4.	createUninstall	Boolean	Enter **True** if catalog item is to trigger an uninstall; otherwise, enter **False**.

Return Value

Returns one of the following values:

- Returns TRUE for success.
- Returns FALSE for failure.

AddCM12App

You can use the AddCM12App web method to add a System Center 2012 Configuration Manager application to a catalog item.

Parameters

The AddCM12App web method includes the following parameters:

Table 11-4 • AddCM12App Parameters

#	Parameters	Data Type	Description
1.	catalogItemID	Integer	ID of the catalog item.
2.	cm12AppID	String	Application ID in System Center 2012 Configuration Manager.
3.	deploymentTarget	Enum value	Use one of the following values: • **0**—DeployToUser • **1**—DeployToComputer
4.	createUninstall	Boolean	Enter **True** if catalog item is to trigger an uninstall; otherwise, enter **False**.

Return Value

Returns one of the following values:

- Returns TRUE for success

- Returns FALSE for failure

AddCM12Package

You can use the AddCM12Package web method to add a System Center 2012 Configuration Manager package to a catalog item.

Parameters

The AddCM12Package web method includes the following parameters:

Table 11-5 • AddCM12Package Parameters

#	Parameters	Data Type	Description
1.	**catalogItemID**	Integer	ID of catalog item.
2.	**cmPackageID**	String	Package ID in System Center 2012 Configuration Manager.
3.	**cmPackageData**	String	String in the format of *InstallType*|*PackageName*, where: • *InstallType* is one of the following: • **0**—Install • **1**—Uninstall • **2**—Repair • *PackageName* is a string that identifies the package. For example: `0|AdobeReader`

Return Value

Returns one of the following values:

- Returns TRUE for success

- Returns FALSE for failure

AddCMPackage

The AddCMPackage web method is used internally to add advertisements to a catalog item.

Parameters

The AddCMPackage web method includes the following parameters:

Table 11-6 • AddCMPackage Parameters

#	Parameters	Data Type	Description
1.	**catalogItemID**	Integer	ID of the catalog item.
2.	**cmServer**	String	System Center Configuration Manager site server.
3.	**cmPackageID**	String	System Center Configuration Manager package ID.
4.	**deploymentSettings**	Object of class deployment	Contains number of properties.
5.	**deploymentTechnology**	Enum value	Enter one of the following values to identify the deployment technology: • **1**—System Center 2012 Configuration Manager • **3**—Altiris • **4**—AirWatch / Google Android • **5**—AirWatch / iOS • **6**—AirWatch / Windows • **7**—Casper • **8**—ConfigMgr • **0**—Unknown

Return Value

Returns one of the following values:

• Returns TRUE for success

• Returns FALSE for failure

AddCMTaskSequence

You can use the AddCMTaskSequence web method to add a System Center Configuration Manager task sequence to a catalog item.

Parameters

The `AddCMTaskSequence` web method includes the following parameters:

Table 11-7 • AddCMTaskSequence Parameters

#	Parameters	Data Type	Description
1.	**catalogItemID**	Integer	ID of the catalog item.
2.	**cmServer**	String	Site server.
3.	**cmPackageID**	String	System Center Configuration Manager package ID.
4.	**deploymentSettings**	Object of class deployment	Contains number of properties.
5.	**deploymentTechnology**	Enum value	Enter one of the following values to identify the deployment technology: • **8**—System Center Configuration Manager / ConfigMgr (Current Branch) • **1**—System Center 2012 Configuration Manager • **3**—Altiris • **0**—Unknown
6.	**isOsd**	Boolean	Enter **True** if OSD; otherwise, enter **False**.

Return Value

Returns one of the following values:

• Returns TRUE for success

• Returns FALSE for failure

AddConfigMgrApp

You can use the `AddConfigMgrApp` web method to add a System Center Configuration Manager (Current Branch) application to a catalog item.

Parameters

The `AddConfigMgrApp` web method includes the following parameters:

Table 11-8 • AddConfigMgrApp Parameters

#	Parameters	Data Type	Description
1.	**catalogItemID**	Integer	ID of the catalog item.

Table 11-8 • AddConfigMgrApp Parameters (cont.)

#	Parameters	Data Type	Description
2.	**configMgrAppID**	String	ID of the application in System Center Configuration Manager (Current Branch).
3.	**deployTarget**	Enum value	Use one of the following values: • **0**—DeployToUser • **1**—DeployToComputer
4.	**createUninstall**	Boolean	Enter **True** if catalog item is to trigger an uninstall; otherwise, enter **False**.

Return Value

Returns one of the following values:

- Returns TRUE for success.

- Returns FALSE for failure.

AddConfigMgrPackage

You can use the AddConfigMgrPackage web method to add a System Center Configuration Manager (Current Branch) package to a catalog item.

Parameters

The AddConfigMgrPackage web method includes the following parameters:

Table 11-9 • AddConfigMgrPackage Parameters

#	Parameters	Data Type	Description
1.	**catalogItemID**	Integer	ID of the catalog item.
2.	**cmPackageID**	String	ID of the package in System Center Configuration Manager (Current Branch).

Table 11-9 • AddConfigMgrPackage Parameters (cont.)

#	Parameters	Data Type	Description
3.	**cmPackageData**	String	String in the format of *InstallType|PackageName*, where:

InstallType is one of the following:

- **0**—Install
- **1**—Uninstall
- **2**—Repair

- *PackageName* is a string that identifies the package.

For example:

0|AdobeReader

Return Value

Returns one of the following values:

- Returns TRUE for success.
- Returns FALSE for failure.

AddFlexeraIdForMyAppsLicenseReclamation

You can use the AddFlexeraIdForMyAppsLicenseReclamation web method to add a Flexera Identifier to a catalog item, thus enabling My Apps license reclamation.

Parameters

The AddFlexeraIdForMyAppsLicenseReclamation web method includes the following parameters:

Table 11-10 • AddFlexeraIdForMyAppsLicenseReclamation Parameters

#	Parameters	Data Type	Description
1.	**flexeraID**	String	Flexera identifier of the catalog item, as defined in FlexNet Manager Suite.

Return Value

Returns one of the following values:

- Returns TRUE for success.
- Returns FALSE for failure.

AddUsertoCatalogSecurity

You can use the addUsertoCatalogSecurity web method to add a user to catalog security group.

Parameters

The addUsertoCatalogSecurity web method includes the following parameters:

Table 11-11 • addUsertoCatalogSecurity Parameters

#	Parameters	Data Type	Description
1.	**userNameWithDomain**	String	Domain name\User Name

Return Value

Returns one of the following values:

- Returns TRUE for success
- Returns FALSE for error

AddWorkflowToCatalogItem

You can use the addWorkflowToCatalogItem web method to add a workflow to a catalog item.

Parameters

The addWorkflowToCatalogItem web method includes the following parameters:

Table 11-12 • addWorkflowToCatalogItem Parameters

#	Parameters	Data Type	Description
1.	**catalogName**	String	Name of the catalog item.
2.	**workflowName**	String	Name of the workflow to be attached.

Return Value

Returns one of the following values:

- Returns TRUE for success.
- Returns FALSE for error.

AttachCM12ApplicationDeployment

You can use the AttachCM12ApplicationDeployment web method to attach a System Center 2102 Configuration Manager deployment to an existing application catalog item.

Parameters

The `AttachCM12ApplicationDeployment` web method includes the following parameters:

Table 11-13 • AttachCM12ApplicationDeployment Parameters

#	Parameters	Data Type	Description
1.	**catalogItemID**	Integer	ID of the catalog item.
2.	**deploymentId**	String	Deployment ID of the catalog item in System Center Configuration Manager.
3.	**programType**	String	Enter one of the following values to identify the purpose of this catalog item: • **Install** • **Uninstall** • **Repair**

Return Value

Returns one of the following values:

- Returns TRUE for success.
- Returns FALSE for error.

AttachCM12PackageDeployment

You can use the `AttachCM12PackageDeployment` web method to attach a System Center 2102 Configuration Manager deployment to an existing package catalog item.

Parameters

The `AttachCM12PackageDeployment` web method includes the following parameters:

Table 11-14 • AttachCM12PackageDeployment Parameters

#	Parameters	Data Type	Description
1.	**catalogItemID**	Integer	ID of the catalog item.
2.	**advertisementId**	String	Advertisement ID of package in System Center 2012 Configuration Manager.

Table 11-14 • AttachCM12PackageDeployment Parameters (cont.)

#	Parameters	Data Type	Description
3.	**programType**	String	Enter one of the following values to identify the purpose of this catalog item: ● **Install** ● **Uninstall** ● **Repair**

Return Value

Returns one of the following values:

● Returns TRUE for success.

● Returns FALSE for error.

AttachCM12TaskSequenceDeployment

You can use the `AttachCM12TaskSequenceDeployment` web method to attach a System Center 2012 Configuration Manager deployment to an existing task sequence catalog item.

Parameters

The `AttachCM12TaskSequenceDeployment` web method includes the following parameters:

Table 11-15 • AttachCM12TaskSequenceDeployment Parameters

#	Parameters	Data Type	Description
1.	**catalogItemID**	Integer	ID of the catalog item.
2.	**advertisementId**	String	Advertisement ID of task sequence in System Center 2012 Configuration Manager.
3.	**programType**	String	Enter one of the following values to identify the purpose of this catalog item: ● **Install** ● **Uninstall** ● **Repair**
4.	**isOsdDeployment**	Boolean	Enter **True** if this task sequence is an OSD deployment; otherwise, enter **False**.

Return Value

Returns one of the following values:

- Returns TRUE for success.

- Returns FALSE for error.

AttachConfigMgrApplicationDeployment

You can use the `AttachConfigMgrApplicationDeployment` web method to attach a System Center Configuration Manager (Current Branch) deployment to an existing application catalog item.

Parameters

The `AttachConfigMgrApplicationDeployment` web method includes the following parameters:

Table 11-16 • AttachConfigMgrApplicationDeployment Parameters

#	Parameters	Data Type	Description
1.	**catalogItemID**	Integer	ID of the catalog item.
2.	**deploymentId**	String	Deployment ID of the application in System Center Configuration Manager (Current Branch).
3.	**programType**	String	Enter one of the following values to identify the purpose of this catalog item: • **Install** • **Uninstall** • **Repair**

Return Value

Returns one of the following values:

- Returns TRUE for success.

- Returns FALSE for error.

AttachConfigMgrPackageDeployment

You can use the `AttachConfigMgrPackageDeployment` web method to attach a System Center Configuration Manager (Current Branch) deployment to an existing package catalog item.

Parameters

The `AttachConfigMgrPackageDeployment` web method includes the following parameters:

Table 11-17 • AttachConfigMgrPackageDeployment Parameters

#	Parameters	Data Type	Description
1.	**catalogItemID**	Integer	ID of the catalog item.
2.	**advertisementId**	String	Advertisement ID of the package in System Center Configuration Manager (Current Branch).
3.	**programType**	String	Enter one of the following values to identify the purpose of this catalog item: **Install** **Uninstall** **Repair**

Return Value

Returns one of the following values:

- Returns TRUE for success.
- Returns FALSE for error.

AttachConfigMgrTaskSequenceDeployment

You can use the `AttachConfigMgrTaskSequenceDeployment` web method to attach a System Center Configuration Manager (Current Branch) deployment to an existing task sequence catalog item.

Parameters

The `AttachConfigMgrTaskSequenceDeployment` web method includes the following parameters:

Table 11-18 • AttachConfigMgrTaskSequenceDeployment Parameters

#	Parameters	Data Type	Description
1.	**catalogItemID**	Integer	ID of the catalog item.
2.	**advertisementId**	String	Advertisement ID of the task sequence in System Center Configuration Manager (Current Branch).

Table 11-18 • AttachConfigMgrTaskSequenceDeployment Parameters (cont.)

#	Parameters	Data Type	Description
3.	**programType**	String	Enter one of the following values to identify the purpose of this catalog item: • **Install** • **Uninstall** • **Repair**
4.	**isOsdDeployment**	Boolean	Enter **True** if the catalog item is for OSD deployment; otherwise, enter **False**.

Return Value

Returns one of the following values:

- Returns TRUE for success.
- Returns FALSE for error.

CancelRequest

You can use the `CancelRequest` web method to cancel an App Portal request.

Parameters

The `CancelRequest` web method includes the following parameters:

Table 11-19 • CancelRequest Parameters

#	Parameters	Data Type	Description
1.	**RequestId**	Integer	ID number of the request.

Return Value

Returns one of the following values:

- Returns TRUE for success
- Returns FALSE for failure

CreateAirWatchDeploymentForCatalogItem

You can use the `CreateAirWatchDeploymentForCatalogItem` web method to associate AirWatch mobile apps with existing catalog items.

Parameters

The CreateAirWatchDeploymentForCatalogItem web method includes the following parameters:

Table 11-20 • CreateAirWatchDeploymentForCatalogItem Parameters

#	Parameters	Data Type	Description
1.	**PackageId**	Integer	Package ID (Catalog ID).
2.	**LocationGroupId**	Integer	LocationGroup ID of the AirWatch mobile app.
3.	**BundleId**	String	Bundle ID of the AirWatch mobile app.
4.	**AppId**	Integer	App ID of the AirWatch mobile app.
5.	**Supported**	Supported	• 0 or NONE if the supported device is Android or if it is not known. • 1 or IPHONE_ONLY if the mobile app is supported only on iPhone. • 2 or IPAD_ONLY if the mobile app is supported only on iPad. • 3 or IPHONE_AND_IPAD if the mobile app is supported on both iPhone and iPad.

Return Value

Returns one of the following values:

- Returns TRUE for success
- Returns FALSE for error

CreateCategory

You can use the CreateCategory web method to create a parent category.

Parameters

The CreateCategory web method includes the following parameters:

Table 11-21 • CreateCategory Parameters

#	Parameters	Data Type	Description
1.	**categoryName**	String	Name of the category.

Return Value

Returns one of the following values:

- Returns TRUE for success

- Returns FALSE for error

CreateDefaultData

You can use the `createDefaultData` web method to add sample data to the application. This web method creates sample catalog items, workflows and approval groups, and question templates, and attaches workflows to catalog items.

Parameters

This web method does not have any parameters.

Return Value

Returns one of the following values:

- Returns TRUE for success

- Returns FALSE for error

CreateGeneralCatalogItem

You can use the `createGeneralCatalogItem` web method to add a new general catalog item.

Parameters

The `createGeneralCatalogItem` web method includes the following parameters:

Table 11-22 • createGeneralCatalogItem Parameters

#	Parameters	Data Type	Description
1.	**catalogName**	String	Name of the catalog item.
2.	**shortDescription**	String	Short description of the catalog item.
3.	**longDescription**	String	Long description of the catalog item.
4.	**categoryName**	String	Name of the category where the catalog item should reside. *Note • You can only specify one category name. This value must not be empty or refer to a category that does not exist.*
5.	**catalogTemplateName**	String	Catalog item ID or Template Name of the catalog item. *Note • This value can be empty.*

Table 11-22 • createGeneralCatalogItem Parameters (cont.)

#	Parameters	Data Type	Description
6.	**questionTemplateName**	String	Name of the Question Template. 📄 **Note •** *This value can be empty.*

Return Value

Returns one of the following values:

- Returns TRUE for success

- Returns FALSE for error

📄

Note • *FALSE status could be returned if no category name was specified, a non-existent category name was specified, a wrong question template name was specified, or if a catalog item already exists with same name as the new catalog item.*

CreateGroupCatalog

You can use the createGroupCatalog web method to add a new group catalog item. You can add other catalog items as to this new group catalog item.

Parameters

The createGroupCatalog web method includes the following parameters:

Table 11-23 • createGroupCatalog Parameters

#	Parameters	Data Type	Description
1.	**catalogNameArray**	Array List	Array list of catalog items that will be added to the new group catalog item.
2.	**shortDescription**	String	Short description of the group catalog item.
3.	**longDescription**	String	Long description of the group catalog item.
4.	**categoryName**	String	Name of the category where the group catalog item should reside. 📄 **Note •** *You can only specify one category name. This value must not be empty or refer to a category that does not exist.*

Table 11-23 • createGroupCatalog Parameters (cont.)

#	Parameters	Data Type	Description
5.	**Title**	String	Name of the group catalog item.

Note • This value can be empty.

Return Value

Returns one of the following values:

● Returns TRUE for success

● Returns FALSE for error

Note • FALSE status could be returned if no category name was specified, a non-existent category name was specified, or if a catalog item already exists with same name as the new catalog item.

CreateManagerWorkflow

You can use the `createManagerWorkflow` web method to create a new manager workflow where the approver is the manager of the requester.

Parameters

The `createManagerWorkflow` web method includes the following parameters:

Table 11-24 • createManagerWorkflow Parameters

#	Parameters	Data Type	Description
1.	**workflowName**	String	Name of the new workflow.

Return Value

Returns one of the following values:

● Returns TRUE for success

● Returns FALSE for error

CreateNewCatalogItem

You can use the `CreateNewCatalogItem` web method to create a new catalog item.

Parameters

The CreateNewCatalogItem web method includes the following parameters:

Table 11-25 • CreateNewCatalogItem Parameters

#	Parameters	Data Type	Description
1.	**productName**	String	Name of the product.
2.	**companyName**	String	Name of the company.
3.	**version**	String	Product version.
4.	**searchKeywords**	String	Keywords that help search for this product.
5.	**shortDescription**	String	Short description of the product.
6.	**longDescription**	String	Long description of the product.
7.	**Type**	Integer	Type of the product or packageType. The following values are supported: • **0**—Software • **1**—General • **3**—Group • **4**—Task Sequence • **15**—System Center 2012 Configuration Manager Application • **18**—Altiris Application • **19**—AirWatch / Android Application • **20**—AirWatch / iOS Application • **21**—AirWatch / iPad Application • **22**—AirWatch / Windows Application • **23**—AirWatch / Windows 8 Application • **25**—Casper Package
8.	**visible**	Boolean	Enter **True** to make catalog item visible on the **Browse Catalog** page; otherwise, enter **False**.
9.	**icon**	Byte Array	Icon of the product.
10.	**iconExtension**	String	Icon extension.
11.	**flexeraID**	String	Flexera ID of the product.

Table 11-25 • CreateNewCatalogItem Parameters (cont.)

#	Parameters	Data Type	Description
12.	**templatePackageID**	Integer	Template package ID from which the structure be followed while creating new catalog item. '0' otherwise.
13.	**csvCategoryNames**	String	Single category name or comma separated category names.
14.	**createdBy**	String	Created by.

Return Value

Returns one of the following values:

- Returns integer greater than 0 for success
- Returns -1 for error

CreateQuestionTemplate

You can use the `createQuestionTemplate` web method to create new question template.

Parameters

The `createQuestionTemplate` web method includes the following parameters:

Table 11-26 • createQuestionTemplate Parameters

#	Parameters	Data Type	Description
1.	**templateName**	String	Name of the question template.
2.	**questionTitle**	String	Title of the question.
3.	**questionText**	String	Description of the question.

Return Value

Returns one of the following values:

- Returns TRUE for success
- Returns FALSE for error

CreateSubCategory

You can use the `createSubCategory` web method to create a sub category to an existing category.

Parameters

The createSubCategory web method includes the following parameters:

Table 11-27 • createSubCategory Parameters

#	Parameters	Data Type	Description
1.	categoryName	String	Name of the category.
2.	parentcategoryName	String	Name of the parent category.

Return Value

Returns one of the following values:

- Returns TRUE for success
- Returns FALSE for error

CreateWorkflow

You can use the createWorkflow web method to create new workflow.

Parameters

The createWorkflow web method includes the following parameters:

Table 11-28 • createWorkflow Parameters

#	Parameters	Data Type	Description
1.	workflowName	String	Name of the workflow.
2.	workflowDesc	String	Description of the workflow.
3.	workflowGroupName	String	Name of the approval group.
4.	workflowFamilyName	String	Name of the workflow family.
5.	approverNameWithDomain	String	Domain name\user name

Return Value

Returns one of the following values:

- Returns TRUE for success
- Returns FALSE for error

CreateWorkflowGroup

You can use the `createWorkflowGroup` web method to create new work flow group.

Parameters

The `createWorkflowGroup` web method includes the following parameters:

Table 11-29 • createWorkflowGroup Parameters

#	Parameters	Data Type	Description
1.	**workflowGroupName**	String	Name of the approval group.
2.	**approverNameWithDomain**	String	Domain name\User name
3.	**workflowFamilyName**	String	Name of the workflow family.
4.	**isDefaultWorkflow**	Boolean	Enter **True** to specify that the current workflow is the default workflow; otherwise, enter **False**.

Return Value

Returns one of the following values:

- Returns TRUE for success

- Returns FALSE for error

DeleteAlertsForApp

The `DeleteAlertsForApp` web method will delete the alerts for a particular License ID from MyApps alerts table.

Parameters

The `DeleteAlertsForApp` web method includes the following parameters:

Table 11-30 • DeleteAlertsForApp Parameters

#	Parameters	Data Type	Description
1.	**licenseId**	String	FlexNet Manager Suite Flexera ID of installed application

Return Value

Returns `True` for success or `Exception` for failure.

📄

Note • *Exception could be because of wrong or no LicenseID exists in Alerts table.*

DeleteAlertsForAppByComputer

The DeleteAlertsForAppByComputer web method will delete the alerts for a particular machine and for a particular Flexera ID from the MyApps Alerts table.

Parameters

The DeleteAlertsForAppByComputer web method includes the following parameters:

Table 11-31 • DeleteAlertsForAppByComputer Parameters

#	Parameters	Data Type	Description
1.	**licenseId**	String	FlexNet Manager Suite FlexeraID of installed application.
2.	**machineName**	String	Target machine name

Return Value

Returns True for success or Exception for failure.

> *Note •* *Exception could be because of wrong or no LicenseID/Machine Name combination exists in Alerts table.*

DeleteAlertsForAppByUser

The DeleteAlertsForAppByUser web method will delete the alerts for a particular user and for a particular Flexera ID from the MyApps Alerts table.

Parameters

The DeleteAlertsForAppByUser web method includes the following parameters:

Table 11-32 • DeleteAlertsForAppByUser Parameters

#	Parameters	Data Type	Description
1.	**licenseId**	String	FlexNet Manager Suite FlexeraID of installed application.
2.	**uniqueUserName**	String	Domain Name\User Name

Return Value

Returns True for success or Exception for failure.

> *Note •* *Exception could be because of wrong or no licenseId/uniqueUserName combination exists in Alerts table.*

DeleteAlertsForComputer

The `DeleteAlertsForComputer` web method will delete all the Alerts for a particular computer from MyApps Alerts table.

Parameters

The `DeleteAlertsForComputer` web method includes the following parameters:

Table 11-33 • DeleteAlertsForComputer Parameters

#	Parameters	Data Type	Description
1.	**machineName**	String	Target machine to delete the alert.

Return Value

Returns `True` for success or `Exception` for failure.

Note • Exception could be because of wrong or no machineName exists in Alerts table.

DeleteAlertsForUser

The `DeleteAlertsForUser` web method will delete all the Alerts for a particular user from MyApps Alerts table.

Parameters

The `DeleteAlertsForUser` web method includes the following parameters:

Table 11-34 • DeleteAlertsForUser Parameters

#	Parameters	Data Type	Description
1.	**uniqueUserName**	String	Domain Name\User Name

Return Value

Returns `True` for success or `Exception` for failure.

Note • Exception could be because of wrong or no uniqueUserName exists in the Alerts table.

EnableAllSoftwareCatalogSyncInToServiceNow

You can use the `EnableAllSoftwareCatalogSyncInToServiceNow` web method to select the **Enable all software catalog items to sync with ServiceNow** option. When this option is selected, all existing catalog items will be synced with the ServiceNow service catalog; if this option is not selected, only new and updated catalog items are synced.

Parameters

The EnableAllSoftwareCatalogSyncInToServiceNow web method includes the following parameters:

Table 11-35 • EnableAllSoftwareCatalogSyncInToServiceNow Parameters

#	Parameters	Data Type	Description
1.	enableSyncIntoServiceNow	Boolean	Enter **True** to select the **Enable all software catalog items to sync with ServiceNow** option; otherwise, enter **False**. When this option is selected, all existing catalog items will be synced with the ServiceNow service catalog; if this option is not selected, only new and updated catalog items are synced.

Return Value

Returns one of the following values:

- Returns TRUE for success.

- Returns FALSE for error.

EnableSoftwareCatalogSyncInToServiceNow

You can use the EnableSoftwareCatalogSyncInToServiceNow web method to select the **Sync catalog items with ServiceNow** option for a catalog item. When this option is selected, the specified catalog item will be synced with the ServiceNow service catalog.

Parameters

The EnableSoftwareCatalogSyncInToServiceNow web method includes the following parameters:

Table 11-36 • EnableSoftwareCatalogSyncInToServiceNow Parameters

#	Parameters	Data Type	Description
1.	packageID	Integer	ID of package.
2.	enableSyncIntoServiceNow	Boolean	Enter **True** to select the **Sync catalog items with ServiceNow** option; otherwise, enter **False**. When this option is selected, the specified catalog item will be synced with the ServiceNow service catalog.

Return Value

Returns one of the following values:

- Returns TRUE for success.

- Returns FALSE for error.

ExpireAlertsForApp

The ExpireAlertsForApp web method will expire a non-responded alert.

Parameters

The ExpireAlertsForApp web method includes the following parameters:

Table 11-37 • ExpireAlertsForApp Parameters

#	Parameters	Data Type	Description
1.	**licenseId**	String	FlexNet Manager Suite FlexeraID of installed application.
2.	**alertType**	Integer	Specify one of the following values: • **1** for license reclamation action • **2** for alert action

Return Value

Returns True for success or Exception for failure.

📄

Note • *Exception could be because of wrong or no LicenseID with alertType combination exists in the Alerts table.*

ExpireAlertsForAppByComputer

The ExpireAlertsForAppByComputer web method will expire a non-responded alert.

Parameters

The ExpireAlertsForAppByComputer web method includes the following parameters:

Table 11-38 • ExpireAlertsForAppByComputer Parameters

#	Parameters	Data Type	Description
1.	**licenseId**	String	FlexNet Manager Suite FlexeraID of installed application.
2.	**machineName**	String	MachineName
3.	**alertType**	Integer	Specify one of the following values: • **1** for license reclamation action • **2** for alert action

Return Value

Returns True for success or Exception for failure.

📄

Note • Exception could be because of wrong or no LicenseID, UniqueUserName exists with FlexeraID to expire.

ExpireAlertsForAppByUser

The `ExpireAlertsForAppByUser` web method will expire a non-responded alert.

Parameters

The `ExpireAlertsForAppByUser` web method includes the following parameters:

Table 11-39 • ExpireAlertsForAppByUser Parameters

#	Parameters	Data Type	Description
1.	**licenseId**	String	FlexNet Manager Suite FlexeraID of installed application.
2.	**uniqueUserName**	String	Domain Name\User Name
3.	**alertType**	Integer	Specify one of the following values: • **1** for license reclamation action • **2** for alert action

Return Value

Returns `True` for success or `Exception` for failure.

📄

Note • Exception could be because of wrong or no LicenseID/UniqueUserName combination exists with FlexeraID.

ExpireAlertsForComputer

The `ExpireAlertsForComputer` web method will expire a non-responded alert.

Parameters

The `ExpireAlertsForComputer` web method includes the following parameters:

Table 11-40 • ExpireAlertsForComputer Parameters

#	Parameters	Data Type	Description
1.	**machineName**	String	MachineName

Table 11-40 • ExpireAlertsForComputer Parameters (cont.)

#	Parameters	Data Type	Description
2.	**alertType**	Integer	Specify one of the following values: ● **1** for license reclamation action ● **2** for alert action

Return Value

Returns True for success or Exception for failure.

> 📄
>
> *Note • Exception could be because of wrong or no LicenseID/MachineName combination exists with FlexeraID.*

ExpireAlertsForUser

The ExpireAlertsForUser web method will expire a non-responded alert.

Parameters

The ExpireAlertsForUser web method includes the following parameters:

Table 11-41 • ExpireAlertsForUser Parameters

#	Parameters	Data Type	Description
1.	**uniqueUserName**	String	Domain Name\User Name
2.	**alertType**	Integer	Specify one of the following values: ● **1** for license reclamation action ● **2** for alert action

Return Value

Returns True for success or Exception for failure.

> 📄
>
> *Note • Exception could be because of wrong or no UniqueUserName for alertType exists.*

GetAlertsForAlertAction

The GetAlertsForAlertAction web method will return alert action details.

Parameters

The GetAlertsForAlertAction web method includes the following parameters:

Table 11-42 • GetAlertsForAlertAction Parameters

#	Parameters	Data Type	Description
1.	licenseId	String	FlexNet Manager Suite Flexera ID of installed application. *Note • Can be empty.*
2.	pakcageID	Integer	App Portal catalog name mapped to an alert action. *Note • Can be empty.*
3.	machineName	String	Machine to get the alerts *Note • Can be empty.*
4.	uniqueUserName	String	Domain Name\User Name *Note • Can be empty.*
5.	expired	Boolean	Responded alerts or non-responded alerts

Return Value

A dataset of alerts.

GetAlertsForLicenseReclamation

The GetAlertsForLicenseReclamation web method will return license reclamation alert details of the application or machine.

Parameters

The `GetAlertsForLicenseReclamation` web method includes the following parameters:

Table 11-43 • GetAlertsForLicenseReclamation Parameters

#	Parameters	Data Type	Description
1.	**licenseId**	String	FlexNet Manager Suite Flexera ID of installed application. **Note** • *Can be empty.*
2.	**machineName**	String	Machine to get the alerts. **Note** • *Can be empty.*
3.	**uniqueUserName**	String	Domain Name\User Name. **Note** • *Can be empty.*
4.	**actionType**	String	Uninstall or Keep. **Note** • *Can be empty.*
5.	**expired**	Boolean	Responded alerts or non-responded alerts

Return Value

A dataset of alerts.

GetCatalogItemTemplates

You can use the `GetCatalogItemTemplates` web method to get all the catalog item templates.

Parameters

The `GetCatalogItemTemplates` web method has no parameters.

Return Value

Returns a dataset of templates.

GetCategories

You can use the `getCategories` web method to get all the categories.

Parameters

The `getCategories` web method has no parameters.

Return Value

Returns a dataset of categories.

GetCategoryByID

You can use the `getCategoryByID` web method to get a category by its `categoryID`.

Parameters

The `getCategoryByID` web method includes the following parameters:

Table 11-44 • getCategoryByID Parameters

#	Parameters	Data Type	Description
1.	**categoryID**	Integer	`CategoryID` of the category.

Return Value

Returns the dataset of a category.

GetCategoryByName

You can use the `getCategoryByName` web method to get a category by its name.

Parameters

The `getCategoryByName` web method includes the following parameters:

Table 11-45 • getCategoryByName Parameters

#	Parameters	Data Type	Description
1.	**categoryName**	String	Name of the category.

Return Value

Returns the dataset of a category.

GetDataForUninstallRequestWithNoAlert

The `GetDataForUninstallRequestWithNoAlert` web method will return all uninstall actions taken without an alert in **My Apps**.

Parameters

The `GetDataForUninstallRequestWithNoAlert` web method includes the following parameters:

Table 11-46 • GetDataForUninstallRequestWithNoAlert Parameters

#	Parameters	Data Type	Description
1.	**licenseId**	String	FlexNet Manager Suite FlexeraID of installed application. *Note • Can be empty.*
2.	**machineName**	Sring	Machine to get the alerts. *Note • Can be empty.*
3.	**uniqueUserName**	String	Domain Name\User Name *Note • Can be empty.*

Return Value

Dataset of alerts.

GetLicenseDetails

You can use the `GetLicenseDetails` web method to get details of the App Portal license file from the given folder.

Parameters

The `GetLicenseDetails` web method includes the following parameters:

Table 11-47 • GetLicenseDetails Parameters

#	Parameters	Data Type	Description
1.	**licenseFolder**	String	Folder name which contains the uploaded App Portal license file.

Return Value

List of license details.

GetProduceCodeForUninstall

You can use the GetProduceCodeForUninstall web method to get the produce code for uninstallation using the Smart Uninstall feature.

Parameters

The GetProduceCodeForUninstall web method includes the following parameters:

Table 11-48 • GetProduceCodeForUninstall Parameters

#	Parameters	Data Type	Description
1.	**machineName**	String	Name of machine catalog item will be uninstalled from.
2.	**flexeraId**	String	FlexNet Manager Suite Flexera ID.
3.	**fnmsDBConnectionString**	String	FlexNet Manager Suite database connection details.

Return Value

Returns a string containing produce code information.

GetResolvedRequestVariables

You can use the GetResolvedRequestVariables web method to get resolved request details (variables).

Parameters

The GetResolvedRequestVariables web method includes the following parameters:

Table 11-49 • GetResolvedRequestVariables Parameters

#	Parameters	Data Type	Description
1.	**requestID**	Integer	Request ID

Return Value

Returns a data table of request details.

GetSoftwaresToUninstallFromDevice

You can use the GetSoftwaresToUninstallFromDevice web method to get list of a list of the "alerted" software packages which the user chose to uninstall from the machine.

Parameters

The GetSoftwaresToUninstallFromDevice web method includes the following parameters:

Table 11-50 • GetSoftwaresToUninstallFromDevice Parameters

#	Parameters	Data Type	Description
1.	**machineName**	String	Name of machine.

Return Value

Returns an array of software details.

GetVersion

You can use the GetVersion web method to get version info.

Parameters

The GetVersion web method requires no parameters.

Return Value

Returns a string containing version information.

InsertAlertAction

The InsertAlertAction web method will insert an alert action into the MyApps alerts table.

Parameters

The InsertAlertAction web method includes the following parameters:

Table 11-51 • InsertAlertAction Parameters

#	Parameters	Data Type	Description
1.	**licenseId**	String	FlexNet Manager Suite Flexera ID of installed application.
2.	**packageId**	Integer	App Portal catalog item ID.
3.	**machineName**	String	Target machine to insert the alert
4.	**uniqueUserName**	String	Domain Name\User Name

Return Value

Returns alert ID (Integer) for success, and 0 for insertion failure

> **Note** • *A return of 0 could be because of failure to find the* `PackageID` *in the App Portal database.*

InsertLicenseReclamationAlert

The `InsertLicenseReclamationAlert` web method will insert a license reclamation alert into the `MyApps` alerts table. However, it only occurs if the last used date passed as input satisfies the threshold condition.

Parameters

The `InsertLicenseReclamationAlert` web method includes the following parameters:

Table 11-52 • InsertLicenseReclamationAlert Parameters

#	Parameters	Data Type	Description
1.	**licenseId**	String	FlexNet Manager Suite Flexera ID of installed application.
2.	**packageId**	Integer	App Portal catalog item ID.
3.	**machineName**	String	Target machine to insert the alert
4.	**uniqueUserName**	String	Domain Name\User Name
5.	**lastUsedDate**	Date Time	Application last used in machine

Return Value

Returns alert ID (Integer) for success, and 0 for insertion failure.

> **Note** • *A return of 0 could be because wrong or threshold value condition is not satisfied.*

PublishAltirisCatalogItemEx

You can use the `PublishAltirisCatalogItemEx` web method to create a new Altiris catalog item using advertisement.

Parameters

The `PublishAltirisCatalogItemEx` web method includes the following parameters:

Table 11-53 • PublishAltirisCatalogItemEx Parameters

#	Parameters	Data Type	Description
1.	**productName**	String	Name of the product.
2.	**companyName**	String	Name of the company.

Table 11-53 • PublishAltirisCatalogItemEx Parameters (cont.)

#	Parameters	Data Type	Description
3.	version	String	Product version.
4.	searchKeywords	String	Keywords that help search for this product.
5.	shortDescription	String	Short description of the product.
6.	longDescription	String	Long description of the product.
7.	visible	Boolean	Enter one of the following values: • **True**—Make the catalog item visible on the Browse Catalog tab. • **False**—Do not make the catalog item visible on the Browse Catalog tab.
8.	icon	Byte Array	Icon of the product.
9.	iconExtension	String	Icon extension.
10.	flexeraID	String	Flexera ID of the product.
11.	AltirisPackageOrPolicyID	String	Altiris package or policy ID.

12.	AltirisProgramData	String	String of the format:
			
			`InstallType(Integer)| programID`
			
			where `InstallType` may be one of the following:
			
			• **0**—Install
			
			• **1**—Uninstall
			
			• **2**—Repair
			
			The `programID` is a string. For example:
			
			`0|programID`

13.	DeploymentTarget	Integer	Enter one of the following values: • **0**—DeployToUser • **1**—DeployToComputer
14.	templatePackageID	Integer	To follow a template structure when creating the new catalog item, enter a Template package ID. If you do not want to use a template, enter **0**.
15.	csvCategoryNames	String	Enter a single category name or a comma separated list of category names.

Table 11-53 • PublishAltirisCatalogItemEx Parameters (cont.)

#	Parameters	Data Type	Description
16.	csvGroupNames	String	Enter a comma separated list of property values.
17.	memberShipType	Integer	Enter membership type.

Return Value

Returns one of the following values:

- Returns an integer greater than 0 for success

- Returns -1 for error

PublishCatalogItem

You can use the PublishCatalogItem web method to create a new catalog item using advertisement.

Parameters

The PublishCatalogItem web method includes the following parameters:

Table 11-54 • PublishCatalogItem Parameters

#	Parameters	Data Type	Description
1.	productName	String	Name of the product.
2.	companyName	String	Name of the company.
3.	version	String	Product version.
4.	shortDescription	String	Short description of the product.
5.	longDescription	String	Long description of the product.
6.	icon	Byte Array	Icon of the product.
7.	iconExtension	String	Icon extension.
8.	Imagepath	String	Path to the image.
9.	flexeraID	String	Flexera ID of the product.
10.	ConfigManagerServerName	String	Server name.
11.	ConfigManagerSiteCode	String	Server site code.

Table 11-54 • PublishCatalogItem Parameters

#	Parameters	Data Type	Description
12.	**ConfigManagerID**	String	System Center Configuration Manager ID of the catalog item.

Return Value

Returns one of the following values:

- Returns TRUE for success
- Returns FALSE for error

PublishCatalogItemEx

You can use the `PublishCatalogItemEx` web method to create a new catalog item.

Parameters

The `PublishCatalogItemEx` web method includes the following parameters:

Table 11-55 • PublishCatalogItemEx Parameters

#	Parameters	Data Type	Description
1.	**productName**	String	Name of the product.
2.	**companyName**	String	Name of the company.
3.	**version**	String	Product version.
4.	**shortDescription**	String	Short description of the product.
5.	**longDescription**	String	Long description of the product.
6.	**Visible**	Boolean	Enter one of the following values: • **True**—Make the catalog item visible on the Browse Catalog tab. • **False**—Do not make the catalog item visible on the Browse Catalog tab.
7.	**icon**	Byte Array	Icon of the product.
8.	**iconExtension**	String	Icon extension.
9.	**flexeraID**	String	Flexera ID of the product.

Table 11-55 • PublishCatalogItemEx Parameters

#	Parameters	Data Type	Description
10.	ConfigManagerServerName	String	Server name.
11.	ConfigManagerSiteCode	String	Server site code.
12.	ConfigManagerID	String	System Center Configuration Manager ID of the catalog item.
13.	ConfigManagerData	String	System Center Configuration Manager data.
14.	DeploymentTarget	Enum Value	Enter one of the following values: • **0**—DeployToUser • **1**—DeployToComputer
15.	templatePackageID	Integer	To follow a template structure when creating the new catalog item, enter a Template package ID. If you do not want to use a template, enter **0**.
16.	csvCategoryNames	String	Enter a single category name or comma separated list of category names.
17.	csvGroupNames	String	Enter a comma separated list of property values.
18.	memberShipType	Integer	Enter membership type.
19.	CreateInventoryRecord	Boolean	Enter one of the following values: • **True**—Create an inventory record. • **False**—Do not create an inventory record.
20.	InventoryClassOrQueryName	String	Enter name of inventory class or query.
21.	ItemAttributes	InventoryAttributeObject	Enter the object of the Inventory Attribute.

Return Value

Returns one of the following values:

• Returns integer greater than 0 for success

• Returns -1 for error

PublishCatalogItemForPackage

You can use the PublishCatalogItemForPackage to create a software catalog item (package).

Parameters

The PublishCatalogItemForPackage web method includes the following parameters:

Table 11-56 • PublishCatalogItemForPackage Parameters

#	Parameters	Data Type	Description
1.	**productName**	String	Name of the product.
2.	**companyName**	String	Name of the company.
3.	**version**	String	Product version.
4.	**shortDescription**	String	Short description of the product.
5.	**longDescription**	String	Long description of the product.
6.	**icon**	Byte Array	Icon of the product.
7.	**iconExtension**	String	Icon extension.
8.	**Imagepath**	String	Path to the image.
9.	**flexeraID**	String	Flexera ID of the product.
10.	**ConfigManagerServerName**	String	Server name.
11.	**ConfigManagerSiteCode**	String	Server site code.
12.	**ConfigManagerID**	String	System Center Configuration Manager ID of the catalog item.
13.	**ConfigManagerProgramData**	String	System Center Configuration Manager data.

Return Value

Returns one of the following values:

- Returns TRUE for success

- Returns FALSE for error

ReadDB

You can use the ReadDB web method to get row(s) of data for a given table, column name and value.

Parameters

The ReadDB web method includes the following parameters:

Table 11-57 • ReadDB Parameters

#	Parameters	Data Type	Description
1.	**tableName**	String	Name of table.
2.	**primaryColumn**	String	Name of column.
3.	**primaryColumnValue**	String	Value to be matched.
4.	**password**	String	Pipe (|) separated combination of F1@xera!, short date format of the current date, and a GUID. For example: F1@xera!|6/1/2016|6aa7a31513a162004e5050f32244b0ff

Return Value

Returns a dataset of matched values.

RemoveAltirisPolicy

You can use the RemoveAltirisPolicy web method to delete a policy in Altiris.

Parameters

The RemoveAltirisPolicy web method includes the following parameters:

Table 11-58 • RemoveAltirisPolicy Parameters

#	Parameters	Data Type	Description
1.	**policyGuid**	String	GUID of Altiris policy you want to remove.

Return Value

Returns one of the following values:

- Returns TRUE for success.
- Returns FALSE for error.

SetAlternateApproverAndOutOfOffice

You can use the SetAlternateApproverAndOutOfOffice web method to set an alternate approver for a user. You can also use it to automatically update the approver if a user is out of the office.

Parameters

The `SetAlternateApproverAndOutOfOffice` web method includes the following parameters:

Table 11-59 • SetAlternateApproverAndOutOfOffice Parameters

#	Parameters	Data Type	Description
1.	**uniqueUserName**	String	Unique user name of the user (DomainName\UserName)
2.	**uniqueApproverName**	String	Unique user name of the alternate approver (DomainName\UserName)
3.	**outOfOffice**	String	TRUE or FALSE is passed to indicate whether the user (passed in the `uniqueUserName` parameter) is in the office.

Return Value

Returns one of the following values:

- Returns TRUE for success
- Returns FALSE for failure

SetInstallStatus

You can use the `SetInstallStatus` web method to set the deployment status of an App Portal request.

Parameters

The `SetInstallStatus` web method includes the following parameters:

Table 11-60 • SetInstallStatus Parameters

#	Parameters	Data Type	Description
1.	**RequestId**	Integer	ID number of the request.
2.	**InstallStatus**	StatusIdInfo	Specify one of the following values: • StatusIDInfo.Success • StatusIDInfo.Fail

Return Value

Returns one of the following values:

- Returns TRUE for success
- Returns FALSE for failure

SetInstallStatusWithLease

You can use the `SetInstallStatusWithLease` web method to set the install status Success/Fail with the lease expiration date for the package request.

Parameters

The `SetInstallStatusWithLease` web method includes the following parameters:

Table 11-61 • SetInstallStatusWithLease Parameters

#	Parameters	Data Type	Description
1.	RequestId	String	ID number of the request.
2.	InstallStatus	Boolean	Enter one of the following values: ● **Success** ● **Fail**
3.	LeaseDate	Date / Time	Lease expiration date.

Return Value

Returns one of the following values:

● Returns TRUE for success

● Returns FALSE for failure

StartDeployment

You can use the `StartDeployment` web method to restart the deployment of an App Portal request that has already been submitted.

Parameters

The `StartDeployment` web method includes the following parameters:

Table 11-62 • StartDeployment Parameters

#	Parameters	Data Type	Description
1.	RequestId	Integer	ID number of the request.

Return Value

Returns one of the following values:

● Returns TRUE for success

● Returns FALSE for failure

SynchCurrentForest

You can use the SynchCurrentForest web method to identify and save the domains in the forest where App Portal is installed.

Parameters

The SynchCurrentForest web method does not have any parameters.

Return Value

Returns one of the following values:

- Returns TRUE for success
- Returns FALSE for failure

SyncSingleUserComputer

You can use the SyncSingleUserComputer web method to sync the user and computer information from an external source with App Portal.

Parameters

The SyncSingleUserComputer web method includes the following parameters:

Table 11-63 • SyncSingleUserComputer Parameters

#	Parameters	Data Type	Description
1.	**UserName**	String	User name
2.	**Domain**	String	User's domain name
3.	**ComputerName**	String	Device name

Return Value

Returns one of the following values:

- Returns TRUE for success
- Returns FALSE for failure

UpdateCatalogLicenseInfo

You can use the UpdateCatalogLicenseInfo web method to update the FlexNet Manager Suite license details for the catalog item.

Parameters

The UpdateCatalogLicenseInfo web method includes the following parameters:

Table 11-64 • UpdateCatalogLicenseInfo Parameters

#	Parameters	Data Type	Description
1.	**packageID**	Integer	App Portal catalog item ID.
2.	**flexeraId**	String	FlexNet Manager Suite Flexera ID.
3.	**scopeType**	Integer	Use one of the following values to identify license scope: ● **0**—Global group only. ● **1**—Enterprise group only. ● **2**—Check enterprise group first, but fall back to global group.
4.	**isEnabled**	Boolean	Set this to **True** to enable the FlexNet Manager Suite license position check for the catalog. Otherwise, set it to **False**.

Return Value

There is no return value.

UpdateCatalogLicensePosition

You can use the UpdateCatalogLicensePosition web method to update the FlexNet Manager Suite license position for the catalog item.

Parameters

The UpdateCatalogLicensePosition web method includes the following parameters:

Table 11-65 • UpdateCatalogLicensePosition Parameters

#	Parameters	Data Type	Description
1.	**packageId**	Integer	App Portal catalog item ID.
2.	**isEnabled**	Boolean	Set to **True** to enable a FlexNet Manager Suite license position check for the catalog item.

Return Value

There is no return value.

UpdateCatalogLicenseScope

You can use the `UpdateCatalogLicenseScope` web method to update the license scope of the catalog item in FlexNet Manager Suite.

Parameters

The `UpdateCatalogLicenseScope` web method includes the following parameters:

Table 11-66 • UpdateCatalogLicenseScope Parameters

#	Parameters	Data Type	Description
1.	**packageId**	Integer	App Portal catalog item ID.
2.	**scopeType**	Integer	Use one of the following values to identify license scope: • **0**—Global group only. • **1**—Enterprise group only. • **2**—Check enterprise group first, but fall back to global group.

Return Value

There is no return value.

UpdateDB

You can use the `UpdateDB` web method to update row(s) of data for given table, column name, and value.

Parameters

The `UpdateDB` web method includes the following parameters:

Table 11-67 • UpdateDB Parameters

#	Parameters	Data Type	Description
1.	**tableName**	String	Name of table whose row(s) has to be updated.
2.	**primaryColumn**	String	Column name whose value has to be compared before update
3.	**primaryColumnValue**	String	Column name whose value has to be compared before update
4.	**dataColumnName**	String	Column name whose value has to be updated.
5.	**dataColumnValue**	String	New value to be updated for specified column

Table 11-67 • UpdateDB Parameters (cont.)

#	Parameters	Data Type	Description
6.	**password**	String	Pipe (|) separated combination of `Fl@xera!`, short date format of the current date, and a GUID. For example: `Fl@xera!|6/1/2016|6aa7a31513a162004e5050f32244b0ff`

Return Value

Count of updated rows.

UpdateMyAppsLicenseReclamationPolicyForFlexeraID

You can use the `UpdateMyAppsLicenseReclamationPolicyForFlexeraID` web method to update a software package's My Apps license reclamation configuration policy and settings.

Parameters

The `UpdateMyAppsLicenseReclamationPolicyForFlexeraID` web method includes the following parameters:

Table 11-68 • UpdateMyAppsLicenseReclamationPolicyForFlexeraID Parameters

#	Parameters	Data Type	Description
1.	**flexeraID**	String	FlexNet Manager Suite Flexera ID for the software package.
2.	**licenseReclamationThresholdInDays**	Integer	The number of days for software to remain unused before license reclamation is processed. The lesser between this value and the global My Apps license reclamation threshold is evaluated when creating My Apps alert notifications.
3.	**allowUserDriverUninstall**	Boolean	Whether or not to allow a user to respond to My Apps alert notification before its software license is reclaimed.
4.	**automaticUninstallWhenNotResponded**	Boolean	Whether or not to automatically uninstall the software if user did not respond to a My Apps alert notification in time.
5.	**numberOfDaysAllowedToRespond**	Integer	The number of days a user is allowed to respond to a My Apps alert notification.
6.	**uninstallEvenIfNoUserAssociated**	Boolean	Whether or not to immediately automatically uninstall a software if computer does not have a relationship to any user.

Table 11-68 • UpdateMyAppsLicenseReclamationPolicyForFlexeraID Parameters (cont.)

#	Parameters	Data Type	Description
7.	**expireNotificationIfUsed**	Boolean	Whether or not to expire a My Apps alert notification if the software has been used after the alert was created.
8.	**notifyUserPostUninstall**	Boolean	Whether or not to send an email notification to a user after the software package was automatically uninstalled from his or her computer due to license reclamation.

Return Value

Returns one of the following values:

- Returns TRUE for success.

- Returns FALSE for failure.

UpdateUninstallStatusForDevice

You can use the UpdateUninstallStatusForDevice web method to update the uninstall status for the device.

Parameters

The UpdateUninstallStatusForDevice web method includes the following parameters:

Table 11-69 • UpdateUninstallStatusForDevice Parameters

#	Parameters	Data Type	Description
1.	**machineName**	String	Name of the device/machine.
2.	**flexeraId**	String	FlexNet Manager Suite Flexera ID.
3.	**uninstallSuccessful**	Boolean	Uninstall status.
4.	**uninstallStatusMessage**	String	Uninstall status message.

Return Value

Returns one of the following values:

- Returns TRUE for success.

- Returns FALSE for failure.

Legacy API Web Methods

The legacy API for App Portal is exposed as a Web Service, located at the following URL:

> `http://[AppPortalServer]/ESD/API.asmx`

Visit this page to see detailed examples of these web methods in SOAP 1.1, SOAP 1.2, HTTP GET, and HTTP POST format.

Important • *These web services need to be enabled by selecting the* **Enable App Portal API** *option on the* **Site Management > Settings > Flexera Integration** *view.*

Syntax

These web methods use the following syntax:

webMethodName (`parameter1value, parameter2value, parameter3value, ...`)

Parameter values must be listed in the order in which they appear in the **Parameters** tables provided in this section, separated by commas. Strings must be enclosed in double quotes. Here is an example of a web method with multiple parameters, some of which are strings:

`addWorkflowToCatalogItem ("Adobe Acrobat", "Manager Approval", true)`

Web Methods

The following legacy API web methods are documented in this section:

- addCatalogItemToCategory
- addInventoryItemToInventoryGroup
- addSCCMPackageAndProgramToCatalogItem
- addWorkflowToCatalogItem
- approveRequest
- archiveCatalogItem
- assignInventoryGroupToCatalogItem
- assignMeteringRuleToInventoryGroup
- assignRequest
- associateComputer
- attachQuestionTemplateToCatalogItem
- cancelAllSoftwareRequestsForMachineName
- cancelRequest
- changeCategoryOfCatalogItem
- changeRequestStatus
- createCollectionsAndAdvertisements

- createDeploymentForACatalogItem

- createESDObjects

- createInventoryGroup

- createNewCatalogItem

- createRequest

- deleteKeywordsOfCatalogItem

- deployGetTargetPackages

- getAllCatalogItems

- getAllInventoryGroups

- getAllRequestedOrInstalledSoftwareTitlesForMachine

- getAllRequestedPackageIDsForMachine

- getAllRequestedSoftwareTitlesForMachine

- getDetailsForExistingRequestsByPackageID

- getDetailsForExistingRequestsByRequestID

- getDetailsForExistingRequestsByUser

- getInventoryItemsFromInventoryGroupID

- getInventoryItemsFromInventoryGroupName

- getRequestApprovalStatus

- getSMSPackageIDsFromESDPackageIDs

- getSoftwareHashFromMSIProductID

- importComputer

- incrementInventoryGroupLicenseOwned

- incrementInventoryGroupLicenseUsed

- rejectRequest

- removeAllInventoryRulesFromInventoryGroup

- removeAllWorkflowsFromCatalogItem

- removeCatalogItemFromAllCategories

- removeCatalogItemFromCategory

- removeDeploymentForACatalogItem

- removeInventoryItemFromInventoryGroup

- removeWorkflowFromCatalogItem

- updateActionStatus

- setRequestOnBehalfPropertyForCatalogItem

- unAssignRequest

- updateApprovalRequiredForCatalogItem

- updateCatalogItemBriefDescription

- updateCatalogItemDescription

- updateCatalogItemTitle

- updateCatalogItemVisibility

- updateInventoryGroupCost

- updateInventoryGroupLicenseOwned

- updateInventoryGroupLicenseType

- updateInventoryGroupLicenseUsed

- updateKeyWordsOfCatalogItem

addCatalogItemToCategory

The addCatalogItemToCategory web method is used to add a catalog item to a category.

Parameters

The addCatalogItemToCategory web method includes the following parameters:

Table 11-70 • addCatalogItemToCategory Parameters

#	Parameters	Data Type	Description
1.	**Title**	String	The title of the item to add programs to.
2.	**CategoryName**	String	The name of the category to assign. If the category does not exist, it is created.
3.	**ParentCategoryName**	String	If there are multiple categories with the same name under different hierarchies, specify the parent category name so that the item is added to the correct category hierarchy.

Return Value

Returns one of the following values:

- Returns a **1** for success

- Returns a **-1** for error

addInventoryItemToInventoryGroup

The addInventoryItemToInventoryGroup web method is used to add a single inventory item to an inventory group.

Parameters

The addInventoryItemToInventoryGroup web method has the following parameters.

Table 11-71 • addInventoryItemToInventoryGroup Parameters

$	Parameter	Data Type	Description
1.	**GroupName**	String	Name of inventory group that you want to add an inventory item to.
2.	**InventoryClassNameOrQueryName**	String	Inventory class name.
3.	**ItemAttributes**	Array of InventoryAttributeObject	Inventory attribute object list.
4.	**InventoryAttributeObject**	InventoryAttributeObject	Enter the object of the Inventory Attribute.
5.	**PropertyName**	String	Inventory attribute property name.
6.	**PropertyValue**	String	Inventory attribute property value.
7.	**Included**	Boolean	Use one of the following values: • **True**—To create. • **False**—Otherwise.

Return Value

The return value is 0.

addSCCMPackageAndProgramToCatalogItem

The addSCCMPackageAndProgramToCatalogItem web method is used to adds a System Center Configuration Manager package / program to a catalog item.

Parameters

The addSCCMPackageAndProgramToCatalogItem web method includes the following parameters:

Table 11-72 • addSCCMPackageAndProgramToCatalogItem Parameters

#	Parameters	Data Type	Description
1.	**Title**	String	The title of the item to add programs to.
2.	**PackageServer**	String	The netbios name of the SCCM server where the package exists.
3.	**SMSPackageID**	String	The SCCM PackageID representing the SCCM Package.

Table 11-72 • addSCCMPackageAndProgramToCatalogItem Parameters (cont.)

#	Parameters	Data Type	Description
4.	**SMSPackageData**	String	The formatting for the SMSPackageData is:
			`Program Action(0 - Install,1 - Uninstall,2 - Repair)|Language ID (0 for English)|Office 2007 Install (Program Name)`
			Separate each entry with a comma, such as:
			`0|0|InstallInteractive,1|0|UninstallInteractive`
5.	**TemplatePackageID**	Integer	The template package ID will copy over the existing settings from that catalog item including request options, visibility, approval, approval process, and Actions.

Return Value

Returns one of the following values:

- Returns a **1** for success
- Returns a **-1** for error

addWorkflowToCatalogItem

The addWorkflowToCatalogItem web method will add a workflow to a catalog item. Optionally, you can delete the existing workflows while adding a new workflow.

Parameters

The addWorkflowToCatalogItem web method includes the following parameters:

Table 11-73 • addWorkflowToCatalogItem Parameters

#	Parameters	Data Type	Description
1.	**Title**	String	Name of the catalog item.
2.	**WorkFlowName**	String	Name of the workflow to be attached.
3.	**ReplaceExistingWorkflows**	Boolean	Boolean option to delete existing workflows for the catalog item, if there are any.

Return Value

Returns one of the following values:

- Returns **True** for success
- Returns **False** for error

approveRequest

You can use the `approveRequest` web method to approve an existing request.

Parameters

The `approveRequest` web method includes the following parameters:

Table 11-74 • approveRequest Parameters

#	Parameters	Data Type	Description
1.	**iRequestID**	Integer	The ID of the request to approve
2.	**strReason**	String	The reason for the approval
3.	**strDescription**	String	The description of the approval
4.	**strGUID**	String	The Request GUID, use if RequestID is not provided.

Return Value

Returns one of the following values:

- Returns a **1** for success
- Returns a **-1** for error

archiveCatalogItem

You can use the `archiveCatalogItem` web method to remove a catalog item from the catalog. If the item is software, the System Center Configuration Manager Collections and Advertisements are removed and any existing requests for the software are canceled.

Parameters

The `archiveCatalogItem` web method includes the following parameters:

Table 11-75 • archiveCatalogItem Parameters

#	Parameters	Description
1.	**Title**	The title of the item to archive.

Return Value

Returns one of the following values:

- Returns a **1** for success
- Returns a **-1** for error

assignInventoryGroupToCatalogItem

You can use the `assignInventoryGroupToCatalogItem` web method to assign the specified inventory group to the specified catalog item.

Parameters

The `assignInventoryGroupToCatalogItem` web method includes the following parameters:

Table 11-76 • assignInventoryGroupToCatalogItem Parameters

#	Parameters	Data Type	Description
1.	**GroupName**	String	The name of the inventory group to associate.
2.	**CatalogItem**	String	The name of the catalog item to associate.

Return Value

Returns one of the following values:

- Returns a **1** for success

- Returns a **-1** for error

assignMeteringRuleToInventoryGroup

You can use the assignMeteringRuleToInventoryGroup web method to define a metering rule for an inventory group.

Parameters

The `assignMeteringRuleToInventoryGroup` web method includes the following parameters:

Table 11-77 • assignMeteringRuleToInventoryGroup Parameters

#	Parameters	Data Type	Description
1.	**GroupName**	String	The name of the inventory group to associate.
2.	**MeterRuleName**	String	The Name of the Metering Rule to add.
3.	**MeterRulePartialMatch**	Boolean	Whether the metering rule is a partial match or the exact rule name.
4.	**RelatedSCCMPackageID**	String	The SCCM PackageID to extract the MSI install string.
5.	**MeterRuleDays**	Integer	Number of days to consider software unutilized.

Return Value

Returns one of the following values:

- Returns a **1** for success

- Returns a **-1** for error

assignRequest

You can use the `assignRequest` web method to assign inventory to the specified user.

Parameters

The `assignRequest` web method includes the following parameters:

Table 11-78 • assignRequest Parameters

#	Parameters	Data Type	Description
1.	**strUserName**	String	The user to assign the inventory to.
2.	**strMachine**	String	The machine name to assign the inventory to.
3.	**iLicenseID**	Integer	The ID of the inventory group to assign.
4.	**strAssigner**	String	The name of the assigner.

Return Value

Returns one of the following values:

- Returns a **1** for success

- Returns a **-1** for error

associateComputer

You can use the `associateComputer` web method to associate two computers as the specified site code.

Parameters

The `associateComputer` web method includes the following parameters:

Table 11-79 • associateComputer Parameters

#	Parameters	Data Type	Description
1.	**SourceMachineName**	String	Name of source machine.
2.	**TargetMachineName**	String	Name of target machine.
3.	**strSiteCode**	String	Site code.

attachQuestionTemplateToCatalogItem

Use the `AttachQuestionTemplateToCatalogItem` command to attach a question template to a catalog item.

Parameters

The `AttachQuestionTemplateToCatalogItem` command includes the following parameters:

Table 11-80 • attachQuestionTemplateToCatalogItem Parameters

#	Parameter	Data Type	Description
1.	**Title**	String	Name of the catalog item
2.	**QuestionTemplateName**	String	Name of the question template.

Return Value

Returns one of the following values:

- Returns a **1** when attaching a question template.
- Returns a **0** if there was no template attached.
- Returns a **-1** when encountering an exception.

cancelAllSoftwareRequestsForMachineName

You can use the `cancelAllSoftwareRequestsForMachineName` web method to cancel all software requests for a specified machine and, optionally, all previously completed requests. You can also specify whether to send email notifications about the cancellation.

Parameters

The `cancelAllSoftwareRequestsForMachineName` web method includes the following parameters:

Table 11-81 • cancelAllSoftwareRequestsForMachineName Parameters

#	Parameters	Data Type	Description
1.	**strMachineName**	String	The name of the group to remove inventory rules from.
2.	**bDoNotifications**	Boolean	Whether to generate cancel email notifications
3.	**bCancelCompleted**	Boolean	Whether to cancel completed (installed) items.

Return Value

Returns one of the following values:

- Returns a **1** for success

- Returns a **-1** for error

cancelRequest

You can use the cancelRequest web method to cancel an existing request; you can also specify whether to send email notifications about the cancellation.

Parameters

The `cancelRequest` web method includes the following parameters:

Table 11-82 • cancelRequest Parameters

#	Parameters	Data Type	Description
1.	**iRequestID**	Integer	The ID of the request to cancel
2.	**bDoNotifications**	Boolean	Whether to generate cancel email notifications

Return Value

Returns one of the following values:

- Returns a **1** for success
- Returns a **-1** for error

changeCategoryOfCatalogItem

Use the `ChangeCategoryOfCatalogItem` command to change the category of a catalog item.

Parameters

The `ChangeCategoryOfCatalogItem` command includes the following parameters:

Table 11-83 • ChangeCategoryOfCatalogItem Parameters

#	Parameter	Data Type	Description
1.	**Title**	String	Name of the catalog item.
2.	**CategoryName**	String	Name of the category.

Return Value

Returns one of the following values:

- Returns a **1** when changing the category of catalog item.
- Returns a **0** if the category was not changed.
- Returns a **-1** when encountering an exception.

changeRequestStatus

Use the ChangeRequestStatus command to return a Boolean value stating success or failure about the status of a request.

Parameters

The ChangeRequestStatus command includes the following parameters:

Table 11-84 • ChangeRequestStatus Parameters

#	Parameter	Data Type	Description
1.	**RequestID**	Integer	Request ID of the request.
2.	**Succeeded**	Boolean	Use one of the following values: • **True**—To indicate that the request was successful. • **False**—To indicate that the request failed.

Return Value

Returns one of the following values:

- Returns **True** for success
- Returns **False** for error

createCollectionsAndAdvertisements

The createCollectionsAndAdvertisements web method tests the operation using the HTTP POST protocol, click the 'Invoke' button.

Parameters

There are no parameter

createDeploymentForACatalogItem

You can use the CreateDeploymentForACatalogItem command to create a deployment for a catalog item with a deployment target.

Parameters

The CreateDeploymentForACatalogItem command includes the following parameters:

Table 11-85 • CreateDeploymentForACatalogItem Parameters

#	Parameter	Data Type	Description
1.	**allowRestartOutsideOfMaintWindow**	Boolean	Specify whether to allow machine restart outside of maintenance window.
2.	**CreateUninstall**	Boolean	This parameter can only be used on packages of Type 15 where you want to create both an install and an uninstall at the same time. The parameter value in this case should be True or False otherwise.
3.	**deploymentTarget**	Integer	Use one of the following values: • **0** = Deploy To User • **1** = Deploy To Computer
4.	**DeploymentTechnology**	Integer	Values are either SCCM 2012, or Altiris.
5.	**deployToAllSites**	Boolean	This parameter always has to be set to **False** because you can use this API to communicate with only one site.
6.	**DistributionPoint**	Integer	Use one of the following values: • **1** = Run From DP • **2** = Download From DP
7.	**FunctionName**	String	Use one of the following values: • Install • Uninstall • Repair
8.	**ignoreMaintenanceWindows**	Boolean	Specify whether to ignore maintenance windows.
9.	**isMandatoryOverSlowLink**	Boolean	Specify whether this is mandatory even over slow links.
10.	**isRblDPVisible**	Boolean	Use to specify when a distribution point is available locally. The default value is True.
11.	**isRblNoDPVisible**	Boolean	Use to specify when no distribution point is available locally. The default value is True.

Table 11-85 • CreateDeploymentForACatalogItem Parameters

#	Parameter	Data Type	Description
12.	isSelected	Boolean	True for a selected site.
13.	LanguageID	Integer	Enter 0 for English.
14.	makeAvailableToBootandPXE	Boolean	Make this task sequence available to boot media and PXE.
15.	makeMandatory	Boolean	Make the advertisement mandatory.
16.	noDistributionPoint	Integer	Use one of the following values: • **1** = Don't Run • **2** = Download From RDP • **3** = Run From RDP
17.	OSDProgram	String	Enter the OSDProgramName, or you can leave it blank.
18.	PackageType	Integer	Use one of the following values: • **0, 7** = Software distribution package • **4** = Task sequence • **15** = Application
19.	priority	Integer	Use one of the following values: • **1** = High • **2** = Medium • **3** = Low
20.	ProgramName	String	Enter a program name.
21.	rerunBehavior	Integer	Use one of the following values: • **1** = Never Rerun • **2** = Always Rerun • **3** = Rerun Failed • **3** = Rerun Succeeded
22.	showTaskSequenceProgress	Boolean	Show the task sequence execution progress.
23.	SiteServer	String	Site server string.
24.	siteText	String	Enter the name of the site, such as **LAX** or **ORD**.

Table 11-85 • CreateDeploymentForACatalogItem Parameters

#	Parameter	Data Type	Description
25.	**SMSPackageID**	String	Enter the SMSPackageID of the catalog item.
26.	**taskSeqDistributionPoint**	Integer	Use one of the following values:
			• **1** = Don't Run
			• **2** = Download From RDP
			• **3** = Run From RDP
27.	**Title**	String	Name of the catalog item.
28.	**useRemoteDPForTaskSequence**	Boolean	Use a remote distribution point when no local distribution point is available.
29.	**useUnprotectedDP**	Boolean	Use an unprotected distribution point when no protected distribution point is available

Return Value

Returns one of the following:

- Returns a **1** when successfully creating the deployment for a catalog item.

- Returns a **0** if the deployment was not created.

- Returns a **-1** when encountering an exception.

createESDObjects

You can use the `createESDObjects` web method to trigger a collection and advertisement creation event; it is used to signal System Center Configuration Manager to begin creating pending advertisements and collections.

Parameters

This web method does not have any parameters.

createInventoryGroup

You can use the `createInventoryGroup` web method to create a new inventory group.

Parameters

The `createInventoryGroup` web method includes the following parameters:

Table 11-86 • createInventoryGroup Parameters

#	Parameters	Data Type	Description
1.	**GroupName**	String	The name of the new inventory group, duplicate group names are not allowed.
2.	**LicenseType**	String	The type of license. A new license type will be created if it does not exist.
3.	**Cost**	Double	The cost of the item.
4.	**Owned**	Integer	The quantity owned of the item.
5.	**Used**	Integer	The quantity used of the item.
6.	**MeterRuleName**	String	The name of the associated SCCM Metering Rule name.
7.	**MeterRulePartialMatch**	Boolean	When true the search will use LIKE syntax and search both the Meter Rule Name and Comments field in SCCM.
8.	**MeterRuleDays**	Integer	The number of days for the Metering Rule threshold.

Return Value

LicenseID (Integer).

createNewCatalogItem

You can use the `createNewCatalogItem` web method to create a new catalog item, and, optionally, create an associated inventory group that links to the new catalog item. If the install program has an MSI Product ID specified in the System Center Configuration Manager program, an inventory rule will be created for the inventory group.

Parameters

The `createNewCatalogItem` web method includes the following parameters:

Table 11-87 • createNewCatalogItem Parameters

#	Parameters	Data Type	Description
1.	**Title**	String	The title of the new catalog item. Duplicate titles are not accepted.
2.	**Description**	String	A description of the item.

Table 11-87 • createNewCatalogItem Parameters (cont.)

#	Parameters	Data Type	Description
3.	**Visible**	Boolean	Whether the catalog item is visible (Equivalent to "Is Globally Visible")
4.	**ImageFileName**	String	The file name of the image to display. The file must exist in the `App Portal\Web\Backgrounds\Packages` directory.
5.	**PackageServer**	String	The netbios name of the SCCM server where the package exists
6.	**SMSPackageID**	String	The SCCM PackageID representing the SCCM Package
7.	**SMSPackageData**	String	The formatting for the SMSPackageData is Program Action(0 - Install,1 - Uninstall,2 - Repair)|Language ID (0 for English)|Office 2007 Install (Program Name) 'Separate each entry with a comma e.g. 0|0|InstallInteractive,1|0|UninstallInteractive
8.	**TemplatePackageID**	Integer	The template package ID will copy over the existing settings from that catalog item including request options, visibility, approval, approval process, and Actions.
9.	**CategoryNames**	String	Separate each entry with a comma e.g. Software, Adobe. If the category does not exist it will be created and assigned to the root node.
10.	**GroupNames**	String	Add to security groups on approval. Separate each entry with a comma e.g. Domain\Group1,Domain\Group2
11.	**MembershipType**	Integer	Type 0 for User, 1 for computer or 2 for both
12.	**CreateInventoryRecord**	Boolean	Create a SCCM Inventory Record with the same name and assign it an inventory rule derived from the MSI Product ID of the install program.
13.	**SCCMInventoryAttribute**	String	Add any additional attributes to the inventory rules for the new inventory group. This is in addition to the MSI product ID extracted from the install program.

Return Value

PackageID (integer)

createRequest

The `createRequest` web method will create a new software request and target a user / computer.

Parameters

The createRequest web method includes the following parameters:

Table 11-88 • createRequest Parameters

#	Parameter	Data Type	Description
1.	**iPackageID**	Integer	App Portal catalog item ID.
2.	**strMachine**	String	Machine that the catalog item will be deployed to.
3.	**strRequester**	String	Unique user name of the person submitting the request.
4.	**strTargetUser**	String	Unique user name of the person that is to receive the deployable catalog item.
5.	**bUseApproval**	Boolean	A true/false flag indicating whether App Portal should submit this request as pending approval when applicable or not.
6.	**bSendEmail**	Boolean	A true/false flag indicating whether App Portal should send a confirmation email as a result of this request submission.
7.	**strQuestions**	String	Because this API endpoint does not support questions and answers, this should be hard-coded to the following input argument value: `New String() {}`

deleteKeywordsOfCatalogItem

Use the DeleteKeyWordsOfCatalogItem command to delete all the key words of a catalog item.

Parameters

The DeleteKeyWordsOfCatalogItem command includes the following parameters:

Table 11-89 • DeleteKeyWordsOfCatalogItem Parameters

#	Parameter	Data Type	Description
1.	**Title**	String	Name of the catalog item.

Return Value

Returns one of the following values:

- Returns a **1** when deleting an entry,
- Returns a **0** if there was no row deleted.
- Returns a **-1** when encountering an exception.

deployGetTargetPackages

You can use the deployGetTargetPackages web method to return an XML document of the System Center Configuration Manager package IDs for a given request ID.

Parameters

The deployGetTargetPackages web method includes the following parameters

Table 11-90 • deployGetTargetPackages Parameters

#	Parameters	Data Type	Description
1.	SS_RequestID	Integer	ID number of the request.

Return Value

Returns an XML document of the System Center Configuration Manager Package IDs.

getAllCatalogItems

You can use the getAllCatalogItems web method to return a data table of all catalog items.

Parameters

The getAllCatalogItems web method has no parameters.

Return Value

Data table containing PackageID and Catalog Title.

getAllInventoryGroups

You can use the getAllInventoryGroups web method to return a data table of all the inventory groups and major properties.

Parameters

The getAllInventoryGroups web method includes the following parameter:

Table 11-91 • getAllInventoryGroups Parameters

#	Parameters	Data Type	Description
1.	groupNameFilter	String	Specify the inventory group name to be applied as filter.

Return Value

Data table containing major attributes including name, cost, owned, used.

getAllRequestedOrInstalledSoftwareTitlesForMachine

You can use the getAllRequestedOrInstalledSoftwareTitlesForMachine web method to return an XML document containing the package IDs for all requested software for the specified machine name and package server.

Parameters

The getAllRequestedOrInstalledSoftwareTitlesForMachine web method includes the following parameters:

Table 11-92 • getAllRequestedOrInstalledSoftwareTitlesForMachine Parameters

#	Parameters	Data Type	Description
1.	strMachineName	String	Machine name.

getAllRequestedPackageIDsForMachine

You can use the getAllRequestedPackageIDsForMachine web method to return an XML document properly formatted for MDT integration containing the package IDs for all requested software for the specified machine name and package server.

Parameters

The getAllRequestedPackageIDsForMachine web method includes the following parameters:

Table 11-93 • getAllRequestedPackageIDsForMachine Parameters

#	Parameters	Data Type	Description
1.	strMachineName	String	Machine name.
2.	strServerName	String	Server name.
3.	strProgramFilter	String	Program name to be applied as filter.

Return Value

Returns an XML document.

getAllRequestedSoftwareTitlesForMachine

You can use the getAllRequestedSoftwareTitlesForMachine web method to returns an XML document containing titles of all of the previously requested software; you also have the option to validate whether it is currently installed.

Parameters

The getAllRequestedSoftwareTitlesForMachine web method includes the following parameters:

Table 11-94 • getAllRequestedSoftwareTitlesForMachine Parameters

#	Parameters	Data Type	Description
1.	**strMachineName**	String	Machine name.

getDetailsForExistingRequestsByPackageID

Use the GetDetailsForExistingRequestsByPackageID command to return an XML document containing existing request details for a particular Package ID.

Parameters

The GetDetailsForExistingRequestsByPackageID command includes the following parameters:

Table 11-95 • GetDetailsForExistingRequestsByPackageID Parameters

#	Parameter	Data Type	Description
1.	**iPackageID**	Integer	Package ID of the catalog item.

Return Value

Returns XML document.

getDetailsForExistingRequestsByRequestID

Use the GetDetailsForExistingRequestsByRequestID command to return an XML document that contains existing request details for a particular Request ID.

Parameters

The GetDetailsForExistingRequestsByRequestID command includes the following parameters:

Table 11-96 • GetDetailsForExistingRequestsByRequestID Parameters

#	Parameter	Data Type	Description
1.	**iRequestID**	Integer	Request ID of the request.

Return Value

Returns XML document.

getDetailsForExistingRequestsByUser

Use the GetDetailsForExistingRequestsByUser command to return an XML document containing existing request details for a user.

Parameters

The GetDetailsForExistingRequestsByUser command includes the following parameters:

Table 11-97 • GetDetailsForExistingRequestsByUser Parameters

#	Parameter	Data Type	Description
1.	**strUserName**	String	User name of the user.

Return Value

Returns XML document.

getInventoryItemsFromInventoryGroupID

You can use the getInventoryItemsFromInventoryGroupID web method to get the inventory items from the specified inventory group ID.

Parameters

The getInventoryItemsFromInventoryGroupID web method includes the following parameters:

Table 11-98 • getInventoryItemsFromInventoryGroupID Parameters

#	Parameters	Data Type	Description
1.	**Inventory ID**	Integer	Inventory ID.

getInventoryItemsFromInventoryGroupName

You can use the getInventoryItemsFromInventoryGroupName web method to get the inventory items from the specified inventory group name.

Parameters

The getInventoryItemsFromInventoryGroupName web method includes the following parameters:

Table 11-99 • getInventoryItemsFromInventoryGroupName Parameters

#	Parameters	Data Type	Description
1.	**groupName**	String	Name of inventory group.

getRequestApprovalStatus

Use the `GetRequestApprovalStatus` command to return an XML document that contains the status of a request in the approval process.

Parameters

The `GetRequestApprovalStatus` command includes the following parameters:

Table 11-100 • GetRequestApprovalStatus Parameters

#	Parameter	Data Type	Description
1.	**RequestID**	Integer	Request ID of the request.

Return Value

Returns XML document.

getSMSPackageIDsFromESDPackageIDs

You can use the `getSMSPackageIDsFromESDPackageIDs` web method to return an XML document of System Center Configuration Manager package IDs for corresponding string (separated by commas) of App Portal package IDs.

Parameters

The `getSMSPackageIDsFromESDPackageIDs` web method includes the following parameters:

Table 11-101 • getSMSPackageIDsFromESDPackageIDs Parameters

#	Parameters	Data Type	Description
1.	**strSiteServer**	String	Site server name.
2.	**strESDPackageIDs**	String	App Portal catalog item ID.
3.	**strProgramFilter**	String	Program name.

getSoftwareHashFromMSIProductID

You can use the getSoftwareHashFromMSIProductID web method to return the asset intelligence software hash for a specified MSI product ID.

Parameters

The `getSoftwareHashFromMSIProductID` web method includes the following parameters:

Table 11-102 • getSoftwareHashFromMSIProductID Parameters

#	Parameters	Data Type	Description
1.	**strMSIProductID**	String	The MSI product ID.

Return Value

AI Software Hash (String)

importComputer

You can use the `importComputer` web method to import a specified computer to the defined site and create a discovery record at the central.

Parameters

The `importComputer` web method includes the following parameters:

Table 11-103 • importComputer Parameters

#	Parameters	Data Type	Description
1.	**MachineName**	String	Computer name of the new machine
2.	**SiteCode**	String	The SCCM Site code where the record will be created.
3.	**Subnet**	String	The subnet address for the new computer.
4.	**ADSite**	String	The Active Directory Site code.
5.	**MACAddress**	String	The MAC Address of the computer.
6.	**SMBios**	String	The SMBIOS ID of the computer.
7.	**ComputerToAssociate**	String	The old computer name to associate with the newly created one.

Return Value

Returns one of the following values:

• Returns a **1** for success

• Returns a **0** for error

incrementInventoryGroupLicenseOwned

You can use the `incrementInventoryGroupLicenseOwned` web method to increment the inventory group license owned by the specified quantity.

Parameters

The `incrementInventoryGroupLicenseOwned` web method includes the following parameters:

Table 11-104 • incrementInventoryGroupLicenseOwned Parameters

#	Parameters	Data Type	Description
1.	GroupName	String	The name of the group to update.
2.	iIncrementCount	Integer	The count to add to the existing owned count.

Return Value

Returns one of the following values:

- Returns a **1** for success
- Returns a **-1** for error

incrementInventoryGroupLicenseUsed

You can use the `incrementInventoryGroupLicenseUsed` web method to increment the inventory group license used by the specified quantity. Setting this value will mark the inventory rule as **Manual Entry** and will not use System Center Configuration Manager data to determine total used.

Parameters

The `incrementInventoryGroupLicenseUsed` web method includes the following parameters:

Table 11-105 • incrementInventoryGroupLicenseUsed Parameters

#	Parameters	Data Type	Description
1.	GroupName	String	The name of the group to update.
2.	iIncrementCount	Integer	The count to add to the existing used count.

Return Value

Returns one of the following values:

- Returns a **1** for success
- Returns a **-1** for error

rejectRequest

You can use the `rejectRequest` web method to reject an existing request.

Parameters

The `rejectRequest` web method includes the following parameters:

Table 11-106 • rejectRequest Parameters

#	Parameters	Data Type	Description
1.	iRequestID	Integer	The ID of the request to reject
2.	strReason	String	The reason for the rejection
3.	strDescription	String	The description of the rejection
4.	strGUID	String	The Request GUID, use if RequestID is not provided.

Return Value

Returns one of the following values:

- Returns a **1** for success
- Returns a **-1** for error

removeAllInventoryRulesFromInventoryGroup

You can use the `RemoveAllInventoryRulesFromInventoryGroup` web method to remove all the inventory rules from an inventory group. An inventory group with no rules will have a usage of 0, unless the inventory usage is specifically added.

Parameters

The `RemoveAllInventoryRulesFromInventoryGroup` web method includes the following parameters:

Table 11-107 • RemoveAllInventoryRulesFromInventoryGroup Parameters

#	Parameters	Data Type	Description
1.	GroupName	String	The name of the group to remove inventory rules from.

Return Value

Returns one of the following values:

- Returns a **1** for success
- Returns a **-1** for error

removeAllWorkflowsFromCatalogItem

You can use the `removeAllWorkflowsFromCatalogItem` web method to remove all workflows from a catalog item.

Parameters

The `removeAllWorkflowsFromCatalogItem` web method includes the following parameters:

Table 11-108 • removeAllWorkflowsFromCatalogItem Parameters

#	Parameters	Data Type	Description
1.	Title	String	Title of catalog item.

Return Value

Returns one of the following values:

- Returns TRUE for success.

- Returns FALSE for failure.

removeCatalogItemFromAllCategories

You can use the `removeCatalogItemFromAllCategories` web method to remove a catalog item from all categories.

Parameters

The `removeCatalogItemFromAllCategories` web method includes the following parameters:

Table 11-109 • removeCatalogItemFromAllCategories Parameters

#	Parameters	Data Type	Description
1.	Title	String	The title of the item to remove from all categories.

Return Value

Returns one of the following values:

- Returns a **1** for success

- Returns a **-1** for error

removeCatalogItemFromCategory

You can use the `removeCatalogItemFromCategory` web method to remove a catalog item from a category.

Parameters

The `removeCatalogItemFromCategory` web method includes the following parameters:

Table 11-110 • removeCatalogItemFromCategory Parameters

#	Parameters	Data Type	Description
1.	**Title**	String	The title of the item to add programs to.
2.	**CategoryName**	String	The name of the category to remove the item from.

Return Value

Returns one of the following values:

- Returns a **1** for success
- Returns a **-1** for error

removeDeploymentForACatalogItem

Use the `RemoveDeploymentForACatalogItem` command to remove deployment for a catalog item.

Parameters

The `RemoveDeploymentForACatalogItem` command includes the following parameters:

Table 11-111 • RemoveDeploymentForACatalogItem Parameters

#	Parameter	Data Type	Description
1.	**Title**	String	Name of the catalog item.

Return Value

Returns one of the following values:

- Returns a **1** when removing the deployment for a catalog item.
- Returns a **0** if the deployment was not removed.
- Returns a **-1** when encountering an exception.

removeInventoryItemFromInventoryGroup

You can use the `removeInventoryItemFromInventoryGroup` web method to remove a single inventory item from the inventory group.

Parameters

The removeInventoryItemFromInventoryGroup web method includes the following parameters:

Table 11-112 • removeInventoryItemFromInventoryGroup Parameters

#	Parameters	Data Type	Description
1.	**GroupName**	String	The name of the group to update.
2.	**InventoryItem**	String	The display name of the add remove program entry.
3.	**Publisher**	String	The publisher of the add remove program entry.
4.	**Version**	String	The version of the add remove program entry.

Return Value

Returns one of the following values:

● Returns a **1** for success

● Returns a **-1** for error

removeWorkflowFromCatalogItem

You can use the removeWorkflowFromCatalogItem web method to remove a workflow from a catalog item.

Parameters

The removeWorkflowFromCatalogItem web method includes the following parameters:

Table 11-113 • removeWorkflowFromCatalogItem Parameters

#	Parameters	Data Type	Description
1.	**Title**	String	Title of catalog item.
2.	**workflowName**	String	Name of the workflow to be removed from the catalog.

Return Value

Returns one of the following values:

● Returns TRUE for success.

● Returns FALSE for failure.

updateActionStatus

You can use the updateActionStatus web method to update the status of an action associated with a package.

Parameters

The updateActionStatus web method includes the following parameters:

Table 11-114 • updateActionStatus Parameters

#	Parameters	Data Type	Description
1.	**RequestID**	Integer	ID of catalog item request.
2.	**Status**	String	Status of catalog item request.
3.	**IsApplicableForAllActionsInRequest**	Boolean	Enter True to update same status for all actions in request.

Return Value

Returns one of the following values:

- Returns TRUE for success.

- Returns FALSE for failure.

setRequestOnBehalfPropertyForCatalogItem

Use the SetRequestOnBehalfPropertyForCatalogItem command to set the "request on behalf" property for a catalog item. It allocates the "request on behalf" permission to the user, if provided.

Parameters

The SetRequestOnBehalfPropertyForCatalogItem command includes the following parameters:

Table 11-115 • SetRequestOnBehalfPropertyForCatalogItem Parameters

#	Parameter	Data Type	Description
1.	**Title**	String	Name of the catalog item.
2.	**username**	String	User name of the user.

Return Value

Returns one of the following values:

- Returns **1** when setting the request on behalf property for a catalog item

- Returns **0** if the property was not set.

- Returns **-1** when encountering an exception.

unAssignRequest

You can use the unAssignRequest web method to unassign inventory from the specified user.

Parameters

The unAssignRequest web method includes the following parameters:

Table 11-116 • unAssignRequest Parameters

#	Parameters	Data Type	Description
1.	**strUserName**	String	The user to unassign the inventory from.
2.	**strMachine**	String	The machine name to unassign the inventory from.
3.	**iLicenseID**	Integer	The ID of the inventory group to unassign.
4.	**strAssigner**	String	The name of the assigner.

Return Value

Returns one of the following values:

- Returns a **1** for success
- Returns a **-1** for error

updateApprovalRequiredForCatalogItem

You can use the updateApprovalRequiredForCatalogItem web method to enable or disable approval for a catalog item.

Parameters

The updateApprovalRequiredForCatalogItem web method includes the following parameters:

Table 11-117 • updateApprovalRequiredForCatalogItem Parameters

#	Parameters	Data Type	Description
1.	**Title**	String	The title of the item to change the description of.
2.	**ApprovalRequired**	Boolean	Whether the catalog item requires approval.

Return Value

Returns one of the following values:

- Returns a **1** for success
- Returns a **-1** for error

updateCatalogItemBriefDescription

Use the updateCatalogItemBriefDescription command to update the brief description of a catalog item.

Parameters

The updateCatalogItemBriefDescription command includes the following parameters:

Table 11-118 • updateCatalogItemBriefDescription Parameters

#	Parameter	Data Type	Description
1.	Title	String	Name of the catalog item.
2.	BriefDescription	String	Description of the catalog item.

Return Value

Returns one of the following values:

- Returns a **1** for success
- Returns a **0** for error

updateCatalogItemDescription

You can use the updateCatalogItemDescription web method to update the description of a catalog item.

Parameters

The updateCatalogItemDescription web method includes the following parameters:

Table 11-119 • updateCatalogItemDescription Parameters

#	Parameters	Data Type	Description
1.	Title	String	The title of the item to change the description of.
2.	CategoryName	String	The new description.

Return Value

Returns one of the following values:

- Returns a **1** for success
- Returns a **-1** for error

updateCatalogItemTitle

You can use the updateCatalogItemTitle web method to update the title of a catalog item.

Parameters

The updateCatalogItemTitle web method includes the following parameters:

Table 11-120 • updateCatalogItemTitle Parameters

#	Parameters	Data Type	Description
1.	**CurrentTitle**	String	The title of the item to modify.
2.	**NewTitle**	String	The name of the new title.

Return Value

Returns one of the following values:

- Returns a **1** for success
- Returns a **-1** for error

updateCatalogItemVisibility

You can use the updateCatalogItemVisibility web method to update the visibility of a catalog item.

Parameters

The updateCatalogItemVisibility web method includes the following parameters:

Table 11-121 • updateCatalogItemVisibility Parameter

#	Parameters	Data Type	Description
1.	**Title**	String	The title of the item to change the description of.
2.	**Visible**	Boolean	Whether the catalog item is globally visible.

Return Value

Returns one of the following values:

- Returns a **1** for success
- Returns a **-1** for error

updateInventoryGroupCost

You can use the updateInventoryGroupCost web method to update an inventory group cost.

Parameters

The updateInventoryGroupCost web method includes the following parameters:

Table 11-122 • updateInventoryGroupCost Parameters

#	Parameters	Data Type	Description
1.	GroupName	String	The name of the group to update.
2.	dblLicenseCost	Integer	The new cost of the item.

Return Value

Returns one of the following values:

- Returns a **1** for success
- Returns a **-1** for error

updateInventoryGroupLicenseOwned

You can use the updateInventoryGroupLicenseOwned web method to update the inventory group license owned to the specified quantity.

Parameters

The updateInventoryGroupLicenseOwned web method includes the following parameters:

Table 11-123 • updateInventoryGroupLicenseOwned Parameters

#	Parameters	Data Type	Description
1.	GroupName	String	The name of the group to update.
2.	iNewLicenseCount	Integer	The new quantity owned of the item.

Return Value

Returns one of the following values:

- Returns a **1** for success
- Returns a **-1** for error

updateInventoryGroupLicenseType

You can use the updateInventoryGroupLicenseType web method to update the inventory type of an inventory group.

Parameters

The updateInventoryGroupLicenseType web method includes the following parameters:

Table 11-124 • updateInventoryGroupLicenseType Parameters

#	Parameters	Data Type	Description
1.	**GroupName**	String	The name of the inventory group to update the license type.
2.	**LicenseType**	String	The new license type.

Return Value

Returns one of the following values:

- Returns a **1** for success
- Returns a **-1** for error

updateInventoryGroupLicenseUsed

You can use the updateInventoryGroupLicenseUsed web method to update the inventory group license used to the specified quantity. Setting this value will mark the inventory rule as **Manual Entry** and will not use System Center Configuration Manager data to determine total used.

Parameters

The updateInventoryGroupLicenseUsed web method includes the following parameters:

Table 11-125 • updateInventoryGroupLicenseUsed Parameters

#	Parameters	Data Type	Description
1.	**GroupName**	String	The name of the group to update.
2.	**iNewLicenseUsed**	Integer	The new quantity used of the item.

Return Value

Returns one of the following values:

- Returns a **1** for success
- Returns a **-1** for error

updateKeyWordsOfCatalogItem

Use the updateKeyWordsOfCatalogItem command to update or add a list of comma-separated keywords to a catalog item.

Parameters

The updateKeyWordsOfCatalogItem command includes the following parameters:

Table 11-126 • updateKeyWordsOfCatalogItem Parameters

#	Parameter	Data Type	Description
1.	Title	String	Name of the catalog item
2.	KeyWords	String	Keywords to be added to catalog item.

Return Value

Returns one of the following values:

- Returns a **1** when updating an entry,
- Returns a **0** if there was no row updated
- Returns a **-1** when encountering an exception.

VBScript Examples

The following VB Script examples are provided:

- VBScript
- VB.Net

VBScript

The example VBScript builds a properly formatted SOAP envelope that is posted to the web service API which in turn sends back a response. This response is used to determine success or failure of the web service call.

The script can be reused for other methods by changing the Method name and the appropriate parameters for the SOAP envelope.

```
strAppPortalServer = "WS07"
Method = "createNewCatalogItem"

URL = "http://" & strAppPortalServer & "/esd/api.asmx"
'Do not change this line
nsUrl = "http://sccmexpert.local/API"

Title = "Sample API Application"
Description = "Sample Description"
Visible = "true"
ImageFileName = "software.png"
PackageServer = "SMS01"
SMSPackageID = "SMX00A29"
SMSPackageData =   "0|0|InstallInteractive"
TemplatePackageID = "846"
```

```vbscript
CategoryNames = "Software,Adobe"
GroupNames = "smx\domain admins"
MembershipType = "1"
CreateInventoryRecord = "true"
SCCMInventoryAttributes =  ""


' Create the http request text
Dim strSoapReq
strSoapReq = GenerateSoapBodyStart()
strSoapReq = strSoapReq + GenerateSoapFunctionCallStart(Method)
strSoapReq = strSoapReq + GenerateSoapParameter("Title", Title)
strSoapReq = strSoapReq + GenerateSoapParameter("Description", Description)
strSoapReq = strSoapReq + GenerateSoapParameter("Visible", Visible)
strSoapReq = strSoapReq + GenerateSoapParameter("ImageFileName", ImageFileName)
strSoapReq = strSoapReq + GenerateSoapParameter("PackageServer", PackageServer)
strSoapReq = strSoapReq + GenerateSoapParameter("SMSPackageID", SMSPackageID)
strSoapReq = strSoapReq + GenerateSoapParameter("SMSPackageData", SMSPackageData)
strSoapReq = strSoapReq + GenerateSoapParameter("TemplatePackageID", TemplatePackageID)
strSoapReq = strSoapReq + GenerateSoapParameter("CategoryNames",  CategoryNames)
strSoapReq = strSoapReq + GenerateSoapParameter("GroupNames", GroupNames)
strSoapReq = strSoapReq + GenerateSoapParameter("MembershipType", MembershipType)
strSoapReq = strSoapReq + GenerateSoapParameter("CreateInventoryRecord", CreateInventoryRecord)
strSoapReq = strSoapReq + GenerateSoapParameter("SCCMInventoryAttributes", SCCMInventoryAttributes)
strSoapReq = strSoapReq + GenerateSoapFunctionCallEnd(Method)
strSoapReq = strSoapReq + GenerateSoapBodyEnd()


Dim oHttp
Dim strResult
Set oHttp = CreateObject("Msxml2.XMLHTTP")
oHttp.open "POST", URL, False
oHttp.setRequestHeader "Content-Type", "text/xml"
oHttp.setRequestHeader "SOAPAction", nsUrl + "/" & Method
oHttp.send strSoapReq

strResult = oHttp.responseText

WScript.echo(GetResult(strResult, Method & "Result"))


Function GetResult(byval responseText, byval resultParam)

    Dim oXml
    Set oXml = CreateObject("Msxml2.DOMDocument")
    oXml.Async = False
    oXml.LoadXml responseText

    Dim strPath
    strPath = "/*/*/*/" + resultParam
    Dim oNode
    Set oNode = oXml.documentElement.SelectSingleNode(strPath)
    GetResult = oNode.Text

End Function


Function GenerateSoapBodyStart()
```

```vbscript
        Dim strSoap
        strSoap = "<?xml version=""1.0"" encoding=""utf-8""?>"
        strSoap = strSoap + "<soap12:Envelope "
        strSoap = strSoap + "xmlns:xsi=""http://www.w3.org/2001/XMLSchema-instance"" "
        strSoap = strSoap + "xmlns:xsd=""http://www.w3.org/2001/XMLSchema"" "
        strSoap = strSoap + "xmlns:soap12=""http://www.w3.org/2003/05/soap-envelope"">"
        strSoap = strSoap + "<soap12:Body>"
        GenerateSoapBodyStart = strSoap

End Function


Function GenerateSoapBodyEnd()

        Dim strSoap
        strSoap = "</soap12:Body>"
        strSoap = strSoap + "</soap12:Envelope>"
        GenerateSoapBodyEnd = strSoap

End Function


Function GenerateSoapFunctionCallStart(byval strFunction)

        Dim strSoap
        strSoap = "<" + strFunction + " xmlns=""" + nsUrl + """>"
        GenerateSoapFunctionCallStart = strSoap

End Function


Function GenerateSoapFunctionCallEnd(byval strFunction)

        Dim strSoap
        strSoap = "</" + strFunction + ">"
        GenerateSoapFunctionCallEnd = strSoap

End Function


Function GenerateSoapParameter(byval strParam, byval strValue)

        If strValue = "True" Then
            strValue = "true"
        End If

        If strValue = "False" Then
            strValue = "false"
        End If

        Dim strSoap

        strSoap = "<" + strParam + ">"
        strSoap = strSoap + strValue
        strSoap = strSoap + "</" + strParam + ">"

        GenerateSoapParameter = strSoap

End Function
```

VB.Net

Begin by creating a Web Service reference to the API located at http://servername/ESD/api.asmx.

Example: Connect to the Web Service

```
Dim SSAPI As New AppPortalAPI.API

'Specify the URL to your particular server
SSAPI.Url = "http://ws07/esd/api.asmx"

'This is important to have if you are using your own credentials
'SSAPI.UseDefaultCredentials = True

'Or if you use an account
SSAPI.Credentials = New NetworkCredential("User", "Password", "Domain")
```

Example: Create a New Software Request

```
Dim oRequestID As Object = SSAPI.createRequest(846, "NewPCName3", "SMX\John", "SMX\John", True, False,
New String() {})

If IsNumeric(oRequestID) Then

    Console.WriteLine("Successfully created RequestID {0}", CInt(oRequestID))

Else

    Console.WriteLine("Problem submitting request: {0}", oRequestID.ToString)

End If
```

Example: Import a New Computer Object

```
Dim iResult As Integer = SSAPI.importComputer("NewPCName3", "SMX", "", "", "00:00:00:00:00:00", "", "")

Example: Approve request
Dim iResult As Integer = SSAPI.approveRequest(81972, "API Approval", "Approved via API", "SMX\John", "")

If iResult = 1 Then

    Console.WriteLine("Successfully Approved RequestID {0}",  81972)

End If
```

PowerShell Example

The following PowerShell script example demonstrates how to use App Portal web services.

```
################################################################################
##
## File name: ap_cancel_request.ps1
## Description: This script runs and finds a specific request in App Portal and then
##              cancels it
##
```

```
## Instructions:
##   1. Define the following two variables found the Define variable section
##           $serverName
##           $reqID
##   2. Save the script
##   3. Execute the script
##
##
# Define variables
$serverName = "<enter_app_portal_server_name>"
$URI = "http://$serverName/esd/api.asmx?WSDL"
$reqID = "<enter_request_id>"
$notify = $true


# Define Web Service
$WebService = New-WebServiceProxy -Uri $URI -UseDefaultCredential


# Get details of a specific request
$retRequests = $WebService.GetDetailsForExistingRequestsByRequestID($reqID)


foreach($apRequest in $retRequests){

    write-host About to cancel request with request ID $apRequest.dtRequestDetails.RequestID
    # Cancel a request
    $actionResult = $WebService.cancelRequest($reqID,$notify)
    if ($actionResult -eq "1") {
       Write-Host Action completed successully -ForegroundColor Green
    } else {
       Write-Host Action completed with error -ForegroundColor Red
    }
}
```

12

App Broker REST API Reference

The App Broker REST API powers the App Portal integration with third-party applications. This section describes the App Broker REST API endpoints.

- App Broker REST API Host Location

- Getting Started with App Broker REST API

- Catalog/Category API Endpoints

- Custom Selection API Endpoints

- Custom Filtering API Endpoints

- Custom Sorting API Endpoints

- Custom Pagination API Endpoints

- Users API Endpoints

- User Context API Endpoints

- Order (Package Request) API Endpoints

- Requests API Endpoints

- License API Endpoints

- ServiceNow Computer Provisioning Endpoints

- My Apps API Endpoints

- Approvals API Endpoints

- Development Tip: Postman Chrome Add-On

- Retrieving the Standard Conditions for License Reclamation and Retire/Upgrade Campaigns

Note • App Portal also has a set of API web methods, but they are SOAP based, while App Broker's API is REST and SOAP based. For more information, see App Portal API Reference.

App Broker REST API Host Location

The App Broker REST API, which powers the App Portal integration with third-party applications, is hosted in the ESD virtual directory, the same directory where the App Portal / App Broker administrator and end user website exists.

The API endpoints are accessible through the following URL domain and path:

```
http://APPPORTALSERVERNAME/esd/api
```

Getting Started with App Broker REST API

To begin using the App Broker REST API endpoints, perform the following steps.

Task   ***To get starting using the App Broker REST API endpoints***

1. Install App Portal / App Broker, as described in the *App Portal / App Broker Installation Guide*.

2. Launch App Portal / App Broker by opening the following URL:

   ```
   http://localhost/esd
   ```

   You will be prompted to upload your license file.

   ### Upload App Portal License File

   Upload App Portal License File [   ] Browse

   Upload License
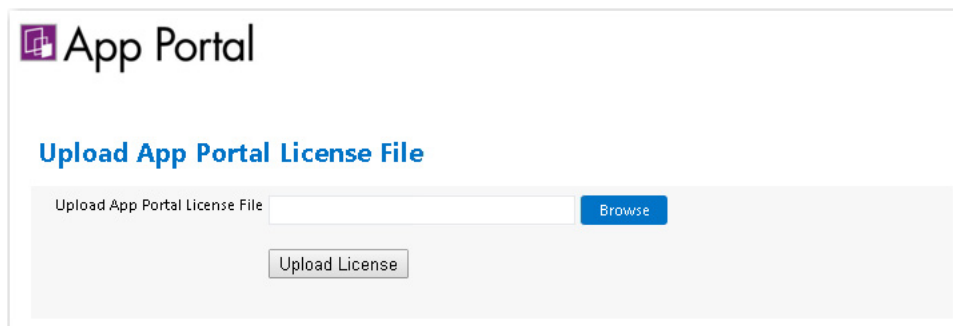
   Important • *The API will not be accessible until this step has been completed. The license file has encrypted information indicating whether you have access to the API endpoints. Any other license file (that does not have encrypted information relative to API access) will not grant access to the API endpoints. Unauthorized users attempting to use the API will receive either a 401 unauthorized or 500 internal server error response from the API.*

3. Next, you need to grant a user agent privilege to access the REST API. To do this, open the **Site Management > Admin Security** view on the App Portal / App Broker **Admin** tab.

4. Open the **Rest API** tab.

5. Click **Add User / Group**. The **Admin Security Add User/Group** dialog box dialog box opens.

6. Use the search fields to locate the user that you want to add.

Note • Select a user, not a group; groups are not recognized during the authentication process.

7. Under **Assign rights**, select **Read/Write/Delete** from the **REST API** list.

8. Click **Assign Rights** to add the user or group. This user will now have access to the REST API. This user's information should be used as network credentials in HTTP requests to the App Broker API.

Catalog/Category API Endpoints

The following are the catalog/category App Broker REST API endpoints:

- Getting All Categories

- Getting a Specific Category

- Getting Subcategories Nested Under a Specific Category

- Get All Catalog Items

- Getting a Specific Catalog Item

- Getting a List of Catalog Items in a Specific Category

Getting All Categories

This section describes the App Broker REST API endpoint for getting a list of all categories.

Table 12-1 • Get All Categories

Endpoint Example	Response Body Example
`[GET] http://localhost/esd/api/categories`	```[` ` {` ` "id": 14,` ` "name": "Microsoft Products",` ` "hasChildren": false,` ` "hasCatalogs": true` ` },` ` {` ` "id": 8,` ` "name": "Adobe Products",` ` "hasChildren": false,` ` "hasCatalogs": true` ` },` ` {...```

Getting a Specific Category

This section describes the App Broker REST API endpoint for getting a specific category, such as Category ID 4.

Table 12-2 • Get Specify Category

Endpoint Example	Response Body Example
`[GET] http://localhost/esd/api/categories/4`	```[` ` {` ` "id": 4,` ` "name": "Templates",` ` "hasChildren": false,` ` "hasCatalogs": true` ` }` `]```

Getting Subcategories Nested Under a Specific Category

This section describes the App Broker REST API endpoint for getting sub-categories nested under a specific category.

Table 12-3 • Get Subcategories Nested Under a Specific Category

Endpoint Example	Response Body Example

`[GET] http://localhost/esd/api/categories/1/children`	<pre>[
	    {
	        "id": 3,
	        "name": "Microsoft",
	        "parent": {
	            "id": 1
	        },
	        "hasChildren": false,
	        "hasCatalogs": true
	    }
	]</pre>

Get All Catalog Items

> *Note • Whenever the client retrieves catalog information, App Broker only sends non-archived and enabled catalog items. The third-party application may occasionally pull data from the App Broker API to get the most up-to-date catalog information. Therefore, when App Broker archives a catalog item, the third-party application will need to request data from the App Broker catalog's endpoint to see the update.*

This section describes the App Broker REST API endpoint for getting all catalog items.

Table 12-4 • Get All Catalog Items

Endpoint Example	Response Body Example

`[GET] http://localhost/esd/api/catalogs`	`[`
	`  {`
	`    "id": 201,`
	`    "name": "Brady Corporation LabelMark v6.1.0.216-0",`
	`    "briefDescription": "",`
	`    "fullDescription": "",`
	`    "type": "softwareCM12Application",`
	`    "currency": "USD",`
	`    "flexeraID": "",`
	`    "imageUrlPath": "/esd/backgrounds/packages/CatalogItem.png",`
	`    "createdOn": "2016-05-13T09:31:23.2",`
	`    "isAvailable": true,`
	`    "isApprovalNeeded": false,`
	`    "isLicenseNeeded": false,`
	`    "licenseScope": "globalOnly",`
	`    "questionTemplateID": 0,`
	`    "hasQuestions": false,`
	`    "hasAlternates": false,`
	`    "keywords": [],`
	`    "categories": []`
	`  },`
	`  {...`

Getting a Specific Catalog Item

This section describes the App Broker REST API endpoint to get a specific catalog item, such as Catalog ID 4.

Table 12-5 • Get a Specific Catalog Item

Endpoint Example	Response Body Example

`[GET] http://localhost/esd/api/catalogs/4`	<pre>[
	    {
	        "id": 4,
	        "name": "Microsoft Silverlight",
	        "briefDescription": "",
	        "fullDescription": "Microsoft Silverlight is a free
	            web-browser plug-in that enables interactive media
	            experiences, rich business applications and immersive
	            mobile apps.",
	        "type": "general",
	        "currency": "USD",
	        "flexeraID": "",
	        "imageUrlPath": "/esd/backgrounds/packages/silverlight.png",
	        "createdOn": "2015-06-14T10:59:20.083",
	        "updatedOn": "2015-06-14T10:59:20.083",
	        "isAvailable": true,
	        "isApprovalNeeded": false,
	        "isLicenseNeeded": false,
	        "licenseScope": "globalOnly",
	        "questionTemplateID": 0,
	        "hasQuestions": false,
	        "hasAlternates": false,
	        "keywords": [],
	        "categories": []
	    }
	]</pre>

Getting a List of Catalog Items in a Specific Category

This section describes the App Broker REST API endpoint to get a list of catalog items in a specific category, such as category 24.

Table 12-6 • Get a List of Catalog Items in a Specific Category

Endpoint Example	Response Body Example
`[GET] http://localhost/esd/api/categories/24/` `catalogs`	```[` ` {` ` "id": 201,` ` "name": "Brady Corporation LabelMark` `v6.1.0.216-0",` ` "briefDescription": "",` ` "fullDescription": "",` ` "type": "softwareCM12Application",` ` "currency": "USD",` ` "flexeraID": "",` ` "imageUrlPath": "/esd/backgrounds/packages/` `CatalogItem.png",` ` "createdOn": "2016-05-13T09:31:23.2",` ` "isAvailable": true,` ` "isApprovalNeeded": false,` ` "isLicenseNeeded": false,` ` "licenseScope": "globalOnly",` ` "questionTemplateID": 0,` ` "hasQuestions": false,` ` "hasAlternates": false,` ` "keywords": [],` ` "categories": []` ` },` ` {...```

Custom Selection API Endpoints

As seen in the previous examples, by default the navigational properties for catalog items are empty arrays. This is by design to improve efficiency. The "select" query string key gives callers the ability to populate navigational properties. In the example of catalog items, "keywords" and "categories" can be explicitly populated by the caller.

● Getting All Catalog Items With Their Keywords

Getting All Catalog Items With Their Keywords

This section describes the App Broker REST API endpoint to get all catalog items along with each catalog item's keywords.

Table 12-7 • Get All Catalog Items With Their Keywords

Endpoint Example	Response Body Example

`[GET] http://localhost/esd/api/`
`catalogs?select=keywords`
	``[
	    {
	        "id":11,"name":"Adobe Reader v8.0",
	        "briefDescription":"Leading software for
	            viewing PDF files",
	        "fullDescription":" Adobe Reader software
	            is the free trusted standard for
	            reliably viewing, printing, and
	            annotating PDF documents. It's the only
	            PDF file viewer that can open and
	            interact with all types of PDF content,
	            including forms and multimedia. ",
	        "type":"software","currency":"USD",
	        "flexeraID":"arl://MGS-APP-00000014874",
	        "imageUrlPath":"/esd/backgrounds/packages/
	            Adobe Reader v8.0..jpg",
	        "createdOn":"2015-08-28T15:49:23.34",
	        "isAvailable":true,
	        "isApprovalNeeded":false,
	        "isLicenseNeeded":true,
	        "licenseScope":"globalOnly",
	        "questionTemplateID":0,
	        "hasQuestions":false,
	        "hasAlternates":false,
	        "keywords":[{"description":"visibility"}],
	        "categories":[]
	    },
	    {...```

Custom Filtering API Endpoints

You have the ability to filter data returned from these APIs. The "filter" query string key is used to filter API data returned.

● Get All Updated Catalog Items

● Get Only Catalog Items Available in App Store After a Specific Date

Get All Updated Catalog Items

This section describes the App Broker REST API endpoint to get all catalog items that have been updated after they were created.

Table 12-8 • Get All Updated Catalog Items

Endpoint Example	Response Body Example
`[GET] http://localhost/esd/api/catalogs?` `    filter=updatedOn!=null`	```[
{
"id":7,
"name":"Microsoft Silverlight",
"briefDescription":"",
"fullDescription":"Microsoft Silverlight is a free
web-browser plug-in that enables interactive
media experiences, rich business applications
and immersive mobile apps.",
"type":"general",
"currency":"USD",
"flexeraID":"arl://MGS-APP-00000127234",
"imageUrlPath":"/esd/backgrounds/packages/
silverlight.png",
"createdOn":"2015-08-28T06:40:39.03",
"updatedOn":"2015-08-28T06:40:39.03",
"isAvailable":true,
"isApprovalNeeded":false,
"isLicenseNeeded":true,
"licenseScope":"globalOnly",
"questionTemplateID":1002,
"hasQuestions":true,
"hasAlternates":false,
"keywords":[],
"categories":[]
},
{...
``

Get Only Catalog Items Available in App Store After a Specific Date

This section describes the App Broker REST API endpoint to get only catalog items that are available in the app store and were created after October 1, 2015.

Table 12-9 • Get Only Catalog Items Available in App Store After a Specific Date

Endpoint Example	Response Body Example
```[GET] http://localhost/esd/api/catalogs? filter= isAvailable=true and createdOn > DateTime(2015, 10, 1)```	```[{ "id":315, "name":"AP-5155 Google Picasa 2.7.0 1.0", "briefDescription":"", "fullDescription":"", "type":"software", "currency":"USD", "flexeraID":"arl://MGS-APP-00000073198", "imageUrlPath":"/esd/backgrounds/packages/ CatalogItem.png", "createdOn":"2015-10-07T15:15:13.507", "isAvailable":true, "isApprovalNeeded":false, "isLicenseNeeded":true, "licenseScope":"globalOnly", "questionTemplateID":0, "hasQuestions":false, "hasAlternates":false, "keywords":[], "categories":[] }, {...```

Custom Sorting API Endpoints

You can sort data returned from the REST API endpoints. The "sort" query string key is used to order the data that is returned. To sort data in ascending order, enter the desired property name as query string value. To sort data in descending order, simply precede the desired property name with a minus (-) character. Any filter provided will be applied before the data is ordered as requested.

● Getting Catalog Items Ordered by Ascending Cost

● Getting Catalog Items Ordered by Descending Cost and Ascending Creation Date

Getting Catalog Items Ordered by Ascending Cost

This section describes the App Broker REST API endpoint to get catalogs ordered by ascending cost.

Table 12-10 • Get Catalog Items Ordered by Ascending Cost

Endpoint Example
[GET] http://localhost/esd/api/catalogs?sort=cost

📄

Note • When listing catalog items in ascending order, catalog items that have no cost are listed first; the cost property would not appear. To show all catalog items with a cost, then append 'filter=cost != null' as a query string to the URL.

Getting Catalog Items Ordered by Descending Cost and Ascending Creation Date

This section describes the App Broker REST API endpoint to get catalogs ordered by descending cost, then by ascending creation date.

Table 12-11 • Get Catalog Items Ordered by Descending Cost and Ascending Creation Date

Endpoint Example
[GET] http://localhost/esd/api/catalogs?sort=-cost,createdOn

Custom Pagination API Endpoints

You can paginate data returned from the REST API endpoints.

● **Limit the amount of data returned**—The pageSize query string key is used to limit the amount of data returned from the API endpoint. If pageSize is not provided in the query string, then the default page size value of 10,000 is used.

● **Select a page of data**—The page query string key is used to select a page of data returned from the API endpoint. Any filtering and/or sorting that is specified will be applied before the data is paginated as requested.

The API response header provides metadata detailing pagination information:

```
X-Pagination -->
{"currentPage":1,"pageSize":10000,"totalCount":87,"totalPages":1,"prevPage":"","nextPage":""}
```

For an example of custom pagination API endpoints, see the following topic:

● Getting Page 2 of a Catalog Item List With a Limited Number of Records Returned

Getting Page 2 of a Catalog Item List With a Limited Number of Records Returned

This section describes the App Broker REST API endpoint to get page 2 of a catalog item list and to limit the number of records returned to 5.

Table 12-12 • Getting Page 2 of Catalog Items With Limited Number of Records Returned

Endpoint Example	X-Pagination Header Example

`[GET] http://localhost/esd/api/catalogs?`
   `pageSize=5&page=2`
	`X-Pagination -->`
	`{`
	    `"currentPage":2,`
	    `"pageSize":5,`
	    `"totalCount":87,`
	    `"totalPages":18,`
	    `"prevPage":"/esd/api/catalogs?pageSize=5&page=1",`
	    `"nextPage":"/esd/api/catalogs?pageSize=5&page=3"`
	`}`

Users API Endpoints

The following are the users API endpoints:

● Getting All Users

● Getting a Specific User

● Getting a List of Machines Associated With a Specific User

Getting All Users

This section describes the App Broker REST API endpoint to get all users.

Table 12-13 • Get All Users

Endpoint Example	Response Body Example

`[GET] http://localhost/esd/api/users`	<pre>[
	   - {
	         uniqueUserName: "FLEX\\Rajneesh",
	         userFullName: "Rajneesh Sehgal",
	         adsPath: "CN=Rajneesh Seghal,OU=Development,
	                 OU=Information Technology,OU=Accounts,DC=flex,
	                 DC=local",
	         userDomain: "FLEX",
	         email: "Not Defined",
	         adGuid: "8eb92f18aa179349a0c61508afd726ff",
	         userOU: "OU-Development,OU=Information Technology,
	                 OU=Accounts,DC=flex,DC=local",
	         userNameExcludingDomain: "Rajneesh",
	       - memberGroups: [
	          - {
	                id: "87a6cfcd02790c43bfb2261eda070c88",
	                name: ""
	            },
	          - {
	                id: "8eb92f18aa179349a0c61508afd726ff",
	                name: ""
	            },
	          - {
	                id: "677d95d630b7df4db6b36cbddfb62645",
	                name: "CN=Enterprise Admins,CN=Users,DC=flex,
	                     DC=local"
	            },
	          - {
	                id: "692b5eb939048f419111f1a6cee93ce4",
	                name: ""
	            },
	          - {
	                id: "6890487642b29840ae029c6c347ff227",
	                name: ""
	            },</pre>

Getting a Specific User

This section describes the App Broker REST API endpoint to get a specific user.

Table 12-14 • Get a Specific User

Endpoint Example	Response Body Example
| `[GET] http://localhost/esd/api/users/`<br>`    domain=FLEX/user=JohnDoe` | ```
{
    uniqueUserName: "FLEX\\JohnDoe",
    userFullName: "John Doe",
    adsPath: "CN=John Doe,OU=Accounting,OU=Finance,OU=Accounts,
             DC=flex,DC=local",
    userDomain: "FLEX",
    email: "johndoe@flexerasoftware.com",
    adGuid: "33296b091b2ea74e968473daae161424",
    userOU: "OU=Accounting,OU=Finance,OU=Accounts,DC=flex,
             DC=local",
    userNameExcludingDomain: "JohnDoe",
  - memberGroups: [
      - {
            id: "692b5eb939048f419111f1as6cee93ce4",
            name: ""
        },
      - {
            id: "87a6cfcd02790c43bfb2261eda070c88",
            name: ""
        },
      - {
            id: "33296b091b2ea74e968473daae161424",
            name: ""
        },
      - {
            id: "6890487642b29840ae029c6c347ff227",
            name: ""
        }
    ],
  - userDeviceMemberGroups: [
      - {
            id: "692b5eb939048f419111f1as6cee93ce4",
            name: ""
        },
      - {
``` |

Getting a List of Machines Associated With a Specific User

This section describes the App Broker REST API endpoint to get a list of machines associated with a specific user. This information is used by App Broker to deploy packages to that user.

Table 12-15 • Get a List of Machines Associated With a Specific User

Endpoint Example	Response Body Example
`[GET] http://localhost/esd/api/users/domain=FLEX/user=JohnDoe/` `machines`	``` [{ "name": "WIN-7X64", "requestType": "userMapped" }] ```

User Context API Endpoints

User context is optional. If a user context is not provided, App Broker assumes the request context is a Data Crawler, which the third-party application would, in most cases, use to populate their database with App Broker data.

In cases where App Broker receives or requires user context (such as for deployment), this information is sent to App Broker through the following query string parameters:

```
dn (domain)
un (user name)
dev (user's device name)
```

Order (Package Request) API Endpoints

The App Broker REST API endpoint to place an order requires an HTTP POST method. The user context supplied in the URL query string is stored in the App Broker database as the requester of the order. Target information is provided in the request body in JSON format. The following is a sample order.

Table 12-16 • Order (Package Request) API Endpoints

Endpoint Example (Input)	Response Body Example (Output)

URI Example
 	
`[POST] http://localhost/esd/api/`
`orders?dn=FLEX&un=JaneDoe&dev=WIN-10X64`
 	
Request Body Example:
Without Prior License Reservation
 	
`{`
`   "targets":[`
`      {`
`         "uniqueUserName":"FLEX\\JaneDoe",`
`         "machineName":"WIN-10x64",`
`         "catalogs":[`
`            {`
`               "ID":6`
`            }`
`         ]`
`      }`
`   ]`
`}`
 	
Request Body Example:
With Prior License Reservation
 	
`{`
`   "targets":[`
`      {`
`         "uniqueUserName":"FLEX\\JaneDoe",`
`         "machineName":"WIN-10x64",`
`         "catalogs":[`
`            {`
`               "ID":6,`
`               "ReservationId":108`
`            }`
`         ]`
`      }`
`   ]`
`}`
	`{`
	`   "id": 101,`
	`   "name": FLX-101,`
	`   "requests": [`
	`      {`
	`         "dateTime": "2015-08-31T17:20:58.927",`
	`         "guid": "290223d0-ea74-4279-aacf-4355f24b8d72",`
	`         "machineName": "WIN-10X64",`
	`         "orderNo": "101",`
	`         "requestID": "2071",`
	`         "uniqueUserName": "FLEX\\JaneDoe",`
	`         "catalogID": "6",`
	`         "authorizationStatus": "pendingApproval",`
	`         "deploymentStatus": "notApplicable",`
	`         "status": "active",`
	`         "availableActions": [`
	`            "cancel"`
	`         ]`
	`      }`
	`   ]`
	`}`

Note • If a license reservation ID is not part of the request body to the Orders API, then App Broker will automatically attempt to reserve a license if applicable.

In the above example, the requester is `FLEX\JaneDoe`. The requester is requesting an order for `FLEX\JaneDoe` at machine `WIN-10X64` for a catalog item with an ID of 6.

As seen in the JSON string, "`targets`" accept an array of data; therefore, you can request multiple targets by appending a new target object {...} within the array brackets [ ].

Also, for each target, you can request multiple catalog items since "`catalogs`" also accepts an array of data. Each catalog object is in the following format, with multiple objects separated by commas within the array brackets [ ]:

`{"ID":#}`

The response to this order request is an order data object in JSON format with relative information: requester, target, IDs, active or canceled, deployment status, etc.

The request data model (`api/requests/#` or nested under `api/orders/#`) contains an array of actions available for the given request. Expect to see either `Cancel`, `Uninstall`, or an empty array.

- [Getting a Specific Order](#)
- [Getting a Package Request for a Specific User](#)

Getting a Specific Order

This section describes the App Broker REST API endpoint for getting a specific order (given the order ID from above).

Table 12-17 • Get a Specific Order

Endpoint Example	Response Body Example

`[GET] http://localhost/esd/api/orders/101`	<pre>[
	    {
	        "id": 101,
	        "name": "FLX-101",
	        "orderDate": "2015-08-31T17:20:59.253",
	        "requests": [
	            {
	            "dateTime": "2015-08-31T17:20:59.253",
	            "guid": "290223d0-ea74-4279-aacf-4355f24b8d72",
	            "machineName": "WIN-7X64",
	            "orderNo": 101,
	            "requestID": 2071,
	            "uniqueUserName": "FLEX\\JaneDoe",
	            "catalogID": 6,
	            "authorizationStatus": "pendingApproval",
	            "deploymentStatus": "notApplicable",
	            "deployments": [
	                {
	                    "technology": "sccm2012",
	                    "status": "notApplicable",
	                    "code": "0"
	                }
	            ],
	            "status": "active",
	            "availableActions": [
	              "cancel"
	              ]
	            }
	        ]
	    }
	]</pre>

Getting a Package Request for a Specific User

This section describes the App Broker REST API endpoint for getting a package request for a specific user (given the order scenario in Getting a Specific Order).

Table 12-18 • Get Package Request for Specific User

Endpoint Example	Response Body Examples
`[GET] http://localhost/esd/api/users/domain=FLEX/` `    user=JohnDoe/requests`	```[` ` {` ` "dateTime": "2015-06-15T19:19:21.49",` ` "guid": "26095792-436c-4d5f-8c38-e224e52c9549",` ` "machineName": "win-7x64",` ` "orderNo": 1,` ` "requestID": 1,` ` "uniqueUserName": "FLEX\\JohnDoe",` ` "catalogID": 6,` ` "authorizationStatus": "pendingApproval",` ` "deploymentStatus": "notApplicable",` ` "deployments": [` ` {` ` "technology": "sccm2012",` ` "status": "notApplicable",` ` "code": "0"` ` }` `],` ` "status": "active",` ` "availableActions": ["cancel"]` ` },` `{...`

🗋

Important • *The above example includes the property* `deploymentStatus` *in the API response. This property may soon be obsolete. The property* `deployments[].status` *should be referenced instead.*

Requests API Endpoints

After orders have been placed, given a request ID, the client can submit a cancel or uninstall. The request data model includes a node called `availableActions`, which indicates the available actions (cancel or uninstall) to take on a request. This information is available when looking up a request (`http://localhost/esd/api/orders/101`).

Table 12-19 • Requests API Endpoints

Task	API Endpoint
Submitting a cancel request	To submit a cancel request, the package request must be: `"availableActions": ["cancel"]`

Table 12-19 • Requests API Endpoints

Task	API Endpoint
Submitting an uninstall request	To submit an uninstall request, the package request must be: `"availableActions": ["uninstall"]`
Changing a request	The API endpoint to change a request will require a HTTP POST method.
Canceling a request	To cancel a request with ID 28: `[POST] http://localhost/esd/api/requests/28/cancel`
Uninstalling a package	To uninstall a package associated to request with ID 28: `[POST] http://localhost/esd/api/requests/28/uninstall`

License API Endpoints

The App Broker REST API endpoint checks license availability on a per-catalog-item basis. The license scope used is relative to the license scope of the catalog item App Portal is checking for.

The license scope information for each catalog item is available in the catalog item's API endpoint. The user context should be provided when checking for license availability.

- Getting License Available Count

- Getting License Availability

- Reserving a License Before Request Submission

Getting License Available Count

This section describes the App Broker REST API endpoint to get the license available count (as a numeric integer) for a catalog item with an ID 18:

Table 12-20 • Get License Available Count

Endpoint Example	Response Body Example

`[GET] http://localhost/esd/api/catalogs/18/licenses/available/count?`
`   dn=FLEX&un=JohnDoe&dev=WIN-7X64`
	`{`
	`   "result": 1`
	`}`

Getting License Availability

This section describes the App Broker REST API endpoint to get the license availability (as a Boolean true/false flag) for a catalog item with an ID of 18.

Table 12-21 • Get License Availability

Endpoint Example	Response Body Example

`[GET] http://localhost/esd/api/catalogs/18/licenses/availability?`
`   dn=FLEX&un=JohnDoe&dev=WIN-7X64`
	`{`
	`    "result": true`
	`}`

Reserving a License Before Request Submission

This section describes the App Broker REST API endpoint to post a license reservation for a catalog item with an ID of 18.

Table 12-22 • Reserving a License Before Request Submission

Endpoint Example (Input)	Response Body Example (Output)

URI Example
 	
`[POST] http://localhost/esd/api/catalogs/18/`
`   licenses?dn=FLEX&un=JohnDoe&dev=WIN-7X64`
	1

Request Body Example
 	
`{`
`    "uniqueUserName":"FLEX\\JaneDoe",`
`    "machineName":"WIN-10x64"`
 	
`}`	

The result of posting a license reservation is receiving a reservation ID. This reservation ID should be provided in the JSON payload when submitting a request to avoid duplicate reservation.

ServiceNow Computer Provisioning Endpoints

App Portal's integration with ServiceNow enables you to use ServiceNow as your front end app store, while App Portal performs the behind-the-scenes fulfillment of OS deployment and application migration software requests, as described in Using the Employee App Provision Request Wizard to Request Task Sequence Catalog Items.

This integration addresses the new hire/job change use case: the computer provisioning tasks which have to be performed when an employee joins a company or when the role of the employee changes. A service catalog request can be submitted from ServiceNow using the **Employee App Provision Request Wizard** and the entire workflow will be taken care of by App Portal, including creating and importing a new machine, and installing all of the software applications that the employee needs.

The following API endpoints are used to perform this ServiceNow integration regarding computer provisioning:

● Getting Additional Applications for OSD Checkout

- Getting Applications Associated to User and Machine Based on Conditional Roles

- Importing New Computer in System Center Configuration Manager and Associating a User

- Returning All Available System Center Configuration Manager Sites

- Getting Task Sequence Catalog Items

- Getting Status of Task Sequence / OSD Requests

- Getting Installed OS Information for a Machine

- Getting the Deployment Technology Details for a Machine

- Getting the Settings Related to Task Sequences

- Getting the Applications That Can Be Migrated

- Getting the Roles Applicable to a User

- Getting the Machines Associated to a User

- Submitting a Task Sequence / OSD Request

- Getting Additional Apps for Employee App Provisioning

Getting Additional Applications for OSD Checkout

This section describes the App Broker REST API endpoint to get a list of additional applications that can be installed during the checkout of an OSD task sequence catalog item.

Table 12-23 • Get Additional Applications for OSD Checkout

Endpoint Example	Response Body Example
`[GET] http://<SERVERNAME>/esd/api/apps?osdCompatible=` `   true&email=<logged-in_user_email>` `[GET] http://<SERVERNAME>/esd/api/apps?osdCompatible=` `   true&email=<logged-in_user_email>&searchText=<searchText>`	```[` ` {` ` "isUsed": false,` ` "catalogID": 11362,` ` "cost": 0,` ` "flexeraID": "",` ` "isLicenseNeeded": false,` ` "isUninstallable": false` ` },` ` {` ` "isUsed": false,` ` "catalogID": 11363,` ` "cost": 0,` ` "flexeraID": "",` ` "isLicenseNeeded": false,` ` "isUninstallable": false` ` }` `]```

Getting Applications Associated to User and Machine Based on Conditional Roles

This section describes the App Broker REST API endpoint to get a list of applications that are associated to a specific user/machine based upon conditional roles.

Table 12-24 • Get Additional Applications for OSD Checkout

Endpoint Example	Response Body Example

`[GET] http://<SERVERNAME>/esd/api/roles/`
`   domain=AppPortal/user=UserName/`
`   machine=MachineName/apps`
	`[`
	`    {`
	`        "catalogID": 15,`
	`        "name": ".NET Framework 3.0",`
	`        "cost": 30,`
	`        "flexeraID": ""`
	`    },`
	`    {`
	`        "catalogID": 20,`
	`        "name": ".NET Framework SDK 1.1 ",`
	`        "cost": 0,`
	`        "flexeraID": "arl://MGS-APP-00000039578"`
	`    }`
	`]`

Importing New Computer in System Center Configuration Manager and Associating a User

This section describes the App Broker REST API endpoint to import a new computer into System Center Configuration Manager and associating a user to that computer.

Table 12-25 • Importing New Computer into System Center Configuration Manager and User Association

Endpoint Example	Response Body Example (Output)

URI Example
 	
`[POST] http://<SERVERNAME>/esd/api/computers`
	`{`
	   `"computerResourceId": "65"`
	`}`

Request Body Example
 	
`{`
   `"UserName": "SatheeshChandran",`
   `"FullName": "",`
   `"UserEmail": "",`
   `"UserDomain": "AppPortal",`
   `"ComputerName": "SCHAPSOMECOM44",`
   `"DeploymentMapping":`
   `{`
      `"SiteServer": "ITAAP1511CASLAX",`
      `"MacAddress":"01:23:45:67:89:ab",`
      `"SMBIOS": "00000000-0000-1001-8000-010203041561"`
   `}`
`}`	

Input Parameter Details

The following are the details for the parameters listed in the Request Body Example:

Table 12-26 • Input Parameter Details of Request Body Example

Parameter	Description
UserName	User name to which the new computer will be associated. (Optional) This is not a required field, but if the **UserDomain** parameter has a value, this parameter must also have a value; if it does not, the command will fail. Also, the provided user name must exist in the App Portal database.
FullName	Full name of the user. (Optional)
UserEmail	Email address of the user to which the new computer will be associated. (Optional)
UserDomain	Domain name to which the user belongs. (Optional) This is not a required field, but if the **UserName** parameter has a value, this parameter must also have a value; if it does not, the command will fail. Also, the provided domain must exist in the App Portal database.

Table 12-26 • Input Parameter Details of Request Body Example

Parameter	Description
ComputerName	Name of the computer that you want to import into System Center Configuration Manager. The computer name cannot be more than 15 characters. (Required) *Important • Do not enter the name of an existing computer.*
SiteServer	Server name of the System Center Configuration Manager server into which the computer will be imported. (Required)
MacAddress	MAC Address of the computer that is being imported. Hexadecimal values are accepted. *Important • Specify either a MAC address or a SMBIOS GUID; only one is required. If you enter value for SMBIOS, do not also enter a value for MacAddress.*
SMBIOS	SMBIOS address of the computer that is being imported. *Important • Specify either a MAC address or a SMBIOS GUID; only one is required. If you enter value for MacAddress, do not also enter a value for SMBIOS.*

Output Details

If the import is successful, the API responds with the resource ID of the computer that is imported.

Returning All Available System Center Configuration Manager Sites

This section describes the App Broker REST API endpoint to return a list of all of the available System Center Configuration Manager sites. This endpoint would be used to enable the requester to choose which System Center Configuration Manager site to import the new computer into.

Table 12-27 • Importing New Computer into System Center Configuration Manager and User Association

Endpoint Example	Response Body Example

`[GET] http://<SERVERNAME>/esd/api/`
`   deployments/SCCMSites`
	```[```
	``` {```
	``` "site": "ConfigMgr CAS Lax - LAX",```
	``` "serverName": "ITA98765.APPPORTAL.MYCORP.COM"```
	``` },```
	``` {```
	``` "site": "SCHAPCM16KOL - KOL",```
	``` "serverName": "ITA35155.APPPORTAL.MYCORP.COM"```
	``` }```
	```]```

Output Details

The output provides a list of available System Center Configuration Manager sites. The parameter `"site"` gives the site name and the parameter `"ServerName"` gives the corresponding server name for that site.

Getting Task Sequence Catalog Items

This section describes the App Broker REST API endpoint to return a list of task sequence catalog items.

Table 12-28 • Getting Task Sequence Catalog Items

Endpoint Example	Response Body Example
`[GET] http://<SERVERNAME>/esd/api/catalogs/` `    tasksequence?isOsDeployment=<true/false>`	```[` ` {` ` "id": 18,` ` "name": "TaskSequence_For_Win10_10July",` ` "briefDescription": "",` ` "type": "general",` ` "currency": "USD",` ` "imageUrlPath": "/esd/backgrounds/packages/",` ` "isAvailable": false,` ` "isApprovalNeeded": false,` ` "isLicenseNeeded": false,` ` "licenseScope": "globalOnly",` ` "hasQuestions": false,` ` "hasAlternates": false,` ` "keywords": [],` ` "categories": []` ` },` ` {` ` "id": 19,` ` "name": "TestTaskSequence_10July",` ` "briefDescription": "",` ` "type": "general",` ` "currency": "USD",` ` "imageUrlPath": "/esd/backgrounds/packages/",` ` "isAvailable": false,` ` "isApprovalNeeded": false,` ` "isLicenseNeeded": false,` ` "licenseScope": "globalOnly",` ` "hasQuestions": false,` ` "hasAlternates": false,` ` "keywords": [],` ` "categories": []` ` }` `]```

Input Parameter Details

The `isOsDeployment` parameter in the URL expects a boolean value: `true` or `false`.

Output Details

The output returns a list of task sequences.

Getting Status of Task Sequence / OSD Requests

This section describes the App Broker REST API endpoint to give the status of task sequence / OSD requests.

Table 12-29 • Getting the Status of Task Sequence / OSD Requests

Endpoint Example	Response Body Example

[GET] http://<SERVERNAME>/esd/api/requests/
    <requestId>
	<pre>[
	    {
	        "dateTime": "2017-05-15T11:44:30.723",
	        "guid": "b79ff7f7-3222-4c49-88c3-e97d3bc7b966",
	        "machineName": "CHEDEV01",
	        "orderNo": 18,
	        "requestID": 1021,
	        "uniqueUserName": "APPPORTAL\\SatheeshChandran",
	        "installationDate": "2017-05-15T11:44:29",
	        "catalogID": 14,
	        "authorizationStatus": "approvalNotRequired",
	        "deployments":
	            [
	                {
	                    "technology": 8,
	                    "status": "installationPending",
	                    "code": "0"
	                }
	            ],
	        "status": "active",
	        "availableActions":
	            [
	                "cancel"
	            ],
	        "taskSequenceApps":
	            [
	                {
	                    "packageTitle": "AdWords Tester3",
	                    "packageId": 13,
	                    "roleName": "Test Role",
	                    "briefDescription": "",
	                    "catalogCost": 0
	                },
	                {
	                    "packageTitle": "Fail_Ping_12272016",
	                    "packageId": 11,
	                    "roleName": "",
	                    "briefDescription": "",
	                    "catalogCost": 0
	                },
	                {
	                    "packageTitle": "FirFox New Pkg",
	                    "packageId": 20,
	                    "roleName": "",
	                    "briefDescription": "",
	                    "catalogCost": 0
	                }
	            ]
	    }
	]</pre>

Input Parameter Details

The requestId parameter in the URL expects an integer value, the ID of the request that is submitted.

Output Details

The output returns the status of task sequence / OSD requests.

Getting Installed OS Information for a Machine

This section describes the App Broker REST API endpoint to return the installed operating system for a machine..

Table 12-30 • Getting Installed OS Information for a Machine

Endpoint Example	Response Body Example

`[GET] http://<SERVERNAME>/esd/api/computers/`
`   ComputerName=<machinename>/`
`   OperatingSystemInfo`
	`[`
	`   {`
	`       "operatingSystem": "Microsoft Windows 10",`
	`       "servicePack": ""`
	`   }`
	`]`

Input Parameter Details

The ComputerName parameter in the URL expects a a valid machine name.

Output Details

The output returns the operating system information of the specified machine.

Getting the Deployment Technology Details for a Machine

This section describes the App Broker REST API endpoint to get the deployment technology details for a machine..

Table 12-31 • Getting the Deployment Technology Details for a Machine

Endpoint Example	Response Body Example

`[GET] http://<SERVERNAME>/esd/api/computers/`
`   ComputerName=<machinename>/`
`   DeploymentMapping`
	`[`
	`   {`
	`       "computerResourceId": "16777221",`
	`       "smBios": "00000000-0000-0000-0000-000000000000"`
	`   }`
	`]`

Input Parameter Details

The ComputerName parameter in the URL expects a a valid machine name.

Output Details

The output returns the deployment technology information of the specified machine, whether it is present in System Center Configuration Manager or not.

Getting the Settings Related to Task Sequences

This section describes the App Broker REST API endpoint to get a list of the settings related to task sequences..

Table 12-32 • Getting the Settings Related to Task Sequences

Endpoint Example	Response Body Example

`[GET] http://<SERVERNAME>/esd/api/admin/`
`   TaskSequenceSettings`
	`{`
	`    "enableAppDetection": true,`
	`    "enableUserAppSelection": true,`
	`    "enableAdditionalApps": false,`
	`    "processBothInserts": true`
	`}`

Output Details

The output returns settings related to task sequences.

Getting the Applications That Can Be Migrated

This section describes the App Broker REST API endpoint to get a list of applications that can be migrated from a source

machine to a target machine.

Table 12-33 • Getting the Applications That Can Be Migrated

Endpoint Example	Response Body Example

`[GET] http://<SERVERNAME>/esd/api/ apps?targetmachinename=<machinename> &machineDomain=<domain>& sourcemachinename=<machinename>& migratable=true`	<pre>[
	    {
	        "catalogID": 11,
	        "name": "Fail_Ping_12272016",
	        "cost": 0,
	        "flexeraID": "arl://MGS-APP-00000235880",
	        "recommended": false,
	        "upgrade": false,
	        "deployable": true,
	        "upgradedPackage": "",
	        "enableUserSelection": true,
	        "applicationUsageInformation": "Usage Pattern:
	        Infrequently Used.",
	        "briefDescription": ""
	    },
	    {
	        "catalogID": 13,
	        "name": "AdWords Tester3",
	        "cost": 50,
	        "flexeraID": "arl://MGS-APP-00000127234",
	        "recommended": false,
	        "upgrade": false,
	        "deployable": true,
	        "upgradedPackage": "",
	        "enableUserSelection": true,
	        "applicationUsageInformation":
	            "Usage Pattern: Infrequently Used.",
	        "briefDescription": ""
	    },
	    {
	        "catalogID": 23,
	        "name": "Silverlight 5 [Microsoft]",
	        "cost": 50,
	        "flexeraID": "arl://MGS-APP-00000126928",
	        "recommended": false,
	        "upgrade": true,
	        "deployable": true,
	        "upgradedPackage": "AdWords Maker _JRB",
	        "enableUserSelection": false,
	        "applicationUsageInformation": "Silverlight 5
	            [Microsoft] will be upgraded by AdWords Maker
	            _JRB. Usage Pattern: Infrequently Used.",
	        "briefDescription": "Some desc",
	        "applicationUpgradeInformation": "Silverlight 5
	            [Microsoft] will be upgraded by AdWords Maker"
	    }
	]</pre>

Prerequisites

In order to get obtain some of the applications for a user and machine:

- **Application migration enabled**—The global setting **Enable application migration and installation of additional applications** option must be selected.

- **Not designated as core application**—On the **General > Global** tab of the **Catalog Item Properties** dialog box for the catalog item, the **Core application** option must not be selected.

- **Flexera ID**—Catalog item must have an associated Flexera ID identified (from the FlexNet Manager Suite Application Recognition Library).

Endpoint Example Parameter Details

The following are the details for the parameters listed in the endpoint example.

Table 12-34 • Endpoint Example Parameter Details

Parameter	Description
`targetmachinename`	Enter a valid machine name, which is the target.
`domain`	Enter the domain to which the machine belongs.
`sourcemachinename`	Enter a valid machine name from which the applications have to be migrated.

Output Details

The output returns a list of software applications that can be migrated.

Getting the Roles Applicable to a User

This section describes the App Broker REST API endpoint to get the details of the role(s) applicable to the user..

Table 12-35 • Getting the Roles Applicable to a User

Endpoint Example	Response Body Example

`[GET] http://<SERVERNAME>/esd/api/`
`   roles?domain=<domain>&username=<username>`
`   &machinename=<machinename>&getRoles=true`
	`[`
	`   {`
	`      "roleID": 2,`
	`      "roleName": "TestRole2",`
	`      "roleDescription": ""`
	`   }`
	`]`

Input Parameter Details

The following are the details for the parameters listed in the Request Body Example:

Table 12-36 • Input Parameter Details of Request Body Example

Parameter	Description
ComputerName	Enter a valid machine name.
domain	Enter the domain to which the user belongs.
userName	Enter a valid user name for whom the roles need to be found.

Output Details

The output returns a list of roles and details for those roles.

Getting the Machines Associated to a User

This section describes the App Broker REST API endpoint to get a list of machines associated to the user..

Table 12-37 • Getting the Machines Associated to a User

Endpoint Example	Response Body Example
`[GET] http://<SERVERNAME>/esd/api/users/domain=<domain>/` `    user=<username>/machines`	```[` ` {` ` "name": "ITAAPACRESSODEV",` ` "requestType": "userMapped"` ` },` ` {` ` "name": "ITAAPPHOWEDEV",` ` "requestType": "userMapped"` ` },` ` {` ` "name": "ITAAP1511CASLAX",` ` "requestType": "userMapped"` ` }` `]```

Input Parameter Details

The following are the details for the parameters listed in the Request Body Example:

Table 12-38 • Input Parameter Details of Request Body Example

Parameter	Description
domain	Enter the domain to which the machine belongs.
username	Enter a valid user name for whom the machines have to be fetched.

Output Details

The output returns a list of machines associated to the user.

Submitting a Task Sequence / OSD Request

This section describes the App Broker REST API endpoint to submit a task sequence/OSD request to App Portal..

Table 12-39 • Submitting a Task Sequence / OSD Request

Endpoint Example	Response Body Example

[POST] http://<SERVERNAME>/esd/api/
    servicenow/requests/
    SN1001?dn=appportal&un=spatel&dev=
    itaapccnet01
	<pre>{
	    "requestId":"0",
	    "appPortalOrder":
	    {
	        "targets":
	        [
	            {
	                "uniqueUserName":"APPPORTAL\\spatel",
	                "machineName":"NuMacSat01",
	                "catalogs":
	                [
	                    {
	                        "id":14,
	                        "reservationId":0
	                    }
	                ]
	            }
	        ],
	        "RolesAndApps":
	        [
	            {
	                "RoleId":"1",
	                "MigrationType":"1",
	                "CatalogIdsSelectedForMigrateAndInstall":
	                    "1,2,3",
	                "ProcessBothInserts":"true",
	                "CreateAssociation":"false",
	                "OldMachineName":"chedev01",
	                "OsdBuildId":"xyztxt",
	                "MacAddr":"12:34:56:78:98:76"
	            }
	        ]
	    }
	}</pre>

Input Parameter Details

The following are the details for the parameters listed in the Request Body Example:

Table 12-40 • Input Parameter Details of Request Body Example

Parameter	Description
RequestId	Can be any string.
UniqueUserName	Unique name for the target user.
Machine	Target machine where the task sequence / OSD should be deployed.
Catalogs	The catalog item for which the request is being made.
RoleId	The role that is applicable to the target user.
MigrationType	Possible values are: • **1**—In-place migration • **2**—Side by side migration • **3**—No data migration 📄 *Note • Option 3, no data migration, is already handled in different scenarios from Employee App Provisioning in ServiceNow.*
CatalogIdsSelectedForMigrateAndInstall	IDs of catalog items that are part of role, selected as part of migratable apps and additional apps.
ProcessBothInserts	Insert both source machine and target machine into collection.
CreateAssociation	Create association between source and target computers.
OldMachineName	Name of the old or source computer.
OsdBuildId	Build ID with 6-character-long string
MacAddr	MAC address of the target computer.

Output Details

The output gives HTTP status 200.

Getting Additional Apps for Employee App Provisioning

This section describes the App Broker REST API endpoint to get a list of additional applications to migrate.

Table 12-41 • Getting Additional Applications for Employee App Provisioning

Endpoint Example	Response Body Example

`[GET] http://<SERVERNAME>/esd/api/`
`   apps?osdCompatible=true&searchText=${searchText}`
	```[```
	 ``` {```
	 ``` "isUsed": false,```
	 ``` "catalogID": 23,```
	 ``` "catalogTitle": "AdWords Maker _JRB",```
	 ``` "cost": 50,```
	 ``` "isLicenseNeeded": false,```
	 ``` "isUninstallable": false,```
	 ``` "briefDescription": "Some desc",```
	 ``` "showInventoryCost": true```
	 ``` },```
	 ``` {```
	 ``` "isUsed": false,```
	 ``` "catalogID": 13,```
	 ``` "catalogTitle": "AdWords Tester3",```
	 ``` "cost": 50,```
	 ``` "isLicenseNeeded": false,```
	 ``` "isUninstallable": false,```
	 ``` "briefDescription": "",```
	 ``` "showInventoryCost": true```
	 ``` }```
	 ```]```

Prerequisites

In order to get obtain a list of additional applications to migrate:

- **Application migration enabled**—The global setting **Enable application migration and installation of additional applications** option must be selected.

- **Not designated as core application**—On the **General > Global** tab of the **Catalog Item Properties** dialog box for the catalog item, the **Core application** option must not be selected.

- **Flexera ID**—Catalog item must have an associated Flexera ID identified (from the FlexNet Manager Suite Application Recognition Library).

Input Parameter Details

The SearchText parameter is optional; if it is passed with a value, the API will search with that value against the catalog item title, brief description, and long description, and will return the matching results.

Output Details

The output returns the list of applications that can be selected as part of OSD checkout as additional applications.

My Apps API Endpoints

When App Portal is integrated with FlexNet Manager Suite, it has access to the FlexNet Manager Suite Application Recognition Library (ARL), which uniquely identifies applications that have been installed on users machines. Administrators have enabled license reclamation and alert actions to prompt end users to address compliance issues. Some applications are configured to be auto-uninstalled if there are compliance issues.

App Broker provides the following API endpoints that provide My Apps data.

- Getting a List of Installed Applications on a User's Machine

- Getting a List of a User's Pending My Apps Alerts

- Getting a List of a User's Resolved My Apps Alerts

- Getting a List of a User's Machine Policy Score

- Getting a List of All My Apps Alerts

- Getting a Single My Apps Alert

- Getting a List of Uninstall Alert Questions

- Getting a List of Keep Alert Questions

- Invoking Uninstall Action in Response to an Alert

- Invoking Keep Action in Response to an Alert

- Invoking Compliance Action in Response to an Alert

- Question Metadata Returned from Uninstall and Keep Alerts

- Error Returned When Using IIS 7.5 on Windows Server 2008 R2 Machine

Getting a List of Installed Applications on a User's Machine

This section lists the App Broker REST API endpoint to get a list of installed applications on a user's machine (including pending and resolved alerts).

Table 12-42 • Get List of Installed Applications on a User's Machine

Endpoint Example
`[GET] http://localhost/esd/api/users/domain=FLEX/user=JohnDoe/machine=WIN-7X64/apps`

Getting a List of a User's Pending My Apps Alerts

This section lists the App Broker REST API endpoint to get a list of pending My Apps alerts that a user needs to address for their machine.

Table 12-43 • Get a List of a User's Pending My Apps Alerts

Endpoint Example
`[GET] http://localhost/esd/api/users/domain=FLEX/user=JohnDoe/machine=WIN-7X64/alerts`

Getting a List of a User's Resolved My Apps Alerts

This section lists the App Broker REST API endpoint to get a list of My Apps alerts that a user has previously resolved for their machine:

Table 12-44 • Get List of a User's Resolved My Apps Alerts

Endpoint Example
`[GET] http://localhost/esd/api/users/domain=FLEX/user=JohnDoe/machine=WIN-7X64/resolvedalerts`

Getting a List of a User's Machine Policy Score

This section lists the App Broker REST API endpoint to get a list of a user's machine policy score. It returns a percentage breakdown of issues related to installed applications.

Table 12-45 • Get a List of a User's Machine Policy Score

Endpoint Example
`[GET] http://localhost/esd/api/users/domain=FLEX/user=JohnDoe/machine=WIN-7X64/policyscore`

Getting a List of All My Apps Alerts

This section describes the App Broker REST API endpoint to get a list of all My Apps alerts.

Table 12-46 • Getting a List of All My Apps Alerts

Endpoint Example	Response Body Example
`[GET] http://localhost/esd/api/alerts`	``` [{ "id": 22184, "machineName": "ITAAPCCNET01", "uniqueUserName": "APPPORTAL\\AppPortal", "type": "confessional", "notificationDate": "2017-03-03T19:45:58.793", "response": "notResponded", "status": "pending", "smartUninstallRequired": false, "availableActions": ["Compliance"] , { "id": 22187, "machineName": "ITAAPCCNET01", "uniqueUserName": "APPPORTAL\\AppPortal", "type": "licenseReclamation", "notificationDate": "2017-03-03T19:45:58.8", "response": "notResponded", "status": "pending", "smartUninstallRequired": true, "availableActions": ["Uninstall", "Keep"] }] ```

Alert Metadata

This section describes the alert metadata returned when getting a list of My Apps alerts:

Table 12-47 • Alert Metadata

Item	Description
id	Unique identifier of alert resource.
machineName	Name of machine with alert.
uniqueUserName	User associated to machine.

Table 12-47 • Alert Metadata

Item	Description
type	Specifies the type of alert generated as one of the following: ● **LicenseReclamation** ● **Compliance**
notificationDate	Date/time alert was generated.
response	Specifies the current response status of the alert as one of the following: ● **Keep** ● **Uninstall** ● **NotResponded** ● **Compliance**
status	Specifies the current status of the alert as one of the following: ● **Pending** ● **Resolved**
smartUninstallRequired	If smart uninstall is required because the app doesn't have an uninstall program in the deployment technology, this item is set to **True**. It smart uninstall is not required, this property is set to **False**.
availableActions	Lists the available actions: ● **Compliance** ● **Uninstall** ● **Keep**

Getting a Single My Apps Alert

This section describes the App Broker REST API endpoint to get a single My Apps alert.

Table 12-48 • Getting a List of All My Apps Alerts

Endpoint Example	Response Body Example
`[GET] http://localhost/esd/api/alerts/22184`	```[{ "id": 22184, "machineName": "ITAAPCCNET01", "uniqueUserName": "APPPORTAL\\AppPortal", "type": "confessional", "notificationDate": "2017-03-03T19:45:58.793", "response": "notResponded", "status": "pending", "smartUninstallRequired": false, "availableActions": ["Compliance"] }]```

Alert Metadata

This section describes the alert metadata returned when getting a single My Apps alert:

Table 12-49 • Alert Metadata

Item	Description
id	Unique identifier of alert resource.
machineName	Name of machine with alert.
uniqueUserName	User associated to machine.
type	Specifies the type of alert generated as one of the following: ● **LicenseReclamation** ● **Compliance**
notificationDate	Date/time alert was generated.
response	Specifies the current response status of the alert as one of the following: ● **Keep** ● **Uninstall** ● **NotResponded** ● **Compliance**

Table 12-49 • Alert Metadata

Item	Description
status	Specifies the current status of the alert as one of the following: • **Pending** • **Resolved**
smartUninstallRequired	If smart uninstall is required because the app doesn't have an uninstall program in the deployment technology, this item is set to **True**. It smart uninstall is not required, this property is set to **False**.
availableActions	Lists the available actions: • **Compliance** • **Uninstall** • **Keep**

Getting a List of Uninstall Alert Questions

This section describes the App Broker REST API endpoint to get a list of the questions that a user is required to answer when responding to an uninstall alert.

Table 12-50 • Getting a List of Uninstall Alert Questions

Endpoint Example	Response Body Example
`[GET] http://localhost/esd/api/` `    alerts/22184/uninstallquestions`	```[` ` {` ` "id": 7,` ` "name": "UninstallQuestion1",` ` "type": "dropDownList",` ` "description": "Please select the reason for uninstalling",` ` "isRequired": true,` ` "isMaskInput": false,` ` "focus": "requestSpecific",` ` "target": "requester",` ` "answers": [` ` {` ` "id": 13,` ` "text": "I do not use this software regularly",` ` "value": "I do not use this software regularly",` ` "isDefault": false` ` },` ` {` ` "id": 16,` ` "text": "Other",` ` "value": "Other",` ` "isDefault": false` ` }` `],` ` "conditionals": [` ` {` ` "questionID": 8,` ` "value": " Other"` ` }` `]` ` },```

Table 12-50 • Getting a List of Uninstall Alert Questions

Endpoint Example	Response Body Example
| | ```json
{
    "id": 8,
    "name": "UninstallQuestion2",
    "type": "multiLine",
    "description": "Please specify the reason",
    "isRequired": true,
    "isMaskInput": false,
    "focus": "requestSpecific",
    "target": "requester",
    "conditionals": [
        {
            "questionID": 7,
            "value": "Other"
        }
    ]
}
]
``` |

Uninstall Alert Question Metadata

This section describes the uninstall alert question metadata that is returned.

Table 12-51 • Uninstall Alert Question Metadata

Item	Description
id	Unique identifier of alert resource.
name	Name of question.
type	User interface format of question, such as **dropDownList** or **multiLine**.
description	Description of question.
isRequired	Specifies (**true** or **false**) whether a response is required.
isMaskInput	Specifies (**true** or **false**) whether content should be masked in the user interface (such as for a password field).
focus	Specifies the bundle format of the question as one of the following: • **RequestSpecific** • **ItemSpecific**

Table 12-51 • Uninstall Alert Question Metadata

Item	Description
target	Specifies the appropriate audience for the question as one of the following: ● **Requester** ● **Approver** ● **Either**
answers	Provides the following information about the response choices: ● **id**—Unique identifier of response choice. ● **text**—Text display of response choice. ● **value**—Value of response choice. ● **isDefault**—Whether response choice should be preselected in user interface (**true**) or not (**false**).
conditionals	Provides the identifier for the question and conditional value: ● **questionID**—Unique identifier of question resource. ● **value**—Selected response choice to require response to conditional question.

Getting a List of Keep Alert Questions

This section describes the App Broker REST API endpoint to get a list of the questions that a user is required to answer when responding to a keep alert.

Table 12-52 • Getting a List of Keep Alert Questions

Endpoint Example	Response Body Example

`[GET] http://localhost/esd/api/`
`   alerts/22184/keepquestions`
	<pre>[
	    {
	        "id": 7,
	        "name": "KeepQuestion1",
	        "type": "dropDownList",
	        "description": "Please select the reason for keeping",
	        "isRequired": true,
	        "isMaskInput": false,
	        "focus": "requestSpecific",
	        "target": "requester",
	        "answers": [
	            {
	                "id": 13,
	                "text": "I use this software regularly",
	                "value": "I use this software regularly",
	                "isDefault": false
	            },
	            {
	                "id": 16,
	                "text": "Other",
	                "value": "Other",
	                "isDefault": false
	            }
	        ],
	        "conditionals": [
	            {
	                "questionID": 8,
	                "value": " Other"
	            }
	        ]
	    },</pre>

Table 12-52 • Getting a List of Keep Alert Questions

Endpoint Example	Response Body Example
| | ```
{
    "id": 8,
    "name": "KeepQuestion2",
    "type": "multiLine",
    "description": "Please specify the reason",
    "isRequired": true,
    "isMaskInput": false,
    "focus": "requestSpecific",
    "target": "requester",
    "conditionals": [
        {
            "questionID": 7,
            "value": "Other"
        }
    ]
}

]
``` |

Keep Alert Question Metadata

This section describes the keep alert question metadata that is returned.

Table 12-53 • Keep Alert Question Metadata

Item	Description
id	Unique identifier of alert resource.
name	Name of question.
type	User interface format of question, such as **dropDownList** or **multiLine**..
description	Description of question.
isRequired	Specifies (**true** or **false**) whether a response is required.
isMaskInput	Specifies (**true** or **false**) whether content should be masked in the user interface (such as for a password field).
focus	Specifies the bundle format of the question as one of the following: • **RequestSpecific** • **ItemSpecific**
target	Specifies the appropriate audience for the question as one of the following: • **Requester** • **Approver** • **Either**
answers	Provides the following information about the response choices: • **id**—Unique identifier of response choice. • **text**—Text display of response choice. • **value**—Value of response choice. • **isDefault**—Whether response choice should be preselected in user interface (**true**) or not (**false**).
conditionals	Provides the identifier for the question and conditional value: • **questionID**—Unique identifier of question resource. • **value**—Selected response choice to require response to conditional question.

Invoking Uninstall Action in Response to an Alert

This section describes the App Broker REST API endpoints to invoke an uninstall action in both a system administrator

context and in a user context.

- System Administrator Context

- User Context

System Administrator Context

This section describes the App Broker REST API endpoint to invoke an uninstall action as a system administrator in response to an alert.

Table 12-54 • Invoking Uninstall Action in Response to an Alert (System Administrator)

Endpoint Example (Input)	Response Body Example (Output)
URI Example `[PUT] http://localhost/esd/api/alerts/22184`	Status code of 200 with empty body.

Request Body Example
 	
<pre>{
    "response":"uninstall","questions":
        [
            {"questionId":5,"answers":
                [
                    {"answer":"I said so."
                    }
                ]
            },
            {"questionId":6,"answers":
                [
                    {"answer":"I said so."
                    }
                ]
            }
        ]
 	
}</pre>	

User Context

This section describes the App Broker REST API endpoint to invoke an uninstall action under a user context in response to an alert.

Table 12-55 • Invoking Uninstall Action in Response to an Alert (User Context)

Endpoint Example (Input)	Response Body Example (Output)

URI Example
 	
`[PUT] http://localhost/esd/api/alerts/`
`   22184?dn=appportal&un=jsmith`
	Status code of 200 with empty body.

Request Body Example
 	
<pre>{
    "response":"uninstall","questions":
        [
            {"questionId":5,"answers":
                [
                    {"answer":"I said so."
                    }
                ]
            },
            {"questionId":6,"answers":
                [
                    {"answer":"I said so."
                    }
                ]
            }
        ]
}</pre>	

Invoking Keep Action in Response to an Alert

This section describes the App Broker REST API endpoints to invoke a keep action in both a system administrator context and in a user context.

- System Administrator Context

- User Context

System Administrator Context

This section describes the App Broker REST API endpoint to invoke a keep action as a system administrator in response to an alert.

Table 12-56 • Invoking Keep Action in Response to an Alert (System Administrator)

Endpoint Example (Input)	Response Body Example (Output)
URI Example `[PUT] http://localhost/esd/api/alerts/22185`	Status code of 200 with empty body.

Request Body Example
 	
<pre>{
    "response":"keep","questions":
        [
            {"questionId":7,"answers":
                [
                    {"answer":"I use this software occasionally."
                    }
                ]
            },
            {"questionId":9,"answers":
                [
                    {"answer":"Weekly"
                    }
                ]
            }
        ]
}</pre>	

User Context

This section describes the App Broker REST API endpoint to invoke a keep action in a user context in response to an alert.

Table 12-57 • Invoking Keep Action in Response to an Alert (User Context)

Endpoint Example (Input)	Response Body Example (Output)
URI Example `[PUT] http://localhost/esd/api/alerts/22185?dn=appportal&un=jsmith`	Status code of 200 with empty body.

Request Body Example
 	
 <pre>{
    "response":"keep","questions":
        [
            {"questionId":7,"answers":
                [
                    {"answer":"I use this software occasionally."
                    }
                ]
            },
            {"questionId":9,"answers":
                [
                    {"answer":"Weekly"
                    }
                ]
            }
        ]
}</pre>	

Invoking Compliance Action in Response to an Alert

This section describes the App Broker REST API endpoint to invoke a compliance action in response to an alert.

Table 12-58 • Invoking Compliance Action in Response to an Alert

Endpoint Example (Input)	Response Body Example (Output)
URI Example `[PUT] http://localhost/esd/api/alerts/22186`	Status code of 200 with empty body.

Request Body Example
 	
 <pre>{
    "response":"compliance"
}</pre>	

Question Metadata Returned from Uninstall and Keep Alerts

This section describes the question metadata that is returned from uninstall and keep alerts.

Table 12-59 • Question Metadata Returned from Uninstall and Keep Alerts

Item	Description
response	Defines the response to the alert as one of the following: • **Keep** • **Uninstall** • **Compliance**
questions	For each question, provides the following information: • **questionId**—Unique identifier of the question. • **answers**—Lists the possible answers to the question.

Error Returned When Using IIS 7.5 on Windows Server 2008 R2 Machine

If you are attempting to call App Broker REST API endpoints on a machine using IIS Version 7.5 (which is shipped with Windows Server 2008 R2), the response returns the following error:

405 - HTTP verb used to access this page is not allowed. The page you are looking for cannot be displayed because an invalid method (HTTP verb) was used to attempt access

To resolve this issue, add the following this section to the ~\App Portal\Web\Web.config file:

```
<system.webServer>
   <modules runAllManagedModulesForAllRequests="true">
      <remove name="WebDAVModule"/>
   </modules>
</system.webServer>
```

Approvals API Endpoints

You can use App Broker's API approvals endpoints to enable you to use your own user interface for approvals, while still utilizing the App Portal / App Broker approval workflow infrastructure.

After requests have been made and require approval, you may use these endpoints to retrieve a list of an approver's pending requests, approve or reject a request, and also assign a request to another approver.

App Broker provides the following API endpoints to enable you to perform approvals using your own user interface:

• Getting a List of an Approver's Pending Requests

• Getting a List of an Approver's Processed Requests

• Approving or Rejecting a Request

- Assigning a Request to Another Approver

Getting a List of an Approver's Pending Requests

This section describes the App Broker REST API endpoint to return a list of pending requests for a given approver.

Table 12-60 • Get a List of an Approver's Pending Requests

Endpoint Example	Response Body Example (Output)

`[GET] http://localhost/esd/api/`
`   users/domain=appportal/`
`   user=jsmith/approvals`
 	
`[GET] http://localhost/esd/api/`
`   users/domain=appportal/`
`   user=jsmith/`
`   approvals?status=pending`
	``[

{
"adGuid": "16cedd2b2c2e8c489d248ff0e7c3f8fa",
"approverName": "John Smith",
"approverUniqueName": "APPPORTAL\\jsmith",
"requests": [
{
"request": {
"requestID": 173,
"orderID": 166,
"packageID": 328,
"packageTitle": "Bhoomi v1.0",
"packageType": 328,
"requestType": "install",
"targetMachine": "ITAAPCCNET01",
"targetUser": "AutomationEndUser1",
"targetDeploymentTechnology": "SCCM2012",
"requestedOn": "2017-02-06T17:41:44"
},
"approvalType": "linear",
"approvers": [
{
"adGuid": "16cedd2b2c2e8c489d248ff0e7c3f8fa",
"approverLevel": 1,
"isCurrentApprover": true,
"action": "pending",
"availableActions": [
"approve",
"reject"
]
}
],
"approvalStatus": "pending"
}
]
}
]```

Getting a List of an Approver's Processed Requests

This section describes the App Broker REST API endpoint to return a list of requests for a given approver that have either been approved or rejected.

Table 12-61 • Get a List of an Approver's Pending Requests

Endpoint Example	Response Body Example (Output)
`[GET] http://localhost/esd/api/` `   users/domain=appportal/` `   user=jsmith/` `   approvals?status=processed`	```[` ` {` ` "adGuid": "16cedd2b2c2e8c489d248ff0e7c3f8fa",` ` "approverName": "John Smith",` ` "approverUniqueName": "APPPORTAL\\jsmith",` ` "requests": [` ` {` ` "request": {` ` "requestID": 175,` ` "orderID": 168,` ` "packageID": 328,` ` "packageTitle": "Bhoomi v1.0",` ` "packageType": 328,` ` "requestType": "install",` ` "targetMachine": "ITAAPCCNET01",` ` "targetUser": "AutomationEndUser1",` ` "targetDeploymentTechnology": "sccM2012",` ` "requestedOn": "2017-02-06T17:41:44"` ` },` ` "approvalType": "linear",` ` "approvers": [` ` {` ` "adGuid": "16cedd2b2c2e8c489d248ff0e7c3f8fa",` ` "approverLevel": 1,` ` "isCurrentApprover": true,` ` "action": "processed",` ` "availableActions": []` ` }` `],` ` "approvalStatus": "processed"` ` }` `]` ` }` `]```

Approving or Rejecting a Request

This section describes the App Broker REST API endpoint for an approver to approve or reject a request. Optionally, the approver post additional information in the request body.

Table 12-62 • Get a List of an Approver's Pending Requests

Endpoint Example	Response Body Example (Output)

URI Example
 	
`[POST] http://localhost/esd/api/requests/27/approve?dn=appportal&un=jsmith`
 	
`[POST] http://localhost/esd/api/requests/27/reject?dn=appportal&un=jsmith`	

Request Body Examples
 	
Providing an explanation for the rejection:
 	
`    {"reason":"my reason"}`
 	
Providing an explanation and recommending a rejection:
 	
`    {"reason":"my reason","recommendReject:true}`
 	
Permitting approver to override approval:
 	
`    {"overrideApprover":true}`	

Assigning a Request to Another Approver

This section describes the App Broker REST API endpoint to assign a request to another approver..

Table 12-63 • Assigning a Request to Another Approver

Endpoint Example	Response Body Example (Output)
URI Example `[POST] http://localhost/esd/api/requests/27/reassign?dn=appportal&un=jsmith`	
Request Body Example `    {"reassignTo":"APPPORTAL\\JaneDoe"}`	

Development Tip: Postman Chrome Add-On

A convenient client tool to use when working with App Portal REST API is a Chrome add-on called Postman. To use Postman, add the following in the URL headers:

`"Content-Type: application/json`

Below is a screen shot of Postman:

Figure 12-1: Postman Chrome Add-On

For more information, see the Postman web site:

https://www.getpostman.com/

Adding or Editing the Standard Conditions for License Reclamation and Retire/Upgrade Campaigns

This section describes the App Broker REST API endpoint to add or edit the standard conditions for license reclamation and retire/upgrade campaigns.

Table 12-64 • Adding or Editing the Standard Conditions

Endpoint Example (Input)	Response Body Example (Output)

URL Example
 	
`[POST] http://ServerName/esd/api/Campaigns?flexeraid=arl://`
`   MGS-APP-00000205221&CampaignType=1`
	`{`
	`    "result": "Conditions updated`
	`    successfully"`
	`}`

Request Body Example

```
[
    {
        "propertyType": "Group",
        "propertyValue": "93910ce85afb9d4e9daace2eb7ff1e97",
        "visible": "True", "applyChildOU": true
    },
    {
        "propertyType": "OU",
        "propertyValue": "74a376f2f096ee43ac71f7f36526f53d",
        "visible": "True", "applyChildOU": true
    },
    {
        "propertyType": "ADproperty", "propertyName": "l",
        "propertyValue": "goa", "visible": "True",
        "operator": "=", "applyChildOU": true,
        "propertyLabel": "City"
    },
    {
        "propertyType": "Collection", "visible": "False",
        "deploymentTechnology": "8",
        "propertyDisplayName": "All Systems"
    }
]
```

> 📄
>
> **Note •** *In the above sample input, the parameter* propertyValue *for AD group and OU is a hexadecimal value of the group/OU, and the parameter* deploymentTechnology *value is 1 for SCCM 2012 and 8 for ConfigMgr.*

Retrieving the Standard Conditions for License Reclamation and Retire/Upgrade Campaigns

This section describes the App Broker REST API endpoint to retrieve the standard conditions for license reclamation and retire/upgrade campaigns.

Table 12-65 • Retrieving the Standard Conditions

Endpoint Example	Response Body Example

`[GET] http://ServerName/esd/api/`
`   Campaigns?flexeraid=arl://MGS-`
`   APP-00000205221&CampaignType=1`
	``[

{
"campaignType": 1,
"flexeraId": "arl://MGS-APP-00000205221",
"propertyType": "OU",
"propertyName": "organizationalUnitUser",
"propertyValue": "74a376f2f096ee43ac71f7f36526f53d",
"visible": "True", "applyChildOU": true,
"propertyDisplayName": "74a376f2f096ee43ac71f7f36526f53d"
},
{
"campaignType": 1,
"flexeraId": "arl://MGS-APP-00000205221",
"propertyType": "Group",
"propertyName": "memberOf",
"propertyValue": "93910ce85afb9d4e9daace2eb7ff1e97",
"visible": "True", "applyChildOU": true,
"propertyDisplayName": "93910ce85afb9d4e9daace2eb7ff1e97"
},
{
"campaignType": 1,
"flexeraId": "arl://MGS-APP-00000205221",
"propertyType": "AD property", "propertyName": "l",
"propertyValue": "goa", "operator": "=", "visible": "True",
"applyChildOU": true, "propertyDisplayName": "goa",
"propertyLabel": "City"
}
]```

13

Troubleshooting

Information on troubleshooting issues with App Portal are included in this section.

- How App Portal Responds to Failure Statuses Received from System Center Configuration Manager

- Known Issues

How App Portal Responds to Failure Statuses Received from System Center Configuration Manager

In System Center Configuration Manager, if the deployment of an application fails, it continues to attempt to install the application. In previous releases, App Portal would not continue to monitor a failed application after the first status report from System Center Configuration Manager. Therefore, on occasion, App Portal would report a failed status even though System Center Configuration Manager eventually reported success.

Changes have been implemented into App Portal 2015 R2 Hotfix v10.0.1 to account for the above issue. In App Portal 2015 R2 Hotfix v10.0.1 and later, there are three unique scenarios where App Portal considers failed statuses from System Center Configuration Manager:

- Scenario #1: Received New Failed Status and Specified Time Threshold Has Passed Since System Center Configuration Manager's Last Evaluation Date/Time

- Scenario #2: Did Not Receive New Status, Current Status is Failed, and "Automatically Fail if Final Status is Not Received" Threshold Has Passed

- Scenario #3: No Status Received, and "Automatically Fail if No Status is Received" Threshold Has Passed

- No Scenarios Met

Scenario #1: Received New Failed Status and Specified Time Threshold Has Passed Since System Center Configuration Manager's Last Evaluation Date/Time

In Scenario #1, App Portal has received a new status from System Center Configuration Manager, it is a failed status, and the specified time limit has passed since System Center Configuration Manager's last evaluation date/time. You specify this time limit in the **Monitor threshold for failed deployments to prevent false flags** field on the **Site Management > Settings > Timers** tab.

To set the **Monitor threshold for failed deployments to prevent false flags** threshold value, perform the following steps.

Task   ***To set the "Monitor threshold for failed deployments to prevent false flags" value:***

1. On the **Admin** tab, open **Site Management**.

2. Open the **Settings > Timers** tab.

3. Set **Monitor threshold for failed deployments to prevent false flags** to the desired hours threshold.

4. Click **Save**.

If this scenario is met, App Portal will do the following:

- Turn off monitoring.

- Invoke external actions (if any).

- Flag to send failure emails (if configured to do so).

Scenario #2: Did Not Receive New Status, Current Status is Failed, and "Automatically Fail if Final Status is Not Received" Threshold Has Passed

In Scenario #2, App Portal has not received any new status from System Center Configuration Manager, the current status is failed, and the **Automatically fail if final status is not received after *n* hours** threshold has passed.

The **Automatically fail if final status is not received after *n* hours** value is set on the catalog item's **Catalog Item Properties** dialog box. If this value is not set (which by default it is not), then App Portal falls back to the global setting of 7 days.

To set the **Automatically fail if final status is not received after *n* hours** threshold value for the catalog item, perform the following steps.

Task   ***To set the "Automatically fail if final status is not received after n hours" value:***

1. On the **Admin** tab, open **Catalog Management**.

2. Open the **Deployment >Global** tab of the **Catalog Item Properties** dialog box for the desired catalog item.

3. Set **Automatically fail if final status is not received after *n* hours** to the desired hours threshold.

4. Click **Save**.

If this scenario is met, App Portal will do the following:

- Turn off monitoring.

- Invoke external actions (if any).

- Flag to send failure emails (if configured to do so).

Scenario #3: No Status Received, and "Automatically Fail if No Status is Received" Threshold Has Passed

In Scenario #3, App Portal has not received any status whatsoever from System Center Configuration Manager, and the **Automatically fail if no status is received after *n* hours** threshold has passed.

The **Automatically fail if no status is received after *n* hours** value is set on the catalog item's **Catalog Item Properties** dialog box. If this value is not set (which by default it is not), then App Portal falls back to the global setting of 7 days.

To set the **Automatically fail if no status is received after *n* hours** threshold value for the catalog item, perform the following steps.

Task   ***To set the "Automatically fail if no status if received after n hours" value:***

1. On the **Admin** tab, open **Catalog Management**.

2. Open the **Deployment >Global** tab of the **Catalog Item Properties** dialog box for the desired catalog item.

3. Set **Automatically fail if no status is received after *n* hours** to the desired hours threshold.

4. Click **Save**.

If this scenario is met, App Portal will do the following:

- Turn off monitoring.

- Invoke external actions (if any).

- Flag to send failure emails (if configured to do so).

No Scenarios Met

If none of the three above failure scenarios are met, then App Portal will continue to monitor System Center Configuration Manager periodically to see if there are any status changes related to the deployment.

Known Issues

This section documents App Portal's known issues.

- App Portal Website Will Not Start After Installation

App Portal Website Will Not Start After Installation

App Portal cannot run on a server that includes the following combination of applications:

- Windows Server 2008 R2 64bit

- Windows Server Update Services (WSUS 3.1)

App Portal cannot run with this combination due to the default setting during the WSUS installation of having compression enabled. This compression runs in 64-bit mode and App Portal runs in 32-bit mode. There are two optional workarounds for this issue.

- Install App Portal on a web server where WSUS is not installed.

- Run the following command on the server where App Portal and WSUS are installed:

  ```
  %windir%\system32\inetsrv\appcmd.exe set config -section:system.webServer/httpCompression /-
  [name='xpress']
  ```

Part 2

Using the App Portal Enterprise App Store

This section of this guide documents how to interact with the App Portal storefront, which is where users can request software for their computer or mobile device, or request an account to use a cloud application.

- Requesting Catalog Items

- Viewing Request Status and Details

- Approving or Rejecting Requests on the Approve/Reject Tab

- Using the My Apps Tab to Manage Your Applications and Software Policy Score™

Note • For information on how administrators can configure catalog items, see Managing Your Catalog.

14

Requesting Catalog Items

You use the App Portal storefront to request software for your desktop or laptop computer (Windows or iOS operating systems) or for your mobile phone (Google Android, iOS, or Windows Phone operating systems). You can even request an account to use a cloud application (such as Salesforce or Office 365).

The App Portal storefront interface is divided into sections to organize the content. The menu items displayed in the top navigation menu depend on the user's rights and configuration settings.

Figure 14-1: App Portal Storefront

You submit requests for catalog items for software or other assets on the **Browse Catalog** tab. All catalog items are listed on the **Browse Catalog** tab, and you can either browse through categories or perform a search to locate the catalog items that you want to request.

After searching the catalog, you can either perform an express checkout of a single item or a standard checkout of multiple items. Users with the required permissions, can request catalog items on behalf of other users. In addition to being able to request software or hardware items, you can also request the deployment of an operating system on either an existing or new computer.

Information about submitting catalog item requests is organized into the following sections:

● Locating Catalog Items

● Requesting General, Software, and Task Sequence Catalog Items

● Requesting Mobile Application Catalog Items

● Requesting Cloud Catalog Items

● Browse Catalog Tab Reference

Locating Catalog Items

You submit requests for software and other assets on the App Portal **Browse Catalog** tab.

On the **Browse Catalog** tab, you can request desktop and mobile applications, as well as OS deployments and cloud applications. Users with the required permissions, can request catalog items on behalf of other users. You can browse through categories or perform a search to locate catalog items. You can view catalog items in card, list, or detailed view.

Figure 14-2: Browse Catalog Tab

Information browsing for catalog items on the **Browse Catalog** tab is described in the following sections:

- Locating Catalog Items Using the Menus

- Searching for Catalog Items

- Viewing Catalog Items in the Results Pane

- Sorting Catalog Items

Locating Catalog Items Using the Menus

You can use the menus on the **Browse Catalog** tab to locate the catalog items that you want to request.

- Browse Categories Menu

- Filter By Device Menu

- Results Pane

*Note • If a user does not have a registered mobile device, that user will not see any mobile displayed on the **Browse Catalog** tab. Also, if a user has only iOS mobile registered, Android-only mobile applications will not be visible on the **Browse Catalog** tab for that user, and vice versa.*

Browse Categories Menu

You can use the **Browse Categories** menu in the left pane to browse to the category that contains the catalog item you want to request. In this list, if the category name is listed in bold, it indicates that it contains subcategories.

Click on the category to display its subcategories.

To locate an item by browsing categories, select a category (or subcategory) in the **Browse Categories** menu. All of the items that you have access to in that category will be displayed in the Results Pane.

Figure 14-3: Displaying the Contents of the Selected Subcategory in the Results Pane

Filter By Device Menu

If your App Portal catalog contains both desktop and mobile application catalog items, and you have a mobile device registered with App Portal, you can use the **Filter By Device** menu to toggle the display to view desktop items, mobile items or both.

Results Pane

The right pane either lists all of the catalog items in the selected category (or the search results).

Figure 14-4: Search Results in the Results Pane

Catalog items, which can be listed in either card or list format, include icons that provide additional information about each software item. For more information, see Viewing Catalog Items in the Results Pane and Icons Displayed on the Browse Catalog Tab and on Checkout Screens.

Searching for Catalog Items

Instead of browsing through the catalog categories until you locate the item you are interested in, you can use the **Search** box to search for catalog items in the catalog.

Figure 14-5: App Portal Search Box

To search for catalog items, perform the following steps:

Task *To locate items in the catalog:*

1. Open the **Browse Catalog** tab.

2. Enter a search term in the **Search Catalog** box and then press Enter.

App Portal then performs either an exact match or a token match:

Exact Match to Catalog Item Name

App Portal starts by doing a *exact* match on the catalog item name. If an exact match is found, App Portal returns the matching catalog item immediately and does not perform any further searches. For example, if you entered **Adobe Photoshop CS5 v12.0.3** in the **Search Catalog** box, and there is a catalog item named exactly that, then that catalog item will be immediately returned in the search results.

*Important • In order for an exact match to be made, the text you enter in the **Search Catalog** box must exactly match the content of the **Title** field on the **General > Title and Description** subtab of the catalog item's Catalog Item Properties dialog box.*

Token Match

If an exact match is *not* found, then App Portal splits the search string into multiple strings, using the space character as a delimiter. For example, the search term `Microsoft Office` would be split into two strings `Microsoft` and `Office`. Then, using the split tokens, App Portal searches the following attributes in the listed order:

1. **Keyword**—App Portal searches the keyword for *any* split search tokens for an *exact* match (such as **Keyword** = `Microsoft` *or* **Keyword** = `Office`) and adds any matching catalog items to the search results.

2. **Catalog Item Title**—App Portal searches the catalog item **Title** field for *all* split search tokens for a "contains" match (such as if the **Title** contains both `Microsoft` *and* `Office`) and adds any matching catalog items to the search results.

3. **Brief Description**—App Portal searches the catalog item **Brief Description** for *all* split search tokens for a "contains" match (such as if the **Brief Description** contains both `Microsoft` *and* `Office`) and adds any matching catalog items to the search results.

4. **Full Description**—Searches the catalog item **Full Description** for *all* split search tokens for a "contains" match (such as if the **Full Description** contains both `Microsoft` *and* `Office`) and adds any matching catalog item to the search results.

App Portal then combines the results from all of the queries above and displays the search results.

Search Results

The search results are displayed in the Results pane:

Figure 14-6: Search Results in the Results Pane

Viewing Catalog Items in the Results Pane

The Results Pane either lists all of the catalog items in the selected category or the search results. Catalog items can be displayed in either *card* or *list* view. Additional catalog item information can be viewed on the *detail* view.

- Card View

- List View

- Detail View

- Sorting Catalog Items

Card View

When in *card* view, catalog items are displayed in three or more columns; the number of columns that are displayed depends upon the width of the browser window.

Figure 14-7: Card View

For each catalog item, a product icon is displayed along with the product title, star rating, informational icons, an **Add to Cart** button and, possibly, an **Install Now** button.

- **Add to Cart**—Click **Add to Cart** to add a catalog item to the cart. You can add multiple catalog items at once.

- **Install Now**—Click **Install Now** to bypass the checkout process and request immediate installation. For some catalog items, the **Install Now** button is not available.

For more information about the **Add to Cart** and **Install Now** buttons, see Checkout Methods: Standard and Express Checkout.

List View

To view the catalog items in a *list* view, click on the list icon above the columns of items.

Figure 14-8: Buttons to Toggle Between Card and List View

When viewing catalog items in list view, catalog items are displayed in one column.

Figure 14-9: List View

In addition to the product icon, product title, star rating, informational icons, and **Add to Cart** / **Install Now** buttons, the list view also includes a description of the catalog item, if one exists. You can click the arrow button next to the word **Description** to toggle between viewing and hiding the description.

As in the card view, you click **Add to Cart** to add a catalog item or multiple catalog items to the cart, or you can click **Install Now** to bypass the checkout experience when requesting a single catalog item.

Detail View

You can view additional information about a catalog item—such as its full description and all of its ratings and reviews—by clicking on the catalog item name in either the *card* or *list* view to open the *detail* view.

Figure 14-10: Detail View

Sorting Catalog Items

If you are viewing a large number of catalog items in the results pane, you may wish to sort the catalog items. To sort a list of catalog items, use the **Sort by** list.

Figure 14-11: Sort By List

The following types of sorts can be performed using the **Sort by** list:

Table 14-1 • Sort Types

Sort Type	Description
Title: a-z	Alphabetical order from A to Z
Title: z-a	Alphabetical order from Z to A
Newest first	Catalog items added to the catalog most recently will be listed first.
Rating	Catalog items with the highest user rating will be listed first.
Price: Low to high	Most expensive catalog items will be listed first.
Price: High to low	Least expensive catalog items will be listed first.
Approval required first	Catalog items requiring administrator approval will be listed first.
Approval not required first	Catalog items that do not require administrator approval will be listed first.

Requesting General, Software, and Task Sequence Catalog Items

After you locate the catalog item(s) that you want to request (as described in Locating Catalog Items), you need to either perform a standard or express checkout.

- **Standard checkout**—Click the **Add to Cart** button on one or multiple catalog items to add them to the cart, and then click **View cart and checkout** to begin the standard checkout experience.

- **Express checkout**—Click the **Install Now** button on a single catalog item to bypass the standard checkout experience.

Information about submitting a request for catalog items is presented in the following sections:

- Checkout Methods: Standard and Express Checkout

- Requesting a Single Catalog Item Using Express Checkout

- Requesting Catalog Items Using Standard Checkout

- Icons Displayed on the Browse Catalog Tab and on Checkout Screens

Note • The procedure for requesting a mobile application catalog item is not the same as the procedure for requesting other catalog items. See Requesting Mobile Application Catalog Items.

Note • For information on requesting cloud applications, see Requesting Cloud Catalog Items.

Checkout Methods: Standard and Express Checkout

When requesting a catalog item, you can either click the **Add to Cart** button to proceed with the standard checkout process (as described in Requesting Catalog Items Using Standard Checkout) or you can bypass the checkout process on some catalog items by clicking the **Install Now** button.

Figure 14-12: Install Now Button on Browse Catalog Tab

When you click the **Install Now** button, a catalog item request is automatically generated for that single catalog item, bypassing the checkout experience altogether. In the event that you have more than one associated device, a pop-up window will prompt you to select the desired target system.

Figure 14-13: Choose Target Dialog Box

If the catalog item has a standard approval workflow associated with it, and you click **Install Now**, a message will be displayed stating that installation will begin once the request has been approved.

Express checkout is enabled by the App Portal administrator at a global level by selecting the **Enable express checkout** option on the **Catalog Behavior** tab of the **Site Management > Settings > Web Site** view, as described in Enabling Express Checkout: Install Now Button.

However, even when express checkout is enabled, not all catalog items will display an **Install Now** button. Also, in some instances, you cannot use express checkout even when the **Install Now** button is displayed.

- Conditions Preventing Display of Install Now Button

● Conditions That Prevent Use of Express Checkout

Conditions Preventing Display of Install Now Button

If any of the following conditions are met, the **Install Now** button will not be displayed even when the **Enable express checkout option** is selected.

Table 14-2 • Conditions Preventing Display of Install Now Button

Condition	Description
Question templates	If the catalog item has an associated question template, the **Install Now** button is not displayed.
Custom approvers	If the catalog item has an approval workflow associated with it that prompts the requester to select a custom approver, the **Install Now** button is not displayed. *Note • If the catalog item has a standard approval workflow associated with it, the Install Now button will be displayed. When the requester clicks Install Now, a message will be displayed stating that installation will begin once the request has been approved.*
Constraints, Leasing, or Allow switch to? settings	If the catalog item has **Constraints, Leasing**, or **Allow switch to?** settings defined, the **Install Now** button is not displayed.
Task sequence catalog items	For task sequence catalog items, the **Install Now** button is not displayed.
Cloud catalog items	For cloud catalog items—such as Box, Office 365 or Salesforce—the **Install Now** button is not displayed.
General catalog items	For **General** catalog items, the **Install Now** button is not displayed.
Group catalog items	For **Group** catalog items, the **Install Now** button is not displayed.
File upload	If a catalog item has the **Allow File Upload?** option selected on the **General > Global** tab of the **Catalog Item Properties** dialog box, which enables a user to upload a file during checkout, the **Install Now** button is not displayed.

Conditions That Prevent Use of Express Checkout

Even if the **Install Now** button is displayed, you cannot perform express checkout in the following scenarios:

● **Multiple catalog item request**—You can only use the **Install Now** button to request one catalog item at a time. If you want to request more than one catalog item in the same request, you are required to add all catalog items to the cart and proceed through the regular checkout process.

● **Request on behalf**—If you are requesting a catalog item on behalf of another user, you cannot use the **Install Now** button to submit the request. You instead are required to add the catalog item to the cart and proceed through the regular checkout process.

Requesting a Single Catalog Item Using Express Checkout

As described in Checkout Methods: Standard and Express Checkout, catalog items have either an **Add to Cart** button or an **Add to Cart** button *and* an **Install Now** button.

You can request one catalog item at a time using the **Install Now** button, bypassing the standard multi-page check out process.

If you only want to request one catalog item, and none of the conditions listed in Conditions That Prevent Use of Express Checkout exist, you can request a catalog item using express checkout.

Task   ***To request a catalog item using express checkout:***

1. Search for and locate the catalog item you want to request, as described in Searching for Catalog Items.

2. On the catalog item that you want to request, click **Install Now**.

3. In the event that you have more than one associated device, a pop-up window will prompt you to select the desired target system.

4. Select the desired target device and click **Install**.

    - **No approval required**—If no approval is required, the installation process will be launched.

    - **Approval required**—If the catalog item has a standard approval workflow associated with it, a message will be displayed stating that installation will begin once the request has been approved.

Requesting Catalog Items Using Standard Checkout

As described in Checkout Methods: Standard and Express Checkout, catalog items have either an **Add to Cart** button or an **Add to Cart** button *and* an **Install Now** button. You can request one catalog item at a time using the **Install Now** button, bypassing the standard multi-page check out process.

If express checkout is not available, due to the reasons listed in Conditions Preventing Display of Install Now Button, or if you cannot use express checkout due to the reasons described in Conditions That Prevent Use of Express Checkout, you need to use standard checkout to request catalog items.

The following topics explains how to request catalog items using standard checkout.

- Adding Catalog Items to Your Shopping Cart

- Checking Out

Adding Catalog Items to Your Shopping Cart

Note • The procedure for requesting mobile application catalog items varies slightly from the procedure for desktop catalog items. For information on requesting mobile application catalog items, see Requesting Mobile Application Catalog Items.

After you have located the catalog item that you would like to request, your next step is to add that catalog item to your shopping cart and check out.

Each time you add an item to the cart, the count (a large yellow number to the right of the cart icon) is increased.

Figure 14-14: Cart Count

When you are ready to check out, click on the cart icon. The **Cart Summary** pop-up opens and prompts you to checkout.

Figure 14-15: Cart Summary Pop-Up

Review the items in the cart, remove any items that you don't want to request by clicking on the **X** next to the item, and then click **View cart and checkout**. After you click **View cart and checkout**, checkout proceeds as described in Checking Out.

To add a catalog item to your shopping cart, perform the following steps:

Task   ***To add a catalog item to your shopping cart:***

1. Follow the instructions in Searching for Catalog Items to locate the catalog item you want to request.

2. Once you locate the item, begin the checkout process by clicking the **Add to Cart** button in the catalog item card. When an item is added to the shopping cart, the cart count will increase.

Important • *An OSD task sequence catalog item cannot be added to the cart unless the cart is empty. When you click the* **Add to Cart** *button on an OSD task sequence catalog item, the Checkout Wizard will automatically open.*

3. Add additional items to the cart, if desired.

4. Note the following about adding catalog items to your shopping cart:

   •   **Creating an order**—If you add more than one catalog item to the cart and then check out, those items are treated as one order and are tracked as one unit.

   •   **Bundled catalog items**—Catalog items can be configured to be selected as a bundle of separate applications. This is called a *group catalog item*.

If you add a group catalog item to your cart, all of the applications in that group are added to the cart. However, if the **Allow removal from bundle?** option is selected for a catalog item on its **Catalog Item Properties** dialog box, you can choose to remove that catalog item from the bundle before adding it to your cart by clearing the checkbox.

- **Maximum number of items in the shopping cart**—You can add items to the cart up to the administrator-defined cart limit (which is defined in the **Maximum items for shopping cart** field on the **Security** tab of the **Site Management > Settings** view).

5. If desired, you can remove items from your shopping cart, as described in Removing Items from the Cart.

6. Proceed with the steps in Checking Out.

Checking Out

After your items are added to the cart, the next step is to check out and submit your request. The number of panels that will be displayed during a software or general catalog item checkout depends upon the options specified on the catalog item.

Note • This section describes all of the possible Checkout Wizard panels a requester could encounter when checking out a catalog item. For instructions specific to checking out a task sequence catalog item, see Requesting an OSD Task Sequence Catalog Item.

- Overview of the Checkout Wizard

- Launching Checkout

- Choosing a Target or Target Option

- Searching for Targets

- Entering a Target Device / User

- Choosing an Approval Workflow

- Choosing Scheduling Options

- Responding to Questions

- Uploading Files

- Selecting a New Computer to Import for an OS Deployment

- Choosing Roles to Specify Groups of Applications to Migrate During an OS Deployment

- Choosing Existing Applications to Migrate During an OS Deployment

- Choosing Additional Applications to Install During an OS Deployment

- Submitting a Request

Note • For detailed information on all possible Checkout Wizard panels that could be displayed during standard checkout, see Checkout Wizard.

Overview of the Checkout Wizard

The panels of the App Portal Checkout Wizard list the catalog items in a table, with summary information at the top of the screen.

Figure 14-16: Choose Target Panel of Checkout

Information on the checkout screens is organized into the following areas:

- **Summary box**—This box includes the total number of catalog items in the cart, along with the total price of all items.

- **Action area**—Below the checkout page name, instructions and actions that apply to all items in the cart are listed. For example, on the **Choose Target** panel of the checkout, if the user has more than one registered computer, they are prompted to select the machine onto which to install all of the software in the cart.

- **"Your Items" column**—The **Your items** column of the table lists the items in the cart, including informational icons to indicate license status. To remove an item from the cart, click the **X** in the top right corner of the cell.

- **"Action" column**—The **Action** column prompts the user to take some action regarding that catalog item, such as to make a selection or answer a question, or provides instructions or information specific to that catalog item.

- **Next button**—Click to proceed to the next panel in the Checkout Wizard.

Launching Checkout

To begin the checkout process, perform the following steps.

Task   ***To specify the target of the request:***

1.   Perform the steps in Adding Catalog Items to Your Shopping Cart.

2.   Click the **Cart** icon.

The Cart Summary pop-up dialog box opens, listing the items in the cart.

3.   Click **View cart and checkout**. For most requesters, the **Choose Target** view of the Checkout Wizard opens.

Note • When a requester is requesting a catalog item for themselves, the **Choose Target** panel is not displayed (and the checkout is automatically advanced to the next panel) if:

- The requester has only one registered device.
- The catalog item only allows for install (instead of both install and uninstall).

The number of panels that will be displayed during checkout depends upon the options specified on the catalog item and the type of catalog item you are requesting (general, software, task sequence, cloud). Proceed with the following steps, depending upon which panels are displayed:

Panel	Procedure
Choose Target	See Choosing a Target or Target Option.
Respond to Questionnaire Panel	See Responding to Questions.
Choose Target /Users for Request On Behalf Panel	See Searching for Targets.
Enter Target /Users Panel	See Entering a Target Device / User.
Choose Approval Workflow Panel	See Choosing an Approval Workflow.
Choose Scheduling Options Panel	See Choosing Scheduling Options.
Upload Files Panel	See Uploading Files.
Import New Computer Panel	See Selecting a New Computer to Import for an OS Deployment.
Choose Roles Panel	See Choosing Roles to Specify Groups of Applications to Migrate During an OS Deployment.

Panel	Procedure
Choose Existing Applications Panel	See Choosing Existing Applications to Migrate During an OS Deployment.
Choose Additional Applications Panel	See Choosing Additional Applications to Install During an OS Deployment,
Submit Request Panel	See Submitting a Request.

Choosing a Target or Target Option

On the **Choose Target** panel of the Checkout Wizard, you will need to specify who this item is being requested for. You can either submit a request for yourself or on behalf of another user (if you have the required security permission).

📄

*Note • When a requester is requesting a catalog item for themselves, the **Choose Target** panel is not displayed (and the checkout is automatically advanced to the next panel) if:*

● *The requester has only one registered device.*

● *The catalog item only allows for install (instead of both install and uninstall).*

Task   ***To choose a target option:***

1.   Perform the steps in Launching Checkout. The **Choose Target** panel of the Checkout Wizard opens.

The number of options that are listed on the **Choose Target** panel vary depending upon the catalog item's selected properties (especially the "request on behalf options"), the requester's security permissions, and whether or not the requester has direct reports.

***Important • The Choose Target** panel is only displayed if the user has the ability to request to a device other than their current one, or if the item allows for both install and uninstall. In the absence of these choices, the **Me on machine DEVICENAME** and **Install** options are selected by default and the checkout is automatically advanced to the next panel.*

2. On the **Choose Target** panel, select one of the following options:

Requester	Choose Target Option	Purpose of Selecting	Next Step
Request for self	**Me on machine DEVICENAME**	Select this option to request that the catalog item be installed on your current device.	Depends upon other catalog item properties.
	Myself	Select this option to request that this general catalog item be manually delivered to your current device or assigned to the current user.	Depends upon other catalog item properties.
	DEVICENAME	Select a device name to request that the catalog item be installed on that device. For **General** catalog items, the item will be manually delivered to that device. *Note • All of the requester's assigned are listed.*	Depends upon other catalog item properties.
	Reimage my computer (DEVICENAME) with a new Operating System	Select this option to request that the operating system be installed on your current device. *Note • This option is listed for OSD task sequence catalog items only.*	Depends upon other catalog item properties.
	Build an unknown computer and migrate my data from MACHINENAME to the new computer	Select if you want to instruct App Portal to build an unknown computer and migrate data from my current computer. *Note • This option is listed for OSD task sequence catalog items only.*	Depends upon other catalog item properties.

Requester	Choose Target Option	Purpose of Selecting	Next Step
Request on behalf of another user	**People who report to me**	Select this option to be prompted to choose the device of one of your direct reports as the target of this request.	Proceed with the steps in Selecting a Target from a List of Direct Reports.
	Search for people or computers	Select this option to specify that you want this catalog item to be installed on a device that you will select by performing a search of users or computers.	Proceed with the steps in Selecting a Target from a List of Users / Computers.
	Search using account attributes	Select to be able to search a list of users by Active Directory property value to locate the target device(s) / user(s) of the request. *Note • The properties that are available for searching are specified on the **Site Management > Active Directory > Property Mapping** view.*	Proceed with the steps in Selecting a Target Using Account Attributes.
	Add machine names or user IDs manually	Select if you want to manually add a list of machine names or user IDs to identify the target device(s) / user(s) of the request.	Proceed with the steps in Entering a Target Device / User.
	Image a new computer or existing computer	Select if you want to identify a new computer as the target. The new computer can either be imported or selected from a list (if already registered with your selected deployment technology). *Note • This option is listed for OSD task sequence catalog items only.*	Proceed with the steps in Selecting a New Computer to Import for an OS Deployment.

*Important • If App Portal is pointing to a different instance of System Center Configuration Manager than the System Center Configuration Manager client on the requester's computer, then the following error message will be displayed on the **Choose Target** panel:* `Cannot select because this machine is not a recognized client.`

Note • For more information on specifying the target location of catalog items, see the Choose Target Panel topic.

3. Click **Next** and proceed with checkout.

Responding to Questions

If a question template is associated with one or more of the catalog items in the cart, the **Respond to Questionnaire** panel is displayed, prompting the user to answer questions. Questions are listed either at the top section or in the table below:

- **Questions in the top section**—These questions apply to all catalog items in the request. When one of these questions is defined, its **Focus** property is set to **Request Specific**.

- **Questions in the table**—These questions apply to the individual catalog item in the row in which it appears. When one of these questions is defined, its **Focus** property is set to **Item Specific**.

Note • For more information, see Managing Questions and Question Templates.

Figure 14-17: Respond to Questionnaire Panel

To respond to questions associated with a catalog item, perform the following steps.

Task   **To answer questions on the Respond to Questionnaire panel:**

1. If questions are associated with one of the catalog items in your cart, the **Respond to Questionnaire** panel will open during checkout.

If the questions are associated with all of the catalog items in your cart, the questions will be listed at the top of the screen. If the questions pertain to a specific catalog item, the questions will be listed in the table below next to the catalog item.

2. Provide responses to the listed questions and click **Next**.

Note • You must answer questions marked as Required in order to proceed with checkout.

Searching for Targets

When the **Search for people or computers**, **Search using account attributes**, or **People who report to me** option is selected on the **Choose Target** panel, the next step in the checkout process will be to search and specify the targets of the request.

● Selecting a Target from a List of Users / Computers

● Selecting a Target Using Account Attributes

● Selecting a Target from a List of Direct Reports

Selecting a Target from a List of Users / Computers

To select a target by searching a list of users / computers, perform the following steps.

Task   ***To select a target from a list of users/computers:***

1. On the **Choose Target** panel of the Checkout Wizard, select **Search for people or computers**, as described in Choosing a Target or Target Option, and click **Next**. The Choose Target /Users for Request On Behalf Panel panel opens.

2. Search for targets using the **Filter By** fields: **User Name**, **Full Name** or **Machine Name**.

3. Once the record is located, select the checkbox and select the **Add Selected Records** button at the bottom of the top grid.

Note • When each item is selected, it goes through several checks to validate the selection against the items being requested. If there is a problem with adding one of the selections, a warning icon is displayed. Hover over the icon to display the message. Not all warnings prevent the device from being added.

4. After selecting the targets, click **Next** to continue.

Selecting a Target Using Account Attributes

To select a target device by searching a list of users by Active Directory property value, perform the following steps.

Note • *The properties that are available for searching are specified on the **Site Management > Active Directory > Property Mapping** view*

Task   ***To search for a target device using account attributes:***

1. On the **Choose Target** panel of the Checkout Wizard, select **Search using account attributes**, as described in Choosing a Target or Target Option, and click **Next**. The Choose Target /Users for Request On Behalf Panel panel opens.

2. Use the **Select a property** and **Select a value** lists to specify an Active Directory property/value.

3. Click **Search**. Users/ that match the selected property/value pair are listed.

4.   Use the **Filter By** fields to further refine the list.

5.   Once the record is located, select the checkbox and select the **Add Selected Records** button at the bottom of the top grid.

Note • When each item is selected, it goes through several checks to validate the selection against the items being requested. If there is a problem with adding one of the selections, a warning icon is displayed. Hover over the icon to display the message. Not all warnings prevent the device from being added.

6.   After selecting the targets, click **Next** to continue.

Selecting a Target from a List of Direct Reports

To select a target device by searching a list of your direct reports, perform the following steps.

Task   ***To search for a target from a list of direct reports:***

1.   On the **Choose Target** panel of the Checkout Wizard, select **People who report to me**, as described in Choosing a Target or Target Option, and click **Next**. The Choose Target /Users for Request On Behalf Panel panel opens, listing only those users who report to you.

---

*Note • The **People who report to me** option on the **Choose Target** panel is only displayed if the **Enable request to AD manager?** option is selected for the catalog item, and the requester has direct reports defined in the user data source (such as in Active Directory).*

2. Search for targets using the **Filter By** fields: **User Name**, **Full Name** or **Machine Name**.

3. Once the record is located, select the checkbox and select the **Add Selected Records** button at the bottom of the top grid.

Note • *When each item is selected, it goes through several checks to validate the selection against the items being requested. If there is a problem with adding one of the selections, a warning icon is displayed. Hover over the icon to display the message. Not all warnings prevent the device from being added.*

4. After selecting the targets, click **Next** to continue.

Entering a Target Device / User

If you select **Add machine names or user IDs manually** option on the **Choose Target** panel of the Checkout Wizard, the **Enter Target /Users** panel opens, where you are prompted to manually add a list of machine names or user IDs to identify the target.

Note • *The **Add machine names or user IDs manually** option is listed on the **Choose Target** panel if the **Enable request to manual list?** option is selected for one of the catalog items in the cart and the requester has been assigned the **Request on Behalf** permission.*

Task   ***To specify a target by entering a device or user name:***

1. Perform the steps in Launching Checkout. The **Choose Target** panel of the Checkout Wizard opens.

2. Select **Add machine names or user IDs manually** and click **Next**. The Enter Target /Users Panel panel opens.

3. Enter a target device or user in the box at the top of the panel, and then click **Add** to add it to the **Selected** table.

*Important • On the **Enter Target /Users** panel, to enter a user as a target, enter just the user name in the box, without the domain name. For example, enter* jsmith, *not* MYDOMAIN/jsmith.

When you enter a target device or user in the box and click **Add**, that device (with all associated users) or that user (with all associated) are listed in the table below.

- **Removing an item from the list**—You may select more than one target device or user name. To remove an item from the **Selected** list, click the **Remove** button.

- **Switching to a different user of the same device**—If you enter a device or user name, a device along with an associated user is added to the **Selected** list. If you want to select that device but with a different assigned user, click the user icon in the **Action** column. A user name selection dialog box opens.

Select a different user from the list and then click **Switch User**.

4. Click **Next** to continue.

Choosing an Approval Workflow

In the event that a catalog item requires approval and you are requesting it on behalf of another user, the **Choose Approval Workflow** panel of the checkout procedure is displayed.

To approve a request on behalf of another user, perform the following steps:

Task   ***To approve a request on behalf of another user:***

1. Perform the steps in Checking Out. The **Approval** panel opens.

2. Select one of the following options:

- **User targets approval process**—Use the approval process of the target user of the request.

- **Use my approval process**—Use the approval process of the requester.

> 📄
>
> ___
>
> **Note •** *If you select this option and if enabled, the requester can select their own approver on the* **Approve / Reject**
> *tab. See* Approving or Rejecting Requests on the Approve/Reject Tab *for more information.*

3. Click **Next** and continue with checkout.

Choosing Scheduling Options

If the **Enable user defined scheduling?** option is selected on the **General > Global** tab of the Catalog Item Properties
dialog box for that catalog item, the **Choose Scheduling Options** panel is displayed during checkout, which prompts the
requester to choose when the request should be fulfilled. The options displayed to the requester depend upon whether the
catalog item requires approval.

📋

___

Task   ***To choose scheduling options:***

1. Perform the steps in Checking Out to checkout a catalog item that has user defined scheduling options enabled. The
    Choose Scheduling Options Panel opens.

2. The options that are displayed on the **Choose Scheduling Options** panel depend upon the options selected for that catalog item in the **Scheduling options** section of the Catalog Item Properties dialog box and also whether or not that catalog item requires approval. Select one of the following options:

Approval?	Option	Description
No approval required	**Receive at a Specific Time**	Select this option to enable the requester to select the date and time when they would like the catalog item delivered.
	Receive ASAP	Select this option to request that App Portal deliver the catalog item automatically as soon as possible after the catalog item is requested.
Approval required	**Notify machine owner when approved**	Select this option to request that App Portal notify the machine owner when the request has been approved.
	Deliver automatically after approval	Select this option to request that App Portal deliver the catalog item automatically after approval.

3. If leasing options are selected on the **Deployment > Leasing** subtab of the Catalog Item Properties dialog box for a catalog item in the cart, you are prompted to select an **Install Method** in the **Action** table at the bottom of the **Choose Scheduling Options** panel:

Select one of the following options:

- **Permanent Installation**—Select this option if this catalog item will be permanently installed.

- **Leased Installation**—Select this option if this catalog item will be leased, and also select a date when the software will be uninstalled.

4. Click **Next** to continue.

Uploading Files

If the **Allow File Upload** option is selected on the **General > Global** of the **Catalog Item Properties** dialog box for a catalog item, you may be prompted to upload a file on the **Upload Files** panel.

Task   ***To upload a file:***

1. Perform the steps in Checking Out. The **Upload Files** panel of the Checkout Wizard opens.

2. To upload a file, click **Select files**. A dialog box opens prompting you to select a file.

3. Select the files to upload and click OK. The uploaded files are now listed at the top of the panel.

4. Click **Next** to proceed with checkout.

Selecting a New Computer to Import for an OS Deployment

If, when checking out an OSD task sequence catalog item, you select **Image a new computer or existing computer** on the **Choose Target** panel, the **Import New Computer** panel opens.

📄

*Note • The **Image a new computer or existing computer** option is displayed on the **Choose Target** panel for OSD task sequence catalog items if the **Enable request on behalf?** option is selected for that catalog item and if the requester has the **Request on Behalf** role.*

📋

Task   **To select a computer to import:**

1. Add an OSD task sequence catalog item to the cart, as described in Adding Catalog Items to Your Shopping Cart. The **Choose Target** panel of the Checkout Wizard opens.

2. On the **Choose Target** panel, select **Image a new computer or existing computer** and click **Next**. The **Import New Computer** panel of the Checkout Wizard opens.

3.   In the **New computer name** field, enter the name of the computer that you want to image, or select a computer from the list.

> 📄
>
> **Note •** *If a computer has already been configured with your deployment technology, it will be available for selection from the list. If you want create a new computer object in your deployment technology (which enables App Portal to support bare-metal installations), enter a name for the new computer in the* **New computer name** *field, and you will then be prompted to enter additional information.*

4.   If you entered a name in the **New computer name** field (instead of making a selection from the list), you will be prompted to enter the following information to configure the new computer with your deployment technology:

Field	Description
Time Zone	Select the time zone for the specified deployment technology site.
SCCM Site	Select the deployment technology site where you want to create a new computer object.
MAC Address	Enter the MAC address of the computer you are importing. 📄 **Note •** *Either the MAC address or SMBIOS GUID must be entered.*
SMBIOS GUID	Enter the SMBIOS GUID of the computer you are importing. 📄 **Note •** *Either the MAC address or SMBIOS GUID must be entered.*

5.   If you are replacing an existing computer and wish to create a computer association between the existing computer and the new computer—so that you can transfer user data and applications to the new computer, enter the name of the existing computer in the **Old computer name** field or select the old computer from the list.

6.   Under **Build Type**, select one of the following options:

- **New Computer (No data migration)**—Select this option to perform a "bare-metal" installation, with no corporate operating system present on the computer and with no user data or applications to capture or restore.

- **In-Place Migration (Backup and restore data)**—Select this option to perform an in-place upgrade of an existing corporate operating system, and with user data and applications that need to be captured and restored to the existing system.

- **Side-by-Side Migration (Migrate data from old computer to new computer)**—Select this option to perform a side-by-side transfer of an existing corporate operating system from one computer to another, with user data and applications that need to be captured from the existing system and restored to the replacement system.

> 💡
>
> **Tip •** *If you want to perform an in-place migration, instead of selecting the* **Image a new computer or existing computer** *option on the* **Choose Target** *panel and then selecting the* **In-Place Migration** *option on this panel, you could have instead selected the* **Reimage my computer DEVICENAME with a new Operating System** *option on the* **Choose Target** *panel.*

7.   If you want to associate the specified computer to a user (which enables role evaluation and email communication), enter the following user information:

- **Domain**

- **User ID**

- **Full Name**

- **Email Address**

📄

*Note • As soon as you specify the **Domain** and **User ID** of an existing user, App Portal will return the **Full Name** and **Email Address** of that user.*

8.   Click **Import Computer** to import the specified computer.

When you click **Import Computer**, the specified computer is listed in the **Action** column of the table, and displays the **Machine Name** along with the **Full Name** and **User Name** of the associated computer user (if it exists).

Your Items	Action				
Windows 10 2017 ✕	**Machine Name**	**Full Name**	**User Name**		
	Old Machine: ENT-W7X64 New Machine: ENDUSER-W7	Admin Flexera	FLEX\AD	👤	Remove

Note the following regarding items in this list:

- **Removing an item from the list**—To remove a computer from the list, click the **Remove** button.

- **Switching to a different user of the same device**—If no user is assigned to the computer or if you want to select a different assigned user, click the user icon in the **Action** column. A user name selection dialog box opens.

User Name:

Type Target UserID or Name ▾

Switch User   Cancel

Select a different user from the list and then click **Switch User**.

9. Click **Next** to continue.

Choosing Roles to Specify Groups of Applications to Migrate During an OS Deployment

The **Choose Roles** panel opens when you are checking out an OSD task sequence catalog item that has a role selected on the **Deployment > Roles** subtab of the Catalog Item Properties dialog box.

Roles are a grouping of applications, computer variables, and/or Microsoft User State Migration Tool (USMT) profiles that App Portal can use to determine which applications to install on the target operating system.

- If the **Allow user role selection** option is also selected on the **Deployment > Roles** subtab, then the requester is able to select a role.

- If the **Allow user role selection** option is not selected, the roles will be listed, but they will automatically be selected and the requester will be unable to clear the selection.

Task   *To choose roles to specify groups of applications to migrate during an OS deployment:*

1. Perform the steps in Checking Out to check out an OSD task sequence catalog item. The **Choose Roles** panel of the Checkout Wizard opens.

2. On the **Choose Roles** panel, select the roles that contain applications that you want to have installed on the target operating system (or just review the automatically selected roles), and then click **Next** to continue.

Choosing Existing Applications to Migrate During an OS Deployment

You can choose to display the **Choose Existing Applications to Migrate** panel during the checkout of OSD task sequence catalog items. This panel lists the applications that are deployed on the source machine's current operating system, as determined by either the FlexNet Manager Suite or App Portal inventory function.

The **Choose Existing Applications to Migrate** panel only appears if the **Enable application migration and installation of additional applications** option is selected on the **Site Management > Settings > Deployment > OS Deployment** tab.

Figure 14-18: OS Deployment Settings Related to Application Migration

If the **Enable requester to specify which existing applications to migrate** option is also selected here, then the requester has the option of selecting or deselecting applications. If this option is not selected, all existing applications are automatically selected and cannot be unselected.

Note • *To prevent a catalog item from being listed on the **Choose Existing Applications to Migrate** panel (because, for example, it is a core application that is automatically included with your corporate OS image), select the **Core application** option on the **General > Global** tab of that catalog item's Catalog Item Properties dialog box.*

Task   *To choose individual applications to migrate during an OS deployment:*

1.   Perform the steps in Checking Out to check out an OSD task sequence catalog item. The **Choose Existing Applications to Migrate** panel of the Checkout Wizard opens.

2.   Select the applications that you want to have installed on the target operating system and then click **Next**.

Note • *If the **Enable requester to specify which existing applications to migrate** option is not selected on the **Site Management > Settings > Deployment > OS Deployment** tab, all existing applications are automatically selected and cannot be unselected.*

Note • *Because these applications are selected during checkout, they are written to the computer object within System Center Configuration Manager as variables so that they can be used by the Task Sequence process.*

Choosing Additional Applications to Install During an OS Deployment

The **Choose Additional Applications to Install During an OS Deployment** panel appears during the checkout of OSD task sequence catalog items, and lists software catalog items that are available for installation on the target operating system.

The **Choose Additional Applications to Install During an OS Deployment** panel appears during an OSD task sequence catalog item checkout if the **Enable application migration and installation of additional applications** and **Prompt requester to select additional applications to install** options are is selected on the **Site Management > Settings > Deployment > OS Deployment** panel.

*Note • To prevent a catalog item from being listed on the **Choose Additional Applications to Install During an OS Deployment** panel (because, for example, it is a core application that is automatically included with your corporate OS image), select the **Core application** option on the **General > Global** tab of that catalog item's Catalog Item Properties dialog box.*

To choose additional applications to install during an OS deployment, perform the following steps.

Task   ***To choose additional applications to install during an OS deployment:***

1. Perform the steps in Checking Out to check out an OSD task sequence catalog item. The **Choose Additional Applications to Install During an OS Deployment** panel of the Checkout Wizard opens.

2. Select the applications you want to install during OS deployment, and then click **Add Applications** to add them to the selected list below.

*Important • This grid lists the first 100 applications in the App Portal catalog. To locate an application that is not listed, use the **Search** box.*

3. Click **Next** to continue.

Note • Because these applications are selected during checkout, they are written to the computer object within System Center Configuration Manager as variables so that they can be used by the Task Sequence process.

Submitting a Request

After all required information has been submitted, the **Submit Request** panel opens, listing a summary of this request. If a catalog item requires approval, a description of the approval process for that catalog item is listed in the table.

To complete the submission of a request, perform the following steps.

Task **To complete the submission of a request:**

1. Proceed through the Checkout Wizard, as described in Checking Out, until the **Submit Request** panel is displayed, with a summary of the catalog items that will be requested, along with the target machine and user names. If approval is required for a catalog item, a summary of the approval process will be listed in the **Action** column of the table.

2. Click **Submit**. The request is processed, and the **Request Complete** panel opens, displaying an order number.

3. You can then either click **View Status** to view this request on the **My Requests** tab, or click **Continue Shopping** to create another request.

Note • *For information on viewing the details, status, and progress of a request, see Viewing Request Details and Viewing Request Status and Details.*

Removing Items from the Cart

To remove catalog items from the cart, perform the following steps:

Task   **To remove an item from the cart:**

1.   Click the **Cart** icon.

The Cart Summary pop-up dialog box opens.

2.   Then click either **Empty Cart** (to remove all items from the cart) or click the **X** next to the item you want to remove.

Icons Displayed on the Browse Catalog Tab and on Checkout Screens

Icons are displayed next to catalog items on the **Browse Catalog** tab to provide more information about that catalog item's approval status and license availability. The following icons are displayed on the **Browse Catalog** tab:

Table 14-3 • Icons Displayed on the Browse Catalog Tab

Icon	Name	Browse Catalog Tab?	Checkout Screens?	Purpose
	Requires Approval	Yes	No	Catalog item has an associated approval template, which means that it must be approved prior to deployment.
	License Required	Yes	Yes	Catalog item requires a license.

Table 14-3 • Icons Displayed on the Browse Catalog Tab

Icon	Name	Browse Catalog Tab?	Checkout Screens?	Purpose
	Mobile Application	Yes	Yes	Catalog item is a mobile application. *Note • Displayed in top left corner for mobile application catalog items.* *Note • If you do not have a mobile device that is registered with App Portal, you will not see any mobile applications displayed on the **Browse Catalog** tab. Also, if you have only iOS mobile registered, Android-only mobile applications will not be visible on the **Browse Catalog** tab, and vice versa.*
	Install Time	No	Yes	Indicates the amount of time it will take to install this catalog item.
	Installed	Yes	No	Catalog item is already installed on your machine.
	Alternate Catalog Item	Yes	No	An alternate catalog item exists for this catalog item. *Note • Sometimes when a user selects a catalog item and goes to check it out, they are prevented from doing so for various reasons, such as if their machine is not found, their machine is not on the network, or the version that they want is not in the catalog. If administrators have associated an alternate catalog item for this item, the user will be able to request this alternate item.*
	License Source: FlexNet Manager Suite	No	Yes	Source of this catalog item's license is FlexNet Manager Suite.
	License Available (n)	No	Yes	A license is available for this catalog item.
	License Not Available	No	Yes	No licenses are available for this catalog item.

Table 14-3 • Icons Displayed on the Browse Catalog Tab

Icon	Name	Browse Catalog Tab?	Checkout Screens?	Purpose
⟳	**Requires Reboot**	No	Yes	Indicates the installation of this catalog item requires that the machine be rebooted.
★★★★☆ ☆☆☆☆☆	**Star rating**	Yes	No	These stars indicate the rating (1 to 5 stars in half star increments) that other users have given to this application after it has been installed on their machine.
				If all stars are gray, either application rating is disabled or no users have rated the application.

Note • A different set of informational icons are used on the **My Requests** *tab. For more information, see* Viewing Status, Info, and Actions Icons on the My Requests Tab.

Requesting Mobile Application Catalog Items

You can choose to request a mobile application catalog item by itself by clicking the **Install Now** button on the **Browse Catalog** tab. In this case, the mobile application's checkout procedure will open in pop-up; you will not be required to open the cart.

You can link a mobile application catalog item with its associated desktop catalog item so that when one of the linked applications is requested, the user will be informed that the other linked catalog item is also available. Then you can request both the desktop application and its associated mobile application in the same request. App Portal will deploy the desktop application using System Center Configuration Manager or Symantec Altiris, while it will use AirWatch to deploy the mobile application. In this case, the checkout procedure of the two catalog item types will be combined.

- Requesting a Mobile Application on the Browse Catalog Tab

- Requesting a Mobile Application Using the App Portal Mobile Interface

- Requesting a Desktop Catalog Item That is Linked to a Mobile Catalog Item

Requesting a Mobile Application on the Browse Catalog Tab

There are several scenarios for that you could experience when requesting a mobile application on the **Browse Catalog** tab.

- Mobile Application / No Approval Required / Not Linked to Desktop Item

- Mobile Application / Approval Required / Not Linked to Desktop Item

- Mobile Application / Linked to Desktop Item

Mobile Application / No Approval Required / Not Linked to Desktop Item

If a you click **Install Now** on a mobile application that is not linked to a desktop application, and which does not require approval, a dialog box opens prompting you to select the desired mobile device for deployment. When you click **Install**, the mobile application will be deployed via AirWatch.

Figure 14-19: Requesting a Non-Linked Mobile Application / No Approval

Mobile Application / Approval Required / Not Linked to Desktop Item

If you click **Install Now** on a mobile application that is not linked to a desktop catalog item but which does require approval, a similar dialog box opens, and prompts you for a response to a question. When you click **Install**, the request will be submitted for approval and, when approved, will be deployed by AirWatch.

Mobile Application / Linked to Desktop Item

If you click **Install Now** on a mobile application that is linked to a desktop catalog item, you will be informed that a desktop catalog item exists, and you are prompted to indicate whether you would also like to request the linked desktop catalog item.

Figure 14-20: Prompt to Add Linked Desktop Item to Cart

If you click **Yes**, both items are added to the cart.

Figure 14-21: Both Desktop and Mobile Catalog Item In Cart

If you click **No**, the request will proceed as described in the previous scenarios.

Requesting a Mobile Application Using the App Portal Mobile Interface

Important • Single sign-on authentication is not supported when using the App Portal mobile interface.

You can also request mobile applications from a mobile device using the App Portal mobile user interface.

Figure 14-22: App Portal Mobile Interface Login Screen

The same user experience is available in the App Portal mobile application as there is in the desktop version. However, instead of a checkout process, there is just an **Install** button, similar to most mobile app stores.

You can use the **Browse Categories** list to locate catalog items, or use the search box.

Figure 14-23: Browsing in the App Portal Mobile User Interface

After locating the desired mobile application, click the **Install** button to send the request to App Portal. If no approval is required, the mobile application will be installed. If approval is required, deployment will begin when approval is received.

Figure 14-24: Mobile Application Catalog Items in Mobile UI

Requesting a Desktop Catalog Item That is Linked to a Mobile Catalog Item

If you add a desktop catalog item that is linked to a mobile catalog item to the cart, when you opens the cart, the linked mobile application catalog item will be displayed in the **Actions** table, and you will be prompted to specify whether or not you want to also request the mobile app. If you select the mobile device, the mobile application will be requested.

Figure 14-25: Both Desktop and Mobile Catalog Item In Cart

If you select to also request the mobile application, both catalog items will be included on the same request, but two different request IDs will be created.

Requesting Cloud Catalog Items

If App Portal is integrated with a cloud application (such as Box, Office 365, or Salesforce), you can request a cloud application account in the App Portal storefront on the **Browse Catalog** tab by checking out a cloud catalog item.

When you check out a cloud catalog item, an account in that cloud application will automatically be created for you, and you will then receive an email from the cloud application vendor that includes account login details.

Task   ***To check out a cloud catalog item:***

1.   Locate a cloud catalog item on the **Browse Catalog** tab as described in Searching for Catalog Items.

2.   On the cloud catalog item, click **Add to Cart**. The cloud catalog item is added to the cart.

3. Click the **Cart** icon.

The **Cart Summary** pop-up dialog box opens, listing the items in the cart.

4. Click **View cart and checkout**. The **Choose Target** panel of the Checkout Wizard opens.

5. Select the **Myself** option to request that this cloud catalog item is assigned to you, and click **Next**. The **Submit Request** panel opens.

6. Click **Submit** to complete this request. The **Request Complete** panel opens.

7. Follow the instructions in the email that you will receive from the cloud application vendor to login to the cloud application.

Browse Catalog Tab Reference

This section contains information on the views and wizards that are accessible from the **Browse Catalog** tab, the App Portal storefront.

- Catalog Item View

- Checkout Wizard

Catalog Item View

On the **Browse Catalog** tab, you can request desktop and mobile applications, as well as OS deployments and cloud applications. All catalog items are listed on the **Browse Catalog** tab, and you can either browse through categories or perform a search to locate the catalog items that you want to request.

After searching the catalog, you can either perform an express checkout of a single item or a standard checkout of multiple items.

Figure 14-26: Browse Catalog Tab

The following sections provide information about browsing for and checking out catalog items on the **Browse Catalog** tab:

- Browse Categories and Filter By Device Menus

- Search Box and Results Pane

- Catalog Item Card Views

- Icons Used on Catalog Item Cards

Browse Categories and Filter By Device Menus

You can use the **Browse Categories** menu in the left pane to browse to the category that contains the catalog item you want to request. In this list, if the category name is listed in bold, it indicates that it contains subcategories.

Figure 14-27: Browse Categories Menu

Click on the category to display its subcategories.

Figure 14-28: Browse Categories Menu Expanded

To locate an item by browsing categories, select a category (or subcategory) in the **Browse Categories** menu. All of the items that you have access to in that category will be displayed in the Results Pane.

If your App Portal catalog contains both desktop and mobile application catalog items, and you have a mobile device registered with App Portal, you can use the **Filter By Device** menu to toggle the display to view desktop items, mobile items or both.

Figure 14-29: Filter By Device Menu

For more information, see Locating Catalog Items Using the Menus.

Search Box and Results Pane

Instead of browsing through the catalog categories until you locate the item you are interested in, you can use the **Search** box to search for catalog items in the catalog.

Figure 14-30: App Portal Search Box

For more information, see Searching for Catalog Items.

Catalog Item Card Views

The Results Pane either lists all of the catalog items in the selected category or the search results. Catalog items can be displayed in either *card* or *list* view. Additional catalog item information can be viewed on the *detail* view.

For more information, see Viewing Catalog Items in the Results Pane

Icons Used on Catalog Item Cards

Icons are displayed next to catalog items on the **Browse Catalog** tab to provide more information about that catalog item's approval status and license availability. For a list of all icons used on catalog item cards, see Icons Displayed on the Browse Catalog Tab and on Checkout Screens.

Checkout Wizard

If you are performing a standard checkout, after you add catalog items to the cart, you check out using the Checkout Wizard and submit your request. The panels that will be displayed during catalog item checkout depends upon the options specified on the catalog items in the cart. This section describes all possible panels of the Checkout Wizard.

- Choose Target Panel

- Choose Target /Users for Request On Behalf Panel

- Choose Target Users for Request On Behalf Panel

- Enter Target /Users Panel

- Import New Computer Panel

- Choose Roles Panel

- Choose Existing Applications to Migrate Panel

- Choose Additional Applications to Install During OS Deployment Panel

- Respond to Questionnaire Panel

- Upload Files Panel

- Choose Approval Workflow Panel

- Choose Scheduling Options Panel

- Submit Request Panel

- Request Complete Panel

Choose Target Panel

On the **Choose Target** panel of the **Checkout** wizard, the user is prompted to specify the target location for the selected catalog items.

Figure 14-31: Choose Target Panel / Checkout Wizard

The number of options that are listed on the **Choose Target** panel vary depending upon both catalog item properties and the user's security permissions.

- **Options set on the catalog item**—The number of options selected in the **Request options** section of the **General > Global** tab of the **Catalog Item Properties** dialog box for the catalog item impact how many options are listed on the **Choose Target** panel.

- **User's Admin and/or Catalog Security permissions**—The visibility of some of the options on the **Choose Target** panel also depends upon the requester's assigned **Admin Security** and **Catalog Security** permissions, especially the **Request on Behalf** permission.

- **Whether user has direct reports**—The **People who report to me** option on the **Choose Target** panel is only displayed if the **Enable request to AD manager?** option is selected for the catalog item, and the requester has direct reports defined in the user data source (such as in Active Directory).

For more information, see Determining the Options Listed on Choose Target Panel.

The following table lists all of the target options that could be listed on the **Choose Target** panel.

Table 14-4 • Choose Target Panel / Checkout Wizard

Choose Target Option	When Displayed	Purpose of Selecting	Next Checkout Panel
Me on machine DEVICENAME	Displayed for **Software** catalog items.	Select this option to request that the catalog item be installed on your current device.	Depends upon other catalog item properties.
Myself	Displayed for General and Cloud catalog items.	Select this option to request that this general catalog item be manually delivered to your current device or assigned to the current user.	Depends upon other catalog item properties.
DEVICENAME *Note • Lists all of the assigned to the requester.*	Displayed for **Software**, **Task Sequence**, and **General** catalog items.	Select a device name to request that the catalog item be installed on that device. For **General** catalog items, the item will be manually delivered to that device.	Depends upon other catalog item properties.
Reimage my computer (DEVICENAME) with a new Operating System	Displayed for OSD **Task Sequence** catalog items.	Select this option to request that the operating system be installed on your current device.	Depends upon other catalog item properties.
Build an unknown computer and migrate my data from MACHINENAME to the new computer	Displayed for OSD **Task Sequence** catalog items if the **Enable unknown computer deployment (OSD Only)** option is selected.	Select if you want to instruct App Portal to build an unknown computer and migrate data from my current computer.	Depends upon other catalog item properties.
People who report to me	Displayed for **Software**, **Cloud**, and **Task Sequence** catalog items when the following conditions are true: - The **Enable request to AD manager?** option must be selected for at least one of the catalog items in the cart. - The requester must have direct reports defined in the user data source (such as in Active Directory).	When you select this option, the of your direct reports are listed, and you are prompted to select target(s) from the list.	When you click **Next**. the Choose Target /Users for Request On Behalf Panel opens.

Table 14-4 • Choose Target Panel / Checkout Wizard

Choose Target Option	When Displayed	Purpose of Selecting	Next Checkout Panel
Search for people or computers	Displayed for **Software** or **Cloud** catalog items when the following conditions are true: ● The **Enable request on behalf?** option must be selected for one of the catalog items in the cart. ● The requester must have the **Request on Behalf** role.	Select this option to specify that you want this catalog item to be installed on a device that you will select by performing a search of users or computers.	When you click **Next**, the Choose Target /Users for Request On Behalf Panel opens, where the requester can search a list of users by machine name, full name, or user name to locate the target device(s) / user(s) of the request.
Image a new computer or existing computer	Displayed for OSD **Task Sequence** catalog items if the following conditions are met: ● The **Enable request on behalf?** option must be selected. ● The requester must have the **Request on Behalf** role. 📄 *Note •* *Requester may also need permission in System Center Configuration Manager to create a new computer.*	Select if you want to select a computer to import and the build type: new computer, in-place migration, or side-by-side migration.	When you click **Next**, the Import New Computer Panel opens.
Search using account attributes	Displayed for **Software**, **Cloud**, and **Task Sequence** catalog items when the following conditions are true: ● The **Enable request to AD property?** option must be selected for one of the catalog items in the cart. ● The requester must have **Request on Behalf** permission.	Select to be able to search a list of users by Active Directory property value to locate the target device(s) / user(s) of the request. The properties that are available for searching are specified on the **Site Management > Active Directory > Property Mapping** view.	When you click **Next**, the Choose Target /Users for Request On Behalf Panel opens.

Table 14-4 • Choose Target Panel / Checkout Wizard

Choose Target Option	When Displayed	Purpose of Selecting	Next Checkout Panel
Add machine names or user IDs manually	Displayed for **General**, **Software**, **Cloud**, or **Task Sequence** catalog items if the following conditions are met: • The **Enable request to manual list?** option must be selected for at least one of the catalog items in the cart. • The requester must have **Request on Behalf** permission.	Select if you want to manually add a list of machine names or user IDs to identify the target device(s) / user(s) of the request.	When you click **Next**, the Enter Target /Users Panel opens.

Determining the Options Listed on Choose Target Panel

Some of the options that are listed on the **Choose Target** panel depend upon which options are selected in the **Request options** section of the **General > Global** tab of the **Catalog Item Properties** dialog box for that catalog item.

Figure 14-32: Request Options on General > Global Tab of Catalog Item Properties Dialog Box

Important • *Even if one of the "request on behalf" options is selected for a catalog item, it will only be displayed during checkout for those requesters who have been assigned the* **Request on Behalf** *permission under Catalog Security.*

The following table lists the option that will be displayed on the **Choose Target** panel for each of the request options selected on the **Catalog Item Properties** dialog box.

Table 14-5 • Catalog Item Request Options

Request Option Selected	Option Displayed on Choose Target Panel
Enable request on behalf? Select to enable the requester to request catalog items for another person or device. Requester can search by machine name, full name, or user name to locate the target device(s) / user(s) of the request.	Search for people or computers If this option is selected, the Choose Target /Users for Request On Behalf Panel panel opens. *Note • Only displayed for requesters that have been assigned the **Request on Behalf** role.*
Enable request to AD property? Select to enable the requester to search by Active Directory account attributes to locate the target device(s) / user(s) of the request.	Search using account attributes If this option is selected, the Choose Target /Users for Request On Behalf Panel panel opens. *Note • Only displayed for requesters that have been assigned the **Request on Behalf** role.*
Enable request to AD manager? Select to prompt the requester to select target(s) from a list of his/her direct reports.	People who report to me If this option is selected, the Choose Target /Users for Request On Behalf Panel panel opens. *Note • Only displayed for requesters who have direct reports defined in the user data source (such as in Active Directory).*
Enable request to manual list? Select to enable the requester to manually add a list of machine names or user IDs to identify the target.	Add machine names or user IDs manually If this option is selected, the Enter Target /Users Panel panel opens. *Note • Only displayed for requesters that have been assigned the **Request on Behalf** role.*
Enable unknown computer deployment (OSD Only)?	**Build an unknown computer and migrate my data from MACHINENAME to the new computer** If this option is selected, App Portal will instruct SCCM to build an unknown computer and migrate the requester's data from their current machine to the new computer.

Important • *If App Portal is pointing to a different instance of System Center Configuration Manager than the System Center Configuration Manager client on the requester's computer, then the following error message will be displayed on the* **Choose Target** *panel:* `Cannot select because this machine is not a recognized client.`

Choose Target /Users for Request On Behalf Panel

On the **Choose Target /Users for Request On Behalf Panel** panel of the Checkout Wizard, the user is prompted to search for and specify the targets of the request.

Figure 14-33: Choose Target /Users for Request on Behalf Panel / Checkout Wizard

The **Choose Target /Users for Request On Behalf** panel is displayed when a requester who has the **Request on Behalf** role selects the **Search for people or computers** or **Search using account attributes** option on the **Choose Target** panel. It is also displayed when a requester who has direct reports defined in the data source (such as Active Directory) selects the **People who report to me** option on the **Choose Target** panel.

The following table explains when these three options are displayed on the **Choose Target** panel:

Table 14-6 • Choose Target Panel "Request on Behalf" Option Requirements

"Request on Behalf" Option on Choose Target Panel	Conditions Required to Be Met
Search for people or computers	The **Enable request on behalf?** option must be selected for one of the catalog items in the cart.
Search using account attributes	The **Enable request to AD property?** option must be selected for one of the catalog items in the cart.
People who report to me	The **Enable request to AD manager?** option must be selected for one of the catalog items in the cart. Also, the requester must have direct reports defined in the data source (such as Active Directory).

The **Choose Target /Users for Request on Behalf** panel is divided into two grids.

● The top grid is used to search and locate targets.

● The bottom grid contains the selected targets.

Search for targets using the **Filter By** fields: **User Name**, **Full Name** or **Machine Name**.

When searching using account attributes, you are prompted to select a property and a value to generate the list of possible target /users.

Once the record is located, select the checkbox and select the **Add Selected Records** button at the bottom of the top grid.

After you have selected all targets, click **Next** to continue.

Choose Target Users for Request On Behalf Panel

On the **Choose Target Users for Request On Behalf Panel** panel of the Checkout Wizard, the user is prompted to search for and specify the target users of the **General** catalog item request.

Figure 14-34: Choose Target Users for Request on Behalf Panel / Checkout Wizard

The **Choose Target Users for Request On Behalf** panel is displayed when requesting a **General** catalog item on behalf of another user. Examples of this scenario include requesting a **General** catalog item when a requester who has the **Request on Behalf** role selects the **Search for people or computers** or **Search using account attributes** option on the **Choose Target** panel, and it is also displayed when a requester who has direct reports defined in the data source (such as Active Directory) selects the **People who report to me** option on the **Choose Target** panel. For requests of Software catalog items the Choose Target /Users for Request On Behalf Panel appears, or for requests that contain a General catalog item and a Software catalog item with Request on Behalf enabled on both, the selection panel that appears first is the Choose Target /Users for Request On Behalf Panel.

The following table explains when these three options are displayed on the **Choose Target** panel:

Table 14-7 • Choose Target Panel "Request on Behalf" Option Requirements

"Request on Behalf" Option on Choose Target Panel	Conditions Required to Be Met
Search for people or computers	The **Enable request on behalf?** option must be selected for one of the catalog items in the cart.
Search using account attributes	The **Enable request to AD property?** option must be selected for one of the catalog items in the cart.

Table 14-7 • Choose Target Panel "Request on Behalf" Option Requirements

"Request on Behalf" Option on Choose Target Panel	Conditions Required to Be Met
People who report to me	The **Enable request to AD manager?** option must be selected for one of the catalog items in the cart.
	Also, the requester must have direct reports defined in the data source (such as Active Directory).

The **Choose Target Users for Request on Behalf** panel is divided into two grids.

- The top grid is used to search and locate target users.

- The bottom grid contains the selected target users.

Search for targets using the **Filter By** field: **User Name**. When searching using account attributes, you are prompted to select a property and a value to generate the list of possible target /users. Enter a value and click **Search** to generate the list of possible target users.

Once the record is located, select the checkbox and select the **Add Selected Records** button at the bottom of the top grid.

After you have selected all targets, click **Next** to continue.

Enter Target /Users Panel

On the **Enter Target /Users** panel of the Checkout Wizard, which is displayed when you select **Add machine names or user IDs manually** option on the **Choose Target** panel and click **Next**, you are prompted to manually add a list of machine names or user IDs to identify the target.

> *Note • The **Add machine names or user IDs manually** option is listed on the **Choose Target** panel if the **Enable request to manual list?** option is selected for one of the catalog items in the cart and the requester has been assigned the **Request on Behalf** permission.*

Figure 14-35: Enter Target /Users Panel / Checkout Wizard

Enter a target device or user in the box at the top of the panel, and then click **Add** to add it to the **Selected** table.

*Important • On the **Enter Target /Users** panel, to enter a user as a target, enter just the user name in the box, without the domain name. For example, enter `jsmith`, not `MYDOMAIN/jsmith`.*

When you enter a target device or user in the box and click **Add**, that device (with all associated users) or that user (with all associated) are listed in the table below.

- **Removing an item from the list**—You may select more than one target device or user name. To remove an item from the **Selected** list, click the **Remove** button.

- **Switching to a different user of the same device**—If you enter a device or user name, a device along with an associated user is added to the **Selected** list. If you want to select that device but with a different assigned user, click the user icon in the **Action** column. A user name selection dialog box opens.

Select a different user from the list and then click **Switch User**.

Import New Computer Panel

If you select **Image a new computer or existing computer** on the **Choose Target** panel when checking out a Task Sequence catalog item, the **Import New Computer** screen opens. On this panel, you are prompted to select the computer to import and the build type: new computer, in-place migration, or side-by-side migration.

*Note • The **Image a new computer or existing computer** option is displayed on the **Choose Target** panel for **Task Sequence** catalog items if the **Enable request on behalf?** option is selected for that catalog item and if the requester has the **Request on Behalf** role.*

Figure 14-36: Import New Computer Panel / Checkout Wizard

Use the following fields to specify the computer to image:

Table 14-8 • Import New Computer Panel Properties

Property	Description
New computer name	Enter the name of the computer that you want to image, or select it from the list.
Old computer name	If you are replacing an existing computer and wish to create a computer association between the existing computer and the new computer, enter the name of the existing computer or select it from the list.
	A computer association creates a relationship between a source and destination computer for the side-by-side migration of user state data. The source computer contains the user state data and settings that will be migrated to the specified destination computer.

Table 14-8 • Import New Computer Panel Properties

Property	Description
Build Type	Select one of the following options to confirm the build type that should occur: • **New Computer (No data migration)**—This is a "bare-metal" installation, with no corporate operating system present on the computer and with no user data to capture or restore. • **In-Place Migration (Backup and restore data)**—This is an in-place upgrade of an existing corporate operating system, and with user data that needs to be captured and restored to the existing system. • **Side-by-Side Migration (Migrate data from old computer to new computer)**—This is a side-by-side transfer of an existing corporate operating system from one computer to another, with user data that needs to be captured from the existing system and restored to the replacement system. *Tip • If you want to perform an in-place migration, instead of selecting the **Image a new computer or existing computer** option on the **Choose Target** panel and then selecting the **In-Place Migration** option on this panel, you could have instead selected the **Reimage my computer DEVICENAME with a new Operating System** option on the **Choose Target** panel.*
User	If you want to associate the specified computer to a user, enter the user associated with this new computer. Associating a user allows for role evaluation and email communication. Enter the following information: • **Domain** • **User ID** • **Full Name** • **Email Address**
Import Computer	Click to import the specified computer.

When you click **Import Computer**, the specified computer is listed in the **Action** column of the table, and displays the **Machine Name** along with the **Full Name** and **User Name** of the associated computer user (if it exists).

- **Removing an item from the list**—To remove a computer from the list, click the **Remove** button.

- **Switching to a different user of the same device**—If no user is assigned to the computer or if you want to select a different assigned user, click the user icon in the **Action** column. A user name selection dialog box opens.

Select a different user from the list and then click **Switch User**.

Choose Roles Panel

The **Choose Roles** panel opens when you are checking out a task sequence catalog item that has a role selected on the **Deployment > Roles** subtab of the **Catalog Item Properties** dialog box.

● If the **Allow user role selection** option is also selected on the **Deployment > Roles** subtab, then the requester is able to select a role.

● If the **Allow user role selection** option is not selected, the roles will be listed, but they will automatically be selected and the requester will be unable to clear the selection.

Roles are a grouping of applications, computer variables, and/or Microsoft User State Migration Tool (USMT) profiles that App Portal can use to determine which applications to install on the target operating system.

Figure 14-37: Choose Roles Panel / Checkout Wizard

On the **Choose Roles** panel, select the roles that contain applications that you want to have installed on the target operating system (or just review the automatically selected roles), and then click **Next**.

Choose Existing Applications to Migrate Panel

On the **Choose Existing Applications to Migrate** panel, you can select the applications that you want to have installed on the target operating system.

The **Choose Existing Applications to Migrate** panel appears during an OSD task sequence catalog item checkout if the **Enable application migration and installation of additional applications** option is selected on the **Site Management > Settings > Deployment > OS Deployment** tab.

Important • If the Enable requester to specify which existing applications to migrate option is also selected on the Site Management > Settings > Deployment > OS Deployment tab, then the requester will be able to specify which of the existing applications to migrate. If this option is not selected, all applications are automatically selected and cannot be unselected.

The **Choose Existing Applications to Migrate** panel lists the applications that are deployed on the current machine, as determined by either FlexNet Manager Suite or the App Portal inventory function.

Note • If using the FlexNet Manager Suite inventory method, only catalog items with associated Flexera IDs will be listed on the Choose Existing Applications to Migrate panel.

Because these applications are selected during checkout, they are written to the computer object within System Center Configuration Manager as variables so that they can be used by the Task Sequence process.

Figure 14-38: Choose Existing Applications to Migrate Panel / Checkout Wizard

Select the applications that you want to migrate to the new operating system and click **Next** to continue.

Choose Additional Applications to Install During OS Deployment Panel

The **Choose Additional Applications to Install During an OS Deployment** panel appears during the checkout of OSD task sequence catalog items, and lists software catalog items that are available for installation on the target operating system.

The **Choose Additional Applications to Install During an OS Deployment** panel appears during an OSD task sequence catalog item checkout if the **Enable application migration and installation of additional applications** and **Prompt requester to select additional applications to install** options are selected on the **Site Management > Settings > Deployment > OS Deployment** panel.

> *Note • To prevent a catalog item from being listed on the **Choose Additional Applications to Install During an OS Deployment** panel (because, for example, it is a core application that is automatically included with your corporate OS image), select the **Core application** option on the **General > Global** tab of that catalog item's Catalog Item Properties dialog box.*

Figure 14-39: Choose Additional Applications to Install During OS Deployment Panel / Checkout Wizard

Select the applications you want to install during OS deployment, and then click **Add Applications** to add them to the selected list below.

Important • *This grid lists the first 100 applications in the App Portal catalog. To locate an application that is not listed, use the* ***Search*** *box.*

Click **Next** to continue.

Note • *Because these applications are selected during checkout, they are written to the computer object within System Center Configuration Manager as variables so that they can be used by the Task Sequence process.*

Respond to Questionnaire Panel

If a question template is associated with one or more of the catalog items in the cart, the **Respond to Questionnaire** panel is displayed, prompting the user to answer questions. Questions at the top apply to entire request, while questions in the table below apply to individual catalog items.

Figure 14-40: Respond to Questionnaire Panel / Checkout Wizard

Answer the listed questions and click **Next**.

Upload Files Panel

If the **Allow File Upload** option is selected on the **General > Global** of the **Catalog Item Properties** dialog box for a catalog item, you may be prompted to upload a file on the **Upload Files** panel of the Checkout Wizard.

Figure 14-41: Upload Files Panel / Checkout Wizard

To upload a file, click **Select files**. A dialog box opens prompting you to select a file. After you select the files to upload and click OK, the uploaded files are listed at the top of the panel.

Click **Next** to proceed with checkout.

Choose Approval Workflow Panel

In the event that a catalog item requires approval and you are requesting it on behalf of another user, the **Choose Approval Workflow** panel of the checkout procedure is displayed.

Figure 14-42: Choose Approval Workflow Panel / Checkout Wizard

Select one of the following options:

- **User targets approval process**—Use the approval process of the target user of the request.

- **Use my approval process**—Use the approval process of the requester.

Note • If you select this option and if enabled, the requester can select their own approver on the **Approve / Reject** *tab. See Approving or Rejecting Requests on the Approve/Reject Tab for more information.*

After making a selection, click **Next** and continue with checkout.

Choose Scheduling Options Panel

If the **Enable user defined scheduling?** option is selected on the **General > Global** tab of the Catalog Item Properties dialog box for that catalog item, the **Choose Scheduling Options** panel is displayed during checkout, which prompts the requester to choose when the request should be fulfilled..

Figure 14-43: Choose Scheduling Options Panel / Checkout Wizard

The options that are displayed on the **Choose Scheduling Options** panel depend upon the options selected for that catalog item on the Catalog Item Properties dialog box and also whether or not the catalog item requires approval. The following scheduling options are available.

Table 14-9 • Available Scheduling Options

Option	Requires approval?	Required Catalog Item Properties	Description
Receive at a Specific Time	No	Enable user defined scheduling?	Select this option to enable the requester to select the date and time when they would like the catalog item delivered.
Receive ASAP	No	Enable user defined scheduling? Allow ASAP scheduling?	Select this option to request that App Portal deliver the catalog item automatically as soon as possible after the catalog item is requested.
Notify machine owner when approved	Yes	Enable user defined scheduling	Select this option to request that App Portal notify the machine owner when the request has been approved.
Deliver automatically after approval	Yes	Enable user defined scheduling Allow scheduling immediately after approval?	Select this option to request that App Portal deliver the catalog item automatically after approval.

Install Method

If leasing options are selected on the **Deployment > Leasing** subtab of the Catalog Item Properties dialog box for a catalog item in the cart, you are prompted to select the Install Method in the Action table at the bottom of the **Choose Scheduling Options** panel:

Figure 14-44: Install Method Options on the Choose Scheduling Options panel

Select one of the following options:

- **Permanent Installation**—Select this option if this catalog item will be permanently installed.

- **Leased Installation**—Select this option if this catalog item will be leased, and also select a date when the software will be uninstalled.

Submit Request Panel

After all required information has been submitted, the **Submit Request** panel opens, listing a summary of this request. If a catalog item requires approval, a description of the approval process for that catalog item is listed in the table.

The Submit Request panel displays a summary of the catalog items that are being requested, along with the target machine and user names. If approval is required for a catalog item, a summary of the approval process will be listed in the **Action** column of the table.

To submit the request, click **Submit**. The request is processed, and the Request Complete Panel opens.

Figure 14-45: Submit Request Panel / Checkout Wizard

Request Complete Panel

After you click **Submit** on the **Submit Reques**t panel of the Checkout Wizard, the request is processed, and the **Request Complete** panel opens, displaying an order number.

Figure 14-46: Request Complete Panel / Checkout Wizard

On the Request Complete panel, you can either click **View Status** to view this request on the **My Requests** tab, or click **Continue Shopping** to create another request.

Note • For information on viewing the details, status, and progress of a request, see Viewing Request Details and Viewing Request Status and Details.

15

Viewing Request Status and Details

After you have submitted a catalog item request for yourself or on behalf of another user, you can view the status and details of those in-progress requests on the **My Requests** tab and also on the **Reporting** tab of the App Portal storefront. You can view the details of completed (or rejected) requests on the **Processed** tab.

- Viewing Request Status and Details on the My Requests and Processed Tabs

- Viewing Request Reports on the Reporting Tab

- Viewing Request History on the Processed Tab

Viewing Request Status and Details on the My Requests and Processed Tabs

You can view the requests you have submitted for yourself and requests you have submitted on behalf of other users on the **My Requests** and **Processed** tabs of the App Portal storefront. You can open the **My Requests** tab by clicking on it, or by clicking the **View Status** button on the **Request Complete** panel of the Checkout Wizard.

The **My Requests** tab is divided into two panes:

- **Search pane**—You can use the left pane to perform basic and advanced searching of requests.

- **Requests pane**—The right pane displays all the requests generated by the current user or those targeting their current computer.

Figure 15-1: My Requests Tab

Each request is represented by a row in the grid and contains basic information about the request. Details of the request are visible by clicking on the request name in the **Request** column to open the **Request Details** dialog box, as described in Viewing Request Details.

- Searching for a Request on the My Requests Tab

- Viewing Status, Info, and Actions Icons on the My Requests Tab

- Viewing Request Details

Processed Tab

The **Processed** tab has the same general format as the **My Requests** tab, with the addition of the **Requester** and **Target** columns. The **Processed** tab lists all the requests submitted by the current user that were either approved or rejected.

Searching for a Request on the My Requests Tab

By default, all requests are displayed for the requesting user. You can use the fields on the **Basic** and **Advanced** tabs of the Search pane to search for requests to display.

Basic Tab

If the user is assigned the **Manage Requests** role, a **Show all requests** checkbox will be present on the **Basic** tab of the Search pane. When this option is selected, all requests within the last 30 days are displayed. You can also change the **Filter by Date From** and **Filter by Date To** fields accordingly to suit your search preferences.

Figure 15-2: Basic Tab of Search Pane of My Requests Tab

Advanced Tab

You can use the fields on the **Advanced** tab to search by **Source**, **Request**, **Approval Status**, **Install Status**, **Inventory Status**. From the **Advanced** tab, you can also choose to export the information in the list.

Figure 15-3: Advanced Tab of Search Pane of My Requests Tab

Viewing Status, Info, and Actions Icons on the My Requests Tab

The data displayed in the Requests list on the **My Requests** tab will depend on the state of the request. The major states of a request include **Pending Approval** and **Pending Delivery**.

Icons are displayed in the **Status**, **Info**, and **Actions** columns of the Requests list to specify information about the request:

Table 15-1 • Icons Displayed in the Status, Info, and Action Columns

Column	Icon		Description
Status	Pending Approval		When an approval is required before this request can be processed, The **Pending Approval** icon is displayed. Clicking on the icon displays the current approval process, whom has approved the request, and whom is pending approval.
	Approved		When the request has been approved, the **Pending Approval** icon switches to the **Approved** icon.
	Pending Deployment		Indicates that this application has not yet begun to install. Clicking on this icon shows the most recent status from your deployment system.
	In Progress		Indicates that the processing of this request is in progress.
	Schedule		Indicates that this catalog item has been scheduled for deployment.
Status (continued)	Rerun		Indicates an advertisement rerun.
	Waiting for install status messages		Indicates that the application has not begun to install.
	Install Complete		The **Install Complete** icon indicates that the application has successfully been installed on the target end user's machine.
	Install Failed		If the software request fails, then an error icon is displayed.
	Machine policy succeeded		Indicates that App Portal was able to successfully trigger an SCCM policy refresh to force the client to update its SCCM client policy. This, in turn, helps in faster software deployment.
	Request has been completed		Request has been completed.

Table 15-1 • Icons Displayed in the Status, Info, and Action Columns

Column	Icon		Description
Info	Processing Time		If you hover over this icon, the time that has elapsed since the installation of this application was begun is listed.
	Alarm Warning		Hover over this icon to display the amount of time that this action has been processing.
	Completed		When installation of this application is complete, the **Processing time icon** switches to this icon to indicate that processing has been completed and the application has been installed.
	Request has Associated Questions		Indicates that this request has an associated question template.
	Add a Note		Click to add a note to this request.
	License unavailable		This catalog item requires a license and no license is available.
	Lease		Indicates that this catalog item will be leased as of a specified date. If the lease is close to expiring, the Lease Warning icon is displayed. When the lease has expired, the Lease Expired icon is displayed.
Actions	Cancel		Click to cancel this request.
	Uninstall		Click to uninstall this application, which is already installed on your machine.
	Reinstall		Indicates that the catalog item has an option for reinstallation. Click on this icon to initiate the reinstallation of this application. This icon is only displayed when the **Enable Reinstallation / Rerun?** option is selected on the **Deployment > Global** tab of the **Catalog Item Properties** dialog box for that catalog item.

Table 15-1 • Icons Displayed in the Status, Info, and Action Columns

Column	Icon		Description
Actions (continued)	**Repair**		Indicates that this catalog item has an option for repair. Click on this icon to initiate an application repair.
	Rate		Click to rate this installed application (by selecting 1 to 5 stars, in half star increments) and provide any additional comments. This rating will be visible for other users to see as they browse the catalog.

Note • *A rating star icon is only listed in the* ***Action*** *column for applications which have been installed on the logged in user's computer.*

Note • *This option is enabled if administrators have selected the* ***Allow users to rate request option*** *on the* ***Site Management > Settings > Web Site > Catalog Behavior*** *tab.*

Viewing Request Details

You can view the details of each submitted request on the **Request Details** dialog box, which is opened by double-clicking on the request name in the **Request** column on the **My Requests**, **Approve / Reject**, or **Processed** tabs.

- Viewing Summary Information on the General Tab

- Viewing License Information on the Inventory Tab

- Viewing Approval Process Hierarchy and Status on Approval Status Tab

- Viewing Notes on the Notes Tab

- Viewing Questions and Responses on the Questions Tab

- Viewing Deployment Status on the Status Tab

- Viewing Alternate Software on the Alternates Tab

- Viewing Attached Files on the Files Tab

Note • *The number of tabs displayed on the* ***Request Details*** *dialog box depend upon the type of request and the options enabled.*

Viewing Summary Information on the General Tab

The **General** tab of the **Request Details** view contains basic information about the item being requested and the user who requested the item.

Figure 15-4: Request Details View / General Tab

The **General** tab of the **Request Details** view includes the following properties:

Table 15-2 • Request Details View / General Tab

Property	Description
Request Name	Name of the catalog item that was requested.
Description	Long description of the catalog item that was requested.
License Required	Indicates whether or not a license is required for this catalog item.
License Cost	Lists the cost associate with this catalog item, if specified.
Requested On	Date request for this catalog item was submitted.
Approval Status	Indication of the request's approval status.
User Information	Lists information about the person who requested this catalog item.

Viewing License Information on the Inventory Tab

📄

Note • *The Inventory tab is only displayed when viewing a request for a software application catalog item. When viewing a request for a Task Sequence, which are used for operating system deployments, the OSD tab is displayed.*

The **Inventory** tab lists inventory information regarding the requested catalog item. The information displayed on this tab depends upon whether your organization manages inventory and licensing using FlexNet Manager Suite.

- Compliance Management Using FlexNet Manager Suite

- Standard Compliance Management

Compliance Management Using FlexNet Manager Suite

If your organization uses FlexNet Manager Suite to perform compliance management, information about license availability is displayed on the **Inventory** tab.

Figure 15-5: Request Details View / Inventory Tab / Managed by FlexNet Manager Suite

Standard Compliance Management

If your organization does not use FlexNet Manager Suite to perform compliance management, additional inventory details are listed on the **Inventory** tab.

Figure 15-6: Request Details View / Inventory Tab / Without FlexNet Manager Suite

In this view, the current inventory statistics are displayed for the approvers to review. You optionally can mark an item as purchased, select the purchase type, and assign a purchase record to the specific request.

Purchases listed are those which are not already assigned to other requests that have been added to the purchase history for the particular inventory item.

Viewing Approval Process Hierarchy and Status on Approval Status Tab

The **Approval Status** tab shows the current approval process hierarchy. If the user has modify permissions to the Approval Process or Request Management, they can modify the approval process.

- Approvers can be selected and deleted and dragged between levels.

- New approvers can be added using the search for approver area.

- You can select approvers from existing approval groups or search Active Directory for a specific approver.

Viewing Notes on the Notes Tab

On the Notes tab of the Request Details view, you can add notes for whatever purpose you desire. Approvers' approval and reject messages are automatically added as notes.

Figure 15-7: Request Details View / Notes Tab

When adding a new note you can select who is to be notified. Select the appropriate options, if any, for the note notification.

Figure 15-8: Add New Note Dialog Box

To display system events related to this catalog item on this tab, click **Show System Events**.

Figure 15-9: Displaying System Events on Notes Tab

Viewing Questions and Responses on the Questions Tab

The **Questions** tab of the Request Details view displays the questions answered during the checkout process.

The **Answered Questions** subtab of the **Questions** tab lists the questions that were answered during checkout.

Figure 15-10: Request Details View / Questions Tab / Answered Questions Subtab

All unanswered questions, including those required by approvers, are listed on the **Unanswered Questions** subtab, where they can be answered.

Figure 15-11: Request Details View / Questions Tab / Unanswered Questions Subtab

Viewing Deployment Status on the Status Tab

When the Request Type is a software request, the **Status** tab will list information about the software deployment.

Figure 15-12: Request Details View / Status Tab

The **Status** tab of the **Request Details** view includes the following properties:

Table 15-3 • Request Details View / Status Tab

Property	Description
Scheduled for Insert	Date and time that this request is scheduled to be installed. If end-user scheduling is enabled in this catalog item, it will list the date and time that was specified.
Actual Insert Date	Actual date and time that this catalog item was installed.
Is Leased?	Clear the selection of this option to switch from a leased to a permanent installation. Make sure that this option is selected if you want to modify the **Lease End** date and time. *Note • Only appears for leased catalog items.*
Lease End	If this is a leased catalog item, and if the **Allow user to extend lease when approval is not required** option on the **Deployment > Leasing** tab of the **Catalog Item Properties** dialog box for this catalog item is selected, the **Lease End** field is displayed, prompting you to extend the lease of this catalog item by selecting a date and time. *Note • Immediately prior to lease expiration, you should receive an email stating that the lease is about to expire and instructing you to open the **Request Details** view and extend the lease.* *Note • Only appears for leased catalog items.*
Manually Set Install Status	If you want to manually specify the installation status of this catalog item, select **Succeeded** or **Failed** from the list. This option gives you the ability to override the installation status. For example, if a deployment initially fails, App Portal will stop monitoring this catalog item and the and the status will always be set to **Failed**. However, if this deployment eventually is successful, you can change its status by selecting **Succeeded** from this list.
Collection membership state	Click **Check** to check whether the specified device is in the collection. When you click **Check**, the word **Yes** or **No** is listed. If deployment is successful, click **Remove**.

Viewing Alternate Software on the Alternates Tab

When the Request Type is a software request and the request has not yet been submitted to your deployment system for installation, the **Alternates** tab will display alternate items to deploy in place of the current item. This allows the request to be "switched" as necessary.

Figure 15-13: Request Details View / Alternates Tab

If an alternate product is listed and you click Select, you are prompted to select the users to notify of this switch, and to click Switch Request to confirm the switch.

Figure 15-14: Switch Request Dialog Box

Viewing Attached Files on the Files Tab

On the **Files** tab, you can upload and attach files as required for file storage.

Figure 15-15: Request Details View / Files Tab

To upload a file, click the **Upload Files** button to open the Upload view.

Figure 15-16: Upload View

Viewing Request Reports on the Reporting Tab

On the **Reporting** tab, you can view App Portal data in a read-only, searchable, and exportable view. Over 40 reports are included with App Portal. You can view existing reports, create and edit report categories, and even create your own custom reports.

Task   ***To view App Portal reports:***

1.   Open the **Reporting** tab.

2.   In the **App Portal Menu**, open one of the report categories and select the report that you want to view. The report opens in the right pane.

3. If you want to export the report to **Excel**, **PDF**, or **Word** format, click the **Export** button in the toolbar and select the appropriate option:

4. To print the report, click the **Print** button in the toolbar.

Viewing Request History on the Processed Tab

The **Processed** tab has the same general format as the **My Requests** tab, with the addition of the **Requester** and **Target** columns. The **Processed** tab lists all the requests submitted by the current user that were either approved or rejected.

Figure 15-17: Processed Tab

> **Note** • For more information, see *Viewing Request Details*.

16

Viewing Request Details

Each submitted request has a **Request Details** view, which is opened by selecting the **Request** column on the **My Requests** tab. The tabs displayed in the **Request Details** view depend on the type of request and the options enabled.

- General Tab
- Inventory Tab
- Approval Status Tab
- Notes Tab
- Questions Tab
- Status Tab
- Alternates Tab
- Files Tab

General Tab

The **General** tab of the **Request Details** view contains basic information about the item being requested and the user who requested the item.

Figure 16-1: Request Details View / General Tab

The **General** tab of the **Request Details** view includes the following properties:

Table 16-1 • Request Details View / General Tab

Property	Description
Request Name	Name of the catalog item that was requested.
Description	Long description of the catalog item that was requested.
License Required	Indicates whether or not a license is required for this catalog item.
License Cost	Lists the cost associate with this catalog item, if specified.
Requested On	Date request for this catalog item was submitted.
Approval Status	Indication of the request's approval status.
User Information	Lists information about the person who requested this catalog item.

Inventory Tab

📄

*Note • The **Inventory** tab is only displayed when viewing a request for a software application catalog item. When viewing a request for a Task Sequence, which are used for operating system deployments, the **OSD** tab is displayed.*

The **Inventory** tab lists inventory information regarding the requested catalog item. The information displayed on this tab depends upon whether your organization manages inventory and licensing using FlexNet Manager Suite.

- Compliance Management Using FlexNet Manager Suite

- Standard Compliance Management

Compliance Management Using FlexNet Manager Suite

If your organization uses FlexNet Manager Suite to perform compliance management, information about license availability is displayed on the **Inventory** tab.

Figure 16-2: Request Details View / Inventory Tab / Managed by FlexNet Manager Suite

Standard Compliance Management

If your organization does not use FlexNet Manager Suite to perform compliance management, additional inventory details are listed on the **Inventory** tab.

Figure 16-3: Request Details View / Inventory Tab / Without FlexNet Manager Suite

In this view, the current inventory statistics are displayed for the approvers to review. You optionally can mark an item as purchased, select the purchase type, and assign a purchase record to the specific request.

Purchases listed are those which are not already assigned to other requests that have been added to the purchase history for the particular inventory item.

Approval Status Tab

The **Approval Status** tab shows the current approval process hierarchy. If the user has modify permissions to the Approval Process or Request Management, they can modify the approval process.

- Approvers can be selected and deleted and dragged between levels.

- New approvers can be added using the search for approver area.

- You can select approvers from existing approval groups or search Active Directory for a specific approver.

Notes Tab

On the Notes tab of the Request Details view, you can add notes for whatever purpose you desire. Approvers' approval and reject messages are automatically added as notes.

Figure 16-4: Request Details View / Notes Tab

When adding a new note you can select who is to be notified. Select the appropriate options, if any, for the note notification.

Figure 16-5: Add New Note Dialog Box

To display system events related to this catalog item on this tab, click **Show System Events**.

Figure 16-6: Displaying System Events on Notes Tab

Questions Tab

The **Questions** tab of the Request Details view displays the questions answered during the checkout process.

The **Answered Questions** subtab of the **Questions** tab lists the questions that were answered during checkout.

Figure 16-7: Request Details View / Questions Tab / Answered Questions Subtab

All unanswered questions, including those required by approvers, are listed on the **Unanswered Questions** subtab, where they can be answered.

Figure 16-8: Request Details View / Questions Tab / Unanswered Questions Subtab

Status Tab

When the Request Type is a software request, the **Status** tab will list information about the software deployment.

Figure 16-9: Request Details View / Status Tab

The **Status** tab of the **Request Details** view includes the following properties:

Table 16-2 • Request Details View / Status Tab

Property	Description
Scheduled for Insert	Date and time that this request is scheduled to be installed. If end-user scheduling is enabled in this catalog item, it will list the date and time that was specified.
Actual Insert Date	Actual date and time that this catalog item was installed.
Is Leased?	Clear the selection of this option to switch from a leased to a permanent installation.
	Make sure that this option is selected if you want to modify the **Lease End** date and time.
	Note • Only appears for leased catalog items.
Lease End	If this is a leased catalog item, and if the **Allow user to extend lease when approval is not required** option on the **Deployment > Leasing** tab of the **Catalog Item Properties** dialog box for this catalog item is selected, the **Lease End** field is displayed, prompting you to extend the lease of this catalog item by selecting a date and time.
	Note • Immediately prior to lease expiration, you should receive an email stating that the lease is about to expire and instructing you to open the Request Details view and extend the lease.
	Note • Only appears for leased catalog items.
Manually Set Install Status	If you want to manually specify the installation status of this catalog item, select **Succeeded** or **Failed** from the list.
	This option gives you the ability to override the installation status. For example, if a deployment initially fails, App Portal will stop monitoring this catalog item and the and the status will always be set to **Failed**. However, if this deployment eventually is successful, you can change its status by selecting **Succeeded** from this list.
Collection membership state	Click **Check** to check whether the specified device is in the collection. When you click **Check**, the word **Yes** or **No** is listed. If deployment is successful, click **Remove**.

Alternates Tab

When the Request Type is a software request and the request has not yet been submitted to your deployment system for installation, the **Alternates** tab will display alternate items to deploy in place of the current item. This allows the request to be "switched" as necessary.

Figure 16-10: Request Details View / Alternates Tab

If an alternate product is listed and you click Select, you are prompted to select the users to notify of this switch, and to click Switch Request to confirm the switch.

Figure 16-11: Switch Request Dialog Box

Files Tab

On the **Files** tab, you can upload and attach files as required for file storage.

Figure 16-12: Request Details View / Files Tab

To upload a file, click the **Upload Files** button to open the Upload view.

Figure 16-13: Upload View

17

Approving or Rejecting Requests on the Approve/Reject Tab

📄

Note • *Starting with App Portal 2014, a permanent Flexera Software color theme has been applied to the user interface, and the top navigation menu has changed from tabs to menu selections; however, all functionality remains the same.*

The App Portal **Approve / Reject** tab has the same general format as the **My Requests** tab (as described in Viewing Request Status and Details on the My Requests and Processed Tabs) with the addition of **Approve**, **Reassign**, **Reject**, and **Request Info** buttons in the command bar.

Figure 17-1: App Portal Approve/Reject Tab

The items listed here are those pending approval for the current user visiting the site unless the **Show all requests** option is selected in the **Search** pane, in which case all items pending approval are listed.

This section includes the following topics:

- Approving a Request

- Reassigning a Request

- Requesting Additional Information

- Rejecting a Request

Approving a Request

There are two ways to approve or reject a request:

- Approving or Rejecting Requests on the Approve/Reject Tab

- Approving or Rejecting Requests via Email (Flexible Approval)

Approving or Rejecting Requests on the Approve/Reject Tab

To approve a request on the Approve/Reject tab, perform the following steps.

Task   ***To approve a request:***

1. Open the **Approve/Reject** tab. The catalog items that are pending approval are listed, and have a **Status** of **Pending Approval**, which is the following icon

2. Click on the request name. The **Approval** dialog box opens.

📄

> ***Note •*** *Before deciding to approve an item, the approver can open the **Questions** tab to review the requester's answers, open the **Files** tab to view any uploaded files, and view the **Notes** tab to read any associated notes.*

3. Click **Approve**. A pop-up dialog box opens, prompting you to enter any approval notes.

4. If the approver has permissions to override approval, the **Override current approvers** option is available. When this option is selected, the existing approvers are replaced by the current approver and the request is approved.

5. Click **Approve**. The request is no longer listed on the **Approve/Reject** tab, and App Portal instructs your deployment system to install the requested application.

Approving or Rejecting Requests via Email (Flexible Approval)

Flexible approval functionality in App Portal enables flexibility for an approver to approve or reject requests outside the enterprise network and without logging into App Portal. This provides a speedy on-the-go approval (or rejection) process, and subsequent delivery of the request without delays.

To facilitate the flexible approval process, incoming mail configurations are required in **Site Management > Settings > Email > Incoming Email.** For more information, refer to Incoming Email Subtab. Once configured, an approver can approve requests by simply replying to an email notification using predefined keywords (e.g., **Approve** or **Reject** or any others that are defined in the **Flexible Approval - Approval Keywords** and **Flexible Approval - Reject Keywords** templates, respectively) along with any additional comments. The system further parses through these email responses and takes action of approving or rejecting the request accordingly based on the keyword provided in the reply.

For information about email templates used for flexible approval, refer to List of Notification Email Templates and Messages.

Reassigning a Request

Instead of approving or rejecting a request, you have to choice to reassign a request to a different user or group.

Task **To reassign a request to another user or group:**

1. Open the **Approve/Reject** tab. The catalog items that are pending approval are listed, and have a **Status** of **Pending Approval**.

2. Click on the request name. The **Approval** dialog box opens.

3. Click **Reassign**. The **Reassign** dialog box opens.

4. Use the search box to search for a user or select an approval group from the **Browse Approval Groups** list.

5.   Click **Reassign**. The request is reassigned to the select user or group.

Requesting Additional Information

You have the option of requesting additional information from the requester or another user before you make your approval decision.

Task   ***To request additional information:***

1.   Open the **Approve/Reject** tab. The catalog items that are pending approval are listed, and have a **Status** of **Pending Approval**.

2.   Select the check box next to the request and click **Request Info**. The **Send Requests for Review** dialog box opens.

3. Enter a note in the **Enter note for reviewer** text box to explain the information you require.

4. If you want to sent this request for information to the requester, select the **Notify Requester** check box.

5. If you want to send this request for information to someone other than the requester, clear the selection of the **Notify Requester** check box and use the **Search** box to search for and select a different user.

    The requester or the selected user will then receive an email with the text of the note, and a link to review the submitted request.

Rejecting a Request

There are two ways to reject a request:

●   Rejecting a Request Rejecting on the Approve/Reject Tab

●   Rejecting a Request via an Email Reply

Rejecting a Request Rejecting on the Approve/Reject Tab

To reject a request using the Approve/Reject tab, perform the following steps.

Task   **To reject a request:**

1. Open the **Approve/Reject** tab. The catalog items that are pending approval are listed, and have a **Status** of **Pending Approval**.

2. Click on the request name. The **Approval** dialog box opens.

Note • *Before deciding to reject an item, the approver can open the **Questions** tab to review the requester's answers, open the **Files** tab to view any uploaded files, and view the **Notes** tab to read any associated notes.*

3. Click **Reject**. A pop-up dialog box opens, prompting you to enter an explanation for the rejection.

4.   If the approver wishes to recommend the rejection instead of completely rejecting the request, choose the **Recommend reject only** option.

5.   Click **Reject**.

Rejecting a Request via an Email Reply

For information about how to reject a request by simply replying to an email, refer to Approving or Rejecting Requests via Email (Flexible Approval).

18

Using the My Apps Tab to Manage Your Applications and Software Policy Score™

If App Portal is integrated with FlexNet Manager Suite, the App Portal **My Apps** tab is displayed, where you can view a list of applications installed on your , and address automatic and administrator-defined alerts to ensure that those applications comply with corporate software policies. This enables you to assist IT administrators in driving continual software license reclamation and optimization.

Figure 18-1: My Apps Tab

Information about using the **My Apps** tab is described in the following topics:

- Viewing Your Installed Applications on the My Apps Tab

- Viewing Your Software Policy Score™ Chart on the My Apps Tab

- Resolving Alerts on the My Apps Tab

Viewing Your Installed Applications on the My Apps Tab

When App Portal is integrated with FlexNet Manager Suite, it has access to the FlexNet Manager Suite Application Recognition Library (ARL), which uniquely identifies over 110,000 applications (including multiple versions and editions) from over 14,000 publishers.

App Portal uses this information to identify the applications that have been installed on the current user's computer, and those applications are listed in the **Installed Applications** list on the **My Apps** tab.

Figure 18-2: Installed Applications List on My Apps Tab

The following topics describe the **Installed Applications** list:

- Users With Multiple Computers () Can Select Which Device to View

- List is Generated Independently from App Portal's Catalog Items

- User Can Choose to Uninstall an Application From This List

- Information Displayed in the Installed Applications List

Users With Multiple Computers () Can Select Which Device to View

If you have more than one associated computer (device), as determined by the connected deployment technology, you can select the device that you want to view the applications of by making a selection from the **Choose Your Device** list at the top of the **My Apps** tab.

If you only have one associated device, the **Choose Your Device** list is not displayed.

List is Generated Independently from App Portal's Catalog Items

This list of applications is generated by App Portal by using the application recognition information from FlexNet Manager Suite to identify the applications that are installed on each device. Whether or not an App Portal catalog item exists for an application has no bearing upon whether it is included in the **Installed Applications** list.

Items listed in the **Installed Applications** list do not necessarily have a corresponding App Portal catalog item. However, if an installed application does have a corresponding App Portal catalog item, additional data may be displayed in this list, such as **Cost**.

User Can Choose to Uninstall an Application From This List

If an application has no unresolved alerts, a user can choose to uninstall that application (and return its license) by clicking the Uninstall icon in the **Action** column of the **Installed Applications** list:

Note • *If the unused software item does not have an associated uninstall program, the Uninstall icon will not be displayed in the* **Action** *column.*

Information Displayed in the Installed Applications List

The following information is displayed for applications in the installed applications list:

Table 18-1 • Installed Applications List Properties

Property	Description
Application	Application name as defined in FlexNet Manager Suite.
Version	Application version.
Edition	Application edition, if this information was defined in FlexNet Manager Suite.
Publisher	Name of manufacturer of application.

Table 18-1 • Installed Applications List Properties

Property	Description
Classification	Category, defined by FlexNet Manager Suite, which can be used to filter lists of applications. For example, administrators might choose to hide all applications that are classified as **Freeware**, because of the low impact of their licensing. The following classifications are available: • **Beta**—Pre-release application (such as beta releases, alpha releases, or release candidates). • **Component**—Item is used/installed as a component of another application or suite, and is not licensed as a standalone item. • **Commercial**—Requires a license to be purchased for use in a commercial setting. • **Freeware**—Licensed for use in a commercial setting free of charge. • **Malware**—Application is considered to be potentially harmful (such as a virus or a Trojan horse). • **Shareware**—Application is available for download from Internet shareware sites, and typically uses a "try-before-you-buy" licensing model. • **Update**—Application represents an update (such as a service pack) to another application, issued free to all customers regardless of purchasing agreements or support contracts (a "minor" update). • **X Rated**—Application potentially contains objectionable or sexually explicit material.
Is Used?	Indicates whether or not the application has been used during the **License Reclamation Threshold** period defined by the App Portal administrator.
Cost	If application has an associated App Portal catalog item, and the catalog item has an associated cost, the cost is listed in this column.
Action	If an application has no unresolved alerts, an Uninstall button is listed in this column: If you click the Uninstall button, the application will be uninstalled and any associated license will be returned.

Viewing Your Software Policy Score™ Chart on the My Apps Tab

The **Software Policy Score**™ chart on the **My Apps** tab provides a quick way for a user to see the percentage of their installed applications which have license reclamation or optimization issues to address.

Software Policy Score ™

Figure 18-3: Software Policy Score on the My Apps Tab

In order to enforce corporate software policies, App Portal sends out the following types of alerts when it detects a problem with installed software:

- **Unused software alerts**—Application has not been used for the number of days specified by the App Portal administrator in the **License Reclamation Threshold** field.

- **Proof of purchase alert**—When informed by FlexNet Manager Suite that there are no remaining licenses for an application, administrators add that application to the **Proof of purchase** alert action catalog item, which triggers an alert to be sent to all users who have that application installed.

- **Administrator-created action alert**—An administrator can create a custom alert and attach a question template to it to gather information from the application user.

The **Software Policy Score** chart classifies each application on your computer into one of three categories based upon its unresolved alerts, and displays the percentage of applications in each category:

- **No Alerts**—The applications in this category either have never had any alerts or all of their alerts have been resolved.

- **Unused Software Alerts**—The applications in this category have an unresolved unused software alert. Because unused licensed software is a large expense to an enterprise, these types of alerts have a high degree of importance

- **Action Alerts**—The applications in this category have an unresolved proof of purchase or administrator created action alert.

Your goal is to have 100% of your applications in the **No Alerts** category. Each time you resolve an alert, as described in Resolving Alerts on the My Apps Tab, your Software Policy Score improves.

Resolving Alerts on the My Apps Tab

Rather than having administrators send out email notifications to users regarding expired licenses or unused software, administrators can create and enable license reclamation and alert actions to prompt end users to address compliance issues. You resolve these issues in the **My Current Alerts** subtab of the **My Apps** tab.

Figure 18-4: My Current Alerts Subtab of My Apps Tab

Information about resolving alerts is presented in the following topics:

- About Alerts

- Resolving Alerts

About Alerts

On the **My Current Alerts** subtab of the **My Apps** tab, users are prompted to respond to the following types of alerts:

- **Unused software alert**—As soon as the **My Apps** feature is enabled, App Portal will automatically send alerts to users for each installed application that they have not used for the number of days specified by the App Portal administrator in the **License Reclamation Threshold** field. The alert prompts the user to either complete a business justification survey to keep the seldom-used application or uninstall it

  📄

  Note • *Unused software alerts will only be sent for applications that an App Portal administrator has selected for license reclamation.*

- **Proof of purchase alert**—When informed by FlexNet Manager Suite that there are no remaining licenses for an application, administrators add that application to the **Proof of purchase** alert action catalog item, which triggers an alert to be sent to all users who have that application installed. To resolve the alert, users are prompted to provide proof of purchase for the unlicensed software.

- **Administrator-created action alert**—An administrator can create a custom alert and attach a question template to it to gather information. The alert prompts the user to answer questions to provide this information. This information is delivered to the administrator via the standard checkout process.

  📄

  Note • *If the App Portal administrator has selected the **Enable My Apps Notifications** option is in the **My Apps Options** section of the **Admin** tab, each time a user receives an alert on the **My Apps** tab, they will also receive an email notification.*

When an end user resolves an alert, it is listed on the **My Resolved Alerts** subtab. Each time an end user resolves an alert, the Software Policy Score improves for their device.

Resolving Alerts

To resolve an unused software or action alert, perform the following steps:

Task   **To resolve an alert:**

1.   Open the **My Apps** tab. All unresolved alerts are listed on the **My Current Alerts** tab.

2.   To resolve an **Unused Software Alert**, perform the following steps:

   a.   Review the text of the alert you want to resolve, and decide whether you would like to uninstall or keep the application. The following is a sample alert:

   ```
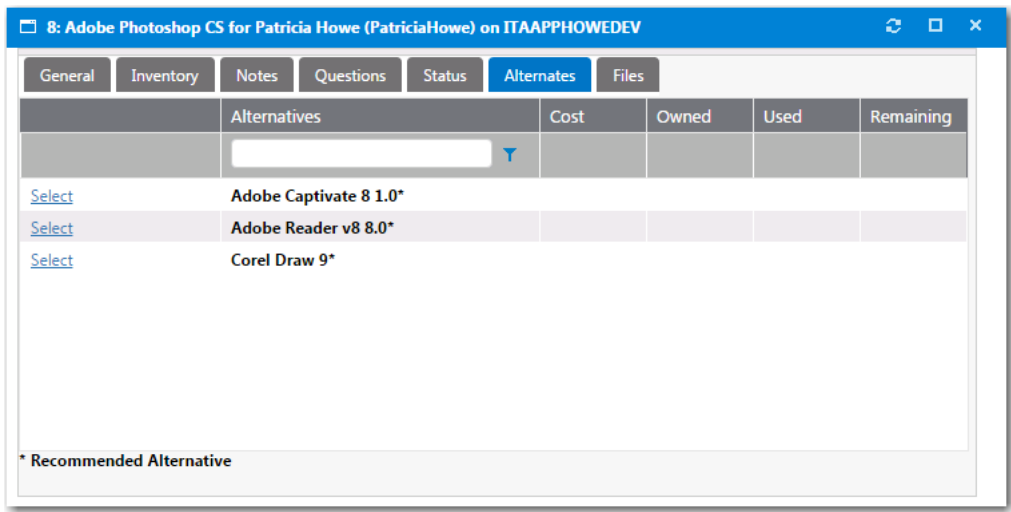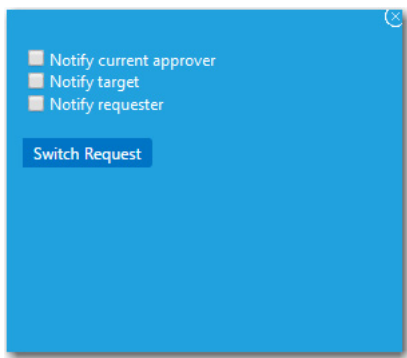   Unused Software Alert: You have not used SQL Compare 10 during the last 80 days, Click Uninstall
   to uninstall this software or click Keep to retain it.
   ```

   b.   Click **Keep** or **Uninstall**. The **Respond to Questionnaire** panel of the **Checkout** process opens, and you are prompted to specify why you want to keep or uninstall the application:

   c.   Answer the listed questions and click **Next**. The **Submit Request** panel opens.

   d.   Click **Submit**. A message appears stating that you have successfully resolved the issue:

3.   To resolve an **Action Alert**, perform the following steps:

a.   Review the text of the alert you want to resolve. The following is a sample alert:

```
Action Alert: You are required to perform an action Uninstall Blacklisted Software for
Calculator 6.1. To perform this action, click here.
```

b.   Click the here link. The **Checkout** process opens, and you may or may not be prompted to answer questions specific to the Action Alert on the **Respond to Questionnaire** panel.

c.   Answer any questions that are listed and then click **Next**. The **Submit Request** panel opens.

d.   Click **Submit**. A message appears stating that you have successfully resolved the issue.

4.   Return to the **My Apps** tab and open the **My Resolved Alerts** tab, where the alerts that you just resolved are now listed.

5.   Now that you have resolved alerts, check the **Software Policy Score** chart on the **My Apps** tab. Each time you resolve an alert, your Software Policy Score improves. Your goal is to have 100% of your applications in the **No Alerts** category.

Index

A

Action Alert 1251
Active Directory 332, 342
    Property Mapping 344
    Virtual Properties 344
ActiveDirectory_Error.log 394
Admin Security 234
AirWatch
    entering settings 82
    settings 293
AirWatch_Error.log 394
AirWatchDeployment.log 394
AirWatchIntegration.log 394
Alert Action 647
Alert Action Catalog Items 646
alerts
    responding to 1251
Altiris
    adding connection settings 73
    Advertisement Folder 37, 82
    Central Site Database Name 37, 81
    Central Site Database Server 37, 81
    Central Site Server 37, 81
    Computer Collection Folder 37, 82
    entering settings 36, 80
    settings 290
    software product 415
    User Collection Folder 37, 82
    user/computer relationship 37, 81
Altiris policy 421
Announcements 381
AP_ExpressCheckout 473
API
    functions 1016

    reference 965
App Broker for BMC
    about 741
App Broker for ServiceNow
    about 682
App Portal
    cookies 233
    cookies when running under HTTPS 233
App Portal service account 49
    required permissions 49
    updating password 50
Approval Groups 665
approval options 506
approval settings 508
approval workflow 506
approval workflows 653
    implementing custom approver feature 492
Approve/Reject tab 1239, 1240, 1241

B

BMC
    service request definition 102
Browse Catalog tab 1125
    about 1125
    checkout 1142
    icons displayed on 1175
    purchasing items 1139

C

Casper
    entering settings 84
    settings 295
Catalog 642