FLEXEra

App Portal / App Broker 2018 R1

Installation Guide

Legal Information

Book Name:	App Portal / App Broker 2018 R1 Installation Guide
Part Number:	APPAPB-2018R1-IG00
Product Release Date:	October 2018

Copyright Notice

Intellectual Property

Restricted Rights Legend

Contents

Contents

1

App Portal / App Broker 2018 R1 Installation Guide

The App Portal / App Broker 2018 R1 Installation Guide explains how to setup and install the web site and the web service, and how to perform post-configuration tasks.

Instructions for installing App Portal / App Broker are presented in the following sections.

Table 1-1 • App Portal / App Broker 2018 R1 Installation Guide

Section	Description
Preparing to Install App Portal / App Broker	Lists the system requirements, and provides a list of steps that you need to take prior to installation.
Installing App Portal / App Broker	Explains how to run the App Portal / App Broker installer.
Installing the App Portal Web Service	Explains how to run the App Portal / App Broker Web Service installer.
Upgrading the App Portal Web Site	Explains how to upgrade an existing installation of App Portal.

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

Contacting Us

Flexera 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.flexera.com

2

Preparing to Install App Portal / App Broker

This chapter lists system requirements and steps you need to take prior to installing App Portal / App Broker.

- App Portal / App Broker Overview

- System Requirements

- Pre-Installation Checklist

- Preparing the App Portal / App Broker Web Site

App Portal / App Broker Overview

App Portal / App Broker provides users with a familiar and easy-to-use storefront to request software automatically from System Center Configuration Manager, Altiris Client Management Suite, JAMF Casper, VMware AirWatch, and MobileIron. You can use App Portal / App Broker to facilitate any type of request including software, OSD images, service packs, computers, and office supplies. You can also use App Portal / App Broker to request access to cloud applications such as Salesforce or Office 365. App Portal / App Broker uses approval and inventory management policies to ensure requests are secure and receive the proper approval.

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.

- Important Points to Consider Prior to Installation

- Getting Support for App Portal / App Broker

- App Portal / App Broker Installation Files

Important Points to Consider Prior to Installation

To have the most productive experience using App Portal / App Broker, review this guide in entirety and consider the following points before performing the installation:

- **Supported upgrade versions**—You can only upgrade to App Portal / App Broker 2018 R1 from the following previous versions:

  - App Portal 2017 R2

  - App Portal 2017

  - App Portal 2016

  - App Portal 2015 R2

  - App Portal 2015

  - App Portal 2014

  For more information, see Upgrading the App Portal Web Site.

- **App Portal / App Broker obtains data from Active Directory as well as your deployment system**—App Portal / App Broker obtains its data from Active Directory as well as your deployment system. User data is refreshed when the Active Directory User Discovery is run. Be sure to schedule this process to run at regular intervals.

- **Four user-to-computer relationship methods**—App Portal / App Broker creates its user-to-computer relationship using one of four methods: last logon, primary console, managed by, and user affinity [for System Center 2012 Configuration Manager and System Center Configuration Manager (Current Branch) only]. Please review and understand what the most effective and reliable method will be for you.

- **App Portal / App Broker Web Service requirement on primary sites**—App Portal / App Broker requires that the App Portal / App Broker Web Service be installed on:

  - **System Center Configuration Manager (Current Branch)**—At the Single Primary site or the CAS Site (if present)

  - **System Center 2012 Configuration Manager**—At the Single Primary site or the CAS Site (if present)

  - **Altiris**—Not required, but ASDK should be enabled.

  - **Casper and AirWatch**—Not required.

- **Service account and DNS alias requirement**—App Portal / App Broker requires a service account and DNS alias established prior to beginning the installation.

- **SysAdmin permissions required**—The installer account and the upgrader account need to have SysAdmin permissions on the SQL Server. This account needs permission to create the App Portal / App Broker database, and also to assign the service account with `DB_DataReader` and `Execute` permission on the deployment technology database and database owner permission on the App Portal / App Broker database during installation.

  Important • The App Portal / App Broker service account must have database owner permission to read/write to the App Portal / App Broker database even after the installation is complete.

Getting Support for App Portal / App Broker

App Portal / App Broker is fully supported by its support staff during your evaluation process and post-sales. You can contact Flexera Software technical support by visiting the Customer Community site at:

https://flexeracommunity.force.com/customer/

When contacting technical support, please provide following information:

Table 2-1 • Required Support Information

Information	Description
Log Files	Include the log files from the Logs directory: • `C:\Program Files (x86)\Flexera Software\App Portal\Logs` • `C:\Program Files (x86)\Flexera Software\AppPortalWebService\Logs` (from the Primary Sites) 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 use the debug logging feature, which can be enabled on the **Site Management > 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 / App Broker web site. *Important • Because debug logging slows down the system considerably, it should only be turned on when performing troubleshooting, preferably before App Portal / App Broker is in a production environment.*
Description	Include a detailed description of the problem including: • Expected behavior • Desired behavior • User experience
Environmental Factors	List the environmental factors that may be unique to you including: • Client firewalls • System lockdown • Anything else that you may think contributes
Steps to Reproduce	Include a detailed list of the steps to follow to reproduce the problem you are experiencing.

App Portal / App Broker Installation Files

These App Portal / App Broker installation files can be downloaded from the Flexera Software Product and License Center. The files that you need to download depend upon whether you are upgrading an existing installation of App Portal or installing App Portal / App Broker for the first time.

Table 2-2 • App Portal / App Broker Installation Files

Files Needed	Purpose
`AppPortalSetup_2018_R1.exe`	Use to both install the App Portal / App Broker web site for the first time, and also use to upgrade a previously installed version.
`AppPortalWebServiceSetup_2018_R1.exe`	Use to install the App Portal / App Broker web service on the deployment technology machine.
`FlexeraServiceGateway2.exe`	Use to install the Flexera Service Gateway.
`App Portal ActiveX Control for Internet Explorer.msi`	Use to install the Active X control for Internet Explorer (if you are prompted).
`Flexera Software AppBroker 2018 R1 Update Set.xml`	If you have purchased App Broker Software for ServiceNow, download this update set `.xml` file. You will import it into your ServiceNow instance. *Note • If you are an existing App Broker for ServiceNow 2016 customer and want to upgrade your ServiceNow instance to App Broker for ServiceNow 2017, contact Flexera Software Technical Support.*

Note • The App Portal / App Broker user documentation, in both PDF and HTML format, can be accessed on the Flexera Software HelpNet site:

http://helpnet.flexerasoftware.com/appportal

System Requirements

App Portal / App Broker requires certain systems configurations in order to function properly. These requirements are exact and if they are not present, it will have negative effects on the installation, operation, and experience of App Portal / App Broker.

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:

Table 2-3 • Environment 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 / App Broker installation, a DNS service is required that supports and contains Reverse DNS Zones.
Database Software	Microsoft SQL Server 2012 or later, including Microsoft SQL Server 2016. - **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. The IIS Application Server and Web Server roles need to be installed. App Portal / App Broker is installed into a virtual directory named `ESD` and is accessible using `http://alias/ESD`. 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 and App Portal / App Broker.

Table 2-3 • Environment Requirements

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
department
title
displayName
distinguishedName
manager
company
l (lower case L) (Only enter the letter l!)
postalCode
sn
givenName
physicalDeliveryOfficeName
```<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>**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 / App Broker client requirements:

Table 2-4 • Client Requirements

Requirement	Description
Desktop Operating Systems	• Windows 7 or greater • Mac OS X 10.7.x or greater 📄 *Note • To deploy software using App Portal / App Broker, the device needs to be managed by Microsoft System Center Configuration Manager, Symantec Altiris, or JAMF Casper.*
Mobile Operating Systems	• Google Android • iOS • Windows Phone 📄 *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: • **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. • **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. 📄 *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: `http://APPPORTALSERVER` 📄 *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

- App Portal / App Broker Service Account Required Permissions

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:

Table 2-5 • App Portal / App Broker Web Service Server

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.
	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`.

App Portal / App Broker Installation Platform

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

Table 2-6 • App Portal / App Broker Installation Platform

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.
	The IIS Application Server and Web Server roles need to be installed.

Table 2-6 • App Portal / App Broker Installation Platform

Requirement	Description
Microsoft .NET Framework	Microsoft .NET Framework 4.6.1 or later
ASP.NET	ASP.NET needs to be installed.

App Portal / App Broker Service Account Required Permissions

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, and requires the following permissions:

Table 2-7 • 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.*

Supported Deployment Technologies

App Portal / App Broker 2018 R1 supports the following deployment technologies for software distribution:

- Microsoft System Center Configuration Manager (Current Branch)

- 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 / App Broker 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 **Site Management > Settings** > **Deployment** view, and then entering the settings on the **ConfigMgr**, **SCCM 2012**, **Altiris**, **AirWatch**, **Casper**, or **MobileIron** subtabs.

Figure 2-1: Site Management > Site Settings > Deployment

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 deployment technologies:

Table 2-8 • Hierarchical Relationships for Deployment Technologies

Technology	Description
System Center Configuration Manager (Current Branch) **System Center 2012 Configuration Manager**	**Single Primary Site OR Central Administration Site > Child Primary Sites** 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).
Altiris Client Management Suite 7.1 or later	**Single Primary Site OR Central Site > Child Primary Sites** 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 web 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 2018 R1 provides support for the following ITSM systems:

- ServiceNow (versions: Kingston and London)
- 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 2018 R1, 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 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 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 2018 R1 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.

Pre-Installation Checklist

The Pre-Installation Checklist provides you with a list of activities and questions that should be completed prior to working with Flexera Software consulting to customize an installation of App Portal / App Broker for your organization.:

Table 2-9 • Sections in the Pre-Installation Checklist

Section	Details
Recommended Configuration	Lists the version of App Portal / App Broker and hardware sizing recommendations for the App Portal / App Broker platform that will be installed.
Pre-Installation Tasks	Lists activities that should be reviewed and completed.
Information to Gather	Provides a list of items you should gather and questions you should answer.
Documents to Gather	Provides a list of documents that you should gather.

Recommended Configuration

The following table provides a summary of the recommended App Portal / App Broker configuration, including hardware sizing recommendations.

Table 2-10 • Recommended App Portal / App Broker Configuration

Component	Development / Lab Environment	Production Environment
Server Count	1	1

Table 2-10 • Recommended App Portal / App Broker Configuration

Component	Development / Lab Environment	Production Environment
Server Role	App Portal / App Broker Web Server	App Portal / App Broker Web Server
Processor	1 processor, 2 core	2 processors, 4 core
Memory (RAM)	8 GB	32 GB
Hard Disk Space	70 GB	70 GB
Database sizing recommendations	50 GB (based on estimated growth size of the deployment technology database of 500 GB)	

Note • *The App Portal / App Broker web service can only be enabled and running on a single web server at a time.*

Tip • *It is recommended that the App Portal / App Broker database reside on its own Microsoft SQL Server. It is not necessary to install App Portal / App Broker on the same SQL Server as the System Center Configuration Manager or Altiris.*

Pre-Installation Tasks

The steps provided in the checklist below are provided to help you prepare for the Flexera Software services engagement. Although Flexera Software is unable to identify every cause for delays in implementation, the checklist below greatly reduces typical delays experienced during an implementation of App Portal / App Broker.

Table 2-11 • Pre-Installation Tasks

#	Task	Task Details	Yes	No	N/A
APT01	**Download App Portal / App Broker content**	Connect to the Flexera Software Product and Licensing Center: https://flexerasoftware.flexnetoperations.com Download all of the files for the version of App Portal / App Broker that will be installed. ● App Portal Setup ● App Portal Web Service Setup ● App Portal ActiveX Control for Internet Explorer ● Flexera Service Gateway Installer ● App Broker - Service Now update set files (App Broker Software for ServiceNow only) Store the downloaded files to a UNC file share. Also, obtain the App Portal / App Broker user documentation from the Flexera Software HelpNet site: http://helpnet.flexerasoftware.com/appportal			
APT02	**Download the App Portal / App Broker license file**	Connect to the Flexera Software Product and Licensing Center to download the license file for App Portal / App Broker. Store the downloaded license file to a UNC file share.			
APT03	**Review App Portal / App Broker Installation Guide**	Review installation guide to identify any risks for the pending implementation of App Portal / App Broker.			
APT04	**Review App Portal / App Broker Release Notes**	Review the release notes to identify any risks for the pending implementation of App Portal / App Broker.			

Table 2-11 • Pre-Installation Tasks (cont.)

#	Task	Task Details	Yes	No	N/A
APT05	**Create service account**	Create a service account for App Portal / App Broker that has the following parameters: • **Deployment technology access** - Full administrator access to System Center Configuration Manager or Symantec Altiris - Read (db_datareader) and EXECUTE access to the System Center Configuration Manager or Symantec Altiris database • **App Portal / App Broker database** - Database owner (DBO) permission • **Client systems access** **Symantec Altiris**—Full administrative access to client systems is required. This is used to connect to WMI over RPC to initiate machine policy retrieval and evaluation cycles. This is also used if client-side commands and actions have been created within App Portal / App Broker. **System Center 2012 Configuration Manager or System Center Configuration Manager (Current Branch)**—Administrative access to client systems is not required.			
APT06	**Create DNS alias (optional)**	Create a DNS alias for App Portal / App Broker that users will use to connect to when they access App Portal / App Broker.			
APT07	**Add DNS alias to trusted sites (if needed)**	To ensure proper functionality of App Portal / App Broker, add the DNS alias to Trusted Sites through Active Directory Group Policy.			

Table 2-11 • Pre-Installation Tasks (cont.)

#	Task	Task Details	Yes	No	N/A
APT08	**Disable/configure firewalls**	App Portal / App Broker uses HTTP (80), SQL (1433), and RPC (to clients) to communicate between systems. If there are firewalls blocking this communication, App Portal / App Broker will not properly function. It is recommended that firewalls on App Portal / App Broker and System Center Configuration Manager systems be disabled. If corporate policy prohibits this, then exceptions are required.			
APT09	**System Center Configuration Manager hardware inventory**	Ensure that hardware inventory in System Center Configuration Manager is enabled and working correctly. It is recommended that the hardware inventory cycle occurs once every 24 hours to ensure that the data collected and used in App Portal / App Broker remains relevant and current.			
APT10	**System Center Configuration Manager software distribution**	Ensure that the software distribution in System Center Configuration Manager is working properly.			
APT11	**System Center Configuration Manager OSD (optional)**	Ensure that OSD in System Center Configuration Manager is working properly.			
APT12	**System Center Configuration Manager Active Directory discovery**	Validate that the following discovery methods are enabled within System Center Configuration Manager: • Active Directory Forest Discovery [System Center 2012 Configuration Manager and System Center Configuration Manager (Current Branch)] • Active Directory User Discovery • Active Directory Group Discovery • Active Directory System Discovery Enable any of the above mentioned discovery methods if they are presently disabled.			

Table 2-11 • Pre-Installation Tasks (cont.)

#	Task	Task Details	Yes	No	N/A
| APT13 | **Extend System Center Configuration Manager user discovery attributes** | Add the following attributes to Active Directory user discovery within System Center Configuration Manager and ensure that a full sync is run following the changes:<br><br>```
mail
department
title
distinguishedName
manager
company
l (lower case L)
postalCode
sn
givenName
physicalDeliveryOfficeName
displayName
```<br><br>**Code: Add Additional Attributes Using PowerShell (x86)**<br><br>```
CD 'C:\Program Files\Microsoft
Configuration Manager\AdminConsole\bin\'

Import-Module .\ConfigurationManager.psd1

CD XXX:

Set-CMDiscoveryMethod –
ActiveDirectoryUserDiscovery -
AddAdditionalAttribute "department",
"title", "sn", "givenName",
"physicalDeliveryOfficeName", "manager",
"company", "l", "postalCode",
"displayName"
``` | | | |
| APT14 | **Download full .NET Framework 4.6.1 (Windows Server 2008 R2 or later)** | Download the full installation of .NET Framework 4.6.1 from Microsoft's download site.

Store downloaded installation file to a UNC file share. | | | |
| APT15 | **Review Computer Browser service (optional)** | On the server that App Portal / App Broker web server will be installed, identify if the Computer Browser service is enabled. If not enabled, it is recommended that this be enabled for installation. | | | |

Table 2-11 • Pre-Installation Tasks (cont.)

#	Task	Task Details	Yes	No	N/A
APT16	**Gather installer account permissions**	The account that will be performing the installation of App Portal / App Broker must have the following permissions/rights:			
		• Local administrator rights to App Portal / App Broker web server.			
		• SQL Server Admin (SA) rights to the SQL Server where the App Portal / App Broker database will be installed.			
		Have access to file store location where the App Portal / App Broker installation files and license file are stored.			
APT17	**Verify SMTP relay functionality**	App Portal / App Broker sends email via existing Customer SMTP system. There are no configuration settings for authentication into SMTP, so the email administrator may need to create an exception to accept SMTP calls from the App Portal / App Broker web server.			
APT18	**Provision the App Portal / App Broker web server**	Based on the information provided above on server sizing, provision the App Portal / App Broker web server prior to the beginning of the services engagement.			

Information to Gather

Prior to Flexera Software consulting personnel starting the customer engagement, you should collect all of the information detailed in the table below. Having this information for day one execution of services helps reduce the risk of delays during implementation phases of the effort.

Table 2-12 • Information to Gather

Query #	Query	Response
APQ01	UNC to App Portal / App Broker installation files	
APQ02	App Portal / App Broker service account credentials	
APQ03	App Portal / App Broker web server name	
APQ04	SCCM CAS/CEN server name	
APQ05	SCCM CAS/CEN database server name	

Table 2-12 • Information to Gather

Query #	Query	Response
APQ06	SCCM CAS/CEN database SQL instance (if any)	
APQ07	Name of all SCCM primary site server(s)	
APQ08	App Portal / App Broker DNS alias	
APQ09	SMTP server name	
APQ10	Email address for App Portal / App Broker (such as `appportal@place.com`).	
APQ11	Do you have a Reverse DNS zone for Intranet?	
APQ12	Is Computer Browser service enabled?	

Documents to Gather

Prior to Flexera Software consulting personnel starting the customer engagement, you should gather the following document examples displayed in the table below. The information within the listed documents will provide the Flexera Software consulting personnel the data that they need to plan for the design of the App Portal / App Broker solution within your environment.

Table 2-13 • Documents to Gather

Doc. #	Document Type	Yes	No	N/A
APD01	Active Directory domain and forest hierarchy diagram			
APD02	System Center Configuration Manager hierarchy diagram			
APD03	Software approval process diagram			
APD04	License procurement process diagram			
APD05	Existing Flexera Software product diagrams			
APD06	Third party integration solution diagrams			
APD07	Third party integration solution API / Web Service data			

Preparing the App Portal / App Broker Web Site

To prepare the App Portal / App Broker web site, perform the following tasks:

● Enable Active Directory User Discovery and Add Attribute Extensions

- Unlock Windows Authentication in IIS for the Default Web Site in Windows Server 2008 R2, 2012, 2012 R2, 2016)

- Creating a Site Alias

- Enabling Roles and Features in Windows Server 2012 / 2016

Enable Active Directory User Discovery and Add Attribute Extensions

App Portal / App Broker collects data from discovery in your deployment system. Active Directory User Discovery must be enabled in System Center Configuration Manager, Altiris Client Management Suite, and /or Casper for App Portal / App Broker to function properly.

Additional Active Directory user discovery extensions are also required. There are twelve (12) attribute extensions that App Portal / App Broker relies on. It is necessary to inventory the additional Active Directory attributes and have them present in your deployment system before you start the user/device sync process in App Portal / App Broker.

⚠️

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 the starting the user/device sync process in App Portal / App Broker or the process will fail.*

To add Active Directory user discovery attribute extensions, perform the following steps.

Task   **To add Active Directory user discovery attribute extensions:**

1. Confirm that at least one account in the domain being inventoried has the following Active Directory attributes populated:

   ```
   DisplayName
   Email Address
   Department
   Title
   Full User Name
   User Name
   Last Name
   First Name
   Office
   Manager
   Company
   City
   Postal Code
   ```

2. Once confirmed, open the Active Directory User Discovery method in the System Center Configuration Manager Console and/or Altiris Management Console and include the following attributes in addition to the existing ones:

   ```
   displayName
   mail
   department
   title
   sn
   givenName
   ```

```
physicalDeliveryOfficeName
distinguishedName
manager
company
l (lower case L) (Only enter the letter l!)
postalCode
```

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.*

3. Initiate a discovery, and once the discovery process is complete, verify that a user account in the All Users collection has the additional attributes listed above.

Unlock Windows Authentication in IIS for the Default Web Site in Windows Server 2008 R2, 2012, 2012 R2, 2016)

In Windows Server, you need to unlock the `windowsAuthentication` section for the **Default Web Site** in IIS to allow web applications to use Windows Authentication, which is a requirement of App Portal / App Broker.

To unlock the Default Web Site option, perform the following steps.

Task   ***To unlock the Default Web Site option:***

1. Open IIS 7 Manager.

2. Select **Default Web Site** in the tree. The **Default Web Site Home** view opens.

3.   Double click **Configuration Editor**. The Configuration Editor opens.

4.   From the **Section** list, expand the tree and select `windowsAuthentication` (which is under `system.webServer >` `security > authentication`).

5. In the **Actions** panel on the right, click **Unlock Section**.

Creating a Site Alias

App Portal / App Broker operates under the security context of a service account. In order for IIS to properly authenticate a user, `it` is required that an alias (DNS A-RECORD) be established prior to installing. This ensures that there will be no authentication problems between Active Directory and IIS when the installation is complete.

Note • If, instead of specifying an alias, you want to specify the actual server name during installation, you do not need to create a DNS A-RECORD because one already exists for the server. However, if you wish to use an alias instead of the server name, a DNS A-RECORD for that alias must be created to access the site.

Enabling Roles and Features in Windows Server 2012 / 2016

If you are installing App Portal / App Broker on Windows Server 2012 or 2016, it is recommended that you perform the following steps to enable roles and features.

Task   ***To enable roles and features in Windows Server 2012 / 2016:***

1. Open the Windows Server 2012 / 2016 Server Manager.

2. Open the **Add Roles and Features** wizard.

3. Select **Server Roles** in the tree. A list of roles is displayed.

4. Under **Server Roles**, expand **Web Server (IIS) > Web Server**, and select all of the roles in the following subsections (except where noted):

   ● **Application Development**

   ● **Security**

- **Performance**

- **Health and Diagnostics** (select all subroles except **ODBC Logging**)

- **Common HTTP Features** (select all subroles except **WebDAV Publishing**)

5. Select **Features** in the tree. A list of features is displayed.

6. Under **Features**, select the following features:

- **.NET Framework 3.5 Features**

  - **.NET Framework 3.5 (includes .NET 2.0 and 3.0)**

  - **HTTP Activation**

- **.NET Framework 4.5 Features**

  - **.NET Framework 4.5**

  - **ASP.NET 4.5**

  - **WCF Services** (select all subfeatures except **Message Queuing (MSMQ Activation)**)

- **Background Intelligent Transfer Service**

  - **IIS Server Extension**

  - **Compact Server**

- **SMB 1.0/CIFS File Sharing Support**

- **Windows Process Activation Service**

- **Remote Server Administration Tools > Feature Administration Tools > BITS Server Extensions Tool**s

- **WoW64 Support**

3

Installing App Portal / App Broker

To install the App Portal / App Broker web site, perform the following steps.

Note • You need to be an administrator to run this installer. To run as an administrator, you can right-click the installer file and select **Run as administrator** *from the context menu.*

Important • Starting with App Portal 2013, your deployment technology is no longer specified during installation. Instead, you specify your deployment technology connection settings on the **Deployment** *tab of the* **Settings** *view, as described in the App Portal / App Broker Administration Guide.*

Task   *To install the App Portal / App Broker web site:*

1. To start the App Portal / App Broker installer, launch AppPortalSetup_2018_R1.exe

   Note • If **OLE DB Driver 18 for SQL Server (x64)** *is not already installed on your machine, you will be prompted to install it before installation will begin. As this is a prerequisite, click* **Install**.

2. The The **Welcome** panel opens . Click **Next**.

3. Click **Next**. The **License Agreement** panel opens.

4. Read and accept the license agreement and click **Next** to continue. The **Destination Folder** panel opens.

5. Accept the default destination or click **Change** and select a different location. Click **Next** to continue.

6. Click **Next**. The **Database Server** panel opens.

   Important • Only Windows authentication is supported when connecting to the App Portal SQL Server database. Therefore, the account running this installer needs DBO permissions to that SQL Server.

7.   Enter the name of the database server that you are installing to or select it from the list.

If you are using a specific database instance (other than the default instance), enter the database server and SQL instance in the following format:

`<SERVERNAME>\<INSTANCE>`

Important • Do not use (Local) as a database name.

8.   In the **Name of database catalog** field, enter the name of the new App Portal database that will be created by this installer, or click **Browse** to select an existing catalog.

9.   Click **Next** to continue.

10.   If you are creating a new database catalog, a message appears stating that a new database catalog will be created. Click **OK** to continue.

The **Logon Information** panel opens.

11.   A user account is required to interact with Active Directory and SQL. This same account will be used for the App Portal service. The account requires administrative rights on clients to make use of the remote policy execution and to rerun advertisements. In the **User name** field, enter user account information in `Domain\Username` format, along with a **Password**.

Note • Enter the credentials that App Portal will use to communicate with System Center Configuration Manager and other deployment technologies, SQL Server, Active Directory, and clients. This must be the same account, so it is recommended that you use a devoted service account. This account must also have administrator rights on all client machines.

12.   Click **Next** to continue. The **App Portal Settings** panel opens.

13.   In the **DNS Alias (A-Record)** field, enter one of the following:

- If you have already created a DNS alias for the identity of the site, enter it in this field.

  Note • If you enter an alias, it needs to already be created on your DNS servers. The App Portal installer will not create it for you.

  Note • If you specify an alias, a DNS A-RECORD for that alias must be created in order to access the App Portal site. It is important that the alias be an DNS A-RECORD, and not a CNAME record.

- If you do not want to use an alias, you can accept the default value, which is the server machine name.

  Note • If you specify the server machine name, you do not need to create a DNS A-RECORD because one already exists for the server.

*Tip • After installation, you can edit the DNS Alias value on the **General** tab of the **Site Management > Settings > Web Site** view.*

14. In the **AD Global Catalog Server** field, confirm or enter the server value.

15. In the SMTP Server fields enter the name of the SMTP Server that will be used for relaying email.

Note • You may need to configure the SMTP server internally to accept relay from this server's IP address.

*Note • You can also enter the mail settings after installation on the **Site Management > Settings > Email** view.*

16. In the **SMTP Account** field, enter the SMTP account name.

17. For the **Computer Discovery Method**, select one of the following options to specify the method to use for discover the active machine visiting the App Portal site:

- **Active X Control**—Will install a signed Active X control that will transfer the computer name from the client to the server. Active X will give the most consistent result. A separate installer,
  `Active X control for Internet Explorer.msi`, is included for large scale distribution of the control. Administrative permissions are required for its installation.

  Note • You can use SCCM to deploy the Active X control, or just add your App Portal site to the Trusted Zone in Internet Explorer.

- **Reverse DNS**—Uses the reverse DNS zones in Active Directory (if present) to look up the computer name by IP address.

  *Note • If you select **Reverse DNS**, every computer in your DNS will be discovered, not just those in SCCM. It only searches the Active Directory DNS, so if you have other DNS providers, it will not work.*

18. Click **Next**. The **Ready to Install the Program** panel opens.

19. Click **Install** to begin the installation. When installation is complete, the **Completed** panel opens.

20. Click **Finish** to close the installer.

4

Installing the App Portal Web Service

Note • *You are required to install the App Portal Web Service when using Microsoft System Center Configuration Manager deployment technology. It is not required when using Altiris, Casper, AirWatch, or MobileIron deployment technology.*

Important • *You must first install the App Portal Web Site, as described in Installing App Portal / App Broker, before installing the App Portal Web Service on any server.*

Important • *If upgrading from an earlier version of App Portal, note that upgrading the existing App Portal web site will not upgrade the existing App Portal Web Services application. You need to manually run the* `AppPortalWebServiceSetup_2018_R1.exe` *installer on your System Center Configuration Manager server.*

The location(s) where you install the App Portal Web Service depends upon the version of System Center Configuration Manager you are using:

- **System Center 2012 Configuration Manager or System Center Configuration Manager (Current Branch)**—When using single primary/CAS with System Center 2012 Configuration Manager or System Center Configuration Manager (Current Branch), you need to install the App Portal Web Service *only* on the single primary/CAS.

To install the App Portal Web Service, perform the following steps:

Task　　**To install App Portal Web Service:**

1. Verify that the Microsoft .NET 4.6.1 or later framework is installed on the CAS or primary site server. If it is not installed, use **Control Panel > Programs and Features > Turn Windows features on or off** to install it.

2. To start the App Portal Web Service installer, open the App Portal Web Service installer file, `AppPortalWebServiceSetup_2018_R1.exe`.

📄

Note • You need to be an administrator to run this installer. To run as an administrator, you can right-click the App Portal Web Service installer file and select **Run as administrator** *from the context menu.*

3.   On the **User Account Control** dialog box, click **Yes**. The **Welcome** panel opens.

4.   Click **Next**. The **License Agreement** panel opens.

5.   Read and accept the license agreement and click **Next** to continue. The **Destination Folder** panel opens.

6.   If you want to install App Portal Web Service in the specified directory, click **Next**. If you want to select a different
directory, click **Change**, select a new directory, and then click **Next**. The **Primary Site Server Setup** panel opens.

The fields on this panel are populated with information that the installer obtained from the Microsoft System Center
Configuration Manager installation on this machine.

7.   Click **Next**. The **Ready to Install the Program** panel opens.

8. Click **Install** to begin the installation. When installation is complete, the **Completed** panel opens.

9. Click **Finish** to close the installer.

10. Upon completion of the installer, a new collection should have been created in Microsoft System Center Configuration Manager named `App Portal Collection for (SiteCode)`. Open the **Configuration Manager Console** and verify that this collection exists.

    Note • The account used to install App Portal Web Service has been granted full administrative access to the site. See the App Portal Configuration Guide for information on configuring site security.

11. Navigate your browser to `http://<sitealias>/esd/`. The App Portal web site opens.

    *Note • You may be prompted to install an Active X control. Click **Install**.*

12. When you first access App Portal you will be prompted to upload your license file provided. Follow the instructions on screen to upload the file.

13. Repeat this procedure for each Primary Site.

5

Upgrading the App Portal Web Site

To upgrade an existing installation of App Portal to App Portal / App Broker 2018 R1, first review the About Upgrading section and then perform the upgrade.

- About Upgrading

- Performing the Upgrade

- Troubleshooting Database Upgrade Failed Error During Upgrade

- Moving App Portal from One Server to Another

Important • In previous releases, App Portal shipped two installers: one for installing a new instance of App Portal and another to upgrade an existing instance. Starting with App Portal 2017, App Portal now provides a unified setup that you can use to both install a new instance of App Portal and upgrade an existing instance.

About Upgrading

When upgrading an existing version of App Portal to App Portal 2018 R1, it is very important that you review the following information **before** you begin the upgrade.

- Supported Upgrade Versions

- Planning Your Upgrade

Supported Upgrade Versions

You can only upgrade to App Portal 2018 R1 from the following previous versions:

- App Portal 2017 R2

- 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 2018 R1, use the App Portal 2018 R1 installer, which can be downloaded from the Flexera Software Product and License Center, as described in Performing the Upgrade.

Planning Your Upgrade

When performing your upgrade to App Portal 2018 R1, it is recommended that you include the following steps in your upgrade process:

- **Review the Release Notes**—Thoroughly review the App Portal / App Broker 2018 R1 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_2018_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.

Performing the Upgrade

To upgrade a previously installed version of App Portal to App Portal 2018 R1, perform the following tasks:

- Using the App Portal Installer to Perform an Upgrade

- Retaining Previous CSS Customizations After Upgrade

Using the App Portal Installer to Perform an Upgrade

Note • In releases prior to App Portal 2017, you upgraded using the App Portal Upgrader executable. Starting with App Portal 2017, you use the same App Portal installer executable to perform both a new installation and an upgrade of an existing installation.

Note • Before upgrading App Portal, make sure that you first uninstall any previously installed App Portal hot fixes.

Important • The administrator account that will be using the App Portal installer to upgrade App Portal and the App Portal database requires at least "Application Administrator" permissions within System Center Configuration Manager. If the account does not have these permissions, an "Access is denied" error is encountered when attempting to upgrade App Portal.

Note • If you have modified any CSS files to customize the colors used in the App Portal interface, those customizations will be lost upon upgrade. However, you can easily alter the colors used in your site using the **Corporate Branding** *tab of the* **Site Management > Settings > Web Site** *view. For more information, see Retaining Previous CSS Customizations After Upgrade.*

To upgrade an existing installation of App Portal using the App Portal installer, perform the following steps:

Task   **To upgrade App Portal:**

1. Obtain the App Portal 2018 R1 installer (`AppPortalSetup_2018_R1.exe`) from the Flexera Software Product and License Center and make it accessible to the machine where App Portal is installed.

2. Right click the App Portal installer file and select **Run as administrator** from the context menu. The **User Account Control** dialog box opens prompting you to confirm that you want to allow the program to make changes to this computer.

3. Click **Yes**. The **Welcome** panel opens, stating that a previous version of App Portal was detected on your computer.

4.   Click **Next**. The **Ready to Install the Program** panel opens.

5.   Click **Install** to begin the upgrade. When the upgrade is complete, the **InstallShield Wizard Completed** panel opens.

6. Click **Finish** to close the wizard.

7. Launch App Portal and, if necessary, specify your deployment technology settings, as described in the *Configuring Your Deployment Technology* section of the *App Portal / App Broker Administration Guide*.

8. Perform a sync of users and computers, as described in the *Entering Common Deployment Technology Settings* topic in the *App Portal / App Broker for ServiceNow Installation Guide*.

📄

Note • Until a sync is performed, macOS machines may not be included in computer listings.

Retaining Previous CSS Customizations After Upgrade

If, in a previous release of App Portal, you have modified any of your App Portal web site's CSS files to customize the colors, fonts, or layout of the App Portal interface, those customizations will be lost upon upgrade, and you will need to take some action to retain those customizations in the upgraded site.

When you are using the App Portal Upgrader, an alert will be displayed if you have customized the CSS styles in any of the following files:

Table 5-1 • Custom CSS Files in Previous Releases of App Portal

CSS File	Location in the App Portal 2015 Installation Directory
Custom.css	AppPortal\AP\Content
wdcssCustom.css	AppPortal\Web
Custom.Flexera.css	AppPortal\Web\App_Themes\Flexera

The following alert is displayed:

After upgrade, older custom themes/css files will become obsolete. Do you want to continue?

If you encounter this alert, click **Yes** to continue the upgrade, and then perform one of the following tasks to retain your user interface customizations in the upgraded site:

● Customize Using the App Portal Interface

● Customize by Editing LESS Files

Customize Using the App Portal Interface

To customize the background, hover, icon, heading, and hyperlink colors used throughout the site (including the navigation bar), then open the **Corporate Branding** tab of the **Site Management > Settings > Web Site** view and specify your desired colors, as described in Customizing the App Portal User Interface Colors at:

http://helpnet.flexerasoftware.com/appportal2016/default.htm#helplibrary/AP_Colors.htm

Customize by Editing LESS Files

If you want to make modifications other than those listed above, you need to edit the CSS classes in the custom LESS files listed in the following table.

Table 5-2 • Custom LESS Files

LESS File	Installed Location
custom.less wdcssCustom.less	\App Portal\Web\Content
Custom.Flexera.less	\App Portal\Web\App_Themes\Flexera

When editing these files, you can you can use the styles in your previously customized corresponding `*.css` file (listed in Custom CSS Files in Previous Releases of App Portal) for reference.

Troubleshooting Database Upgrade Failed Error During Upgrade

Problem

In some instances during the upgrade process, the upgrade may fail and display the following message:

```
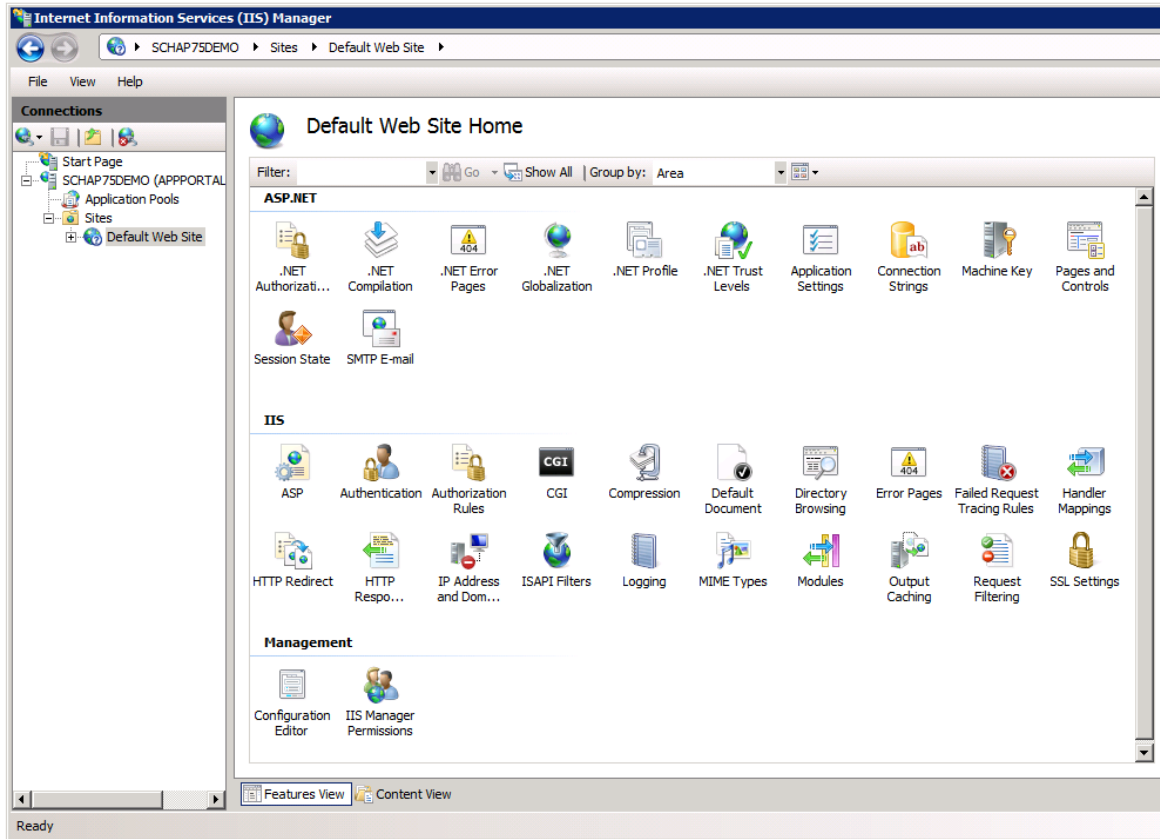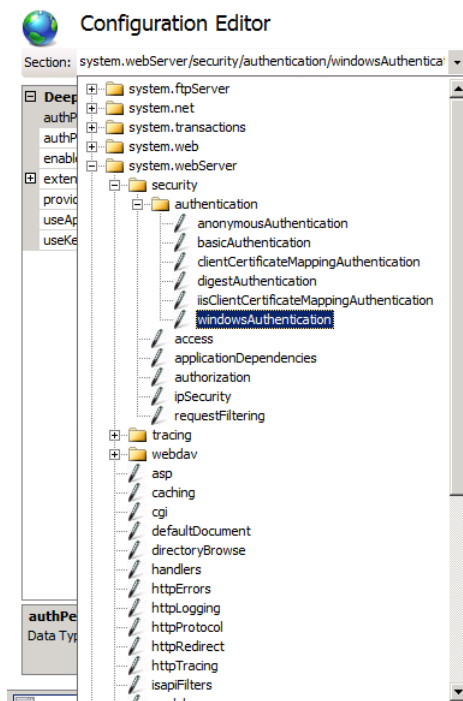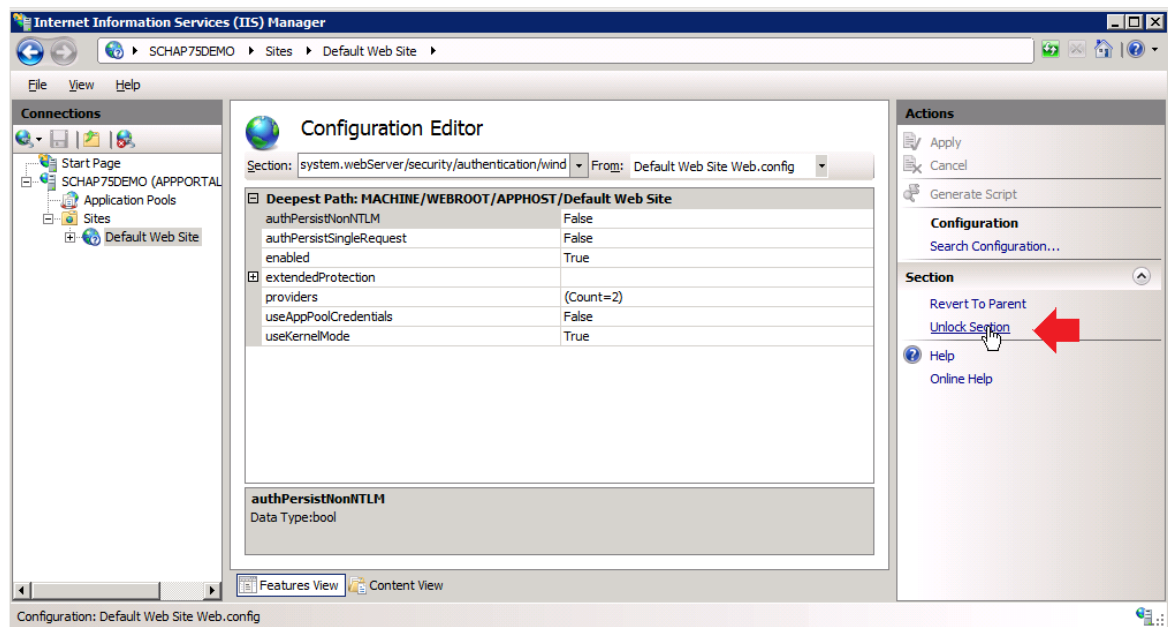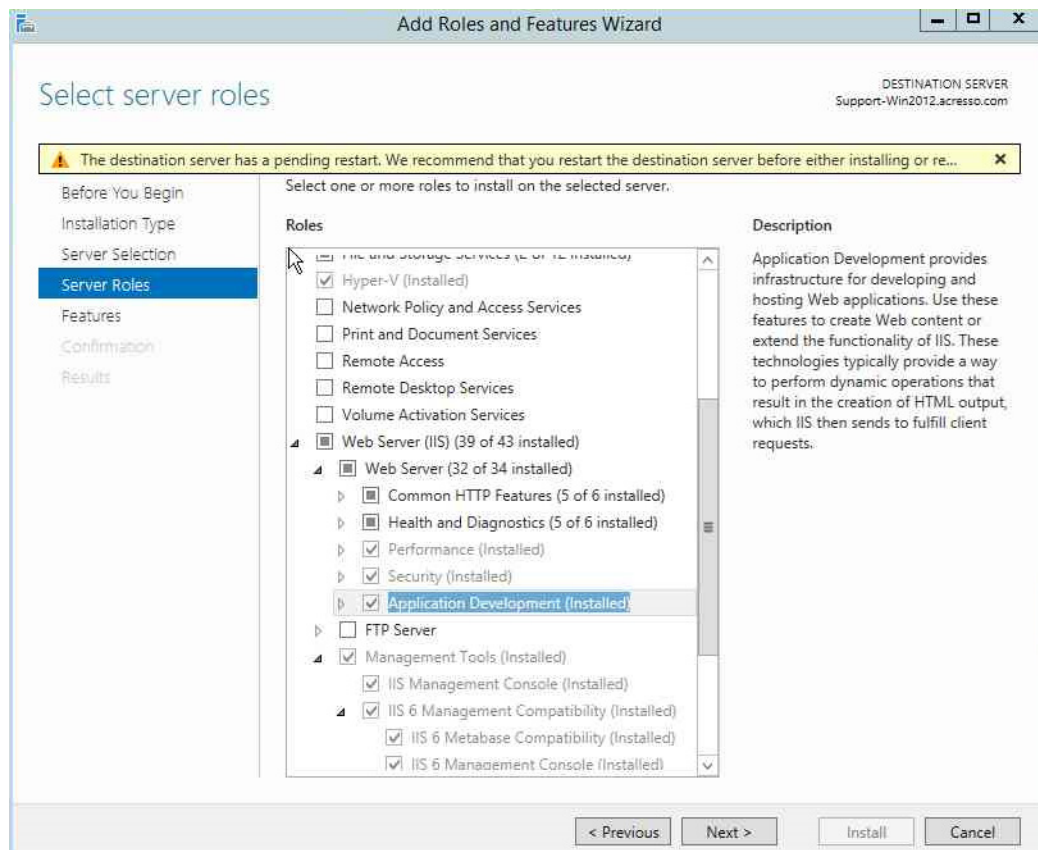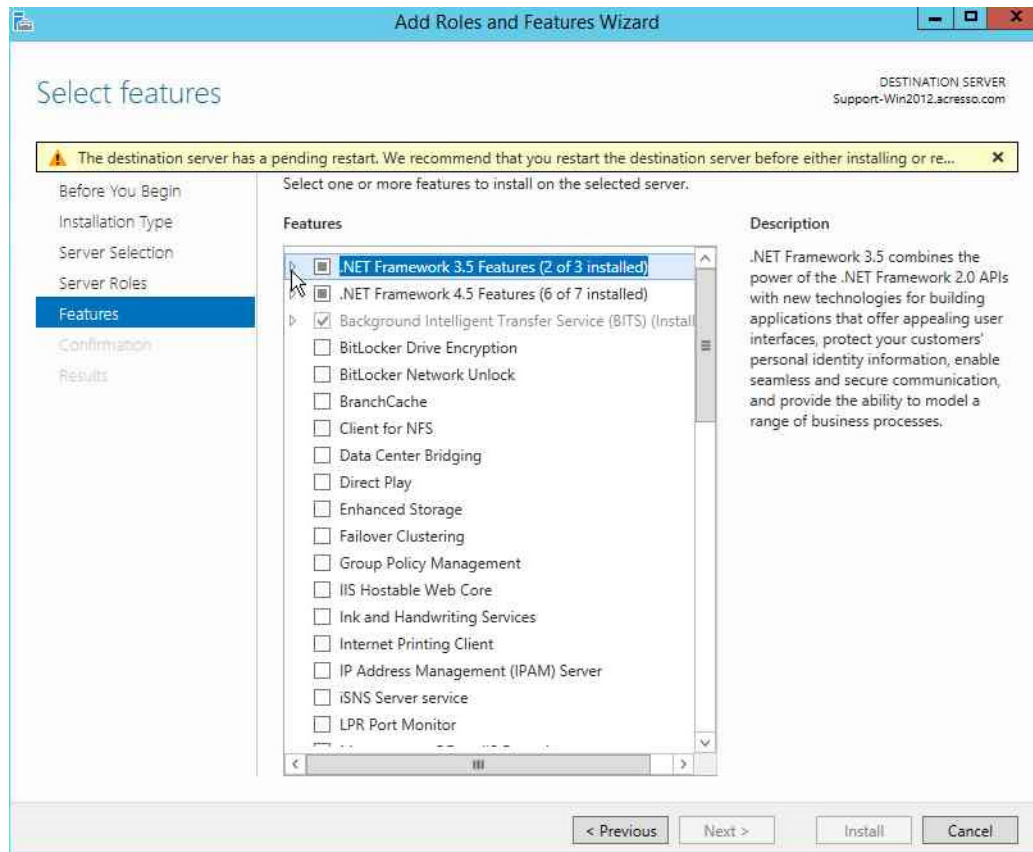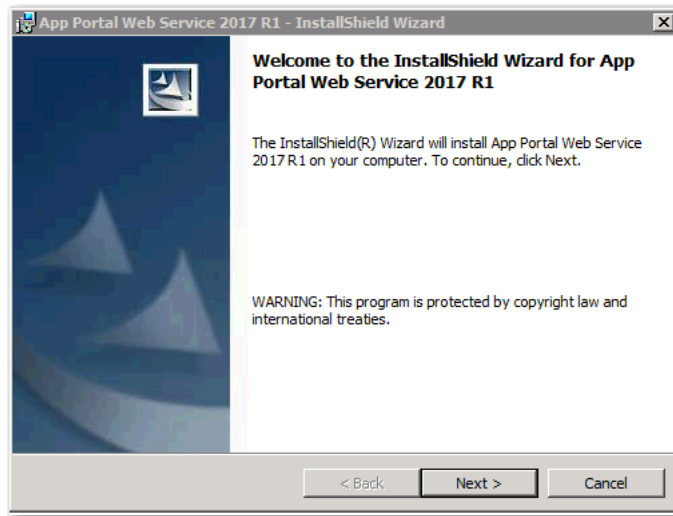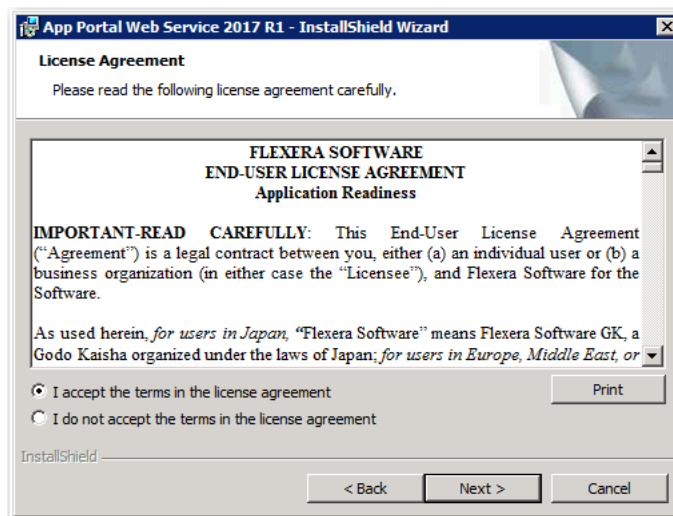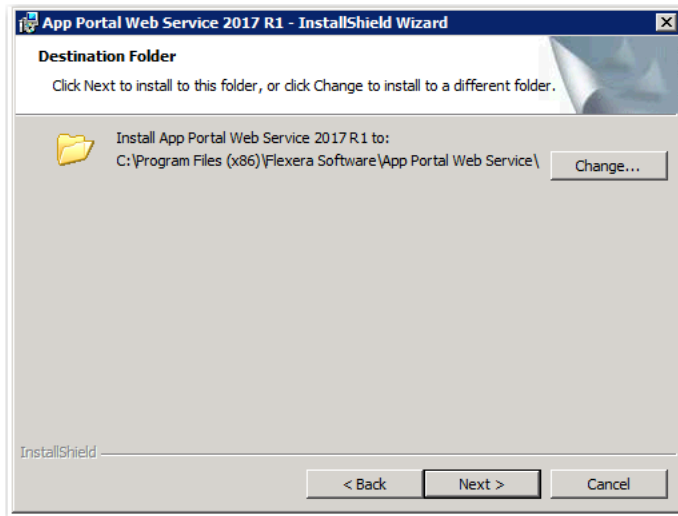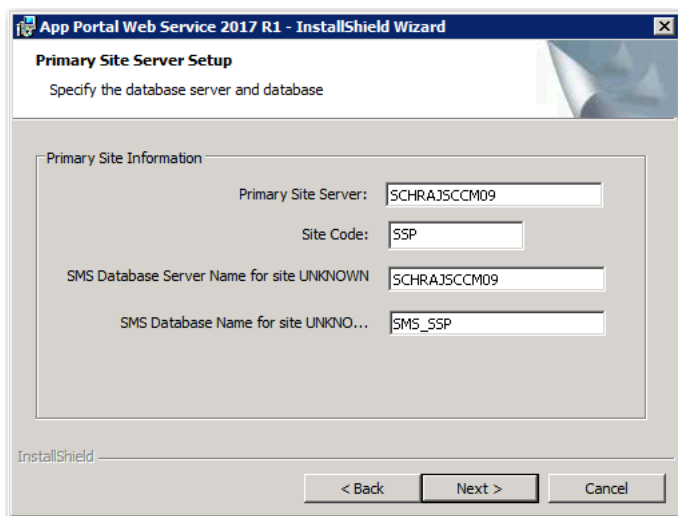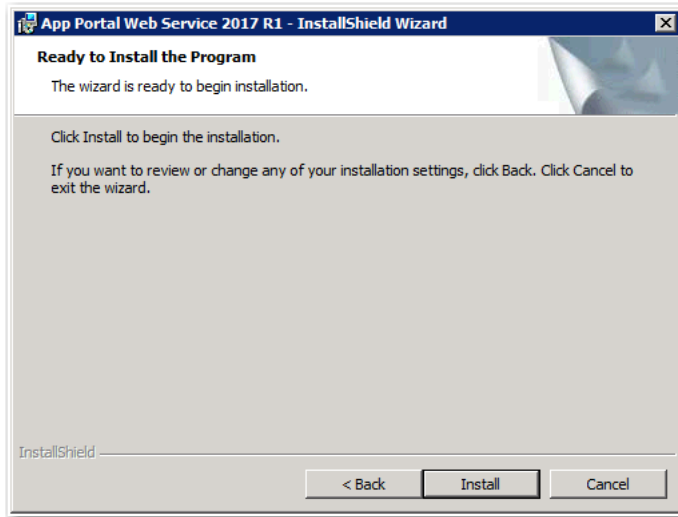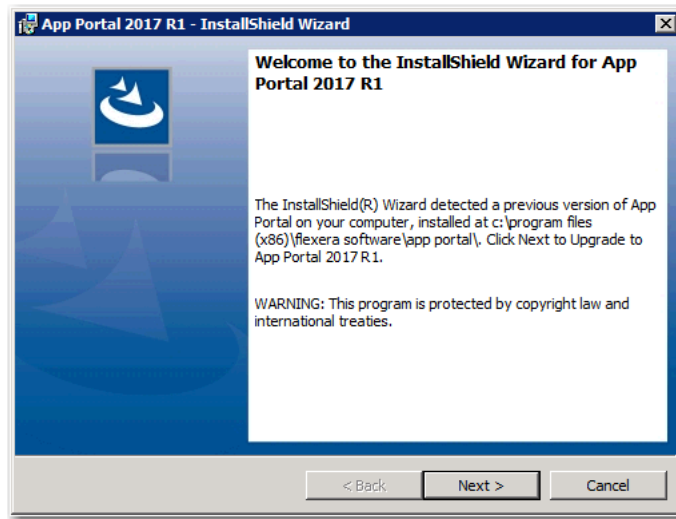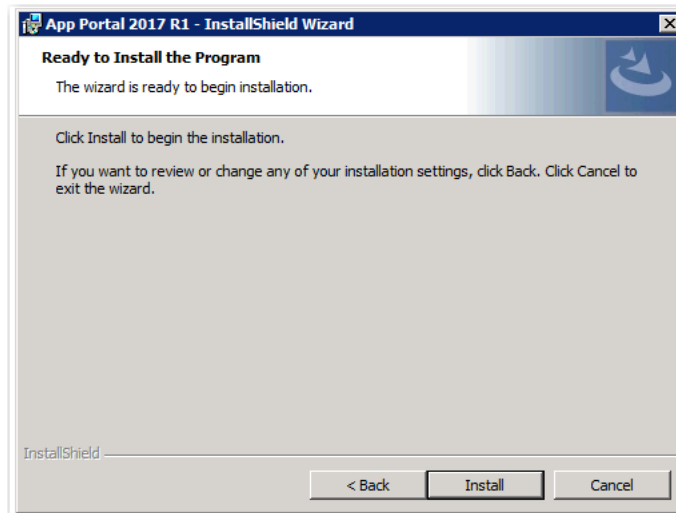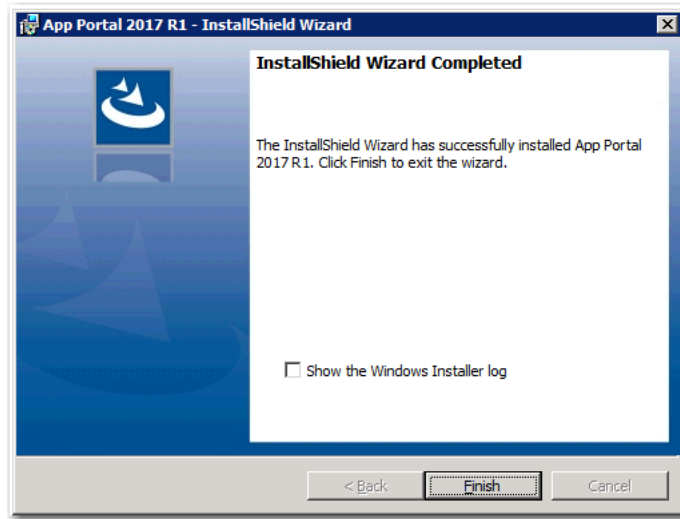Executing Database upgrade script for database AppPortal on FLEXCM

Error detected during database upgrade. Please look at C:\ESD_Error_Log.txt for more information.

Database Upgrade failed. Check C:\ESD_Error_Log.txt for more info and contact Flexera Software for
    assistance.

Done!
```

A review of the `ESD_Error_Log.txt` file will reveal more detail about the cause of the error:

```
Failed to backup the database AppPortal.

Cannot open backup device 'C:\ESD_Upgrade_Backup'. Operating system error 5 (Access is denied).

BACKUP DATABASE is terminating abnormally.
```

Cause

The App Portal Upgrade performs four functions during installation:

1. Upgrade Website

2. Upgrade Database

3. Upgrade Web Services on Primary Sites

4. Backup Self Service Database

Even though the backup is last on the list of options, it is performed first.

The upgrade failure in this case is caused by insufficient permissions of the SQL service account. In order to write a file to the root of the `C:\` drive, an account must be a member of the local administrators group.

Solution

Temporarily add the SQL service account to the local administrators group on the SQL server hosting the App Portal database. This will allow the SQL service account to successfully write a backup copy of the existing App Portal database to the root of the `C:\` drive. Once the upgrade has completed, you can remove the SQL service account from the local administrators group.

Moving App Portal from One Server to Another

You may need to move App Portal from one server to another, such as when you upgrade your server operating system from Windows Server 2008 R2 to Windows Server 2012 or 2016. Because you have an existing database, this activity might require more steps than just uninstalling App Portal from the old server, installing it on the new server, and then pointing to your existing App Portal database. If you are also upgrading to a newer App Portal version at the same time, more complexity is added. In these scenarios, the following steps are recommended.

Task | ***To move App Portal from one server to another:***

1. Backup the App Portal web server and database.

2. Provision the Windows Server 2012 / 2016 system.

3. Disable the `ESDService` on the App Portal web server.

4. Install the same version of App Portal on the Windows Server 2012 system and attach it to the existing App Portal database.

5. Verify the App Portal environment.

6. Change DNS alias, as needed.

7. Decommission the Windows Server 2008 App Portal web server.

8. Once stability is verified, upgrade App Portal to the latest supportable version per the standard upgrade instructions.

Index