# App Portal / App Broker 2017 R2 SP1

# Release Notes

May 2018


**Introduction** ..... 2

**Changes in SP1** ..... 2

- **Support for Microsoft Edge Browser for Device Detection using Web Extensions** ..... 2
  - Deploying WebExtensions in Microsoft Edge ..... 5
- **System Center Configuration Manager Deployment Status ID Mapping to Final Success or Failure Statuses** ..... 5
- **Ability to Change Computer Mappings that App Portal Utilizes for Casper** ..... 6

**New Features** ..... 7

- **Target Device No Longer Required when Requesting General Catalog Items** ..... 7
- **Detailed Applications Installation Status from System Center Configuration Manager** ..... 9
- **New Computer Discovery Method: WebExtensions** ..... 10
  - Deploying WebExtensions to All Computers in a Network ..... 12
    - Deploying WebExtensions in Firefox (Windows) ..... 12
    - Deploying WebExtensions in Windows Chrome (Windows) ..... 12

**Important Information** ..... 13

- **End-of-Life Support for System Center Configuration Manager 2007** ..... 13

**Resolved Issues** ..... 14

- **App Portal / App Broker 2017 R2 SP1** ..... 14
- **App Portal / App Broker 2017 R2** ..... 16

**Upgrading to App Portal 2017 R2** ..... 17

**Applying the 2017 R2 Service Pack 1 to App Portal 2017 R2** ..... 19

**System Requirements** ..... 20

- **Environment Requirements** ..... 20
- **Client Requirements** ..... 22
- **Server Requirements** ..... 23
- **Supported Deployment Technologies** ..... 24
- **Supported ITSM Systems** ..... 26
- **Supported Cloud Applications** ..... 27

**Legal Information** ..... 27

***Important*** • *If upgrading from a previous version to App Portal 2017 R2, read Upgrading to App Portal 2017 R2 before beginning the upgrade. In addition, because App Portal 2017 R2 no longer supports System Center Configuration Manager 2007, if you are still planning on using System Center Configuration Manager 2007, it is recommended that you remain on App Portal 2017 R1 or earlier.*

# Introduction

App Portal enables IT managers to enforce continual software license compliance and control software deployment, while increasing employee satisfaction and the efficiency of application software delivery. The universal enterprise app store ensures that governance is in place to check license availability, obtain proper approvals, and reclaim licenses that are no longer used.

Automated workflow and approvals streamline the process of self-service requests for desktop, mobile, and cloud applications. Integration with Application Readiness and software deployment systems rapidly deliver enterprise software and operating systems to employee's devices, reducing the burden on IT and managing the enterprise application lifecycle from request to reclamation.

AppBroker™ software for ServiceNow® and AppBroker software for BMC leverage asset management data from FlexNet Manager Suite, including product use rights, to ensure proper governance and compliance over the request and installation of software. But with AppBroker, instead of using the App Portal end user interface, employees request software directly in the ServiceNow or BMC MyIT self-service portal.

# Changes in SP1

This section describes the new features included in App Portal / App Broker 2017 R2 SP1.

- Support for Microsoft Edge Browser for Device Detection using Web Extensions
- System Center Configuration Manager Deployment Status ID Mapping to Final Success or Failure Statuses
- Ability to Change Computer Mappings that App Portal Utilizes for Casper

## Support for Microsoft Edge Browser for Device Detection using Web Extensions

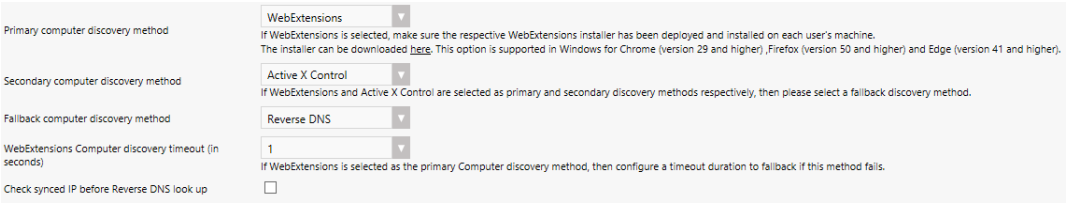
### Computer Discovery Method: WebExtensions

App Portal has several computer discovery methods to determine a user's computer name. In App Portal 2017 R2, a new discovery method using web extensions was added that included supported in Chrome for Windows (version 29 and higher) and Firefox for Windows (version 50 and higher). **With the release of App Portal 2017 R2 SP1, support for using web extensions as the computer discovery with Microsoft Edge (version 41 and higher) has also now also been added**.

***Note*** • *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.*

To enable this functionality, App Portal has added a **WebExtensions** option to the **Computer discovery method** drop-down list (on the **General** tab of the **Site Management > Settings > Web Site** view).

***Note*** • *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 needs 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.*




As background, when a user visits App Portal, App Portal is aware of the context of who the user is but the device is initially unknown. The previous options available in App Portal each had its own limitations, as detailed in the following table.

**Table 1** • Discovery Methods App Portal uses to Identify Device of User accessing App Portal

| Computer discovery method | Limitations |
|---|---|
| **ActiveX** | Only fully supported in Internet Explorer. Also, moving forward Microsoft has dropped support for ActiveX in their Edge browser. |
| **Reverse DNS** | This is a slow process and unreliable particularly if connected through VPN or wirelessly. |
| **SCCM** | Assumes System Center Configuration Manager is updated and assumes Data Sync is complete. |
| **Active Directory** | Retrieves only computers managed by the user. |

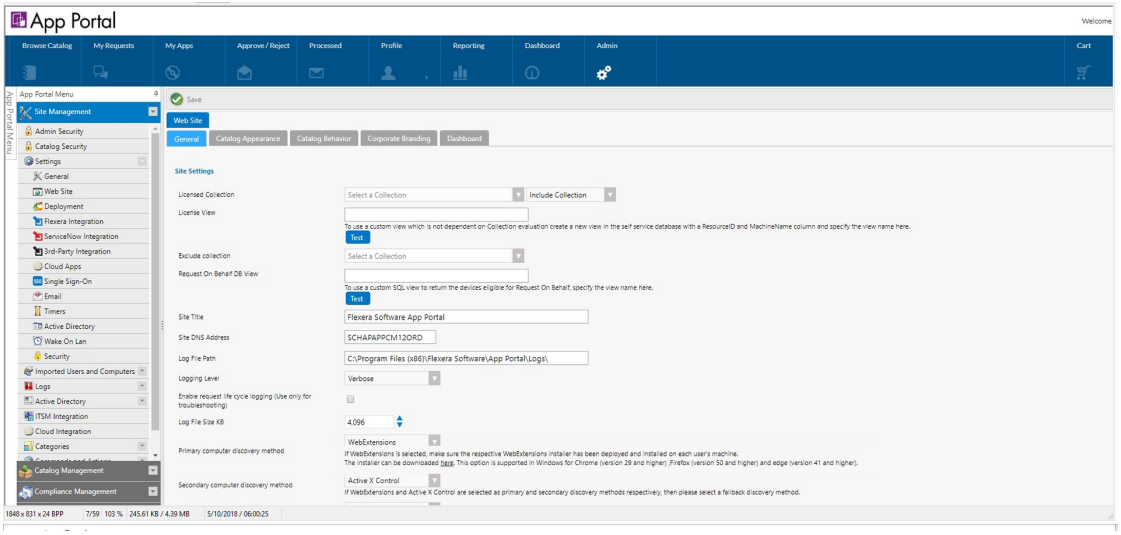
The way App Portal utilizes Microsoft Edge, Chrome for Windows, and Firefox for Windows web extensions is as follows. Enterprise users of Chrome, Edge, and Firefox have web extensions installed that communicate with the host application installed on the client machine. The host application relays the user's machine name to the browser extension which in turn relays the information to App Portal. From here, App Portal sends the information to the App Portal Application Server where further processing can then be done. This gives App Portal the machine name.

In addition to the **WebExtensions** being added as an option the **Primary computer discovery method** drop-down list, the following fields have also been added to support the new **WebExtensions** option:

- **Secondary computer discovery method**—If the **Primary computer discovery method** fails, the secondary discovery method will be used. If the **Secondary computer discovery method** fails, the fallback discovery method will be used.

  ***Note** • If **WebExtensions** and **Active X Control** are selected as primary and secondary discovery methods respectively, then you should enter a fallback discovery method in the **Fallback computer discovery method** field to account for a scenario where the primary and secondary discovery methods may not be not applicable.*

- **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.



## 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.

# System Center Configuration Manager Deployment Status ID Mapping to Final Success or Failure Statuses

In App Portal 2017 R2 SP1, we have enabled a mechanism where Administrator can configure the Success or Failure status IDs mapping for application respectively. When the App Portal tries to get the latest status from System Center Configuration Manager (SCCM), based on the mappings it will mark the request to final Success or Failure status respectively. This will make the status available instantly based on mappings, instead of waiting for Catalog or Global level timers.

As part of App Portal 2017 R2 release, we had the capability to configure the Status IDs (see Detailed Applications Installation Status from System Center Configuration Manager). In this release we are extending these configuration settings and mark the application requests to corresponding final status.

If SCCM returns new ID other than what is configured by Administrator, then App Portal will dynamically add that new ID and which will mark final status based on default mapping from SCCM.

# Ability to Change Computer Mappings that App Portal Utilizes for Casper

A new **Casper Machine Name Configuration** area has been added to the **Casper** tab of the **Site Management > Settings > Deployment** view. This 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 Devices/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.

# New Features

This section describes the new features included in App Portal / App Broker 2017 R2. For changes in 2017 R2 SP1, see Changes in SP1.

- Target Device No Longer Required when Requesting General Catalog Items
- Detailed Applications Installation Status from System Center Configuration Manager
- New Computer Discovery Method: WebExtensions

## Target Device No Longer Required when Requesting General Catalog Items

In App Portal 2017 R2, **General** catalog items no longer require a device target. This lets a user submit **General** catalog item requests even if there are no devices defined for the user making the request, or when submitting **General** catalog item requests on behalf of a user that has no devices defined. Previously, App Portal required a target machine even for a **General** catalog request.

As part of this functionality, a new **Choose Target Users for Request on Behalf Panel** has been added to App Portal / App Broker. 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.

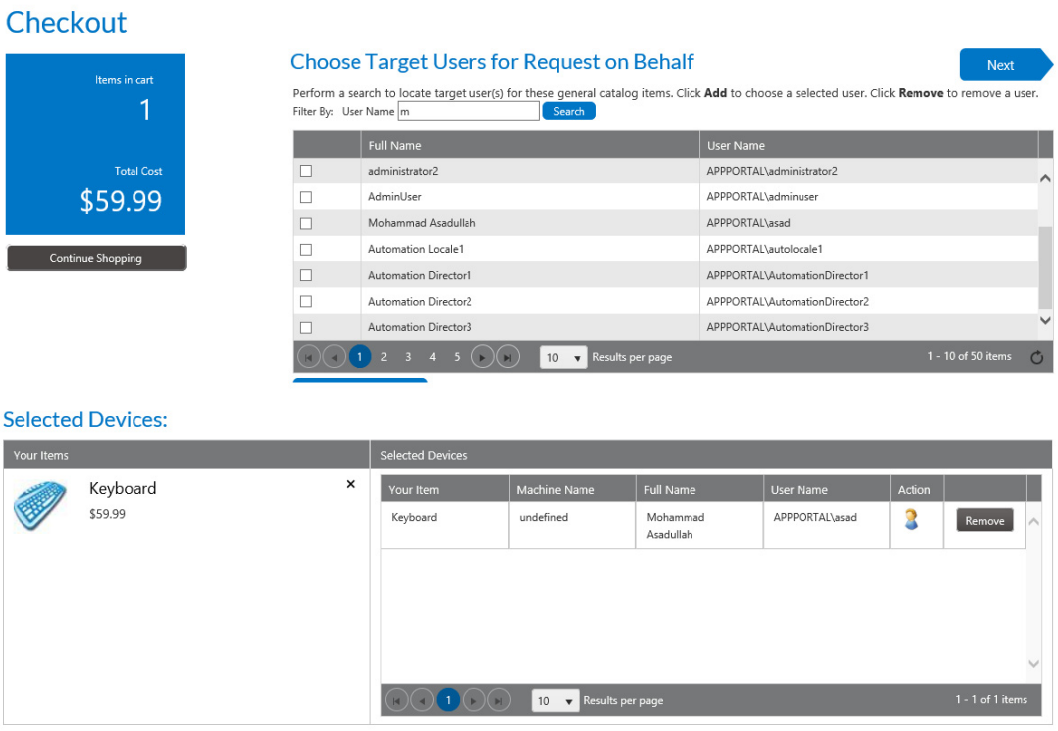



**Figure 1:** Choose Target Users for Request on Behalf Panel / Checkout Wizard

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 Devices/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 Devices/Users for Request On Behalf Panel**.

The following table explains when these three options are displayed on the **Choose Target** panel:

**Table 2** • 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.<br><br>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 devices/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.

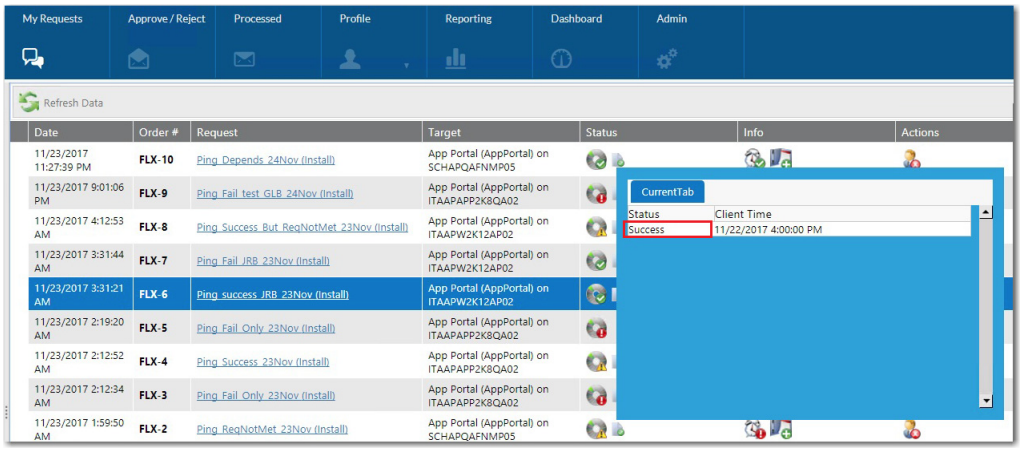
# Detailed Applications Installation Status from System Center Configuration Manager

Detailed application deployment status from System Center Configuration Manager is now provided in App Portal.

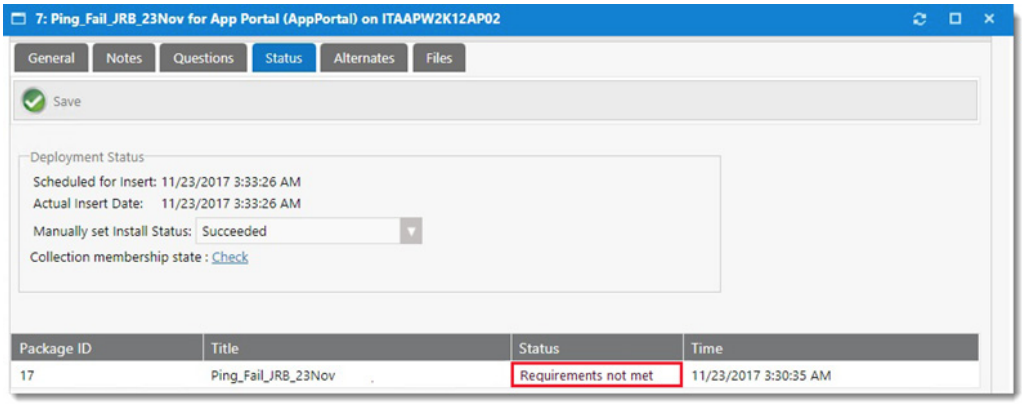
***Note*** • *In order to see deployment status information, the* ***Allow users to see detailed deployment status*** *option must be checked on the* ***My Requests Options*** *area of the* ***Catalog Behavior*** *tab of the* ***Web Site*** *view. By default this option is turned on and is now applicable to packages and applications.*

Application deployment status from System Center Configuration Manager is displayed in the following areas of App Portal:

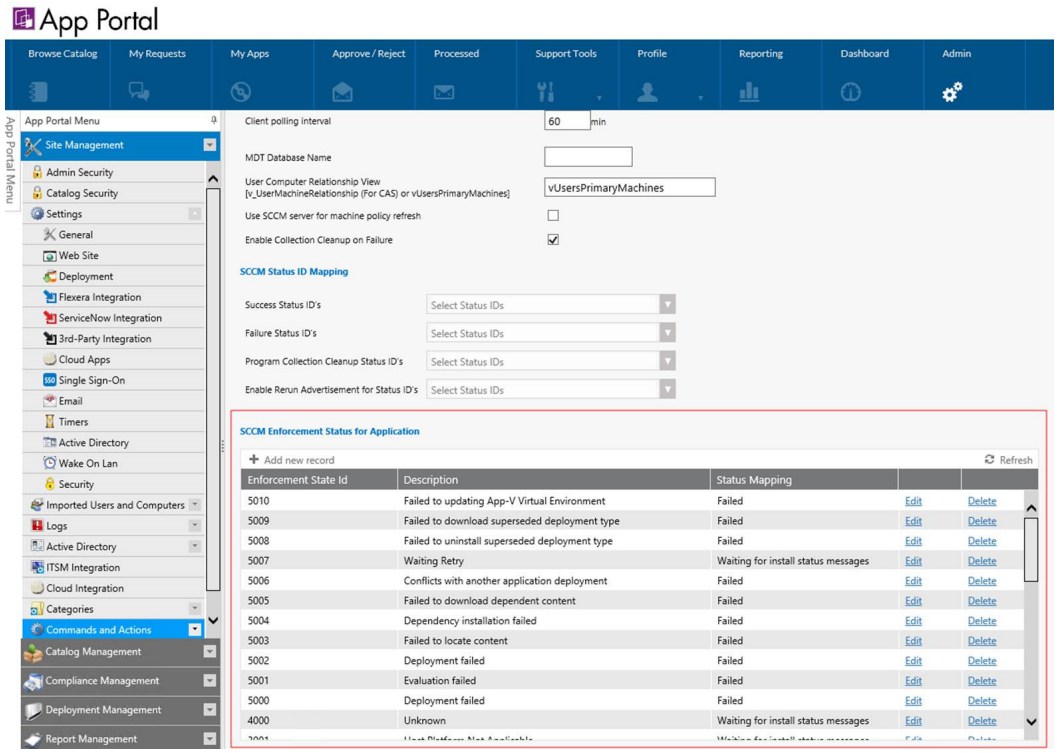
- On the **Status** pop-up dialog box (which opens when you click the **Pending Deployment** icon in the **Status** column of the **My Requests** tab):




- The **Status** column of the **Status** tab of the **Request Details** dialog box:




- In a new **SCCM Enforcement Status for Application** grid available on the **ConfigMgr** tab in **Site Management > Settings > Deployment**:

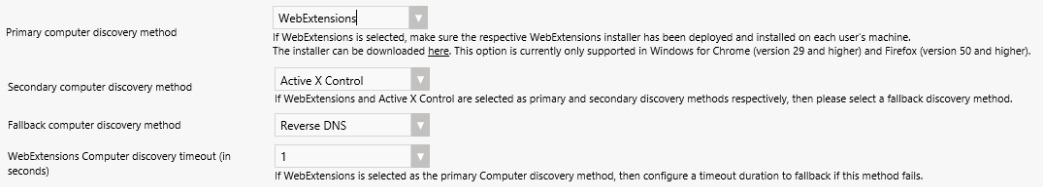



# New Computer Discovery Method: WebExtensions

App Portal has several computer discovery methods to determine a user's computer name. In App Portal 2017 R2, a new discovery method is now supported in Chrome for Windows (version 29 and higher) and Firefox for Windows (version 50 and higher) using web extensions. Support for using web extensions as the computer discovery with Microsoft Edge will be added 2017 R2 SP1 (see Support for Microsoft Edge Browser for Device Detection using Web Extensions). In addition, 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.

To enable this functionality, App Portal has added a **WebExtensions** option to the **Computer discovery method** drop-down list (on the **General** tab of the **Site Management > Settings > Web Site** view).

***Note*** • *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 needs 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.*




As background, when a user visits App Portal, App Portal is aware of the context of who the user is but the device is initially unknown. The previous options available in App Portal each had its own limitations, as detailed in the following table.

**Table 3** • Discovery Methods App Portal uses to Identify Device of User accessing App Portal

| Computer discovery method | Limitations |
|---|---|
| **ActiveX** | Only fully supported in Internet Explorer. Also, moving forward Microsoft has dropped support for ActiveX in their Edge browser. |
| **Reverse DNS** | This is a slow process and unreliable particularly if connected through VPN or wirelessly. |
| **SCCM** | Assumes System Center Configuration Manager is updated and assumes Data Sync is complete. |
| **Active Directory** | Retrieves only computers managed by the user. |

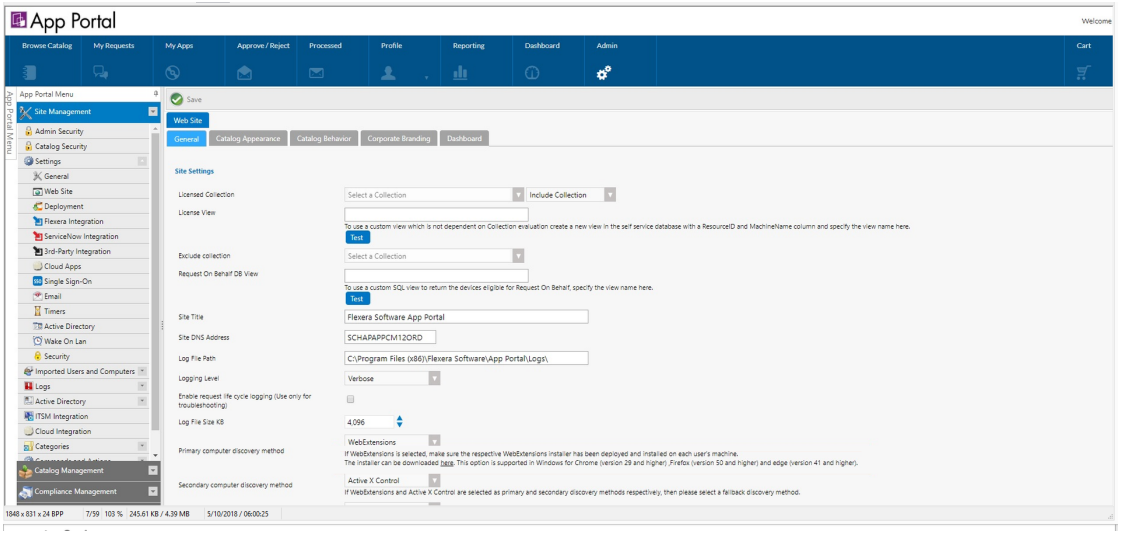
The way App Portal utilizes Chrome for Windows or Firefox for Windows web extensions is as follows. Enterprise users of Chrome and Firefox have web extensions installed that communicate with the host application installed on the client machine. The host application relays the user's machine name to the browser extension which in turn relays the information to App Portal. From here, App Portal sends the information to the App Portal Application Server where further processing can then be done. This gives App Portal the machine name.

In addition to the **WebExtensions** being added as an option the **Primary computer discovery method** drop-down list, the following fields have also been added to support the new **WebExtensions** option:

- **Secondary computer discovery method**—If the **Primary computer discovery method** fails, the secondary discovery method will be used. If the **Secondary computer discovery method** fails, the fallback discovery method will be used.

  ***Note*** • *If **WebExtensions** and **Active X Control** are selected as primary and secondary discovery methods respectively, then you should enter a fallback discovery method in the **Fallback computer discovery method** field to account for a scenario where the primary and secondary discovery methods may not be not applicable.*

- **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.




# 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 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 should 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)

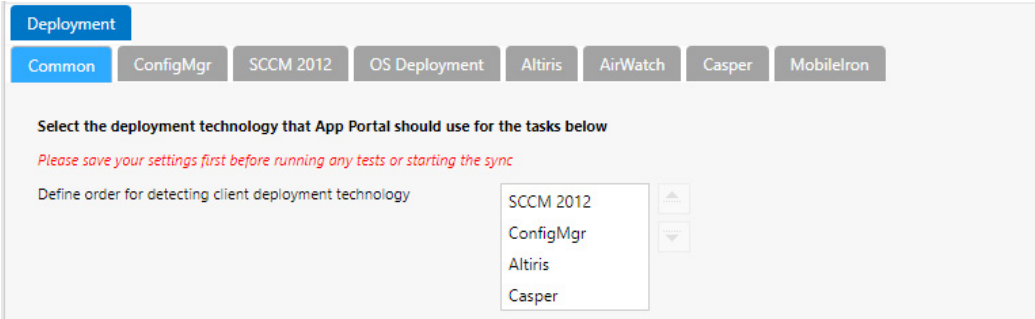
Administrators that are deploying `App Portal WebExtensions.msi` to enterprise user machines need to provide their respective Uniform Resource Identifier (*URI*) in the `APPPORTAL_CHROME_UPDATES_`*`URI`* property. App Portal sets the default value of this property to **http://*localhost*/esd/Downloads/Chrome/WebExtensions/UpdateXML.aspx**. Administrators need to swap ***localhost*** with their respective App Portal host name.

# Important Information

## End-of-Life Support for System Center Configuration Manager 2007

Because end-of-life support for System Center Configuration Manager 2007 (SCCM 2007) has been reached, App Portal 2017 R2 has removed support for System Center Configuration Manager 2007. As a result of this change:

- App Portal Administrators and end users will no longer see references to System Center Configuration Manager 2007. All references have been removed from the App Portal interface. For example, When you select **Settings** under **Site Management** on the **Admin** tab, you will notice that the **Deployment > SCCM 2007** subtab has been removed.




- All APIs that were exposed for System Center Configuration Manager 2007 have been removed.

***Important*** • *If you are still planning on using System Center Configuration Manager 2007, it is recommended that you remain on App Portal 2017 R1 or earlier.*

# Resolved Issues

This section lists the customer issues that were resolved in the following versions of App Portal / App Broker:

- App Portal / App Broker 2017 R2 SP1
- App Portal / App Broker 2017 R2

## App Portal / App Broker 2017 R2 SP1

The following table lists the customer issues that were resolved in App Portal / App Broker 2017 R2 SP1:

| Issue | Description |
|---|---|
| **IOJ-1874971** | If the status for a request does not change for 168 hours (the default value for the setting FailRequestsAfterHoursStatus), App Portal is not automatically failing the request for Task sequences. |
| **IOJ-1872892** | In some Mac environments, syncing occurs twice: once from SCCM and another time from Casper. Now, if there are Mac machines which are present in Casper but they are getting synced first from System Center Configuration Manager (SCCM), App Portal will not sync a second time from Casper. |
| **IOJ-1872854** | App Portal cannot add user to Security group of an External forest to a Catalog item request. |
| **IOJ-1872100** | When canceling a request, devices are not being removed from static groups. |
| **IOJ-1871567** | Computer discovery is picking the first machine from list instead of giving user an option to select the computer. For example, if a user logged in from a MAC machine then App Portal is discovering the Windows machine instead of the MAC machine. |
| **IOJ-1871057** | Catalog items cannot be created for Casper. |
| **IOJ-1869989** | FlexNet Manager Suite connections are failing in multi-tenant environments. |
| **IOJ-1868506** | Catalog items with FlexNet Manager Suite UIDs are not opening if FlexNet Manager Suite is down or under a heavy load. |
| **IOJ-1868046** | When customer clicks a status icon to get detailed application status. the status is not being returned. |
| **IOJ-1867368** | When an MSI's architecture is set to 64-bit, attempts to install the MSI to a 32-bit machine results in an error message stating that “the package is not compatible with this architecture.” |
| **IOJ-1866501** | When requests were configured to be cleaned up from collections, detailed status messages are not being displayed. |

| Issue | Description |
|---|---|
| **IOJ-1866263** | Catalog item pricing is not showing correctly when browser is localized to a different language. |
| **IOJ-1864850** | The **My Requests** details view does not get displayed after an upgrade. |
| **IOJ-1864843** | Devices are not getting cleaned from the collection on a successful install when the browser language is in non-English locale. |
| **IOJ-1864528** | In App Portal 2017 R2 if th FlexNet Manager Suite UID is set in the **WD_Webpackages** table to **CheckFNMPLicensePosition=0** and **CheckFNMPAdvanceLicense=NULL**, it still attempts to connect to the FNMS Server |
| **IOJ-1864522** | Starting in App Portal 2017 R2, **General** catalog items no longer require a device target. Prior to App Portal 2017 R2 SP1, there was no way to disable a feature. If your environment requires disabling of this feature, contact Flexera Technical Support for assistance. |
| **IOJ-1859936** | Sync is failing with 'violation of unique key constraint' error for Casper devices, when devices have the same name but different serial numbers. |
| **IOJ-1859860** | Casper computer sync fails if computer record has no name. |
| **IOJ-1858820** | App Portal SSO integration failure: After SSO integration with Azure Active Directory, App Portal is not able to parse the SAML response generated by the Azure Active Directory when attempting to implement SAML. |
| **IOJ-1857577** | **MyApps** page does not display strings for English locale. |
| **IOJ-1857429** | In the **Request From A Particular Target User** report, all the catalog items are getting displayed irrespective of the user clicked instead of showing only catalog items that are based on the target user selected. |
| **IOJ-1857342** | WebExtensions support missing for Microsoft Edge browser. This has been added in 2017 R2 SP1. See Support for Microsoft Edge Browser for Device Detection using Web Extensions. |
| **IOJ-1857012** | Get Machines List calls are failing intermittently resulting in users being unable to checkout software. |
| **IOJ-1854184** | When attempting to use the **UpdateCatalogImage** method to update an existing icon, that icon does not get updated. |
| **IOJ-1850774** | Casper user computer mappings should have an option to be done through user names. |
| **IOJ-1817712** | AppPortal immediately issues Failed status instead of waiting for 168 hours threshold time set at Global level. |

| Issue | Description |
|---|---|
| **IOJ-1773326** | Applications with requirements remain in pending status. If a status of “requirements not met” is received, App Portal should wait a configurable period of time, and then fail the request. |
| **IOJ-1770684** | Mandatory advertisement setting is not being set for applications.<br> <br>***Note*** *• An updated Web Service setup for the service pack* ***AppPortalWebServiceSetup_2017_R2_SP1.exe*** *is included with this release. This needs to be installed for this issue to be resolved.* |
| **IOJ-1753133** | Statuses pulled into App Portal relate to either success or failure only instead of providing all statuses provided by SCCM. |
| **IOJ-1738346** | Currently the Success, Failure, cleanup and enable rerun Status IDs only applies to Packages and/or task sequences. App Portal needs to provide the same ability for Applications. |
| **IOJ-1815852** | Violation of Unique Key Constraint in **Datasync.log** for Casper Machines. |
| **IOJ-1874914** | My Apps Process alerts causes FNMS application pool to crash. |
| **IOJ-1873986** | Problem adding computers to security groups for General catalog items. |

# App Portal / App Broker 2017 R2

The following table lists the customer issues that were resolved in App Portal 2017 R2.

| Issue | Description |
|---|---|
| **IOJ-1851773** | Previously, if the email address stored in ServiceNow of a user requesting software did not match any user in App Portal, the Validate Request Data work flow step was returning an Invalid Response 500. This scenario has been resolved so that the API responds with empty data, and since no user info indicates invalid user, the HTTP status code is now 200. |
| **IOJ-1840525** | App Portal 2017 supports FNMS 9.2 SP1 or later. An issue has been resolved that was causing the following error to be issued when clicking **Test** on the on the **Site Management > Settings > Flexera Integration** view on the **Admin** tab:<br>`Missing FNMS Required View ID -120000` |
| **IOJ-1851053** | When upgrading from older versions of the App Portal, administrators get unexpected errors when accessing catalog items, including templates, or when attempting to create a new catalog items. |

| Issue | Description |
|---|---|
| **IOJ-1841990** | An issue has been resolved that was causing the User Computer Map Sync for CAS environment to use incorrect settings. No user or computer mappings were being imported from the CAS environment, despite the Primary User being displayed when checking manually in System Center Configuration Manager. |
| **IOJ-1823584** | When Admin Studio creates an App Portal Catalog item for a package, it calls the API CreateSoftwareCatalogForPackage(). After this API is called, and the catalog item is checked out, there were errors when attempting to add the item to the cart. This issue was only happening packages, and not applications but has since been resolved. |
| **IOJ-1818701** | Web service `API PublishCatalogItemForPackage()` was not creating a row in `WD_Package_Deployments`. With this issue resolved, fully functional catalog items are being created by `PublishCatalogItemForPackage()`. |
| **IOJ-1817887** | After scheduling a request for a catalog item which requires a user readiness record, the readiness record in WD_userReadiness was not being updated with the requestID for the matching request. This has been resolved. |
| **IOJ-1752948** | In App Portal 2017 R2, **General** catalog items no longer require a device target. For more information, refer to Target Device No Longer Required when Requesting General Catalog Items. |
| **IOJ-1851905** | An issue has been resolved that was causing the The **My Apps** tab to be blank with no pie chart, alerts, or installed applications displaying. |
| **IOJ-1841456** | An issue with Custom User DataSync has been resolved that was causing the following error:<br>`Unclosed quotation mark after the character string ' '.` |
| **IOJ-1818566** | An issue with **Admin > Deployment Management > User Readiness** has been resolved that was resulting in the following error:<br>`Column 'ReadyID' does not belong to table` |
| **IOJ-1777562** | A problem with a query App Portal was using to get policies has been resolved. `Altiris - spResourceTargetDeltaUpdate` was not being called, resulting in delays in deployment. |

# Upgrading to App Portal 2017 R2

When upgrading an existing version of App Portal to App Portal 2017 R2, it is very important that you review the following information **before** you begin the upgrade.

- Supported Upgrade Versions
- Planning Your Upgrade
- Upgrade Notes

## Supported Upgrade Versions

You can only upgrade to App Portal 2017 R2 from the following previous versions:

- App Portal 2017
- App Portal 2016
- App Portal 2015 R2
- App Portal 2015
- App Portal 2014

To upgrade from one of these supported versions to App Portal 2017 R2, use the App Portal 2017 R2 installer, which can be downloaded from the Flexera Software Product and License Center.

***Important** • If you want to upgrade an installation of App Portal 2013 R2 or earlier to App Portal 2017 R2, you must first upgrade to 2015 R2 or 2016, and then upgrade to 2017. For assistance, contact a member of the Flexera Software Global Consulting Services team.*

## Planning Your Upgrade

When performing your upgrade to App Portal 2017 R2, it is recommended that you include the following steps in your upgrade process:

- **Review the Release Notes**—Thoroughly review this document, the App Portal 2017 R2 SP1 Release Notes.
- **Backup your database**—Prior to upgrading, you need to back up your existing App Portal database. It will not be backed up automatically by the installer. even if you are performing a "fresh" install on an existing database.
- **Backup user interface customizations**—If you have customized your App Portal user interface, back up this directory of files before performing the upgrade:

  `[AppPortalInstallationDirectory]\Web\App_Themes\Flexera`

- **Upgrade and test in a lab environment**—Before rolling out the App Portal upgrade in production, first upgrade App Portal in a lab environment using a clone or subset of your production data and test it thoroughly to make sure it still operates as per your requirements.
- **Production rollout**—When you are ready to roll out the App Portal upgrade to your production environment, it is recommended that you include the following steps:

  **a.** Backup your existing App Portal database.

  **b.** Take a snapshot of the App Portal server, if possible.

  **c.** Provide downtime notice to your end users.

  **d.** Schedule your service window to allow for adequate testing post-production upgrade.

  **e.** Test your recovery model.

## Upgrade Notes

Please note the following regarding upgrading from earlier versions of App Portal:

- **Upgrading the App Portal Web Service**—Upgrading the existing App Portal instance will not upgrade the existing App Portal Web Services application. You need to manually run the `AppPortalWebServiceSetup_2017_R1.exe` installer on your System Center Configuration Manager machine.
- **App Portal logo not being displayed after upgrade**—If you have a problem loading the App Portal logo (which is the default logo provided by App Portal) after upgrading, then you need to manually change the following `AppSetting` entry in the `WD_AppSettings` table from "`CompanyLogoURL`" to "`/esd/Images/ap-logo.jpg`". However, if you are going to be using a custom logo, there is no need to perform this step.
- **My Apps scheduled tasks now run under Service Account**—Starting with App Portal 2017, the My Apps-related scheduled tasks (**App Portal - Process Computers for My Apps Alerts** and **App Portal - Send out My Apps Email Notifications**) will run under the Service Account instead of the System Account. However, if you are upgrading from a previous version, you need to manually change the account that those scheduled tasks will run under; the App Portal installer will not makes these changes.
- **Microsoft .NET Framework 4.6.1**—You should make sure that Microsoft .NET Framework 4.6.1 is installed prior to upgrading an existing installation of App Portal. Microsoft .NET Framework 4.6.1 is not bundled with the installer.

# Applying the 2017 R2 Service Pack 1 to App Portal 2017 R2

To apply the App Portal 2017 R2 Service Pack 1 to an installation of App Portal 2017 R2, perform these steps.

***Task*** ***To apply the 2017 R2 Service Pack 1 to App Portal 2017 R2***

1. Log on to the **Flexera Software Product and License Center** and download the following file:

   `App Portal 2017 R2 Cumulative Service Pack 1.exe`

2. Copy this file to the machine where App Portal 2017 R2 is installed.
3. Double-click on the file to launch the installer. The **Welcome** panel of the **App Portal 2017 R2 Cumulative Service Pack 1** wizard opens.

   A message box opens, stating that a previous installation of App Portal 2017 R2 was detected.

4. Click **OK** to close the message box. The **Next** button on the wizard is enabled.
5. Click **Next**. The **Release Notes** panel of the wizard opens, listing the customer issues that were resolved in this Service Pack.
6. Click **Next**. The **Ready to Install the Program** panel opens.
7. Click **Install**. Progress messages are displayed while the Service Pack is installed. When installation is complete, the **InstallShield Wizard Completed** panel opens.
8. Click **Finish.**

# System Requirements

This section lists the system requirements for App Portal / App Broker:

- Environment Requirements
- Client Requirements
- Server Requirements
- Supported Deployment Technologies
- Supported ITSM Systems
- Supported Cloud Applications

# Environment Requirements

Prior to beginning App Portal / App Broker installation, make sure that your environment meets or is able to meet the following requirements:

| Requirement | Description |
|---|---|
| **Active Directory** | Microsoft Active Directory is required for App Portal / App Broker. It is fully supported under Windows Server 2008 R2 or later domains operating at all functional levels. |
| **DNS** | If you choose **Use Reverse DNS** as a computer discovery method during App Portal installation, a DNS service is required that supports and contains Reverse DNS Zones. |
| **Database Software** | Microsoft SQL Server 2008 R2 or later, including Microsoft SQL Server 2016.<br>• **Collation setting**—`SQL_Latin1_General_CP1_CI_AS` is the required collation setting for App Portal database server. it is the only supported collation. |
| **SMTP Compatible Mail System** | App Portal / App Broker requires an SMTP-compatible mail system, and supports both local and remote SMTP servers. |
| **Internet Information Server (IIS)** | App Portal / App Broker supports the versions of IIS that are installed with Windows Server 2012 or later,<br>The IIS Application Server and Web Server roles need to be installed.<br>App Portal / App Broker is installed into a virtual directory named `ESD` and is accessible using `http://alias/ESD`.<br>A DNS A-RECORD must be created to access the site if you wish to use an alias. |
| **Integrated Authentication** | App Portal / App Broker uses a user's current Active Directory credentials to authenticate to IIS/App Portal / App Broker. |

| Requirement | Description |
| --- | --- |
| **Active Directory User Discovery** | Active Directory User Discovery must be enabled in System Center Configuration Manager and/or Altiris Client Management Suite for App Portal / App Broker to function properly. Additional Active Directory User Discovery extensions are also required.<br><br>Extend the attributes using the Active Directory User Discovery method in the System Center Configuration Manager Console and/or Altiris Management Console. Include the following attributes in addition to the existing ones if performing manually:<br><br>`mail`<br>`department`<br>`title`<br>`displayName`<br>`distinguishedName`<br>`manager`<br>`company`<br>`l (lower case L) (Only enter the letter l!)`<br>`postalCode`<br>`sn`<br>`givenName`<br>`physicalDeliveryOfficeName`<br><br> <br><br>***Important*** • *This is only required if you are using standard discovery from System Center Configuration Manager or Altiris. If you are providing a custom SQL script to perform user and computer discovery, these steps are not required.*<br><br> <br><br>***Caution*** • *The user discoverable attribute displayName is required to be extended in System Center Configuration Manager and/or Altiris Client Management Suite. This needs to be done before performing the user and computer sync process or the process will fail.* |
| **High Speed Connection** | The IIS server should be on the same physical network as the database server, and should be connected at a high speed (greater than or equal to 100 MBit). |

# Client Requirements

The following are the App Portal client requirements:

| Requirement | Description |
| --- | --- |
| **Desktop Operating Systems** | • Windows 7 or greater<br>• Mac OS X 10.7.x or greater<br> <br>***Note*** • *To deploy software to a device using App Portal / App Broker, the device needs to be managed by Microsoft System Center Configuration Manager, Symantec Altiris, or Casper.* |
| **Mobile Operating Systems** | • Google Android<br>• iOS<br>• Windows Phone<br> <br>***Note*** • *To deploy mobile apps using App Portal / App Broker, the device needs to be registered and managed by AirWatch or MobileIron.* |
| **Browser** | App Portal / App Broker supports the following browsers:<br>• **Microsoft Internet Explorer 9.0 or greater**—App Portal / App Broker requires that the client's web browser be Internet Explorer 9.0 or greater; however Internet Explorer 10 or 11 or Microsoft Edge are preferred for the best experience.<br>• **Firefox, Chrome**—App Portal / App Broker also supports Firefox and Chrome browsers; however these browsers do not support Active X and therefore will always discover the computer using the Reverse DNS discovery method.<br> <br>***Note*** • *The fall back to ReverseDNS on these browsers is only done if ActiveX is the primary computer discovery method chosen. If the discovery method is set to SCCM, then App Portal / App Broker will honor that for all browsers.* |
| **Trusted Sites** | The App Portal / App Broker web site must be added to the trusted sites list for Internet Explorer. For example:<br>`http://APPPORTALSERVER`<br> <br>***Important*** • *This is very important.* |

# Server Requirements

The following are the server requirements for the App Portal / App Broker Web Service and the App Portal / App Broker installation platform:

- App Portal / App Broker Web Service Server
- App Portal / App Broker Installation Platform
- Setting Permissions: App Portal Service Account

## App Portal / App Broker Web Service Server

The following are the system requirements for the servers where the App Portal / App Broker Web Service is installed:

| Requirement | Description |
|---|---|
| **Authentication** | Windows Authentication |
| **Microsoft .NET Framework** | Microsoft .NET Framework 2.0 SP1 or later is required on all primary sites. |
| **IIS** | App Portal / App Broker supports the versions of IIS that are installed with Windows Server 2008 R2 or later.<br>The IIS Application Server and Web Server roles need to be installed. |
| **ASP.NET** | ASP.NET needs to be installed. |

The instructions for installing the App Portal / App Broker Web Service depends upon your deployment technology:

- **For System Center 2012 Configuration Manager and System Center Configuration Manager (Current Branch)**, the App Portal / App Broker Web Service is only needed at the CAS or Central site.

  For System Center 2012 Configuration Manager and System Center Configuration Manager (Current Branch), folders will be created called `App Portal Users For Site XXX` and `App Portal Computers for site XXX`.

- **For System Center 2007 Configuration Manager**, the App Portal / App Broker Web Service must be installed on every primary site server in order to service the System Center Configuration Manager clients at that site.

  Therefore, you are required to run the `AppPortalWebServiceSetup.exe` on each primary site, confirming the local server name and System Center Configuration Manager SQL Database of the primary site server. A default System Center Configuration Manager Collection called `App Portal Collection for Site XXX` will be created on each primary site. This collection will be populated as necessary to service the clients that report to that site.

  For System Center 2007 Configuration Manager, an advertisement folder called `App Portal Advertisements for Site XXX` will be created to contain the advertisements created by App Portal / App Broker.

### App Portal / App Broker Installation Platform

The App Portal / App Broker installation platform must meet the following requirements:

| Requirement | Description |
|---|---|
| **Authentication** | Windows Authentication |
| **Operating System** | Windows Server 2012 or later |
| **IIS** | App Portal / App Broker supports the versions of IIS that are installed with Windows Server 2012 or later.<br><br>The IIS Application Server and Web Server roles need to be installed. |
| **Microsoft .NET Framework** | Microsoft .NET Framework 4.6.1 or later |
| **ASP.NET** | ASP.NET needs to be installed. |

### Setting Permissions: App Portal Service Account

App Portal requires that you identify an account (App Portal service account) to use for the interaction with SQL and Active Directory. The App Portal service account will require administrative permissions on the client workstations if you wish App Portal to successfully run machine policy evaluation for accelerated software deployments and rerunning advertisements as necessary.

The service account must have Read permission on the Microsoft System Center Configuration Manager or Altiris Client Management database in SQL and Read/Write permission on the App Portal database that gets created during the installation process. The Installer Account will attempt to provision the Service Account with `DB_DataReader` permissions to the SCCM database and DBO permissions to the App Portal database.

# Supported Deployment Technologies

App Portal / App Broker 2017 R2 SP1 supports the following deployment technologies for software distribution:

- Microsoft System Center Configuration Manager (Current Branch 1710)
- Microsoft System Center 2012 Configuration Manager
- Altiris Client Management Suite 7.1 or later
- AirWatch 9.1.2.4 (for mobile application deployment)
- JAMF Casper Suite 9.6.4
- MobileIron 9.2

***Note*** • *App Portal supports JAMF Casper Suite 9.6.4 on premises version; the cloud version is not supported. Inventory can be collected from Macintosh computers running OS X 10.7.x or later.*

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

- Provide a seamless end user experience while you are upgrading from older versions of System Center Configuration Manager to System Center Configuration Manager (Current Branch).
- Present a single instance to your users even if your organization uses both System Center Configuration Manager and Altiris deployment technologies across your enterprise.
- Provide your users with a universal app store containing both desktop and mobile applications.

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

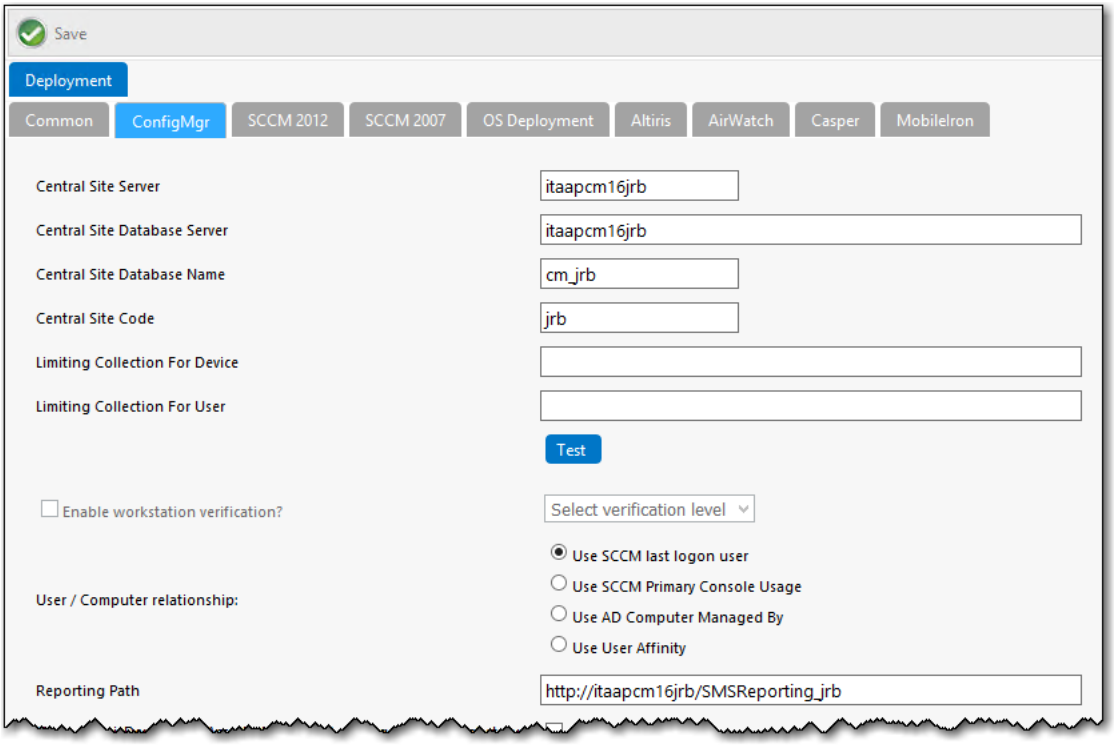



**Figure 2:** Site Management > Site Settings > Deployment Tab

App Portal / App Broker 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 the **Site Management >Settings > Deployment** tab. The following table describes the acceptable hierarchical relationships for the three deployment technologies:

| Technology | Description |
|---|---|
| **System Center Configuration Manager (Current Branch)**<br>**System Center 2012 Configuration Manager** | **Single Primary Site OR Central Administration Site > Child Primary Sites**<br>For System Center Configuration Manager (Current Branch) or System Center 2012 Configuration Manager, App Portal / App Broker 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). |

| Technology | Description |
| --- | --- |
| **Altiris Client Management Suite 7.1 or later** | **Single Primary Site OR Central Site > Child Primary Sites**<br>For Altiris. App Portal / App Broker 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 / App Broker 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 4.6.1 is required to be installed on the IIS server in order to run the App Portal / App Broker service and web site. This is not required when using Altiris Client Management Suite.*

# Supported ITSM Systems

Both App Portal and App Broker include out-of-the-box support for integrating with ITSM systems.

## App Portal

App Portal 2017 R2 SP1 provides support for the following ITSM systems:

- ServiceNow (versions: Helsinki, Istanbul, and Jakarta)
- BMC Remedy IT Service Management Suite

When App Portal's ServiceNow or BMC 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.

***Note*** • *If you would like to integrate with an ITSM system other than ServiceNow or BMC Remedy, you can use App Portal's reusable framework to connect to and configure integration to that system.*

## App Broker Software for ServiceNow

With App Broker Software for ServiceNow 2017 R2 SP1, you can publish App Portal catalog items in the ServiceNow catalog. This enables ServiceNow users to request software directly in the ServiceNow self-service portal, with App Portal performing the license check and automated deployment. Using App Broker Software for ServiceNow, you can also submit a request for OS deployment and/or application migration from within the ServiceNow user interface, using a custom **Employee App Provision Request** wizard.

***Important*** • *To use App Broker Software for ServiceNow, you must have a ServiceNow MID Server that has access to the App Portal / App Broker REST APIs.*

***Important** • In order for the out-of-the-box App Broker Software for ServiceNow workflow to function, you must have also purchased FlexNet Manager Suite and connected it to App Portal.*

### App Broker Software for BMC

With App Broker Software for BMC 2017, 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. Using App Broker Software for BMC enables you to provide your employees with a single service portal for all request types: software, hardware, and other IT services.

***Important** • In order for the out-of-the-box App Broker for BMC workflow to function, you must have also purchased FlexNet Manager Suite and connected it to App Portal.*

## Supported Cloud Applications

App Portal / App Broker 2017 R2 SP1 provides out-of-the-box support for the following cloud applications:

- Box
- Salesforce
- Microsoft Office 365

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.

If you connect App Portal / App Broker to one of these cloud applications, App Portal / App Broker can offer a catalog item that will automatically create an account for the requester in that cloud application.

# Legal Information

### Copyright Notice

Copyright © 2018 Flexera.

This publication contains proprietary and confidential information and creative works owned by Flexera Software LLC and its licensors, if any. Any use, copying, publication, distribution, display, modification, or transmission of such publication in whole or in part in any form or by any means without the prior express written permission of Flexera Software LLC is strictly prohibited. Except where expressly provided by Flexera Software LLC in writing, possession of this publication shall not be construed to confer any license or rights under any Flexera Software LLC intellectual property rights, whether by estoppel, implication, or otherwise.

All copies of the technology and related information, if allowed by Flexera Software LLC, must display this notice of copyright and ownership in full.

## Intellectual Property

For a list of trademarks and patents that are owned by Flexera Software, see http://www.flexerasoftware.com/intellectual-property. All other brand and product names mentioned in Flexera Software products, product documentation, and marketing materials are the trademarks and registered trademarks of their respective owners.

## Restricted Rights Legend

The Software is commercial computer software. If the user or licensee of the Software is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the Software, or any related documentation of any kind, including technical data and manuals, is restricted by a license agreement or by the terms of this Agreement in accordance with Federal Acquisition Regulation 12.212 for civilian purposes and Defense Federal Acquisition Regulation Supplement 227.7202 for military purposes. The Software was developed fully at private expense. All other use is prohibited.