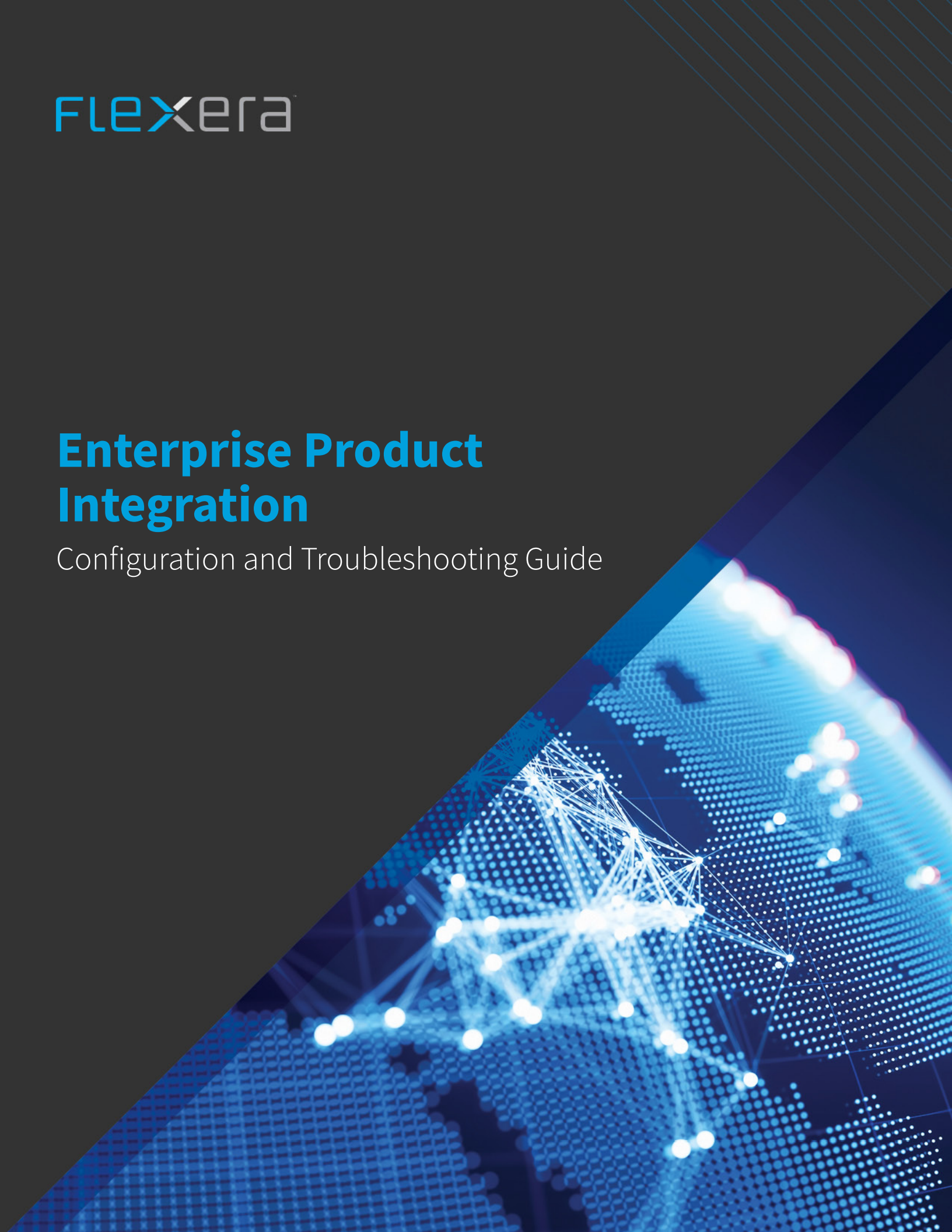




# Enterprise Product Integration

Configuration and Troubleshooting Guide



# Legal Information

**Book Name:** Enterprise Product Integration Configuration and Troubleshooting Guide  
**Part Number:** EPI-0500-CG01  
**Product Release Date:** May 2018

## Copyright Notice

Copyright © 2018 Flexera

This publication contains proprietary and confidential information and creative works owned by Flexera 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 is strictly prohibited. Except where expressly provided by Flexera in writing, possession of this publication shall not be construed to confer any license or rights under any Flexera intellectual property rights, whether by estoppel, implication, or otherwise.

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

## Intellectual Property

For a list of trademarks and patents that are owned by Flexera, see <https://www.flexera.com/producer/company/about/intellectual-property/>. All other brand and product names mentioned in Flexera 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.

# Contents

<b>1</b>	<b>Enterprise Product Integration Configuration and Troubleshooting Guide</b>	<b>7</b>
	Contacting Us	8
<b>2</b>	<b>Prerequisites for Integration</b>	<b>9</b>
	Integrated Environment Overview	10
	Supported Version Matrix	12
	Install and Set Up Applications	13
	Set Up Accounts and Configure Account Access Between Products	16
	AdminStudio Accounts	17
	Required Permissions on Application Catalog Databases	17
	Accounts for Integration of AdminStudio and App Portal with FlexNet Manager Suite	20
	App Portal Accounts	30
	FlexNet Manager Suite On Premises / FlexNet Manager Platform Accounts	31
	FlexNet Manager Suite Cloud Service Account and Token	32
	Workflow Manager Accounts	33
	System Center Configuration Manager Accounts	34
	Establish Two-Way Trusts Between Multiple Domains	34
	Port Requirements	35
	Recommended Proof-of-Concept Configuration	40
<b>3</b>	<b>Installing and Configuring Flexera Service Gateway 2</b>	<b>41</b>
<b>4</b>	<b>Configuring the FlexNet Manager Suite Cloud Environment</b>	<b>43</b>
	Configuring the FlexNet Manager Suite Inventory Beacon	44
	Registering FlexNet Manager Suite Cloud with the Flexera Service Gateway	56
	Registering App Portal with FlexNet Manager Suite Cloud and Flexera Service Gateway	59
<b>5</b>	<b>Configuring FlexNet Manager Suite On Premises</b>	<b>61</b>

<b>Testing FlexNet Manager Suite On Premises Server Authentication Settings</b>	<b>62</b>
<b>Connecting FlexNet Manager Suite On Premises to the Flexera Service Gateway</b>	<b>63</b>
<b>Importing the Application Recognition Library (ARL)</b>	<b>64</b>
<b>Troubleshooting FlexNet Manager Suite Communication Issues</b>	<b>65</b>
Verify FlexNet Manager Suite On Premises Application Server Authentication Settings in IIS	66
Check That ManageSoftWebServiceAppPool Service is Running	67
Verify Domain Credentials Across Computers by Invoking GetTenants and GetFlexeraIDForApplication API	68
Test the FlexNet Manager Suite GetFlexeraIDForApplication API	71
Steps to Take When FlexNet Manager Suite is Unable to Register With the Flexera Service Gateway	73
Resolving Active Directory “Double Hop” Issues Which Occur if FlexNet Manager Suite and SQL Server are on Separate Computers	74
<a href="#">Temporary Solution for “Proof of Concept” Lab Scenario to Address Double-Hop Issue with FlexNet Manager Suite Server</a>	<a href="#">78</a>
<b>Viewing an Application’s Flexera ID in FlexNet Manager Suite</b>	<b>79</b>
<b>Upgrading FlexNet Manager Suite’s Compliance Console</b>	<b>80</b>
<b>6 Configuring App Portal</b>	<b>81</b>
<b>Testing App Portal Server Authentication Settings</b>	<b>82</b>
<b>Connecting App Portal to the Flexera Service Gateway</b>	<b>83</b>
<b>Testing App Portal’s Connection to the Flexera Service Gateway</b>	<b>84</b>
<b>Performing App Portal Troubleshooting</b>	<b>86</b>
Installation Testing and Troubleshooting	86
<a href="#">Verify the App Portal Server Authentication Settings</a>	<a href="#">86</a>
<a href="#">Check the SelfService Service</a>	<a href="#">89</a>
<a href="#">Check the ESDService Service</a>	<a href="#">89</a>
<a href="#">Test FlexNet Manager Suite / FlexNet Manager Platform Server Authentication Settings</a>	<a href="#">91</a>
<a href="#">Invoke GetCategories API</a>	<a href="#">92</a>
<a href="#">Error After Installation on X64 Server with WSUS Role</a>	<a href="#">93</a>
Troubleshooting App Portal Integration Issues	94
<a href="#">App Portal Catalog Item Not Automatically Created When AdminStudio Publishes an Application</a>	<a href="#">94</a>
<a href="#">Preventing App Portal From Possibly Displaying False “Install Failed” Status for Application Deployment on SCCM 2012</a>	<a href="#">96</a>
<b>Upgrading the App Portal Web Site</b>	<b>96</b>
About Upgrading	97
<a href="#">Supported Upgrade Versions</a>	<a href="#">97</a>
<a href="#">Planning Your Upgrade</a>	<a href="#">97</a>
Performing the Upgrade	98
<b>7 Configuring AdminStudio</b>	<b>99</b>
<b>Connecting AdminStudio to the Flexera Service Gateway</b>	<b>100</b>
<b>Testing AdminStudio’s Connection to the Flexera Service Gateway</b>	<b>102</b>
View Flexera Identification Number in Application View	102
View Flexera Service Gateway Messages During Import and Distribution to SCCM	103
<b>Configuring Authentication in Internet Explorer</b>	<b>104</b>
<b>Upgrading AdminStudio</b>	<b>105</b>
Upgrading an Application Catalog	106

Changing the Database Collation of the Upgraded Application Catalog .....	107
<b>8 Configuring Workflow Manager.....</b>	<b>109</b>
Connecting Workflow Manager to the Flexera Service Gateway.....	110
Testing Workflow Manager’s Connection to the Flexera Service Gateway .....	113
Upgrading Workflow Manager .....	113
Troubleshooting Workflow Manager Issues.....	115
Test Center Testing Fails When Triggered by Workflow Manager .....	115
<b>Index .....</b>	<b>117</b>



# Enterprise Product Integration Configuration and Troubleshooting Guide


Flexera Software has developed a unified application usage management solution—comprised of FlexNet Manager Suite (On Premises or Cloud), AdminStudio, App Portal, and Workflow Manager—which gives you a consolidated and centralized approach to maximizing software value and optimizing usage across the application life cycle.



**Note** • FlexNet Manager Suite On Premises was known as FlexNet Manager Platform in earlier releases.

This guide explains how to configure and troubleshoot this enterprise product integration solution. The following main sections are included:

**Table 1-1** • Enterprise Product Integration Configuration and Troubleshooting Guide

Section	Description
<b>Prerequisites for Integration</b>	Describes steps to take before implementing product integration, including configuring accounts and permissions.
<b>Installing and Configuring Flexera Service Gateway 2</b>	Explains how to install the Flexera Service Gateway.
<b>Configuring FlexNet Manager Suite On Premises</b>	Explains how to connect FlexNet Manager Suite On Premises to the Flexera Service Gateway, test the connection, and perform configuration steps.  <b>Note</b> • This product was known as FlexNet Manager Platform in earlier releases.
<b>Configuring the FlexNet Manager Suite Cloud Environment</b>	Explains how to configure the FlexNet Manager Suite Cloud environment.
<b>Configuring App Portal</b>	Explains how to connect App Portal to the Flexera Service Gateway, test the connection, and perform configuration and troubleshooting.

**Table 1-1 •** Enterprise Product Integration Configuration and Troubleshooting Guide

Section	Description
<b>Configuring AdminStudio</b>	Explains how to connect AdminStudio to the Flexera Service Gateway and to test the connection.
<b>Configuring Workflow Manager</b>	Explains how to connect Workflow Manager to the Flexera Service Gateway and test the connection.

## Contacting Us

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

<http://www.flexerasoftware.com>



# Prerequisites for Integration

Before you can use the integrated solution of FlexNet Manager Suite (On Premises or Cloud), AdminStudio, App Portal, and Workflow Manager, you first need to install the products and configure user accounts and domains. The following tasks need to be performed:

- [Integrated Environment Overview](#)
- [Install and Set Up Applications](#)
- [Set Up Accounts and Configure Account Access Between Products](#)
- [Establish Two-Way Trusts Between Multiple Domains](#)
- [Port Requirements](#)
- [Recommended Proof-of-Concept Configuration](#)



---

**Note** • *FlexNet Manager Suite On Premises was known as FlexNet Manager Platform in earlier releases.*

# Integrated Environment Overview

Flexera Software's unified application usage management solution—comprised of FlexNet Manager Suite On Premises or Cloud, AdminStudio, App Portal, and Workflow Manager—gives you a consolidated and centralized approach to maximizing software value and optimizing usage across the application life cycle.

The following diagram gives you an overview of how these integrated applications communicate—via the Flexera Service Gateway—when performing the tasks involved in a single application's life cycle.



**Note** • FlexNet Manager Suite On Premises was known as FlexNet Manager Platform in earlier releases.

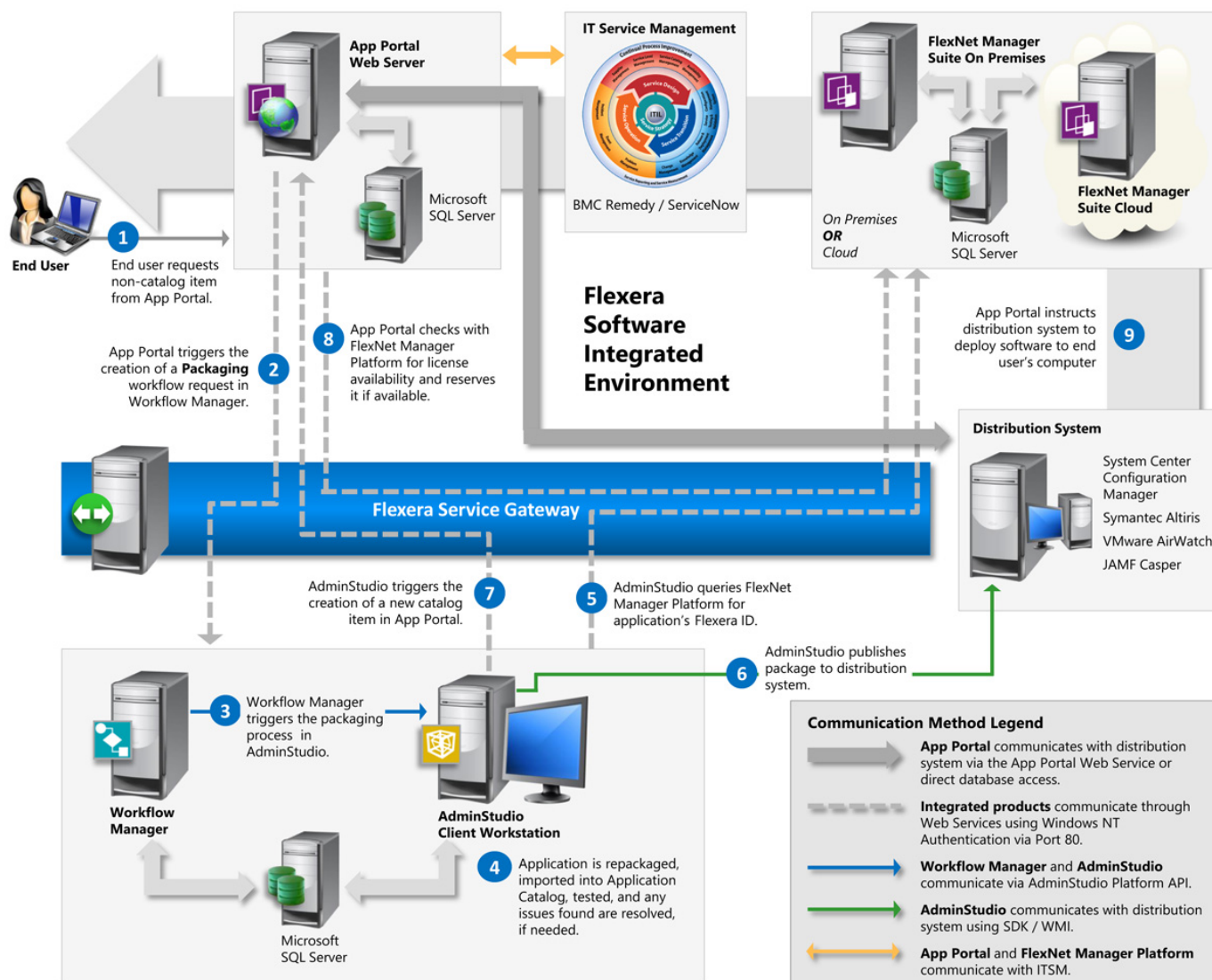


Figure 2-1: Flexera Software Integrated Environment Diagram

This application life cycle workflow includes the following steps:



**Table 2-1 • Flexera Software Integrated Environment Workflow**

#	Step	Description
1.	<b>End user requests non-catalog item from App Portal.</b>	Using the App Portal web site, an end user submits a request for a software item that is not currently in the App Portal catalog.
2.	<b>App Portal triggers the creation of a Packaging workflow request in Workflow Manager.</b>	After the end user's request for new software is approved, App Portal triggers the creation of a <b>Packaging</b> workflow request in Workflow Manager.
3.	<b>Workflow Manager triggers the packaging process in AdminStudio.</b>	Workflow Manager can be configured to trigger AdminStudio tasks such as repackaging, importing a package into the Application Catalog, performing tests, and resolving issues that are found, if needed.
4.	<b>Application is repackaged, imported into Application Catalog, tested, and any issues found are resolved, if needed.</b>	The package is ready for deployment.
5.	<b>AdminStudio queries FlexNet Manager Suite for application's Flexera Identifier.</b>	When the package is imported into the Application Catalog, AdminStudio automatically queries the FlexNet Manager Suite ARL and obtains the application's Flexera Identifier.
6.	<b>AdminStudio publishes package to supported distribution system</b>	After the software has been repackaged and tested, AdminStudio publishes the application to System Center Configuration Manager, Symantec Altiris Server, JAMF Casper Suite Server, or VMware AirWatch.
7.	<b>AdminStudio triggers the creation of a new catalog item in App Portal.</b>	When AdminStudio publishes the application, a catalog item for that application is automatically created in App Portal, identified by the same Flexera Identifier. End user can now request this software in App Portal.
8.	<b>App Portal checks with FlexNet Manager Suite for license availability and reserves it if available.</b>	App Portal queries FlexNet Manager Suite to obtain entitlement and usage data for that application including available license count and the number of licenses used. If a license is available, App Portal will automatically reserve it for the end user.
9.	<b>App Portal instructs deployment system to deploy software to end user's computer.</b>	App Portal instructs distribution system to deploy the software to the end user's computer.

# Supported Version Matrix

For each release of the Flexera Software enterprise products, this matrix lists the inter-product supported versions.

**Table 2-2 • Enterprise Product Integration Supported Version Matrix**

Version	Compatible With				
	AdminStudio	App Portal	Workflow Manager	FNMP / FNMS On Premises	FNMS Cloud
<b>AdminStudio 11.5 SP2</b>		7.5.3 or later	6.5	9.2 SP1 or later	—
<b>AdminStudio 2013</b>		7.5.3 or later	2013	9.2 SP1 or later	—
<b>AdminStudio 2014</b>		7.5.3 or later	2014	9.2 SP1 or later	—
<b>AdminStudio 2015 (2015 SP1)</b>		7.5.3 or later	2015	9.2 SP1 or later	2014 or later
<b>AdminStudio 2016 (2016 SP1, 2016 SP2)</b>		7.5.3 or later	2015 or later	9.2 SP1 or later	2014 or later
				 <b>Note •</b> Creating a Flexera Local Identifier requires FNMS 2015 R2 SP3 or later	
<b>App Portal 7.5.3</b>	11.5 SP2 or later		6.5 or later	9.2 SP1 or later	—
<b>App Portal 7.5.5</b>	11.5 SP2 or later		6.5 or later	9.2 SP1 or later	—
<b>App Portal 2013</b>	11.5 SP2 or later		6.5 or later	9.2 SP1 or later	—
<b>App Portal 2014</b>	11.5 SP2 or later		6.5 or later	9.2 SP1 or later	—
<b>App Portal 2015 (2015 R2)</b>	11.5 SP2 or later		6.5 or later	9.2 SP1 or later	2014 or later
<b>App Portal 2016</b>	11.5 SP2 or later		6.5 or later	9.2 SP1 or later	2014 or later
<b>App Portal 2017</b>				 <b>Note •</b> The Advanced License Check feature requires FlexNet Manager Suite 2015 R2 SP5-02 Hotfix or later.	
<b>Workflow Manager 6.5</b>	11.5 SP2	7.5.3 or later		9.2 SP1 or later	—
<b>Workflow Manager 2013</b>	2013	7.5.3 or later		9.2 SP1 or later	—
<b>Workflow Manager 2014</b>	2014	7.5.3 or later		9.2 SP1 or later	—
<b>Workflow Manager 2015</b>	2015 or later	7.5.3 or later		9.2 SP1 or later	2014 or later
<b>Workflow Manager 2016</b>	2015 or later	7.5.3 or later		9.2 SP1 or later	2014 or later


**Table 2-2 • Enterprise Product Integration Supported Version Matrix**

Version	Compatible With				
	AdminStudio	App Portal	Workflow Manager	FNMP / FNMS On Premises	FNMS Cloud
<b>FNMP 9.2 SP1</b>	11.5 SP2 or later	7.5.3 or later	6.5 or later		
<b>FNMP 9.2.3</b>	11.5 SP2 or later	7.5.3 or later	6.5 or later		
<b>FNMS On Premises 2014 (2014 R2, 2014 R3)</b>	11.5 SP2 or later	7.5.3 or later	6.5 or later		
<b>FNMS On Premises 2015 (2015 R2, all service packs)</b>	11.5 SP2 or later	7.5.3 or later	6.5 or later		
<b>FNMS On Premises 2016</b> <b>FNMS On Premises 2017</b>	11.5 SP2 or later	7.5.3 or later	6.5 or later		
<b>FNMS Cloud 2014 (2014 R2, 2014 R3)</b>	2015 or later	2015 or later	2015		
<b>FNMS Cloud 2015 (2015 R2, all service packs)</b>	2015 or later	2015 or later	2015		
<b>FNMS Cloud 2016</b> <b>FNMS Cloud 2017</b>	2015 or later	2015 or later	2015 or later		



## Install and Set Up Applications

In order to implement the enterprise product integration solution, you need to first install and set up the following versions of these Flexera Software applications:

**Table 2-3 • Installation Instructions for Flexera Software Applications**

Application	Version	Installation and Setup Instructions
<b>AdminStudio</b>  Professional or Enterprise Edition	11.5 SP2 or later	 <p><b>To install and set up AdminStudio:</b></p> <ol style="list-style-type: none"> <li>1. Install AdminStudio, as described in the <i>AdminStudio Installation Guide</i>.</li> <li>2. Open Application Manager and create an Application Catalog database on an SQL Server.</li> <li>3. Connect to the Flexera Service Gateway, as described in <a href="#">Connecting AdminStudio to the Flexera Service Gateway</a>.</li> <li>4. Perform other configuration steps, as described in <a href="#">Configuring AdminStudio</a>.</li> </ol>

**Table 2-3 •** Installation Instructions for Flexera Software Applications

Application	Version	Installation and Setup Instructions
<b>App Portal</b>	7.5.3 or later (for FlexNet Manager Suite On Premises or FlexNet Manager Platform)  9.0.3 or later (for FlexNet Manager Suite Cloud)	 <p><b>To install and set up App Portal:</b></p> <ol style="list-style-type: none"> <li>1. Install App Portal, as described in <a href="#">App Portal Installation Guide</a>.</li> <li>2. During installation, specify your distribution system information.</li> <li>3. Connect to the Flexera Service Gateway, as described in <a href="#">Connecting App Portal to the Flexera Service Gateway</a>.</li> <li>4. Perform other configuration steps, as described in <a href="#">Configuring App Portal</a>.</li> </ol>
<b>FlexNet Manager Suite On Premises</b>	2014 or later	 <p><b>To install and set up FlexNet Manager Suite On Premises:</b></p> <ol style="list-style-type: none"> <li>1. Install FlexNet Manager Suite On Premises, as described in the <i>Installing FlexNet Manager Suite On Premises</i> guide, which is available from the Flexera Software Product and License Center.</li> <li>2. Import the FlexNet Manager Suite On Premises Application Recognition Library, as described in <a href="#">Importing the Application Recognition Library (ARL)</a>.</li> <li>3. Connect to the Flexera Service Gateway, as described in <a href="#">Connecting FlexNet Manager Suite On Premises to the Flexera Service Gateway</a>.</li> <li>4. Perform other configuration steps, as described in <a href="#">Configuring FlexNet Manager Suite On Premises</a>.</li> </ol>

**Table 2-3 •** Installation Instructions for Flexera Software Applications





Application	Version	Installation and Setup Instructions
<b>FlexNet Manager Platform</b>	9.2.3	<div>  <p><b>Note •</b> Starting with the 2014 release, this product's name was changed to <i>FlexNet Manager Suite On Premises</i>.</p> </div> <div>  <p><b>To install and set up FlexNet Manager Platform:</b></p> <ol style="list-style-type: none"> <li>1. Install FlexNet Manager Platform, as described in the <i>FlexNet Manager Platform Installation Guide</i>, which is available from the Flexera Software Product and License Center.</li> <li>2. Import the FlexNet Manager Platform Application Recognition Library, as described in <a href="#">Importing the Application Recognition Library (ARL)</a>.</li> <li>3. Connect to the Flexera Service Gateway, as described in <a href="#">Connecting FlexNet Manager Suite On Premises to the Flexera Service Gateway</a>.</li> <li>4. Perform other configuration steps, as described in <a href="#">Configuring FlexNet Manager Suite On Premises</a>.</li> </ol> </div>
<b>FlexNet Manager Suite Cloud</b>	2014 or later	<p>Perform the following tasks:</p> <ul style="list-style-type: none"> <li>• <a href="#">Configuring the FlexNet Manager Suite Inventory Beacon</a></li> <li>• <a href="#">Registering FlexNet Manager Suite Cloud with the Flexera Service Gateway</a></li> <li>• <a href="#">Registering App Portal with FlexNet Manager Suite Cloud and Flexera Service Gateway</a></li> </ul>

Table 2-3 • Installation Instructions for Flexera Software Applications

Application	Version	Installation and Setup Instructions
Workflow Manager	6.5 or later	 <p><b>To install and set up Workflow Manager:</b></p> <ol style="list-style-type: none"> <li>1. Install Workflow Manager, as described in the <i>Workflow Manager Installation Guide</i>.</li> <li>2. Create companies and user accounts.</li> <li>3. Create workflow templates and projects.</li> <li>4. Connect to the Flexera Service Gateway, as described in <a href="#">Connecting Workflow Manager to the Flexera Service Gateway</a>.</li> <li>5. Perform other configuration steps, as described in <a href="#">Configuring Workflow Manager</a>.</li> </ol>  <p><b>Important</b> • In order for product integration to work, Workflow Manager cannot be installed on the same server as App Portal.</p>

## Set Up Accounts and Configure Account Access Between Products

The Flexera Software Integrated Solution includes AdminStudio, App Portal, FlexNet Manager Suite On Premises or Cloud, the Flexera Service Gateway, Workflow Manager, and Microsoft System Center Configuration Manager (SCCM). All of these products communicate over a company network to provide a complete packaging and deployment solution that tracks usage and reports licensing.

When setting up these integrated Flexera Software products, you need to give certain accounts enhanced permissions to other products. These accounts and permissions are listed by product below.


- [AdminStudio Accounts](#)
- [App Portal Accounts](#)
- [FlexNet Manager Suite On Premises / FlexNet Manager Platform Accounts](#)
- [Workflow Manager Accounts](#)
- [System Center Configuration Manager Accounts](#)



# AdminStudio Accounts

When setting up AdminStudio, you need to give certain accounts enhanced permissions to other products. The following table lists the AdminStudio accounts and the required permissions:

**Table 2-4 • AdminStudio Accounts and Privileges in the Integrated Solution**

AdminStudio Account	Product/Machine Account Needs Access To	Required Privileges
<b>AdminStudio user accounts</b>	<b>Local workstation</b>	Require administrator privileges on the workstation where they are running AdminStudio.
	<b>System Center 2012 Configuration Manager (or later)</b>	Require the Application Administrator role on System Center Configuration Manager.
	<b>FlexNet Manager Suite / FlexNet Manager Platform</b>	See <a href="#">Accounts for Integration of AdminStudio and App Portal with FlexNet Manager Suite</a> .
	<b>App Portal</b>	<p>When integrating with versions of App Portal prior to App Portal 2016, AdminStudio users just require access to the App Portal Web Site using Windows Authentication.</p> <p>When integrating with App Portal 2016 and later, AdminStudio users need to have read and write access to App Portal catalog items so that AdminStudio can create App Portal catalog items.</p>
	<b>SQL Server</b>	<p>In order to connect to an AdminStudio Application Catalog database, users require db_datareader, db_datawriter, execute, alter, and references permissions on the AdminStudio database. For detailed instructions on assigning these permissions, see <a href="#">Required Permissions on Application Catalog Databases</a>.</p> <div>  <p><b>Tip •</b> The AdminStudio user account does not require these permissions if connecting to SQL Server using an SQL Server user account (which already has the appropriate permissions).</p> </div>

## Required Permissions on Application Catalog Databases

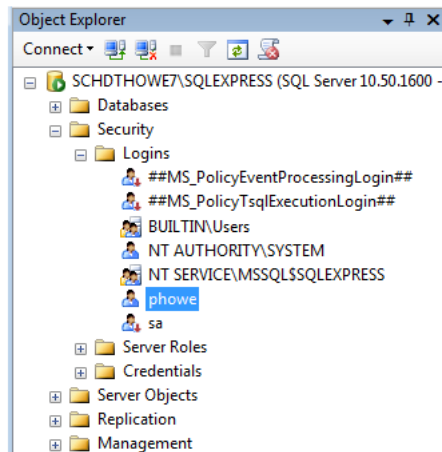
In order to connect to an AdminStudio Application Catalog database, users require db\_datareader, db\_datawriter, and execute, alter, and references permissions on the database.

To assign these required permissions, perform the following steps:

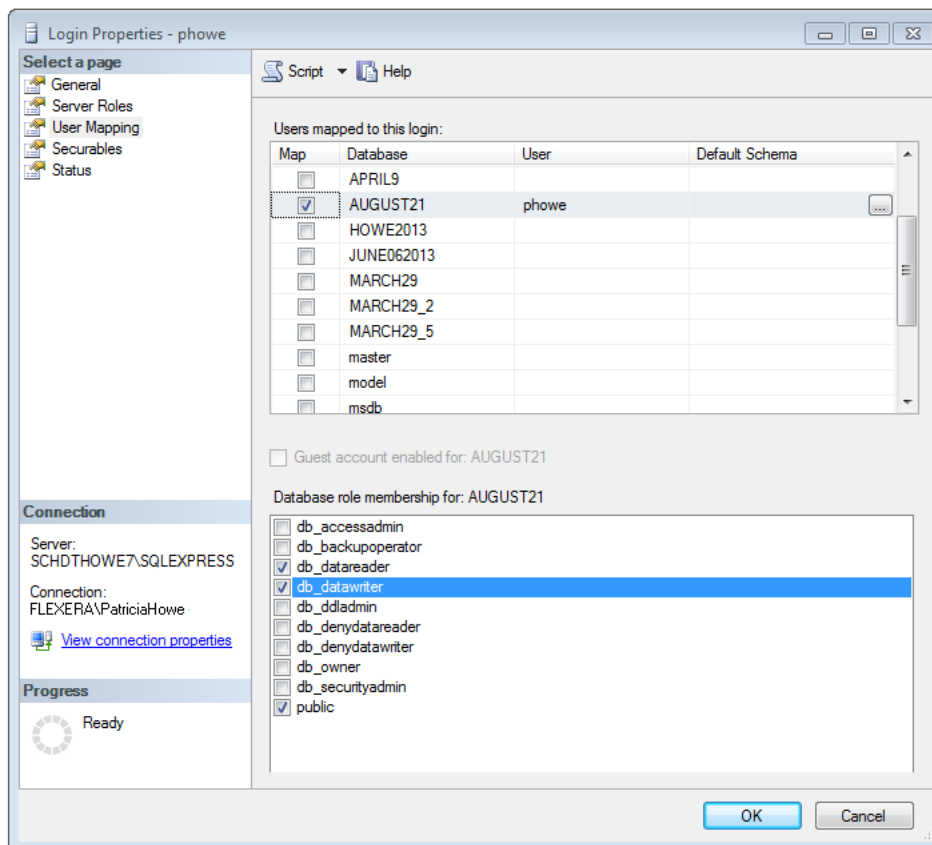
**Task**

**To assign required permissions to an AdminStudio Application Catalog:**

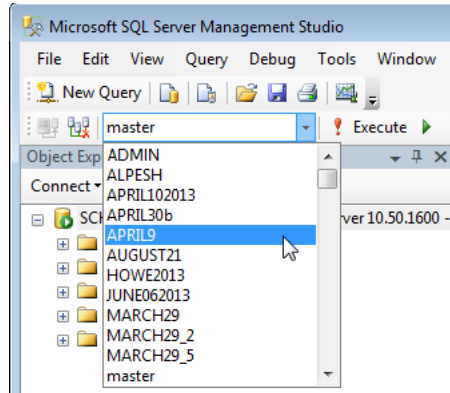
1. Open Microsoft SQL Server Management Studio.
2. In the **Object Explorer**, open the **Security > Logins** node and select the user account or user group that you want to assign permissions to.



3. Select **Properties** from the context menu. The **Login Properties** dialog box opens.
4. Select **User Mapping** in the tree. The **User Mapping** view of the **Login Properties** dialog box opens.



5. In the **Users mapped to this login** list, select the database that you want to assign permissions to.
6. In the **Database role membership for: [DatabaseName]** list, select db\_datareader and db\_datawriter.
7. Click **OK** to close the **Login Properties** dialog box.
8. In the toolbar, open the drop-down list and select the name of the AdminStudio database that you want to assign permissions to.



9. Next, click the **New Query** button in the toolbar to open the **Query Editor**.
10. Enter the following query:

```
grant execute to [username]
grant alter to [username]
grant references to [username]
```

For example:

```
SQLQuery1.sql - SCHDTHOWE7\...52)))*
grant execute to [phowe]
grant alter to [phowe]
grant references to [phowe]
```

11. Click the **Execute** button in the toolbar. The following message will be displayed:  
Command(s) completed successfully.

## Accounts for Integration of AdminStudio and App Portal with FlexNet Manager Suite

There are two requirements for accounts used in either AdminStudio or App Portal to allow integration with FlexNet Manager Suite / FlexNet Manager Platform:

- **Members of an appropriate Active Directory security group**—Because FlexNet Manager Suite or FlexNet Manager Platform is configured to use Windows Authentication, integration accounts must be members of an appropriate Active Directory security group in order to access FlexNet Manager Suite / FlexNet Manager Platform.



---

**Note** • While AdminStudio normally runs under the normal user account, any account used to integrate with FlexNet Manager Suite / FlexNet Manager Platform must be in an appropriate security group.

- **Assigned to suitable roles**—Internally within FlexNet Manager Suite / FlexNet Manager Platform, the accounts must be assigned to suitable roles that provide appropriate access controls.

Meeting these conditions allows the accounts both to look up products (with Flexera Identifiers) in the Application Recognition Library, and to set reservations against available licenses. The procedures for configuring accounts are described below.

- [Permissions to Access FlexNet Manager Suite / FlexNet Manager Platform](#)
- [Privileges Within FlexNet Manager Suite 2015 or Later](#)
- [Privileges Within FlexNet Manager Platform 9.2.3](#)
- [Privileges Within FlexNet Manager Platform](#)
- [Special Settings for Multi-Server Implementations](#)
- [FlexNet Manager System Account on the AdminStudio or AppPortal Machines](#)

## Permissions to Access FlexNet Manager Suite / FlexNet Manager Platform

While it is possible to create an Active Directory domain group from scratch, this requires detailed knowledge of directories where FlexNet Manager Suite or FlexNet Manager Platform is installed. It is far simpler to make use of the existing group used to control access. At the same time, it is good practice to have a distinct group in which integration accounts are contained, named according to enterprise conventions. These two approaches can be used together by creating a custom group which is a child of the existing group now controlling access. The new child group inherits the access rights already functioning in its parent group.



### Task

#### To enable authentication for FlexNet Manager Suite / FlexNet Manager Platform:

1. Identify the Active Directory security group used to grant access to FlexNet Manager Suite / FlexNet Manager Platform. By default, this is called **MGS Compliance Users**.
2. In Active Directory, create a domain group as a child of **MGS Compliance Users** (or equivalent), and name the new group according to corporate conventions (for example, **Flexera Integration Accounts**).
3. Add all the integration accounts (accounts for AdminStudio or App Portal users that may access features from FlexNet Manager Suite / FlexNet Manager Platform) to your new child group.

## Privileges Within FlexNet Manager Suite 2015 or Later

Privileges to access various functional areas within FlexNet Manager Suite 2015 or later are managed through access rights that are assigned to roles within that product. When appropriate roles exist, user accounts must be both created as operators and assigned to the roles in order to inherit access rights.

- [Configuring a New Role Within FlexNet Manager Suite 2015 or Later](#)
- [Creating the Appropriate Service Account Records](#)

### Configuring a New Role Within FlexNet Manager Suite 2015 or Later

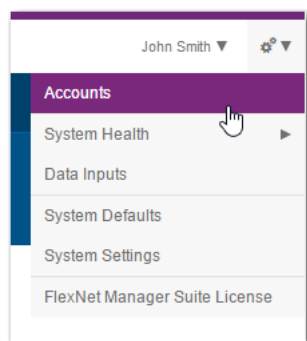
To configure a new role within FlexNet Manager Suite, perform the following steps:



### Task

#### To configure a new role within FlexNet Manager Suite:

1. In FlexNet Manager Suite, select **Accounts** on the **Options** menu:



The **All Accounts** tab of the **Accounts** page opens.

2. Select the **Roles** tab. The **Roles** view opens.

3. Scroll down until you see the Web Service role and click the copy icon.



The **Create a Role** view opens.

**Accounts** Create and allocate roles and manage accounts.

**Create a Role**

Name:

Description: Through the web API, Web Service accounts may access many objects in the FlexNet Manager Suite database. By default, privileges may be limited (for example, read-only).

**Access rights**

Restrict the data available to this role to objects owned by these groups and their descendants.

Location:

Corporate unit:

Cost center:

Category:

[Expand all](#) / [Collapse all](#)

Administration	Custom
Applications	Read only
Business reporting portal	None

4. In the **Name** field, enter **Integration**.
5. Click the arrow next to each of the following product features and select the specified levels of access from the **Privileges** list:

Product Feature	Level of Access
Administration	None
Applications	Select one of the following: <ul style="list-style-type: none"> <li>• If you are using AdminStudio 2016 or later and are going to be creating new local Flexera Identifier entries, select <b>Full</b>.</li> <li>• If you are not using AdminStudio 2016 or later, select <b>Read only</b>.</li> </ul>
Business reporting portal	None
Licenses	Read only
Management views and reports	None
Roles	None

Product Feature	Level of Access
SAP	None
All other features	Read only

After you have set these access levels, the **Access rights** area should look like this:

Administration	None ◀
Applications	Full ◀
Business reporting portal	None ◀
Contracts	Read only ◀
Corporate units	Read only ◀
Cost centers	Read only ◀
Categories	Read only ◀
Inventory devices	Read only ◀
Discovery devices	Read only ◀
Hardware assets	Read only ◀
Licenses	Read only ◀
Locations	Read only ◀
Purchase orders	Read only ◀
Management views and reports	None ◀
Roles	None ◀
SAP	None ◀
Users	Read only ◀
Vendors	Read only ◀

6. Click **Create**.

### Creating the Appropriate Service Account Records

With the role(s) configured, move on to creating the appropriate service account records. These record the account names (identical to the names registered in the Active Directory security group) that will exercise the access rights just defined.

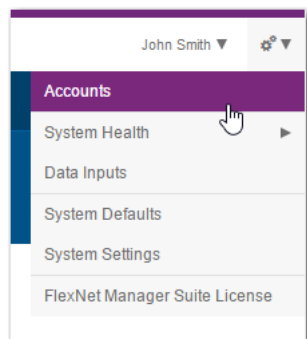


**Tip** • Other procedures are possible, such as importing the accounts from Active Directory and subsequently registering them as service accounts. This procedure assumes that an Active Directory import is inconvenient.

**Task**

**To register a service account and assign to groups within FlexNet Manager Suite 2015 or later:**

1. In FlexNet Manager Suite, select **Accounts** on the **Options** menu:



The **All Accounts** tab of the **Accounts** page opens.

2. Click **Create a service account**. The **Add Service Member to** page opens.

Flexera Software Account Management

My Account Administration

## Add Service Member to Flexera Melbourne QA Engineering 1

*\* Required*

Member Service Description

Email Address  Verify Email

Name

Phone

Use an Existing Address  ▼

Street 1

City

State / Province  ▼ Postal Code

Country  ▼

3. Enter the details of the App Portal Service account and then click **Save**. The **All Accounts** tab of the **Accounts** page opens, listing the new account name.



4. Select the new account in the list and then click **Open**. The **Account Properties** view opens.

The screenshot shows the 'Accounts' management interface. On the left is a sidebar with three buttons: 'All Accounts' (with a group of people icon), 'Unassigned Accounts' (with a person and gear icon), and 'Roles' (with a group of people icon). The main area is titled 'Accounts' with the subtitle 'Create and allocate roles and manage accounts.' Below this, the 'Account Properties' view for the 'App Portal System Account' is displayed. It has a sub-header 'Account' and contains the following fields: 'Account' (appportal@yourcompany.com), 'Name' (App Portal System Account), 'Email' (appportal@yourcompany.com), and 'Job title' (empty). Below these is a 'Permissions' section with 'Status' set to 'Enabled' and 'Role' set to 'Integration'. There are 'x' and '+' icons next to the 'Role' dropdown.

5. Set **Status** to **Enabled**.
6. Set **Role** to **Integration**.
7. Scroll to the bottom of the page and click **Save**.

### Privileges Within FlexNet Manager Platform 9.2.3

Privileges to access various functional areas within FlexNet Manager Suite are managed through access rights that are assigned to roles within that product. When appropriate roles exist, user accounts must be both created as operators and assigned to the roles in order to inherit access rights.

- [Configuring a New Role Within FlexNet Manager Platform](#)
- [Creating the Appropriate Operator Records](#)

#### Configuring a New Role Within FlexNet Manager Platform

To configure a new role within FlexNet Manager Platform, perform the following steps:



#### Task

##### *To configure a new role within FlexNet Manager Platform:*

1. In FlexNet Manager Platform, in the left-hand console tree, select the **Roles** node.
2. Click **Add a new role**.
3. In the **New role** dialog box, enter a unique name for the role you want to create (for example, **Integration Accounts**).
4. Click **OK**.
5. In the left-hand console tree, expand the **Roles** node to expose the newly-created role; right-click the role and select **Manage access rights...** from the context menu. The **Manage Access Rights** dialog box opens.



6. Select the specified levels of access for the following product features:

Product Feature	Level of Access
Software Assets	Administrator access
Custom Views and Reports	Normal access
Business Reporting Portal	No access
Administration	No access
All other areas	Read-only access

7. Click **OK**.



**Tip** • If you are concerned about users from AdminStudio using their accounts to log in to FlexNet Manager Platform and modify license data directly, you can repeat this procedure to create a second role exclusively for users of AdminStudio. Give it a distinct name, and rights identical with the above **except** that **Software Assets** require **Read-only access** for these personnel.

### Creating the Appropriate Operator Records

With the role(s) configured, move on to creating the appropriate operator records. These record the account names (identical to the names registered in the Active Directory security group) that will exercise the access rights just defined.



**Tip** • Other procedures are possible, such as importing the accounts from Active Directory and subsequently registering them as operators. This procedure assumes that an Active Directory import is inconvenient.



**Task**

**To register an operator and assign to groups within FlexNet Manager Platform:**

1. In FlexNet Manager Platform, in the left-hand console tree, select the **Operators** node.
2. Click **Add**.
3. In the **General** tab of the operator properties, to the right of the **Account** field, click the ellipsis button [...] to open the Windows standard **Select User** dialog box.
4. Navigate to, and select, an account you previously registered in your Active Directory security group (such as **Flexera Integration Accounts** or **MGS Compliance**).
5. Record any other details you choose for this account. For example, for users of AdminStudio, you may wish to name the individual personnel for later tracking.
6. On the **Roles** tab, select **Enable operator to use FlexNet Manager Platform**.
7. At the bottom of the panel, click **Add**.
8. Use the fly-out list to choose the appropriate role (double-click, or select the row and click **Select**).
9. Click **OK** to save the operator's properties.
10. Repeat this procedure for each operator.

## Privileges Within FlexNet Manager Platform

Privileges to access various functional areas within FlexNet Manager Platform are managed through access rights that are assigned to roles within that product. When appropriate roles exist, user accounts must be both created as operators and assigned to the roles in order to inherit access rights.

- [Configuring a New Role Within FlexNet Manager Platform](#)
- [Creating the Appropriate Operator Records](#)

### Configuring a New Role Within FlexNet Manager Platform

To configure a new role within FlexNet Manager Platform, perform the following steps:



**Task**

**To configure a new role within FlexNet Manager Platform:**

1. In FlexNet Manager Platform, in the left-hand console tree, select the **Roles** node.
2. Click **Add a new role**.
3. In the **New role** dialog box, enter a unique name for the role you want to create (for example, **Integration Accounts**).
4. Click **OK**.
5. In the left-hand console tree, expand the **Roles** node to expose the newly-created role; right-click the role and select **Manage access rights...** from the context menu. The **Manage Access Rights** dialog box opens.



6. Select the specified levels of access for the following product features:

Product Feature	Level of Access
Software Assets	Administrator access
Custom Views and Reports	Normal access
Business Reporting Portal	No access
Administration	No access
All other areas	Read-only access

7. Click **OK**.



**Tip** • If you are concerned about users from AdminStudio using their accounts to log in to FlexNet Manager Platform and modify license data directly, you can repeat this procedure to create a second role exclusively for users of AdminStudio. Give it a distinct name, and rights identical with the above **except** that **Software Assets** require **Read-only access** for these personnel.

**Creating the Appropriate Operator Records**

With the role(s) configured, move on to creating the appropriate operator records. These record the account names (identical to the names registered in the Active Directory security group) that will exercise the access rights just defined.



**Tip** • Other procedures are possible, such as importing the accounts from Active Directory and subsequently registering them as operators. This procedure assumes that an Active Directory import is inconvenient.



**Task**

**To register an operator and assign to groups within FlexNet Manager Platform:**

1. In FlexNet Manager Platform, in the left-hand console tree, select the **Operators** node.
2. Click **Add**.
3. In the **General** tab of the operator properties, to the right of the **Account** field, click the ellipsis button [...] to open the Windows standard **Select User** dialog box.
4. Navigate to, and select, an account you previously registered in your Active Directory security group (such as **Flexera Integration Accounts** or **MGS Compliance**).
5. Record any other details you choose for this account. For example, for users of AdminStudio, you may wish to name the individual personnel for later tracking.
6. On the **Roles** tab, select **Enable operator to use FlexNet Manager Platform**.
7. At the bottom of the panel, click **Add**.
8. Use the fly-out list to choose the appropriate role (double-click, or select the row and click **Select**).
9. Click **OK** to save the operator's properties.
10. Repeat this procedure for each account.

## Special Settings for Multi-Server Implementations

FlexNet Manager Suite On Premises or FlexNet Manager Platform may be installed on a single server, or on multiple servers so that the database is separate from the core compliance server. In such a multi-server implementation, the **App Pool Identity Account** configured within Microsoft IIS to support the web API (accessed by both AppPortal and AdminStudio) must be trusted by the separate SQL Server computer for delegation. For instructions see, [Resolving Active Directory “Double Hop” Issues Which Occur if FlexNet Manager Suite and SQL Server are on Separate Computers](#).


## FlexNet Manager System Account on the AdminStudio or AppPortal Machines

The FlexNet Manager Suite On Premises / FlexNet Manager Platform system account does not need access to AdminStudio or AppPortal because the communication is driven from the users of those products, not from FlexNet Manager Suite On Premises / FlexNet Manager Platform.

# App Portal Accounts

The following table lists the App Portal accounts and the required permissions,

**Table 2-5 • App Portal Accounts and Privileges in the Integrated Solution**

App Portal Account	Product/Machine Account Needs Access To	Required Privileges
App Pool Identity Account / App Portal ESD Service Account	System Center 2012 Configuration Manager (or later)	<p>Currently requires Application Administrator permission on System Center Configuration Manager.</p>  <p><b>Note •</b> In future releases, only access to the App Portal Web Service and READ access to the SCCM SQL Server database will be required.</p>
App Pool Identity Account / App Portal ESD Service Account	FlexNet Manager Suite / FlexNet Manager Platform	See <a href="#">Accounts for Integration of AdminStudio and App Portal with FlexNet Manager Suite</a> .

# FlexNet Manager Suite On Premises / FlexNet Manager Platform Accounts

The following table lists the FlexNet Manager Suite On Premises / FlexNet Manager Platform accounts and the required permissions.

**Table 2-6 • FlexNet Manager Suite On Premises / FlexNet Manager Platform Accounts and Privileges in the Integrated Solution**

FlexNet Manager Suite On Premises or FlexNet Manager Platform Account	Product/Machine Account Needs Access To	Required Privileges
<b>App Pool Identity Account</b>	<b>FlexNet Manager Platform machine</b>	<p>FlexNet Manager Platform must be configured to work with Windows Authentication.</p> <p>This App Pool Identity account for FlexNet Manager Platform needs to be trusted for delegation with the SQL Server computer. If your enterprise's security protocols require you install FlexNet Manager Platform and SQL Server on separate computers, you will need to enable a trusted delegation on the FlexNet Manager Platform computer to resolve this issue. For instructions, see <a href="#">Resolving Active Directory "Double Hop" Issues Which Occur if FlexNet Manager Suite and SQL Server are on Separate Computers</a>.</p>
<b>FlexNet Manager System Account</b>	<b>AdminStudio and App Portal</b>	<p>The FlexNet Manager Platform system account does not need access to AdminStudio or App Portal because the communication is driven from the users of those products, not from FlexNet Manager Platform.</p>

## FlexNet Manager Suite Cloud Service Account and Token

The following table lists the required FlexNet Manager Suite Cloud account.

**Table 2-7 • FlexNet Manager Suite Cloud Account and Token**

FlexNet Manager Suite Cloud Account	Account Needs Access To	Creating a Service Account and Obtaining a Token
Service Account	Invoke APIs in the FlexNet Manager Suite Cloud	You need to create a FlexNet Manager Suite Cloud Account and obtain an access token, as described in <a href="#">Creating a FlexNet Manager Suite Cloud Service Account and Obtaining a Token</a> .

### Creating a FlexNet Manager Suite Cloud Service Account and Obtaining a Token

To create a FlexNet Manager Suite Cloud service account and obtain an access token (which you will need when connecting App Portal to FlexNet Manager Suite Cloud), perform the following steps.



#### Task

##### To create a FlexNet Manager Suite Cloud Account:

1. Login to FlexNet Manager Suite Cloud.
2. Click on the **Tools** menu in the top right and select **Accounts**.  
The **Accounts** view opens with the **All Accounts** tab selected.
3. Click **Create a service account**. The **Add Service Member** view opens.
4. Enter the details of the App Portal Service account and then click **Save**. The **Display Token** screen opens, listing your access token.
5. Copy this token to a safe location.




**Important •** Save this token to a permanent location. This is the only time the token will be displayed. If you fail to save the token or misplace it, it cannot be retrieved; you would be required to create a new service account in order to obtain a new token.



# Workflow Manager Accounts

The following table lists the Workflow Manager accounts and the required permissions.

**Table 2-8 • Workflow Manager Accounts and Privileges in the Integrated Solution**

Workflow Manager Account	Product/Machine Requiring Privileges	Required Privileges
<b>AMS_SYSTEM account</b>	<b>Workflow Manager server</b>	<p>The AMS_SYSTEM account on the Workflow Manager server requires the following privileges:</p> <ul style="list-style-type: none"> <li>• <b>IIS_WPG group member</b>—Must be a member of the local IIS_WPG group (or IIS_USRS) on the web server.</li> <li>• <b>Modify permissions on file share</b>—Must have “modify” permissions on the Workflow Manager file share.</li> <li>• <b>Email permissions</b>—Permission to send e-mail through the SMTP server.</li> <li>• <b>Active Directory query permission</b>—Permission to query Active Directory.</li> <li>• <b>Local Administrators group member</b>—If you will be calling any of the AdminStudio Platform APIs in the iPlugin DLL, this account must be a member of the local Administrators group.</li> </ul>
<b>App Pool Identity Account</b>	<b>SQL Server</b>	<p>Starting with Workflow Manager 2013, if you configure Workflow Manager to connect to SQL Server with Windows Authentication, the domain account that you specify for the App Pool needs db_reader, db_writer, and execute permissions on the AdminStudio database.</p> <div>  <p><b>Note •</b> The Workflow Manager account does not require these permissions if connecting to SQL Server using an SQL Server user account (which already has db_reader, db_writer, and execute permissions).</p> </div>

## System Center Configuration Manager Accounts

The following table lists the System Center 2012 Configuration Manager (or later) accounts and the required permissions.

**Table 2-9 •** System Center Configuration Manager Accounts and Privileges in the Integrated Solution

System Center 2012 Configuration Manager (or Later) Account	Product/Machine Requiring Privileges	Required Privileges
App Pool identity account	System Center 2012 Configuration Manager (or later) Server	Requires privileges to run System Center Configuration Manager, but does not require special privileges to any of the other products in the integrated solution.

## Establish Two-Way Trusts Between Multiple Domains

Windows NT authentication is used to communicate across these integrated Flexera Software products. Therefore, if the customer's environment contains multiple domains, and if your Flexera Software products are installed on different domains, it is recommended that all domains have two-way trusts between them.

- **A trust between domains is required for communication**—Users in one domain need to be authenticated and authorized to use resources in another domain. To provide authentication and authorization capabilities between clients and servers in different domains, there must be a trust between the two domains. Trusts are the underlying technology by which secured Active Directory communications occur, and are an integral security component of the Windows Server network architecture.
- **Trusts act as bridges that allow only validated authentication requests to travel between domains**—When a trust exists between two domains, the authentication mechanisms for each domain trust the authentications coming from the other domain. Trusts help provide for controlled access to shared resources in a resource domain (the trusting domain) by verifying that incoming authentication requests come from a trusted authority (the trusted domain). In this way, trusts act as bridges that allow only validated authentication requests to travel between domains.
- **Two-way trusts**—How a specific trust passes authentication requests depends on how it is configured; trust relationships can be *one-way*, providing access from the trusted domain to resources in the trusting domain, or *two way*, providing access from each domain to resources in the other domain.

For more information and instructions, see the following articles:

- [MSDN: What Are Domain and Forest Trusts?](#)
- [MSDN: How Domain and Forest Trusts Work](#)
- [TechRepublic: An Overview of the Active Directory Domains And Trusts Console](#)

# Port Requirements


In the integrated solution, FlexNet Manager Suite / FlexNet Manager Platform, AdminStudio, App Portal, and Workflow Manager are required to communicate with each other, and that communication requires that certain ports are opened on firewalls between the products. This section serves as a reference for the ports that the products use, and it can be used as a basis for configuring firewall rules.

- [App Portal / App Broker Outbound Port Requirements](#)
- [AdminStudio Outbound Port Requirements](#)
- [Workflow Manager Outbound Port Requirements](#)
- [FlexNet Manager Suite Outbound Port Requirements](#)
- [Flexera Service Gateway Outbound Port Requirements](#)


## App Portal / App Broker Outbound Port Requirements

App Portal / App Broker has the following outbound port requirements.

**Table 2-10** • App Portal / App Broker Outbound Port Requirements

Target Program	Uses These Ports
<b>Active Directory</b>	See the following article in the Microsoft TechNet Library: <i>Active Directory and Active Directory Domain Services Port Requirements</i> <a href="http://technet.microsoft.com/en-us/library/dd772723(v=WS.10).aspx">http://technet.microsoft.com/en-us/library/dd772723(v=WS.10).aspx</a>
<b>Flexera Service Gateway</b>	<ul style="list-style-type: none"> <li>• HTTP traffic over 8280.</li> <li>• HTTPS traffic over 9443.</li> </ul>  <p><b>Note</b> • This is a one-time lookup of the FlexNet Manager Suite endpoint when the Flexera Service Gateway server is configured (or reconfigured) in App Portal. After that, the FlexNet Manager Suite endpoint is stored in the App Portal database, and no further lookups to the Flexera Service Gateway server are necessary under normal operating conditions.</p>
<b>FlexNet Manager Suite</b>	<ul style="list-style-type: none"> <li>• HTTP traffic over TCP 80.</li> <li>• HTTPS traffic over TCP 443 (or customer-designated alternate port).</li> </ul>

**Table 2-10 • App Portal / App Broker Outbound Port Requirements (cont.)**

Target Program	Uses These Ports
<b>System Center Configuration Manager (App Portal Web Service)</b>	<ul style="list-style-type: none"> <li>• HTTP traffic over TCP 80.</li> <li>• HTTPS traffic over TCP 443 (or customer-designated alternate port).</li> </ul>  <p><b>Note •</b> <i>If using SCCM 2007, the option to refresh client policy requires additional ports between the App Portal/Broker server and the client for RPC/WMI. However, this is very rare, as it also requires the App Portal/Broker service account to have local admin permissions on every client, which typically isn't allowed/realistic in most customer environments. In SCCM 2012/ConfigMgr Current Branch, we take advantage of the client notification channel between the SCCM server and the client, so there is no port requirement for communication directly from App Portal/Broker to the client.</i></p>
<b>SQL Server</b> <ul style="list-style-type: none"> <li>• App Portal Database</li> <li>• FlexNet Manager Suite Database</li> <li>• System Center Configuration Manager Database</li> </ul>	SQL traffic over TCP 1433 (or customer-designated alternate port).
<b>External Systems such as ITSM, Orchestrator, etc.</b>	Usually HTTP (TCP 80) / HTTPS (TCP 443), but dictated by the external system, not App Portal/Broker.


## AdminStudio Outbound Port Requirements

AdminStudio has the following outbound port requirements.


**Table 2-11 • AdminStudio Outbound Port Requirements**

Target Program	Uses These Ports
<b>Active Directory</b>	See the following article in the Microsoft TechNet Library: <i>Active Directory and Active Directory Domain Services Port Requirements</i> <a href="http://technet.microsoft.com/en-us/library/dd772723(v=WS.10).aspx">http://technet.microsoft.com/en-us/library/dd772723(v=WS.10).aspx</a>
<b>App Portal</b>	80
<b>Flexera Service Gateway</b>	9443 8280

**Table 2-11 • AdminStudio Outbound Port Requirements (cont.)**

Target Program	Uses These Ports
<b>FlexNet Manager Suite</b>	80 443 8889
<b>System Center Configuration Manager</b>	9 (Wake on LAN) 67, 68 (DHCP) 69 (TFTP) 80 (HTTP) 135 (RPC) 389 (LDAP) 443 (HTTPS) 445 (Server Message Block, SMB) 636 (LDAP SSL) 2701 (Remote Control) 3268 (LDAP Global Catalog) 3269 (LDAP Global Catalog SSL) 3389 (Remote Assistance) 4011 (BINL) 5985 (Windows Remote Management HTTP) 5986 (Windows Remote Management HTTPS) 8530, 8531 (HTTP and HTTPS) 10123 (Client Notification) 16993 (Power control, provisioning, and discovery) 16995 (Serial over LAN and IDE redirection) 25536 (Wake-up proxy) 
<b>Note •</b> For more information, see the following article in the Microsoft TechNet Library: <a href="http://technet.microsoft.com/en-us/library/hh427328.aspx">Technical Reference for Ports Used in Configuration Manager at http://technet.microsoft.com/en-us/library/hh427328.aspx</a>	
<b>SCCM File Share Server</b>	445 (Server Message Block, SMB)
<b>SMTP Server</b>	25


**Table 2-11 • AdminStudio Outbound Port Requirements (cont.)**

Target Program	Uses These Ports
<b>SQL Server</b>	1433 (SQL Server Service) 1434 (SQL Server Browser) 4022 (SQL Server Service Broker)  <p><b>Note</b> • If SQL Server is configured to listen on an alternate port, make sure the firewall allows communication on that port.</p>
<b>Workflow Manager</b>	80

## Workflow Manager Outbound Port Requirements

Workflow Manager has the following outbound port requirements.


**Table 2-12 • Workflow Manager Outbound Port Requirements**

Target Program	These Ports
<b>Active Directory</b>	See the following article in the Microsoft TechNet Library: <i>Active Directory and Active Directory Domain Services Port Requirements</i> <a href="http://technet.microsoft.com/en-us/library/dd772723(v=WS.10).aspx">http://technet.microsoft.com/en-us/library/dd772723(v=WS.10).aspx</a>
<b>Flexera Service Gateway</b>	9443 8280
<b>SMTP Server</b>	25
<b>SQL Server</b>	1433 (SQL Server Service) 1434 (SQL Server Browser) 4022 (SQL Server Service Broker)  <p><b>Note</b> • If SQL Server is configured to listen on an alternate port, make sure the firewall allows communication on that port.</p>

## FlexNet Manager Suite Outbound Port Requirements

FlexNet Manager Suite has the following outbound port requirements.

**Table 2-13 • FlexNet Manager Suite Outbound Port Requirements**

Target Program	Uses These Ports
<b>Active Directory</b>	See the following article in the Microsoft TechNet Library: <i>Active Directory and Active Directory Domain Services Port Requirements</i> <a href="http://technet.microsoft.com/en-us/library/dd772723(v=WS.10).aspx">http://technet.microsoft.com/en-us/library/dd772723(v=WS.10).aspx</a>
<b>Flexera Service Gateway</b>	9443 8280
<b>SMTP Server</b>	25
<b>SQL Server</b>	1433 (SQL Server Service) 1434 (SQL Server Browser) 4022 (SQL Server Service Broker)  <b>Note •</b> If SQL Server is configured to listen on an alternate port, make sure the firewall allows communication on that port.

## Flexera Service Gateway Outbound Port Requirements

Flexera Service Gateway has the following outbound port requirements.


**Table 2-14 • Flexera Service Gateway Outbound Port Requirements**

Target Program	Uses These Ports
<b>Active Directory</b>	See the following article in the Microsoft TechNet Library: <i>Active Directory and Active Directory Domain Services Port Requirements</i> <a href="http://technet.microsoft.com/en-us/library/dd772723(v=WS.10).aspx">http://technet.microsoft.com/en-us/library/dd772723(v=WS.10).aspx</a>
<b>SMTP Server</b>	25

# Recommended Proof-of-Concept Configuration

When performing a proof-of-concept demonstration of AdminStudio / App Portal / FlexNet Manager Platform integration, the following self-enclosed infrastructure is recommended:

**Table 2-15 • Recommended Proof-of-Concept Configuration**

Machine	Operating System	Applications
<b>Machine 1: AdminStudio</b>	Windows Server OS (2008 R2 or 2012)	<ul style="list-style-type: none"> <li>• System Center 2012 R2 Configuration Manager (or later)</li> <li>• SQL Server 2012 or later</li> <li>• AdminStudio 2014 or later</li> </ul>
<b>Machine 2: App Portal</b>	Windows Server OS (2008 R2 or 2012)	<ul style="list-style-type: none"> <li>• App Portal 2014 or later</li> </ul>
<b>Machine 3: FlexNet Manager Suite On Premises</b>	Windows Server OS (2008 R2 or 2012)	<ul style="list-style-type: none"> <li>• FlexNet Manager Suite On Premises 2014 or later</li> <li>• SQL Server 2012 or later</li> <li>• Flexera Service Gateway</li> </ul>
<b>Machine 4: Domain Controller</b>	Windows Server OS (2008 R2 or 2012)	<ul style="list-style-type: none"> <li>• Domain Controller</li> <li>• DNS / DHCP</li> </ul>
<b>Machine 5: System Center Configuration Manager Client</b>	Windows Desktop OS (Windows 8, 7, or XP)	<ul style="list-style-type: none"> <li>• System Center 2012 R2 Configuration Manager (or later) Client</li> </ul>
		 <p><b>Note •</b> Used to test requesting an application from App Portal and observing it being installed.</p>



# 3

## Installing and Configuring Flexera Service Gateway 2

Flexera Service Gateway 2 is a component that enables AdminStudio, App Portal, Workflow Manager, and FlexNet Manager Suite / FlexNet Manager Platform to communicate.

Information about installing and using Flexera Service Gateway 2 can be found in the following guide:

[Flexera Service Gateway 2 Installation and Administration Guide](#)



# 4

## Configuring the FlexNet Manager Suite Cloud Environment

This section explains how to configure FlexNet Manager Suite Cloud for integration with App Portal.

- [Configuring the FlexNet Manager Suite Inventory Beacon](#)
- [Registering FlexNet Manager Suite Cloud with the Flexera Service Gateway](#)
- [Registering App Portal with FlexNet Manager Suite Cloud and Flexera Service Gateway](#)

# Configuring the FlexNet Manager Suite Inventory Beacon

An inventory beacon is a computer located within your enterprise that gathers software inventory and other information that you specify, and uploads the data to FlexNet Manager Suite.

You download the software to install on an inventory beacon server from FlexNet Manager Suite. After installation, you use the inventory beacon software to download a configuration file that has been customized for this beacon (do not share these files between beacons) and load it into the beacon.

To configure the FlexNet Manager Suite environment, perform the following steps:



## Task

### To configure the FlexNet Manager Suite inventory beacon:

1. Obtain your Service Account details (URL, account name, password, FlexNet Manager Suite Cloud access token) for an instance of FlexNet Manager Suite Cloud.



**Important** • Record your FlexNet Manager Suite Cloud access token in a secure location. This token cannot be obtained again for an existing service account; a new service account would have to be created.

2. On the machine where you want to install the inventory beacon software, launch FlexNet Manager Suite and log in.



Now, it's easier than ever to achieve  
Software License Optimization.

As the complexity of managing software licenses continues to grow, Flexera Software's **FlexNet Manager Suite** is making it easier to maintain continuous license compliance and reduce ongoing costs for software.

The new Software as a Service (SaaS) delivery model of our market leading Software License Optimization solution provides the insights needed to make informed business decisions with features such as:

- At-a-glance license compliance position
- Visibility into areas of overspending and liability
- Views across the whole business, a single business unit, a specific publisher, software product or license

Sign in

Email Address

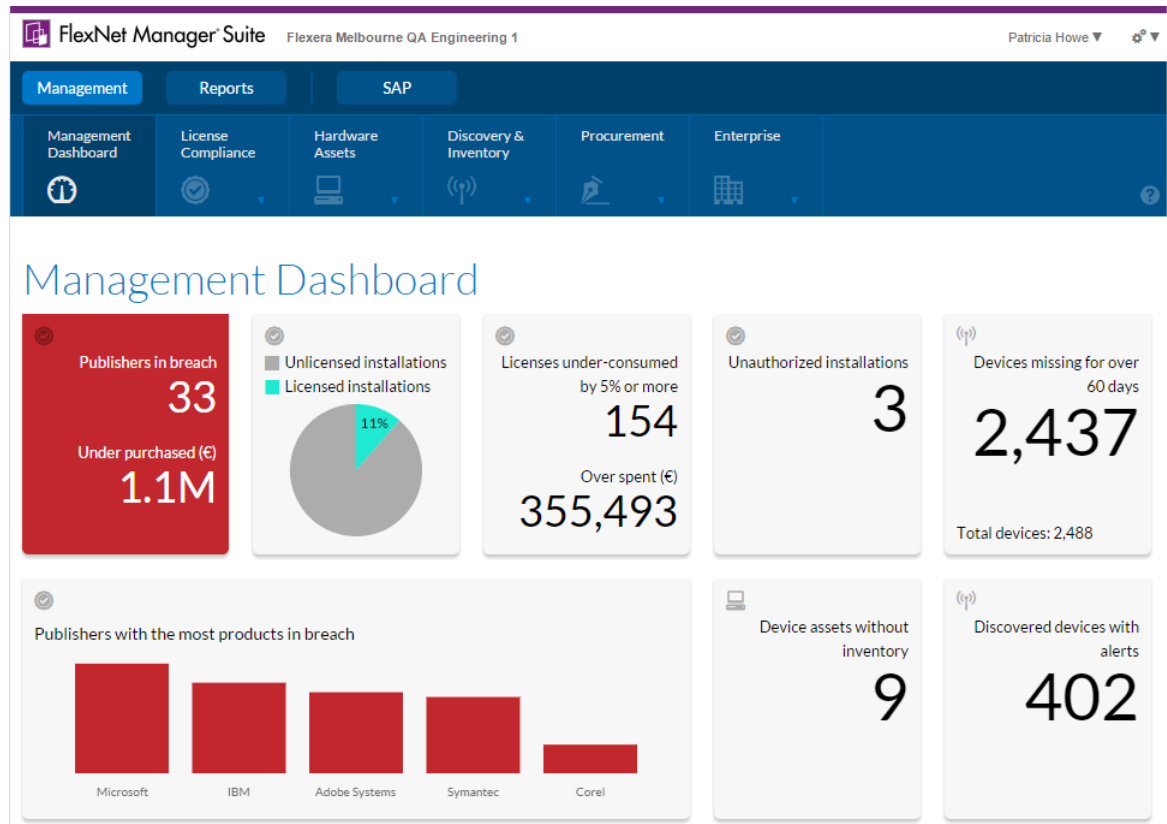
Password

Sign In

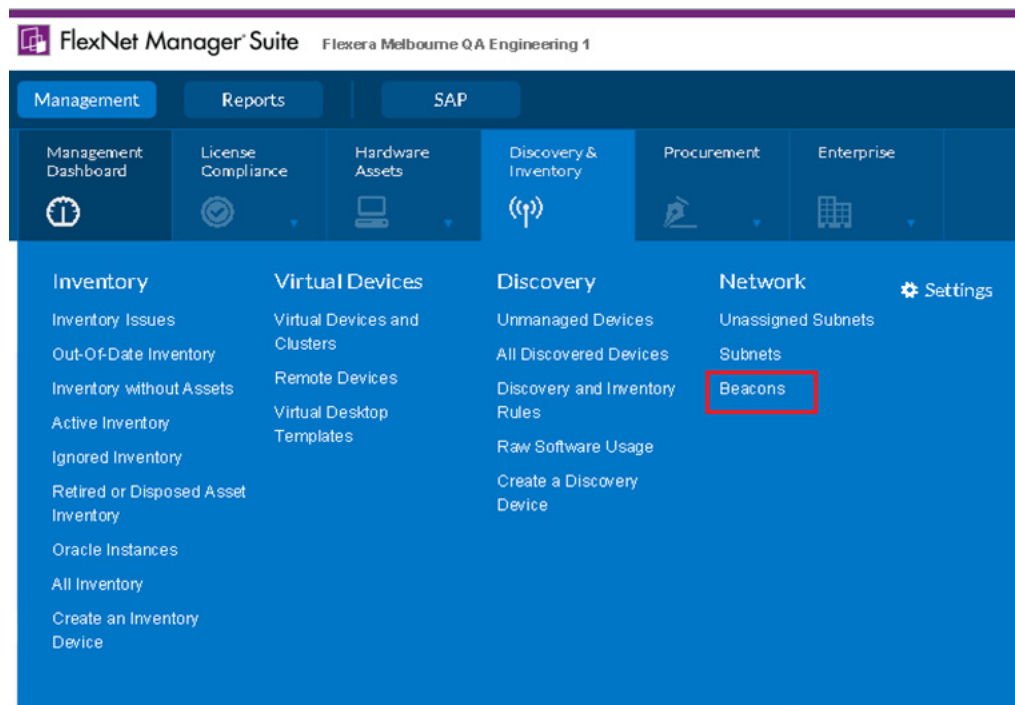
[Having trouble signing in?](#)

[Help with licensing and downloading your product.](#)

The FlexNet Manager Suite Home page is displayed.



3. On the **Discovery & Inventory** tab, click **Beacons** in the **Network** group.



The **Beacons** page opens.

**FlexNet Manager Suite** Flexera Melbourne QA Engineering 1 Patricia Howe

**Management** Reports SAP

Management Dashboard License Compliance Hardware Assets Discovery & Inventory Procurement Enterprise

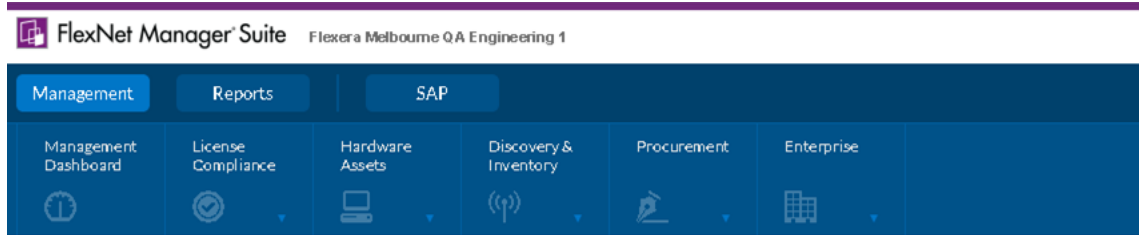
**Beacons** All beacons on your network

13 results returned 20 rows per page

Beacon/Subnet	Beacon status	Policy status	Site name	Actions
AP BLR_2K8QA1	Not reporting normally	Out of date		
AppPortalQA-BLR	Operating normally	Up to date		
+ F83 Inventory Beacon	Never reported	No policy		
ISASBeacon	Operating normally	Up to date		
+ Laurents beacon 1	Never reported	No policy		
+ Laurents Machine Beacon 2	Never reported	No policy		
mgs13beacon	Beacon disabled at server	No policy		
MikeMarinoBeacon	Operating normally	No policy		
+ Rob's training beacon 1	Never reported	No policy		
WalBeaconT2	Beacon disabled at server	No policy		
Win2008R2InvBeacon10(Aamer) 1	Beacon disabled at server	No policy		
Win7Aamer'sBeacon 1	Beacon disabled at server	No policy		
+ Windows7BeaconAamerCreated	Operating normally	Up to date		

13 results returned 20 rows per page

- Click the **Deploy a beacon** button. The **Deploy a Beacon** page opens.



## Deploy a Beacon

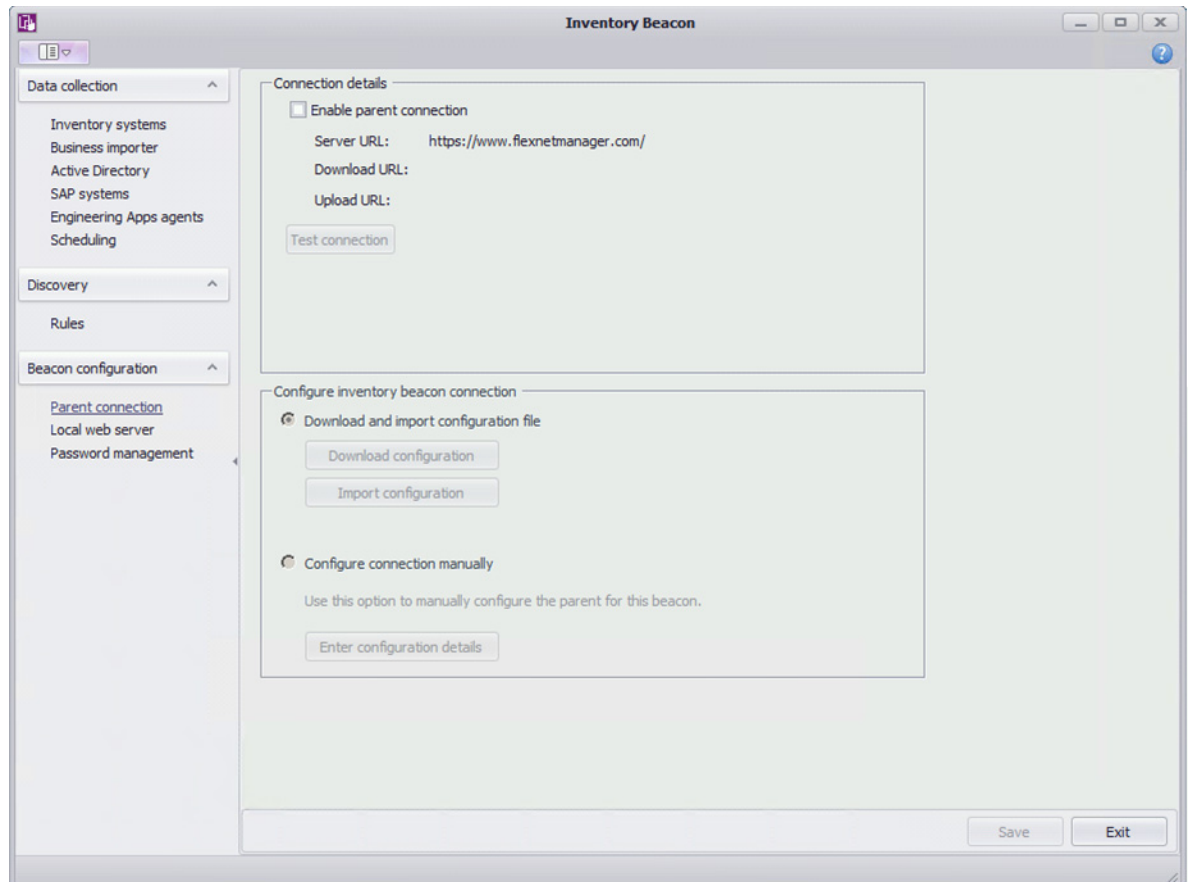


5. Click the **Download a beacon** button. The inventory beacon software is downloaded.
6. Run the inventory beacon installer using the default settings.



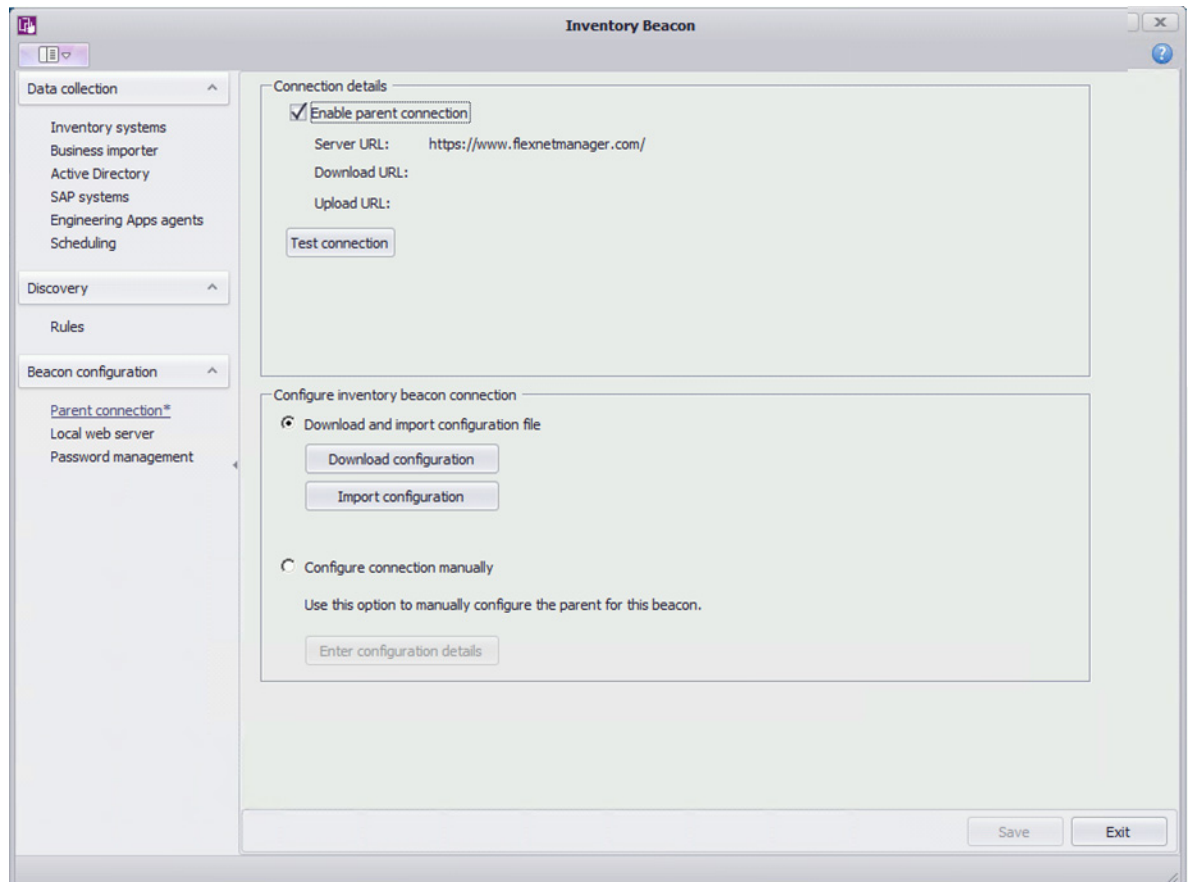
**Important** • Make sure that you connect to the cloud instance and download the inventory beacon software on the machine where you intend to install it.

7. Once installed, launch the **Inventory Beacon** executable and click on **Parent connection** under **Beacon configuration**. The **Parent Connection** details are displayed.



8. Select the **Enable parent connection** option. The **Download configuration** and **Import configuration** buttons under **Configure inventory beacon connection** are enabled.





9. Click the **Download configuration** button. The **Configure a Beacon** page of FlexNet Manager Suite Cloud opens, displaying a **Unique ID** number.

**In Unattended Installation of Inventory Beacons.**

Inventory beacons are now self upgrading. Choose from the **Upgrade mode** options to control this process for each beacon.

For normal operations, ensure that the **Configuration status** is Enabled.

In the **Name** field, provide a meaningful and distinctive name for this beacon that you will recognize later in lists of inventory sources.

When all fields are completed, click the **Download configuration** button to transfer the configuration file to your inventory beacon. When the download is complete, import the configuration file into the inventory beacon, following the instructions available in Help on the beacon.

This establishes communication between your inventory beacon and the FlexNet Manager Suite server. You will also need to configure local connections to your inventory sources where the beacon gathers inventory. For details, see Help on the beacon.

Parent beacon:

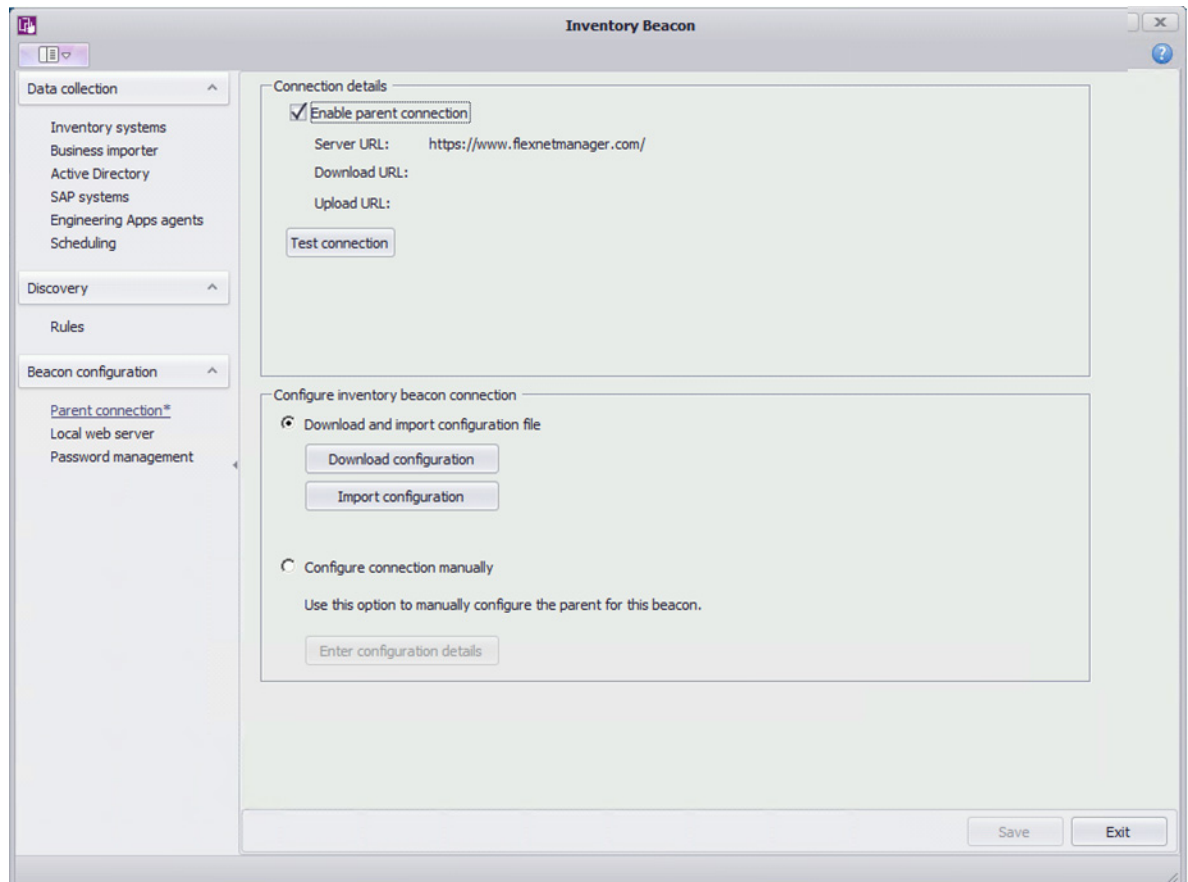
Unique ID: a1234567-b001-3456-c12c-d6789e234567

Name:

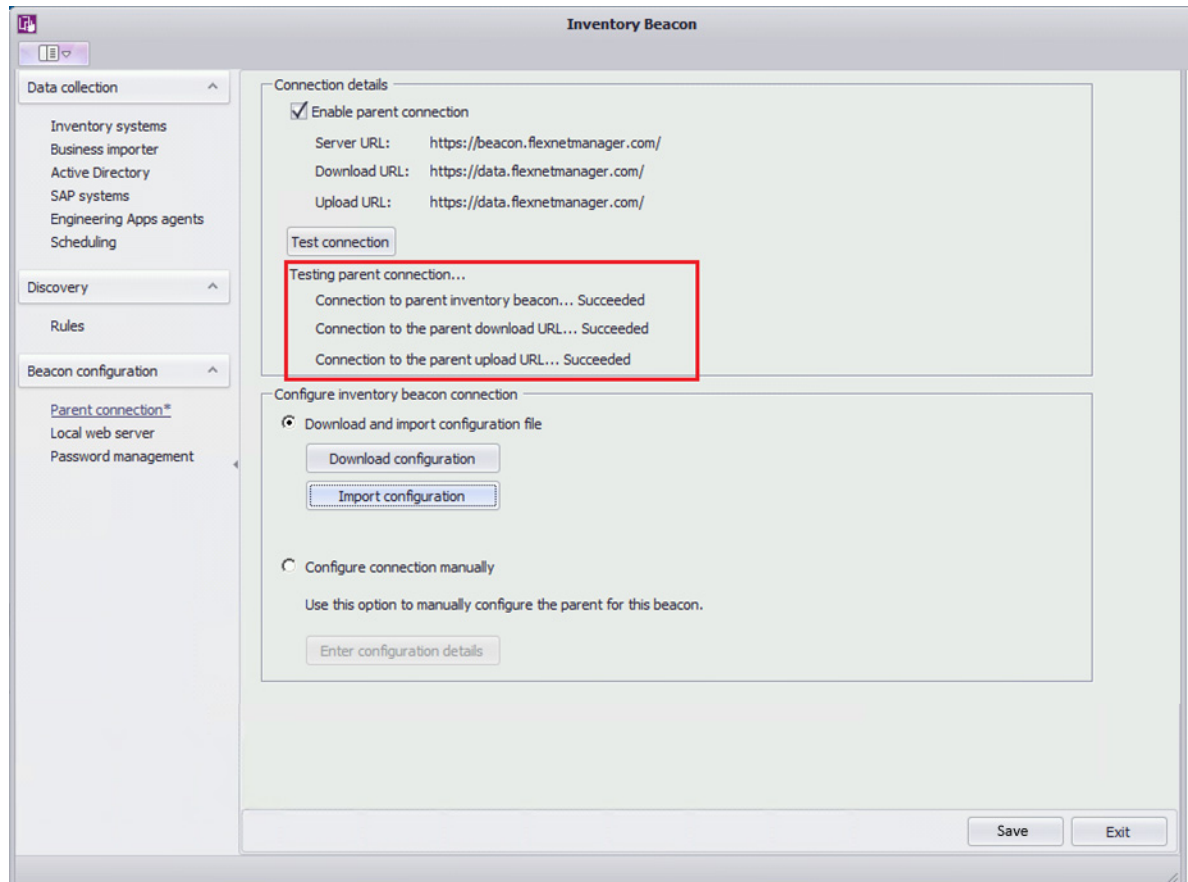
Upgrade mode:  ▼

Configuration status: ☐ Disabled ☒ Enabled

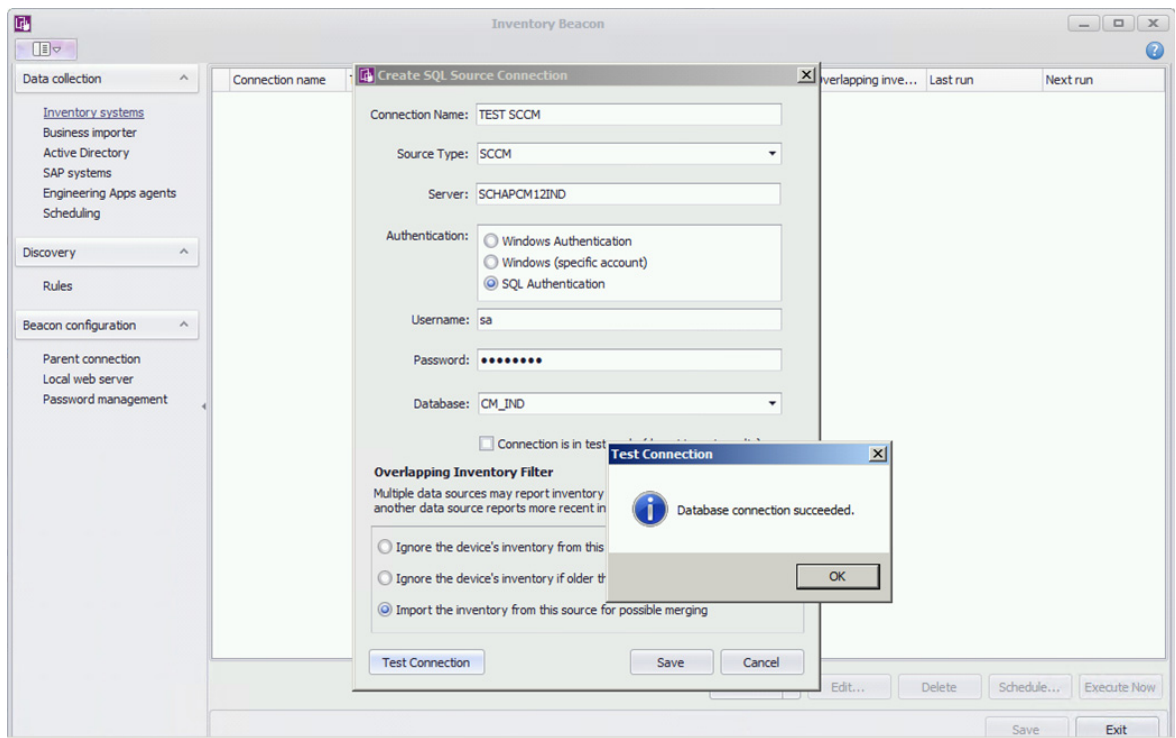
10. In the **Name** field, enter a name to identify this inventory beacon instance.
11. Click the **Download configuration** button.
12. Return to the **Parent Connection** view of the Inventory Beacon software.



13. Click on the **Import configuration** button. You will be prompted to upload a configuration file.
14. Upload the flxconfig configuration file that you downloaded from the **Configure Beacon** page of FlexNet Manager Suite Cloud.
15. Click the **Test connection** button. Progress messages are displayed.

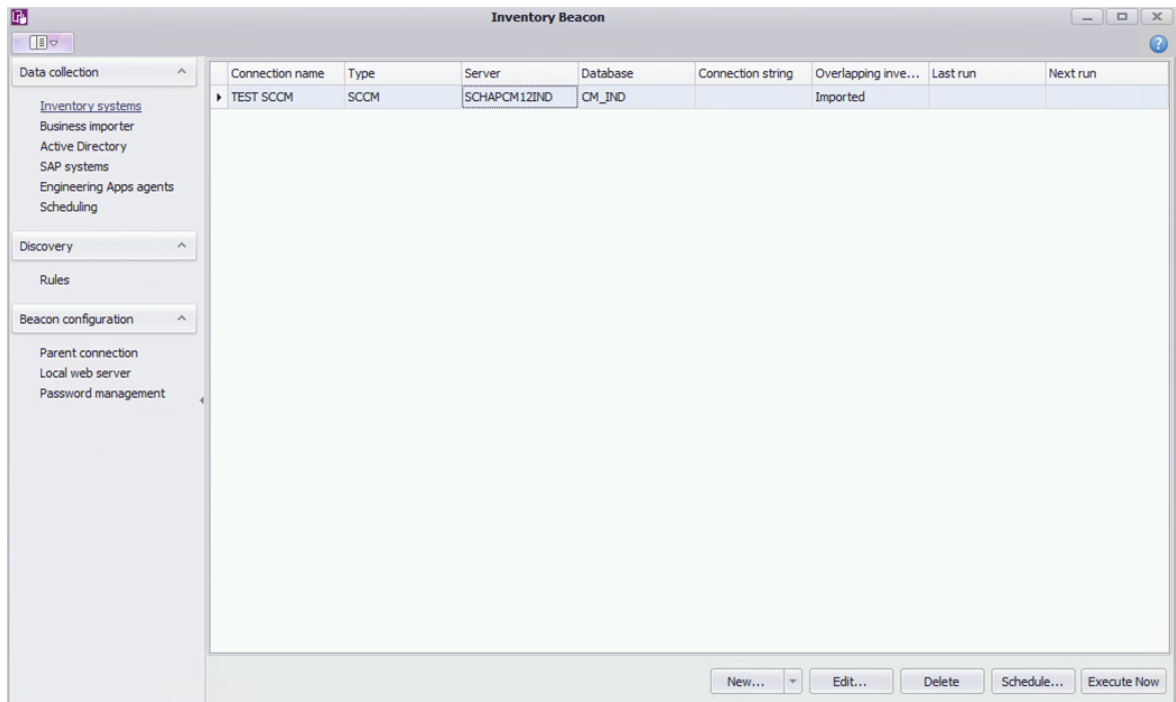


16. Click **Save** and **Exit**, and then relaunch the Inventory Beacon software.
17. Under **Data collection**, click on **Inventory systems** and configure your System Center Configuration Manager instances.

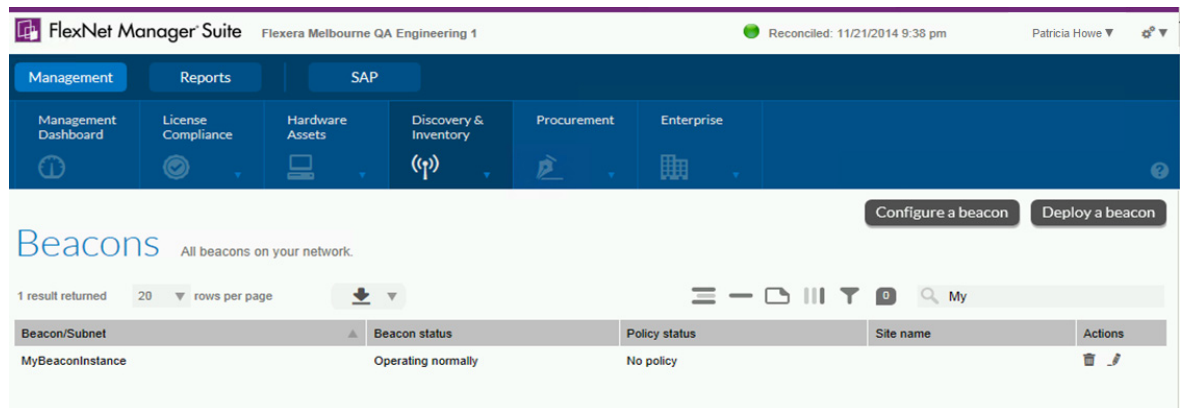


**Tip** • If you face issues configuring with **Windows Authentication** and **Windows (Specific Account)**, then try using **SQL Authentication**. To do this, this you need to set the **Authentication** mode to **SQL** and **Windows Authentication** mode on your SQL server hosting the System Center Configuration Manager database.

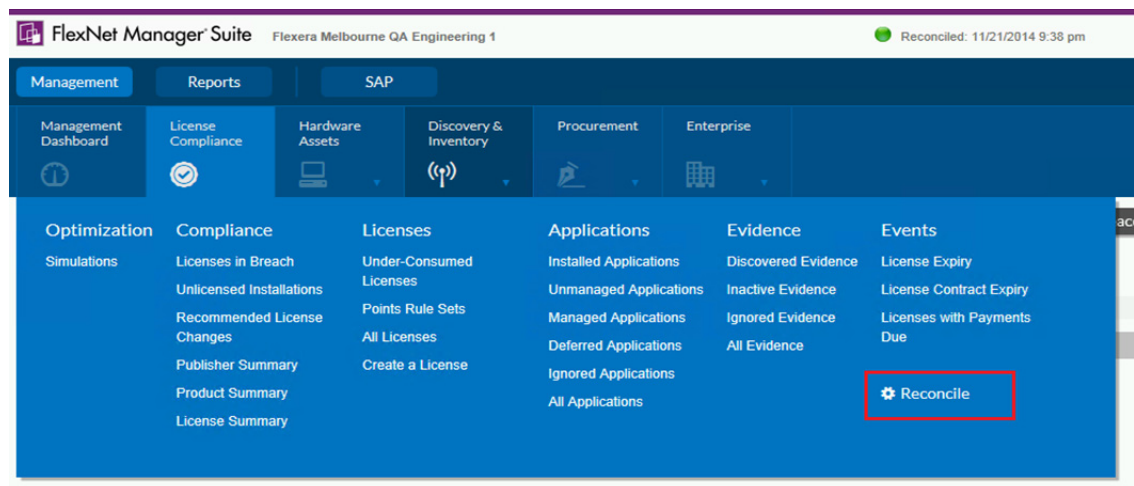
18. Save the inventory system settings. The new inventory system settings will be listed on the **Inventory Systems** view.



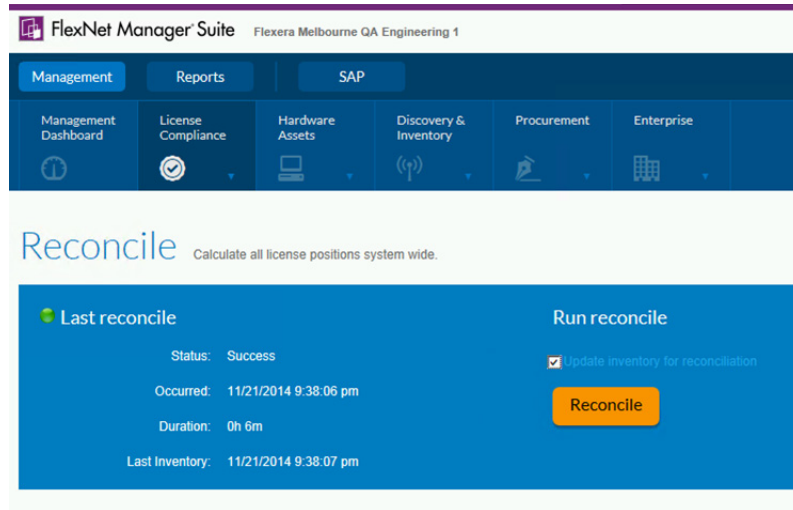
19. Select the connection and click **Execute Now**.
20. Return to FlexNet Manager Suite Cloud.
21. On the **Discovery & Inventory** tab, click **Beacons** in the **Network** group. The **Beacons** page opens and lists the newly installed inventory beacon.



22. On the **License Compliance** tab, click **Reconcile**.



The **Reconcile** page opens.



23. Select the **Update inventory for reconciliation** option and then click the **Reconcile** button.

After about 15 to 20 minutes, your System Center Configuration Manager inventory should be listed in the FlexNet Manager Suite Cloud user interface.

# Registering FlexNet Manager Suite Cloud with the Flexera Service Gateway

To register FlexNet Manager Suite Cloud with the Flexera Service Gateway, perform the following steps.



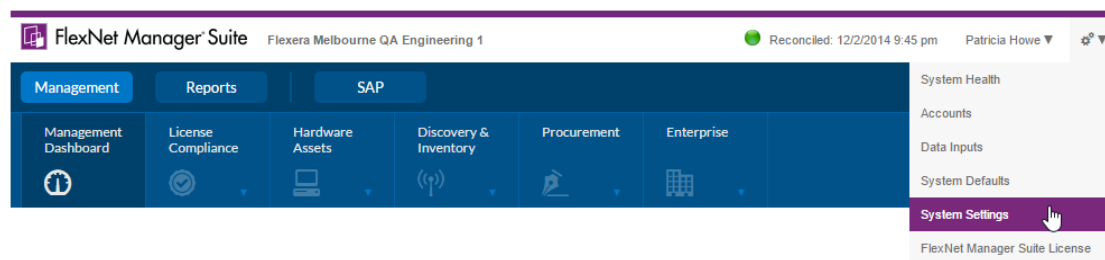
**Note** • In order to perform this step, you need to have a FlexNet Manager Suite license that has the **FNMP API integration enabled** option set to **Yes**. To see if this option is enabled, open the System menu and select **FlexNet Manager Suite License**.



## Task

**To register FlexNet Manager Suite Cloud with the Flexera Service Gateway:**

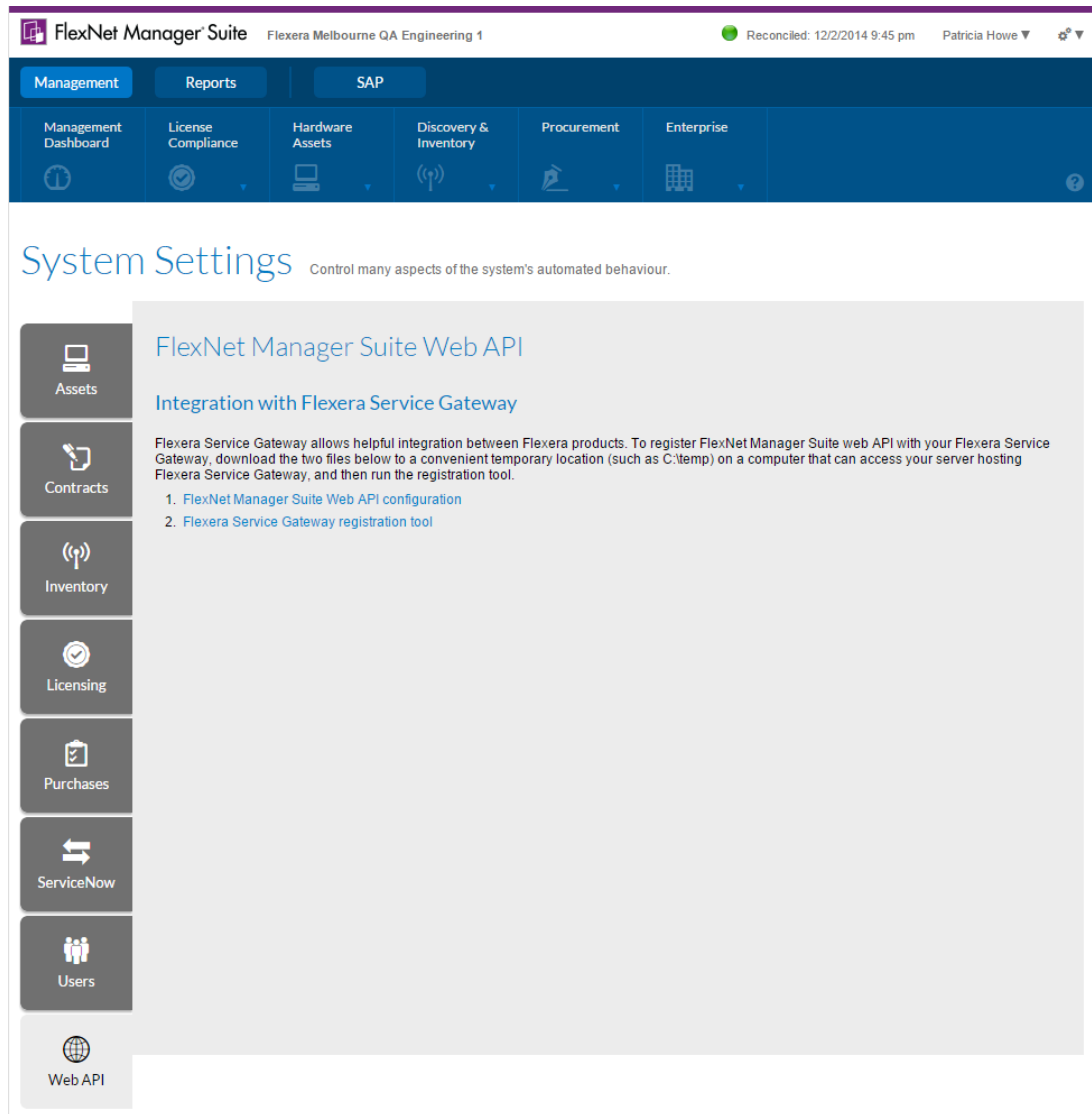
1. Download the Flexera Service Gateway Registration tool and `webapi.config` file from the FlexNet Manager Suite Cloud web site by performing the following steps:
  - a. Click on the Settings icon (top right corner) and then click **System Settings**.



The **System Settings** page opens.

- b. Open the **Web API** tab.





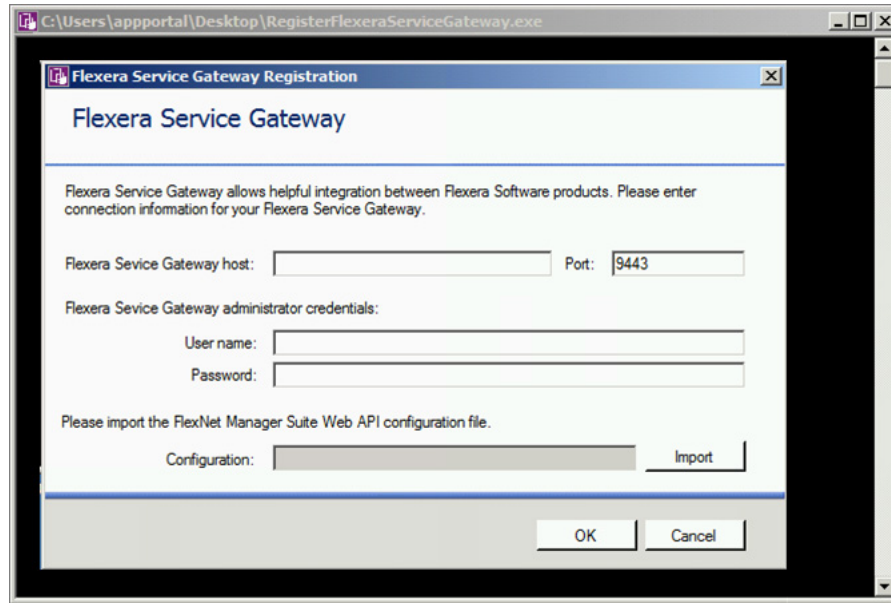
**Note** • The **Web API** tab is only displayed when that license term is present.

- c. Click **FlexNet Manager Suite Web API configuration**. The webapi.config file is downloaded.
- d. Click **Flexera Service Gateway registration tool**. The RegisterFlexeraServiceGateway.exe file is downloaded.



**Note** • While you can download these two files onto any computer, the computer must have network access to “your” gateway server.

2. Run the Flexera Service Gateway Registration tool (RegisterFlexeraServiceGateway.exe) and enter the **Flexera Service Gateway** host name, **Port**, **User name**, and **Password**



**Note** • The host can be an IP address, FQDN, or just a server name (if the DNS is OK).

3. Next to **Configuration**, click **Import** and select the `webapi.config` file that you just downloaded.
4. Click **OK**.

# Registering App Portal with FlexNet Manager Suite Cloud and Flexera Service Gateway

To register App Portal with FlexNet Manager Suite Cloud and Flexera Service Gateway, perform the following steps.



## Task

**To register App Portal with FlexNet Manager Suite Cloud and Flexera Service Gateway:**

1. Obtain the FlexNet Manager Suite Cloud access token for your login name.



**Note** • For instructions on obtaining a FlexNet Manager Suite Cloud access token, see [FlexNet Manager Suite Cloud Service Account and Token](#).

2. Launch App Portal.
3. On the **Admin** tab, select **Site Management > Settings > Integration**.
4. Enter the **Flexera Service Gateway Server Name** and the **FlexNet Manager Platform Cloud Access Token**.

App Portal Menu

- Site Management
- Admin Security
- Catalog Security
- Settings
- Imported Users and Computers
- Error Log
- Email Log
- Expressions
- Active Directory
- Workflows
- Workflow Groups
- Workflow Status
- Categories
- Catalog
- Commands and Actions
- Communication
- Catalog Management
- Inventory Management
- Deployment Management
- History

Save

General Web Site Deployment Active Directory Email Timers WOL Security **Integration**

Enable App Portal API ☒ (http://server/esd/aplasmx) You should modify NTFS Permissions on the aplasmx file to prevent unauthorized access prior to enabling the API.

Intrinsic Swimage Encore Integration

Enable Swimage Encore Integration ☐

Path to Encore API:  e.g. http://EncoreServer:8008/IntegrationWS.asmx

Default Scope ID:  4

Orchestrator Service URL:

Flexera Service Gateway Server Name:  NYCAPPD8801

Following services are currently registered with Flexera Service Gateway

- App Portal [schapppcm12kav]
- FlexNet Manager Platform [flexnetmanager.com]

FlexNet Manager Platform Cloud Access Token:

Alternate FlexNet Manager Platform Username (DOMAIN\Username):

Alternate FlexNet Manager Platform Password:

5. Click **Save**.



# Configuring FlexNet Manager Suite On Premises



---

**Note** • *FlexNet Manager Suite On Premises was previously known as FlexNet Manager Platform.*

When integrated with App Portal and AdminStudio, you can use FlexNet Manager Suite On Premises to automatically manage application licenses for App Portal catalog items. This section explains how to connect FlexNet Manager Suite On Premises to the Flexera Service Gateway so that it can communicate with App Portal and AdminStudio, and how to troubleshoot any issues that you might encounter.

- [Testing FlexNet Manager Suite On Premises Server Authentication Settings](#)
- [Connecting FlexNet Manager Suite On Premises to the Flexera Service Gateway](#)
- [Importing the Application Recognition Library \(ARL\)](#)
- [Troubleshooting FlexNet Manager Suite Communication Issues](#)
- [Viewing an Application's Flexera ID in FlexNet Manager Suite](#)
- [Upgrading FlexNet Manager Suite's Compliance Console](#)



---

**Important** • *To perform the steps in this chapter, you need to have already installed FlexNet Manager Suite On Premises.*

# Testing FlexNet Manager Suite On Premises Server Authentication Settings

The first thing that you should do to prepare the FlexNet Manager Suite On Premises server for integration (even before connecting to the Flexera Service Gateway) is to attempt to browse to the FlexNet Manager Suite ComplianceAPIService documentation page to determine whether you are prompted to enter network credentials. This will test whether the application server's authentication settings are set properly.



## Task

### To test the FlexNet Manager Suite server authentication settings:

1. On the FlexNet Manager Suite server machine, enter the following URL in a web browser:

`http://<FNMPServer>/ManageSoftServices/ComplianceAPIService/ComplianceAPIService.asmx`

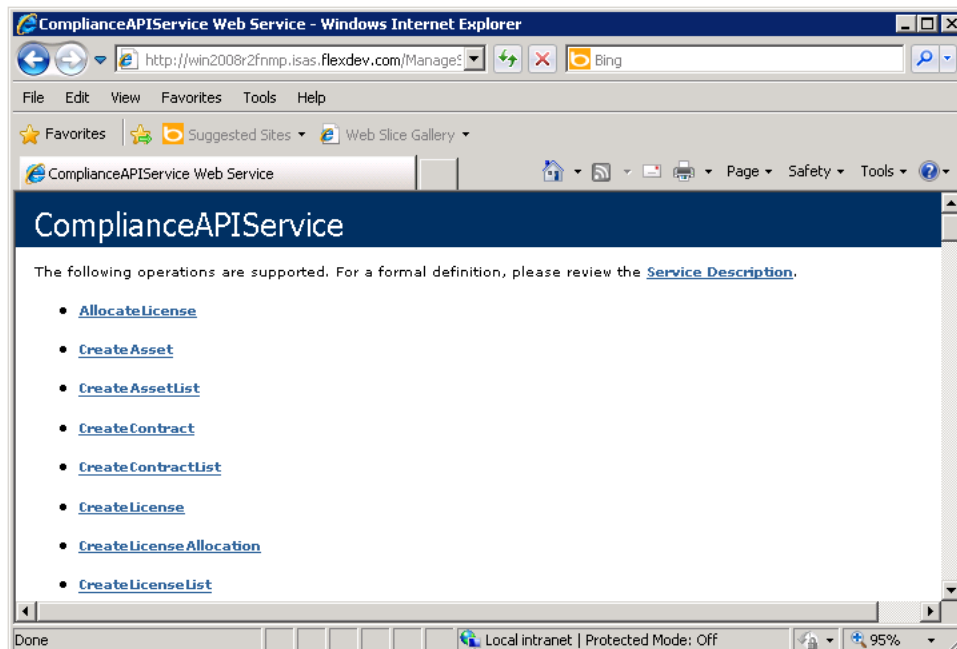
such as:

`http://win2008r2fnmp/ManageSoftServices/ComplianceAPIService/ComplianceAPIService.asmx`



**Tip** • When identifying the FlexNet Manager Suite server in this URL, you can enter either the application server name or the server IP address.

The **ComplianceAPIService** page on the application server should open **without** prompting you to enter network credentials:



If you **are** prompted to enter network credentials, then Windows Authentication is not set up correctly on the FlexNet Manager Suite server and you will need to modify its authentication settings. The problem could be an issue with the group policy settings for network authentication.



---

**Note** • If Windows Authentication is not enabled, App Portal and AdminStudio will be unable to communicate with FlexNet Manager Suite.

2. To modify the authentication settings, see [Verify FlexNet Manager Suite On Premises Application Server Authentication Settings in IIS](#).

## Connecting FlexNet Manager Suite On Premises to the Flexera Service Gateway



---

**Note** • FlexNet Manager Suite On Premises was formerly known as FlexNet Manager Platform.

FlexNet Manager Suite On Premises communicates with App Portal and AdminStudio via the Flexera Service Gateway component.

The procedure for connecting FlexNet Manager Suite On Premises to the Flexera Service Gateway is the same as the procedure for FlexNet Manager Suite Cloud. See [Registering FlexNet Manager Suite Cloud with the Flexera Service Gateway](#).

# Importing the Application Recognition Library (ARL)

FlexNet Manager Suite Cloud and FlexNet Manager Suite On Premises come with an Application Recognition Library, a SKU (stock keeping unit) Library, and several Product Use Rights Libraries (the latter depending on which options you have purchased for the product). The Application Recognition Library is the repository for the FlexeraID that is used to relate application records between FlexNet Manager Suite, AdminStudio, and App Portal.

These libraries are updated regularly by Flexera Software and normally downloaded automatically. At installation time, however, you need to download the libraries to create a baseline ready for product use.

Perform the following procedure as administrator (**FNMS-Admin**) with database rights.



## Task

### To download and import the latest libraries:

1. On the processing server (or application server for a single-server implementation), open a Command Window and navigate to `installation-folder\DotNet\bin\`.
2. Run the **Recognition data import** scheduled task to update these libraries.



**Note** • On this server, the **Recognition data import** Windows scheduled task updates these libraries by default at 1 a.m. daily.



**Tip** • To sign-up for notification of ARL updates, as well as FlexNet Manager Suite hot fix releases, visit:

<http://learn.flexerasoftware.com/SLO-FMS-Software-Content-Library-Updates>



**Important** • For FlexNet Manager Suite Cloud, the latest version of the Application Recognition and Product Use Rights libraries are continually being updated; therefore, there is no need to download these libraries.



# Troubleshooting FlexNet Manager Suite Communication Issues

If other products connected to the Flexera Service Gateway are having trouble communicating with FlexNet Manager Suite, perform the following troubleshooting tasks:

- [Verify FlexNet Manager Suite On Premises Application Server Authentication Settings in IIS](#)
- [Check That ManageSoftWebServiceAppPool Service is Running](#)
- [Verify Domain Credentials Across Computers by Invoking GetTenants and GetFlexeralDForApplication API](#)
- [Resolving Active Directory “Double Hop” Issues Which Occur if FlexNet Manager Suite and SQL Server are on Separate Computers](#)
- [Steps to Take When FlexNet Manager Suite is Unable to Register With the Flexera Service Gateway](#)

## Verify FlexNet Manager Suite On Premises Application Server Authentication Settings in IIS

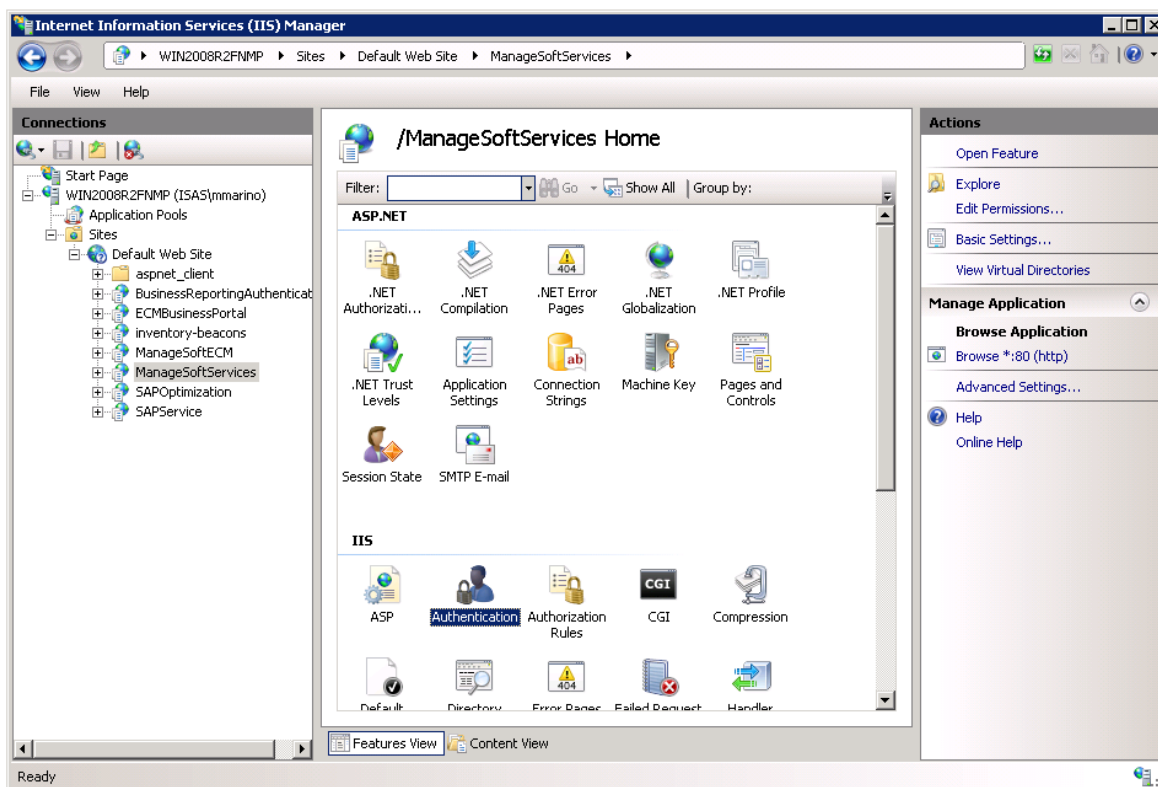
If you are having authentication issues when attempting to connect to FlexNet Manager Suite, perform the following steps on the FlexNet Manager Suite application server machine to verify the application server authentication settings in IIS.



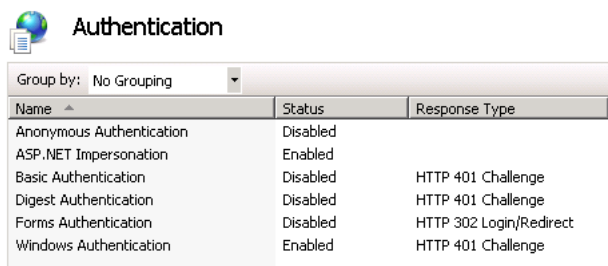
### Task

**To configure FlexNet Manager Suite authentication in IIS:**

1. Open Internet Information Services (IIS) Manager.
2. Select **ManageSoftServices** in the tree. The **Features** view opens.



3. Double-click **Authentication**. The **Authentication** view opens.



4. Make sure that the following three options are set to **Enabled**:

- **ASP.NET Impersonation**

- **Basic Authentication**
- **Windows Authentication**

All other authentication methods should be set to **Disabled**.

## Check That ManageSoftWebServiceAppPool Service is Running

To check that the ManageSoftWebServiceAppPool service is running, perform the following steps:



### Task

**To check the ManageSoftWebServiceAppPool service:**

1. Open Internet Information Services (IIS) Manager.
2. Select **Application Pools** in the tree. The **Application Pools** view opens.
3. In the **Application Pools** list, make sure that the ManageSoftWebServiceAppPool service is started and running under the NetworkService account.



### Application Pools

This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

Filter: <span>Go</span> <span>Show All</span>   Group by: No Grouping					
Name	Status	.NET Frame...	Managed Pipeli...	Identity	Applications
ASP.NET v4.0	Started	v4.0	Integrated	ApplicationPoolIden...	0
ASP.NET v4.0 Classic	Started	v4.0	Classic	ApplicationPoolIden...	0
ASP.NET v4.0 DefaultAppPool	Started	v4.0	Integrated	ApplicationPoolIden...	1
Classic .NET AppPool	Started	v2.0	Classic	ApplicationPoolIden...	0
DefaultAppPool	Started	v2.0	Integrated	ApplicationPoolIden...	0
InventoryBeaconsAppPool	Started	v4.0	Integrated	NetworkService	1
ManageSoftWebServiceAppPool	Started	v4.0	Integrated	NetworkService	4
SAPOptimizationAppPool	Started	v4.0	Integrated	NetworkService	1
SAPServiceAppPool	Started	v4.0	Integrated	NetworkService	1



**Note** • The NetworkService account has non-editable privileges configured by Microsoft that are sufficient for FlexNet Manager Suite.

4. If the service is not started, start it by clicking **Start** in the **Actions** menu.
5. On the **Actions** menu, click **Advanced Settings...** to open the **Advanced Settings** dialog box for this service, and make sure that **Start Automatically** is set to **True**.

## Verify Domain Credentials Across Computers by Invoking GetTenants and GetFlexeraIDForApplication API

On the FlexNet Manager Suite server, once you are able to browse to the **ComplianceAPIService** without being prompted to log in (as described in [Testing FlexNet Manager Suite On Premises Server Authentication Settings](#)), try to invoke the GetTenants and GetFlexeraIDForApplication API. You should be able to invoke them without encountering any issues.



### Task

#### To invoke GetTenants and GetFlexeraIDForApplication APIs:

1. On the FlexNet Manager Suite server machine, enter the following URL in a web browser:

`http://<FNMPServer>/ManageSoftServices/ComplianceAPIService/ComplianceAPIService.asmx`

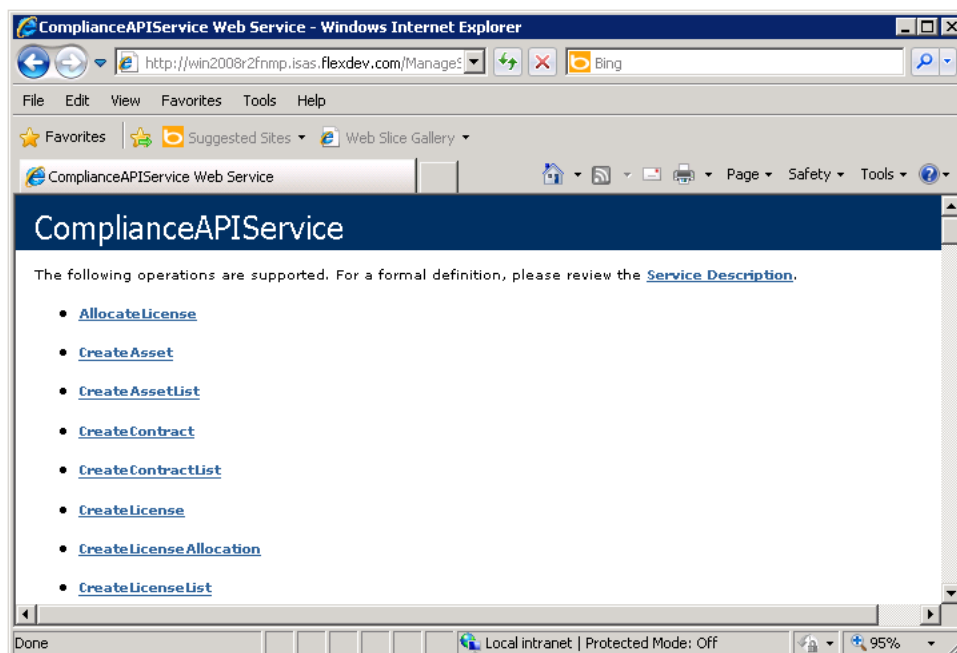
such as:

`http://win2008r2fnmp/ManageSoftServices/ComplianceAPIService/ComplianceAPIService.asmx`

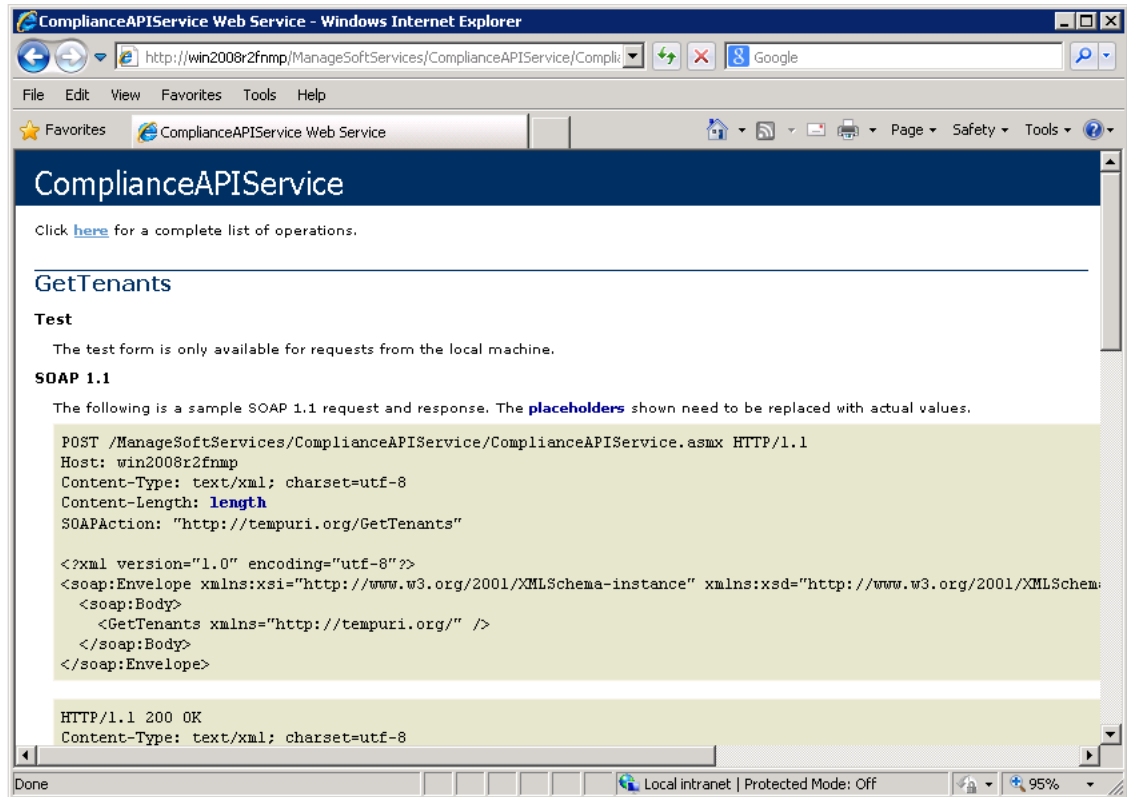


**Tip** • When identifying the FlexNet Manager Suite server in this URL, you can enter either the application server name or the server IP address.

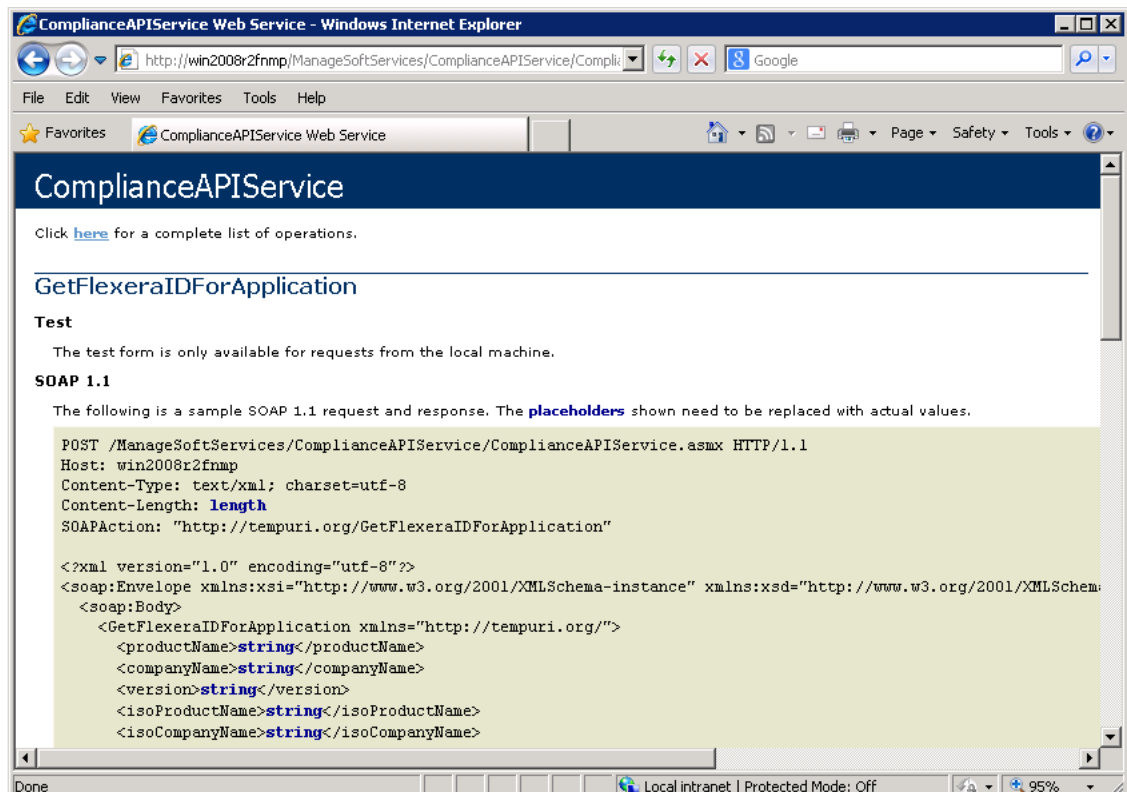
The **ComplianceAPIService** page on the FlexNet Manager Suite server should open **without** prompting you to enter network credentials:



2. Click on **GetTenants** in the list. If this API is working correctly, the following page should be displayed:



3. Return to the main **ComplianceAPIService** page and click on **GetFlexeraIDForApplication** in the list. If this API is working correctly, the following page should be displayed:



If an error message is displayed instead, FlexNet Manager Suite is not configured properly. One of the following could be causing this problem:

- **Prevented by Active Directory policy**—This type of error usually means that the System Administrator has changed the Active Directory policy so that it prevents the Flexera Software services from working.
- **User does not have access to IIS**—The user who is testing the connections may not have access to IIS if they are in the wrong security groups.

# Test the FlexNet Manager Suite GetFlexeraIDForApplication API

To determine whether the FlexNet Manager Suite GetFlexeraIDForApplication API is working correctly (which means that a Flexera Identifier will be returned when AdminStudio searches FlexNet Manager Suite's Application Resource Library), invoke the GetFlexeraIDForApplication API on the FlexNet Manager Suite server.



## Task

### To test the GetFlexeraIDForApplication API:

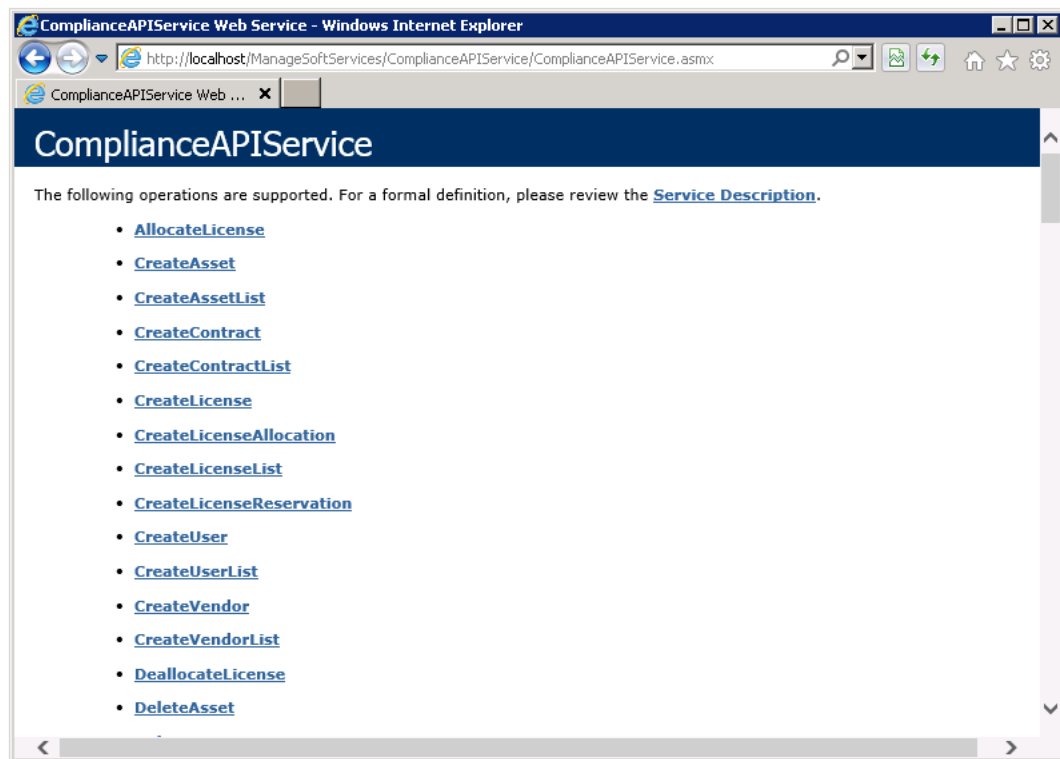
1. On the FlexNet Manager Suite server machine, enter the following URL in a web browser:

`http://localhost/ManageSoftServices/ComplianceAPIService/ComplianceAPIService.aspx`



**Tip** • When identifying the FlexNet Manager Suite server in this URL, enter *Localhost*.

The **ComplianceAPIService** page on the FlexNet Manager Suite server opens:



2. Click on **GetFlexeraIDForApplication** in the list. The **GetFlexeraIDForApplication** page is displayed:

ComplianceAPIService Web Service - Windows Internet Explorer

http://localhost/ManageSoftServices/ComplianceAPIService/ComplianceAPIService.asmx?op=GetFlexeraIDForApplication

## ComplianceAPIService

Click [here](#) for a complete list of operations.

### GetFlexeraIDForApplication

**Test**

To test the operation using the HTTP POST protocol, click the 'Invoke' button.

Parameter	Value
productName:	<input type="text"/>
companyName:	<input type="text"/>
version:	<input type="text"/>
isoProductName:	<input type="text"/>
isoCompanyName:	<input type="text"/>
isoVersion:	<input type="text"/>
isoRegID:	<input type="text"/>
isoOriginalARPProductName:	<input type="text"/>
isoOriginalARPCoName:	<input type="text"/>
isoOriginalARPVersion:	<input type="text"/>
tenantUID:	<input type="text"/>

**SOAP 1.1**

The following is a sample SOAP 1.1 request and response. The [placeholders](#) shown need to be replaced with actual values.

```
POST /ManageSoftServices/ComplianceAPIService/ComplianceAPIService.asmx HTTP/1.1
Host: localhost
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "http://tempuri.org/GetFlexeraIDForApplication"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <GetFlexeraIDForApplication xmlns="http://tempuri.org/">
      <productName>string</productName>
      <companyName>string</companyName>
      <version>string</version>
      <isoProductName>string</isoProductName>
    </GetFlexeraIDForApplication>
  </soap:Body>
</soap:Envelope>
```

3. In the **productName** field, enter **Acrobat**, and in the **companyName** field, enter **Adobe**.

4. Click **Invoke**. The following Flexera Identifier should be returned:

```
<?xml version="1.0" encoding="UTF-8"?>
<string xmlns="http://tempuri.org/">arl://MGS-APP-00000000083</string>
```

- **If a Flexera Identifier is returned**, FlexNet Manager Suite is configured properly.
- **If no Flexera Identifier is returned**, FlexNet Manager Suite is not configured properly. One of the following could be causing this problem:
  - **Prevented by Active Directory policy**—This type of error usually means that the System Administrator has changed the Active Directory policy so that it prevents the Flexera Software services from working.
  - **User does not have access to IIS**—The user who is testing the connections may not have access to IIS if they are in the wrong security groups.



## Steps to Take When FlexNet Manager Suite is Unable to Register With the Flexera Service Gateway

In some instances, you may not be able to register FlexNet Manager Suite with the Flexera Service Gateway. The following message is displayed:

Unable to register with the Flexera Service Gateway. The following error was provided by the gateway:  
Exception occurred in adding service FlexNetManagerSuite. Message:  
com.ctc.wstx.exc.WstxEOFException: Unexpected EOF in prolog at [row,col {unknown-source}]: [1,0]

To resolve this issue, do one of the following:

- **Windows Authentication enabled**—First make sure that Windows Authentication is enabled and working on the FlexNet Manager Suite server.
- **Check the [GetFlexeraIDforApplication web service](#)**—Check the GetFlexeraIDforApplication web service, as described in [Verify Domain Credentials Across Computers by Invoking GetTenants and GetFlexeraIDforApplication API](#).

# Resolving Active Directory “Double Hop” Issues Which Occur if FlexNet Manager Suite and SQL Server are on Separate Computers



**Important** • You must perform this task if FlexNet Manager Suite 9.2.3 or earlier and SQL Server are installed on separate machines. This task is not necessary when using FlexNet Manager Suite 2015 and later.

To enable Windows Authentication with FlexNet Manager Suite, the user’s credentials need to authenticate in two places:

- **First “hop”**—The user accesses IIS and authenticates into FlexNet Manager Suite.
- **Second “hop”**—FlexNet Manager Suite then uses that user’s credentials to connect to the FlexNet Manager Suite database on SQL Server.

For security reasons, IIS is not permitted to pass credentials to a secondary server. Therefore, if FlexNet Manager Suite and SQL Server are not installed on the same machine, IIS will be unable to perform the authentication, and an error will be generated.

If your enterprise’s security protocols require you install FlexNet Manager Suite and SQL Server on separate computers, you will need to enable a trusted delegation on the FlexNet Manager Suite computer to resolve this issue.



**Note** • For more information, see [How to use the System.DirectoryServices namespace in ASP.NET](http://support.microsoft.com/default.aspx?scid=kb;en-us;329986) on the Microsoft Support site:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;329986>

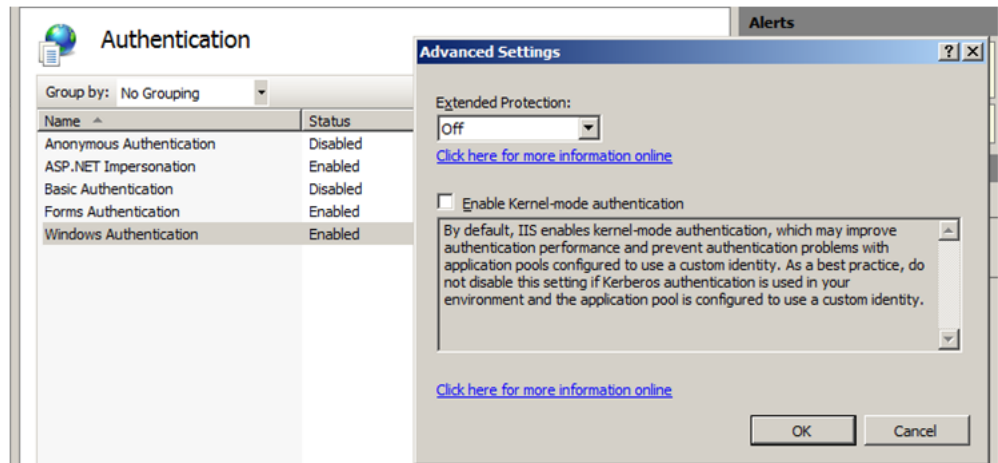
To enable a trusted delegation, perform the following steps on your FlexNet Manager Suite installation:



## Task

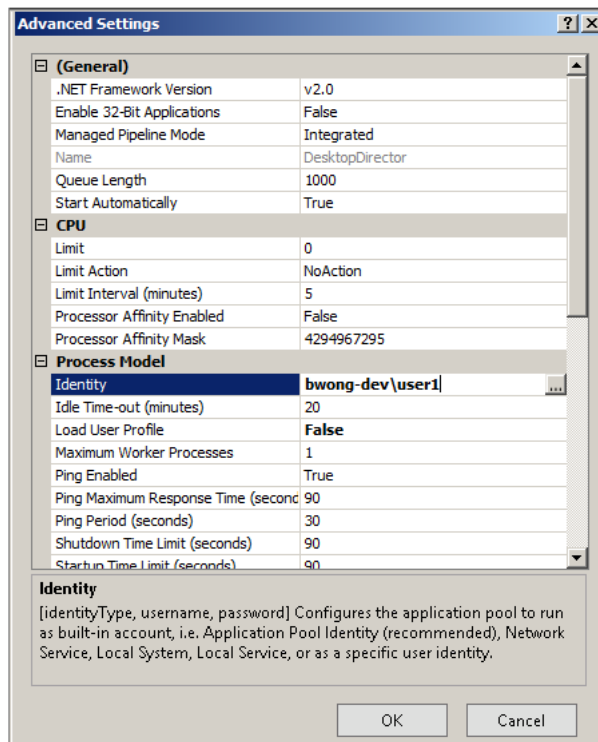
### To enable a trusted delegation:

1. Disable Anonymous Authentication for the following sites in IIS:
  - ManageSoftServices
  - ECMBusinessPortal
  - Suite
  - SAPPortal
2. Ensure that only **ASP.NET Impersonation** and **Windows Authentication** are enabled for ManageSoftServices, ECMBusinessPortal and ManageSoftECM sites in IIS.
3. Clear the selection of the **Enable Kernel mode authentication** option for Windows Authentication on ManageSoftServices, ECMBusinessPortal and ManageSoftECM:



**Note** • You need to disable kernel-mode authentication because it only handles Kerberos authentication, but does not allow delegation. You cannot have both Kernel-mode authentication enabled and also support “double hop” authentication.

4. Create a new Active Directory service account for handling delegation access for FlexNet Manager Suite.
5. In IIS, modify the ManageSoftWebServiceAppPool1 to use the newly created service account.



**Note** • You can choose to re-use the FlexNet Manager Suite Service account instead of creating a new service account for the purpose of delegation.

6. Remove all existing Service Principal Names (SPNs) on <FNMP Admin Server> for IIS:

```
setspn -d http/<FNMP Admin Server> <FNMP Admin Server>
setspn -d http/<FNMP Admin Server>:80 <FNMP Admin Server>
setspn -d http/<FNMP Admin Server (Fully Qualified)> <FNMP Admin Server>
setspn -d http/<FNMP Admin Server (Fully Qualified)>:80 <FNMP Admin Server>
```

7. Run setspn against the new service account user to create a Service Principal Name for the IIS process:

```
setspn -u -s http/<FNMP Admin Server> <FNMP service account user>
setspn -u -s http/<FNMP Admin Server>:80 <FNMP service account user>
setspn -u -s http/<FNMP Admin Server (Fully Qualified)> <FNMP service account user>
setspn -u -s http/<FNMP Admin Server (Fully Qualified)>:80 <FNMP service account user>
```



**Note** • This will allow the FlexNet Manager Suite service account user to authenticate users accessing IIS.

8. Ensure that the SQL Server service account has the necessary SPN created so it can authenticate users accessing the SQL server:

```
setspn -l <SQL Server user service account>
```

It should list the following:

```
...
MSSQLSvc/<SQL Server Machine Name (Fully Qualified)>:1433
MSSQLSvc/<SQL Server Machine Name (Fully Qualified)>
...
```

9. Create an SPN for the flat name as well in case SQL Server has issues discovering the short hand name of the application server:

```
setspn -u -s MSSQLSvc/<SQL Server Machine Name>:1433 <SQL Server service user account>
setspn -u -s MSSQLSvc/<SQL Server Machine Name> <SQL Server service user account>
```

10. Ensure that the SQL Server Reporting Services service account has the necessary SPN created so it can authenticate users accessing reports in the FlexNet Manager Suite web portals:

```
setspn -u -a http/<SQL Server Machine Name> <SQL Server service user>
setspn -u -s http/<SQL Server Machine Name>:80 <SQL Server service user>
setspn -u -s http/<SQL Server Machine Name (Fully Qualified)> <SQL Server service user>
setspn -u -s http/<SQL Server Machine Name (Fully Qualified)>:80 <SQL Server service user>
```

11. Enable Kerberos authentication on the SQL Server Reporting Services reports. (By default, it is disabled.)

12. On the SQL Server machine, edit:

```
<SQL Server Install Dir>\MSRS10_50.MSSQLSERVER\Reporting Services\ReportServer\
rsreportserver.config
```

By default, it is installed at:

```
C:\Program Files\Microsoft SQL Server\MSRS10_50.MSSQLSERVER\Reporting Services\ReportServer
```

13. Add the RSWindowsNegotiate authentication type. For example, the <Authentication> subsection in the file should look something like this:

```
<Authentication>
  <AuthenticationTypes>
    <RSWindowsNegotiate/>
    <RSWindowsNTLM/>
```

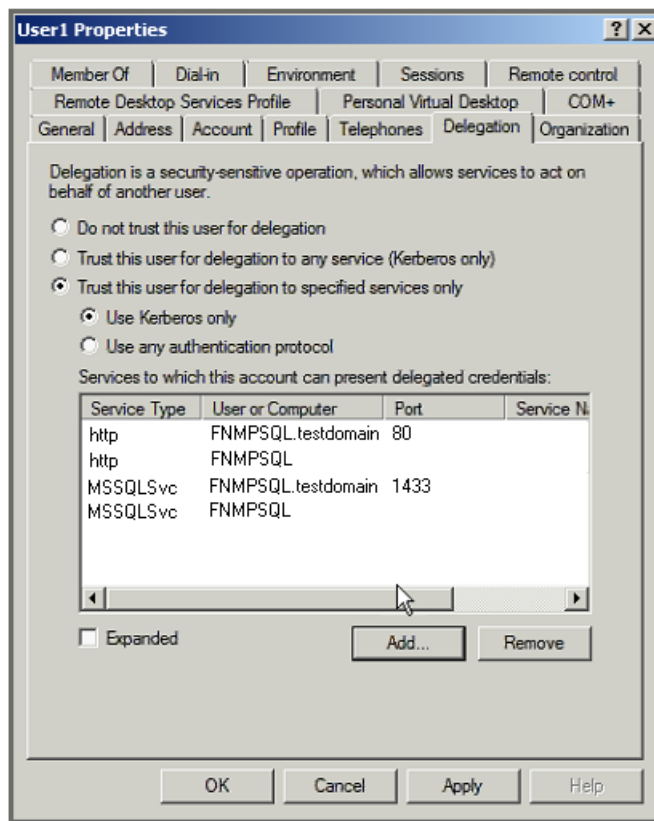
```
</AuthenticationTypes>
<RSWindowsExtendedProtectionLevel>Off</RSWindowsExtendedProtectionLevel>
<RSWindowsExtendedProtectionScenario>Proxy</RSWindowsExtendedProtectionScenario>
<EnableAuthPersistence>true</EnableAuthPersistence>
</Authentication>
```

14. Allow delegation for the <FNMP service account user> so it can delegate the user authentication token from FlexNet Manager Suite to SQL Server and FlexNet Manager Suite to SQL Server Reporting Services.
  - a. First, add the SQL Server service to give delegation access to the <FNMP service account user>.
  - b. Then, add the SQL Server Reporting Services service to give delegation access to the <FNMP service account user>.



**Note** • It is not necessary to modify the delegation tab for the SQL Server service account.

The end result should look something similar to the following:



**Figure 5-1:** User Properties Dialog Box from Active Directory



**Note** • If you are performing a proof-of-concept demonstration of the integrated solution in a **non-production** environment, and need a quicker way to avoid “double-hop” issues, you can use a temporary solution, as described in [Temporary Solution for “Proof of Concept” Lab Scenario to Address Double-Hop Issue with FlexNet Manager Suite Server](#).

## Temporary Solution for “Proof of Concept” Lab Scenario to Address Double-Hop Issue with FlexNet Manager Suite Server

If someone is performing a proof-of-concept demonstration of the integrated solution, and want to avoid performing the steps in [Resolving Active Directory “Double Hop” Issues Which Occur if FlexNet Manager Suite and SQL Server are on Separate Computers](#), you can use this alternate solution.



---

**Caution** • *This solution should **not** be implemented in a production environment.*



---

### Task

**To temporarily address a double-hop issue with FlexNet Manager Suite:**

1. Enable Anonymous authentication on the **ManageSoftServices** application.
2. Disable Windows Authentication on the **ManageSoftServices** application.
3. Change the App Pool account to a domain account that has full access to FlexNet Manager Suite and the FlexNet Manager Suite database.

# Viewing an Application's Flexera ID in FlexNet Manager Suite

To view an application's Flexera ID, perform the following steps:



## Task

### To view an application's Flexera ID:

1. In FlexNet Manager Suite, open the **License Compliance** menu and select **All Applications** (which is under the **Applications** heading). The **All Applications** page opens.

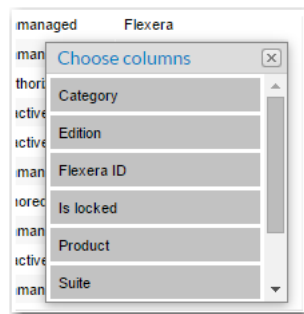
**All Applications** Any applications which can be recognised, regardless of whether they are installed or not.

164,519 results returned 20 rows per page

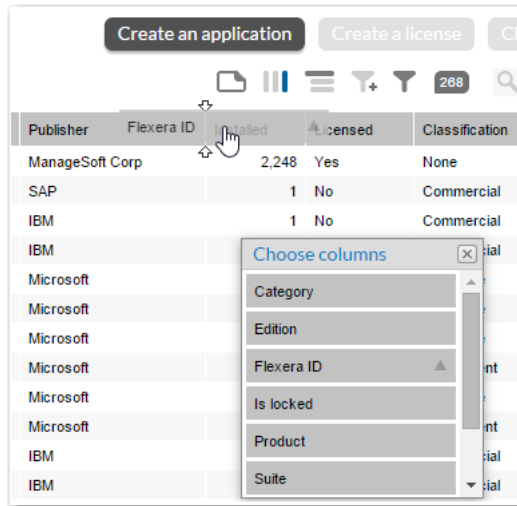
Name	Publisher	Installed	Licensed	Classification	Status	Source
IDB/Explain for DB2 5	IBM	1	No	Commercial	Unmanaged	Flexera (Extended)
"Intro to Design Patterns" 1.0	Microsoft	0	No	Commercial	Inactive	Flexera
"mora win" plug in 1.0	LabelGate	0	No	Commercial	Unmanaged	Flexera
"Roslyn" CTP 1	Microsoft	0	No	Freeware	Unmanaged	Flexera
#1 CD Ripper 1.7	Maskbit Software	1,955	No	Shareware	Authorized	Flexera (Extended)
#1 DVD Ripper 4.3	Apollo Multimedia	0	No	Commercial	Inactive	Flexera
#1 DVD Ripper 6.0	Apollo Multimedia	0	No	Commercial	Inactive	Flexera
#1Backup 2.0	Atype Software	0	No	Shareware	Unmanaged	Flexera
.NET 1.0	SmartQuant	0	No	Commercial	Ignored	Flexera
.NET 2.x Runtime 2.0	Teradata	0	No	Component	Unmanaged	Flexera
.NET and J2EE Interoperability Toolkit 1	Microsoft	0	No	Freeware	Inactive	Flexera
.NET and SAP 2.0	Microsoft	0	No	Component	Unmanaged	Flexera

By default, the **Flexera ID** column is not displayed.

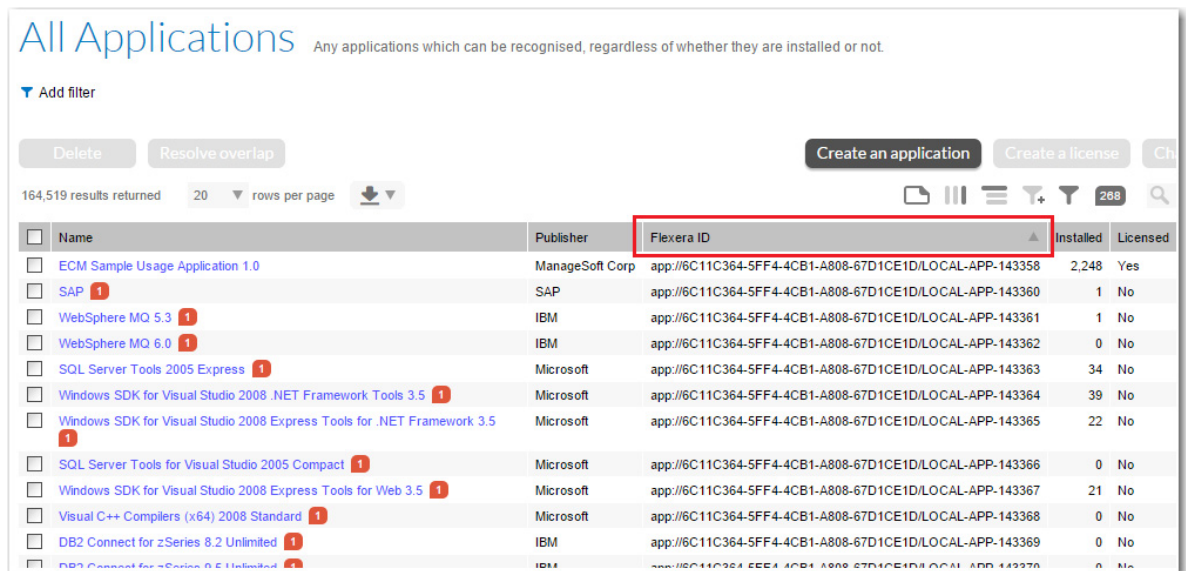
2. Click the **Choose columns to display** icon above the grid. The **Choose columns** list opens.



3. Click on **Flexera ID** in the list and drag it to the heading row of the grid in the location where you want it to appear.



When you let go of the column name, the Flexera ID column will be listed in the grid.



## Upgrading FlexNet Manager Suite's Compliance Console

For instructions on how to upgrade the FlexNet Manager Suite's Compliance Console to a new version, see the *Upgrading Your Compliance Console* topic in the *FlexNet Manager Suite Installation Guide*.



# 6

## Configuring App Portal

When App Portal is integrated with FlexNet Manager Suite / FlexNet Manager Platform and AdminStudio licenses for App Portal catalog items can be managed automatically. This section explains how to connect App Portal to the Flexera Service Gateway so that it can communicate with FlexNet Manager Suite / FlexNet Manager Platform and AdminStudio, and how to troubleshoot any issues that you might encounter.

- [Testing App Portal Server Authentication Settings](#)
- [Connecting App Portal to the Flexera Service Gateway](#)
- [Testing App Portal's Connection to the Flexera Service Gateway](#)
- [Performing App Portal Troubleshooting](#)
- [Upgrading the App Portal Web Site](#)

# Testing App Portal Server Authentication Settings

The first thing that you should do to prepare the App Portal server for integration (even before connecting to the Flexera Service Gateway) is to attempt to browse to the App Portal Integration API Service documentation page to determine whether you are prompted to enter network credentials. This will test whether authentication settings of the App Portal server are set properly.



## Task

### To test the App Portal server authentication settings:

1. On the App Portal server machine, enter the following URL in a web browser:

`http://<AppPortalServer>/ESD/WS/Integration.asmx`

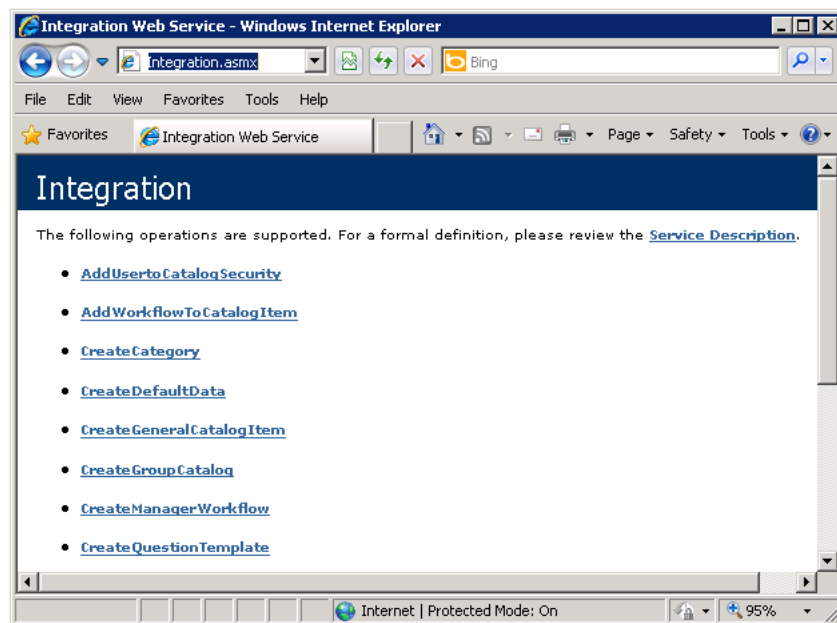
such as:

`http://Win2008R2AppPortal/ESD/WS/Integration.asmx`



**Tip** • When identifying the App Portal server in this URL, you can enter either the application server name or the server IP address.

The **Integration** documentation page on the App Portal server should open **without** prompting you to enter network credentials:



If you **are** prompted to enter network credentials, then Windows Authentication is not set up correctly on the App Portal server and you will need to modify its authentication settings. The problem could be an issue with the group policy settings for network authentication.



**Note** • If Windows Authentication is not enabled, FlexNet Manager Suite / FlexNet Manager Platform and AdminStudio will be unable to communicate with App Portal.

2. To modify the authentication settings, see [Verify the App Portal Server Authentication Settings](#).

## Connecting App Portal to the Flexera Service Gateway

App Portal communicates with FlexNet Manager Suite / FlexNet Manager Platform via the Flexera Service Gateway component. To connect App Portal to the Flexera Service Gateway, perform the following steps.



### Task

#### To connect to the Flexera Service Gateway:

1. In **App Portal**, open the **Admin** tab.
2. Select **Site Management > Settings > Flexera Integration**. The **Flexera Integration** view opens.
3. In the **Flexera Service Gateway Server Name** field, enter the name of your Flexera Service Gateway server.

Save

**Flexera Integration**

Enable App Portal API ☐ (http://server/esd/api.asmx) You should modify NTFS Permissions on the api.asmx file to prevent unauthorized access prior to enabling the API.

Enable Advanced License Check with FlexNet Manager Suite ☒

**Flexera Service Gateway**

Flexera Service Gateway Server Name

Following services are currently registered with Flexera Service Gateway

- App Portal [isasappportal.isas.flexdev.com]
- Workflow Manager [adminstudiopat.isas.flexdev.com]
- FlexNet Manager Suite Cloud [www.flexnetmanager.com]

FNMS Tenant UID (MSP Only)

**FlexNet Manager Suite Cloud Settings**

FlexNet Manager Suite Cloud Access Token

**FlexNet Manager Suite On-Premises Settings**

If the App Portal system account does not have access to FlexNet Manager Suite, provide appropriate credentials.

Username (DOMAIN\Username)

Password

**FlexNet Manager Suite Database Connection Settings**

In order to use the MyApps feature, App Portal system account needs to have read access to the FlexNet Manager Suite database.

Database Server

Database Name

4. Click **Save**.

# Testing App Portal's Connection to the Flexera Service Gateway

After you have performed the steps in [Connecting App Portal to the Flexera Service Gateway](#), if FlexNet Manager Suite / FlexNet Manager Platform is also connected to the Flexera Service Gateway, you should be able to use App Portal to perform the following steps.



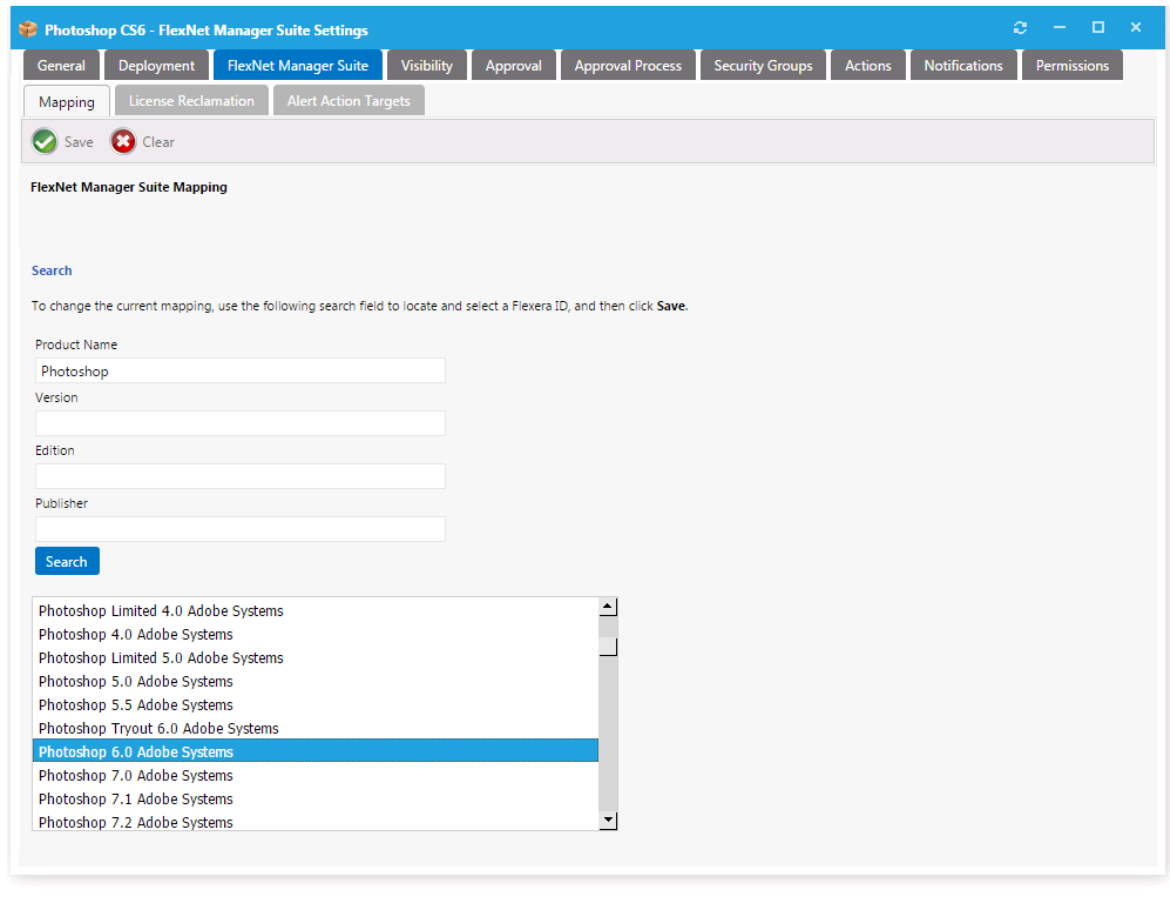
## Task

**To test App Portal's connection to the Flexera Service Gateway:**

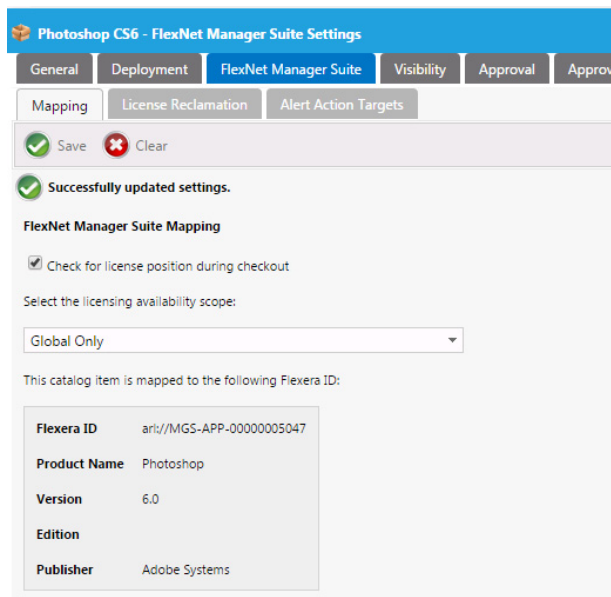
1. Open App Portal.
2. Under **Site Management** on the **Admin** tab, select **Catalog Management**.
3. Under **Current Catalog Items**, select **View All Items**. Existing catalog items are listed.
4. Double-click on an existing catalog item. The **Catalog Item Properties** dialog box for that application opens.
5. Open the **FlexNet Manager Suite** tab.
6. Enter application information in the **Product Name**, **Version**, **Edition**, and **Publisher** fields, and then click **Search**.

The screenshot shows the 'Photoshop CS6 - FlexNet Manager Suite Settings' dialog box. The 'FlexNet Manager Suite' tab is selected. Within this tab, the 'Mapping' sub-tab is active. At the top, there are buttons for 'Save' (with a green checkmark) and 'Clear' (with a red X). Below this is the 'FlexNet Manager Suite Mapping' section. It includes a 'Search' link and a text box with the instruction: 'To change the current mapping, use the following search field to locate and select a Flexera ID, and then click **Save**.' Below the instruction are four text input fields labeled 'Product Name', 'Version', 'Edition', and 'Publisher'. A blue 'Search' button is located below these fields. At the bottom of the mapping section is a large, empty rectangular box for search results.

7. From the list of search results, select the appropriate entry. The selected item will be highlighted.



- Click **Save**. The catalog item is now mapped to a software entry in FlexNet Manager Suite, and the product information is now listed at the top of the dialog box.



If the application is successfully mapped, it indicates that App Portal's connection to FlexNet Manager Suite via the Flexera Service Gateway is configured properly.

9. If the application is not successfully mapped, see [Performing App Portal Troubleshooting](#).

## Performing App Portal Troubleshooting

Tips for performing App Portal troubleshooting are presented in the following sections:

- [Installation Testing and Troubleshooting](#)
- [Troubleshooting App Portal Integration Issues](#)

## Installation Testing and Troubleshooting

To test your App Portal installation to ensure that it can communicate with other products via the Flexera Service Gateway, perform the following configuration tasks:

- [Verify the App Portal Server Authentication Settings](#)
- [Check the SelfService Service](#)
- [Check the ESDService Service](#)
- [Test FlexNet Manager Suite / FlexNet Manager Platform Server Authentication Settings](#)
- [Invoke GetCategories API](#)
- [Error After Installation on X64 Server with WSUS Role](#)

## Verify the App Portal Server Authentication Settings

To verify the App Portal server authentication settings, perform the following steps.

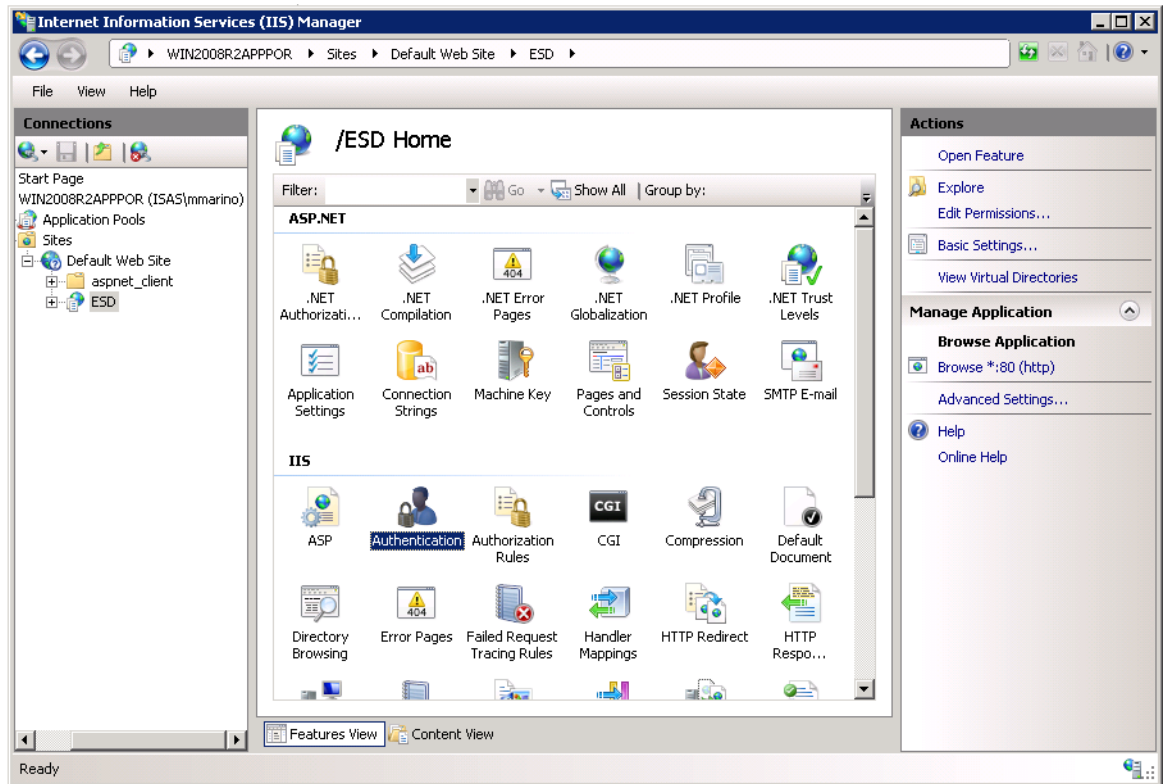


---

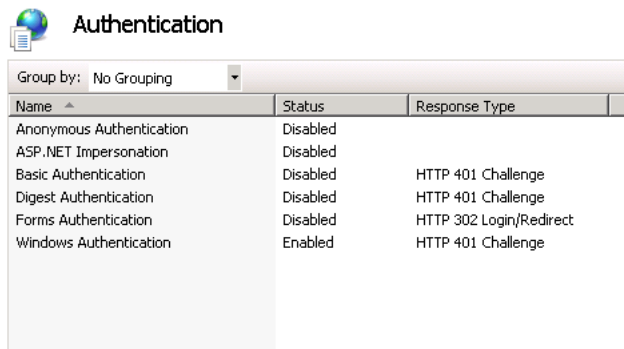
### Task

#### **To verify App Portal server authentication settings:**

1. Open Internet Information Services (IIS) 7.0 Manager.
2. Select **ESD** in the tree. The **Features** view opens.



3. Double-click **Authentication**. The **Authentication** view opens.



4. Make sure that **Windows Authentication** is set to **Enabled**, and that all other authentication methods are set to **Disabled**.
5. If you want to grant access to this site based on an IP address or domain name, go back to the IIS 7 **Features** view and double-click on **IP Address and Domain Restrictions**. The **IP Address and Domain Restrictions** view opens.

**IP Address and Domain Restrictions**

Use this feature to restrict or grant access to Web content based on IP addresses or domain names. Set the restrictions in order of priority.

Group by: No Grouping

Mode	Requestor	Entry Type	
------	-----------	------------	--

**Actions**

- Add Allow Entry...
- Add Deny Entry...
- Edit Feature Settings...
- Revert To Parent
- View Ordered List...
- Help
- Online Help

6. Click **Add Allow Entry**. The **Add Allow Restriction Rule** dialog box opens.

**Add Allow Restriction Rule**

Allow access for the following IP address or domain name:

☒ Specific IP address:

☐ IP address range:

Mask or Prefix:

OK Cancel

7. Enter the IP addresses that you want to be able to access the App Portal Site.
8. Click **OK**.



## Check the SelfService Service

To check that the SelfService application pool service is running, perform the following steps:



### Task

#### To check the SelfService application pool service:

1. Open Internet Information Services (IIS) 7.0 Manager.
2. Select **Application Pools** in the tree. The **Application Pools** view opens.
3. In the **Application Pools** list, make sure that the SelfService service is started and running under the domain account that was specified during the App Portal installation.



#### Application Pools

This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, one or more applications, and provide isolation among different applications.

Filter: <input type="text"/> Go <input type="button" value="Show All"/> Group by: No Grouping					
Name	Status	.NET Frame...	Managed Pipeli...	Identity	Applications
ASP.NET v4.0	Started	v4.0	Integrated	ApplicationPoolIden...	0
ASP.NET v4.0 Classic	Started	v4.0	Classic	ApplicationPoolIden...	0
ASP.NET v4.0 DefaultAppPool	Started	v4.0	Integrated	ApplicationPoolIden...	1
Classic .NET AppPool	Started	v4.0	Classic	ApplicationPoolIden...	0
DefaultAppPool	Started	v4.0	Integrated	ApplicationPoolIden...	0
SelfService	Started	v4.0	Integrated	isas\mmarino	1

4. If the service is not started, start it by clicking **Start** in the **Actions** menu.
5. On the **Actions** menu, click **Advanced Settings...** to open the **Advanced Settings** dialog box for this service, and make sure that the **Start Automatically** property is set to **True**.

## Check the ESDService Service

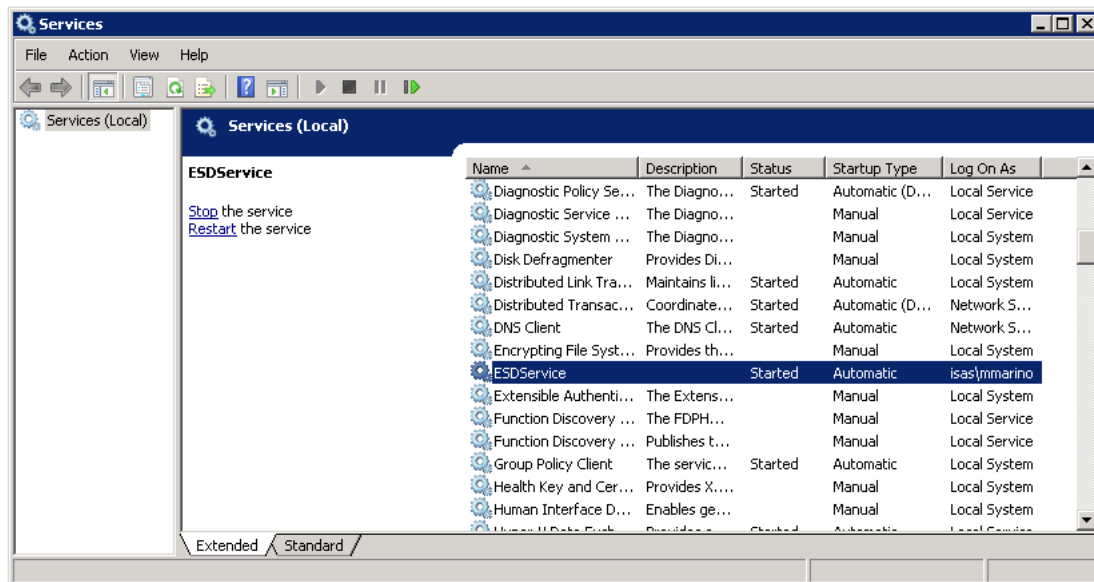
To check that App Portal's ESDService service is running, perform the following steps:



### Task

#### To check the ESDService service:

1. On the App Portal server machine, open the Microsoft Management Console **Services** dialog box.
2. Locate **ESDService** in the list and make sure that the **Status** is set to **Started** and that the **Log On As** column is set to the domain account that was specified during the App Portal installation.



3. If the service is not started, start it by clicking **Start** in the **Actions** menu.
4. On the **Actions** menu, click **Advanced Settings...** to open the **Advanced Settings** dialog box for this service, and make sure that the **Start Automatically** property is set to **True**.

## Test FlexNet Manager Suite / FlexNet Manager Platform Server Authentication Settings

To test the FlexNet Manager Suite / FlexNet Manager Platform server authentication settings, you need to browse to the FlexNet Manager Suite / FlexNet Manager Platform ComplianceAPIService documentation page to determine whether you are prompted to enter network credentials. This will test whether the authentication settings of the FlexNet Manager Suite / FlexNet Manager Platform server are set properly.



### Task

**To test the FlexNet Manager Suite / FlexNet Manager Platform server authentication settings:**

1. On the App Portal server machine, enter the following URL in a web browser:

`http://<FNMPServer>/ManageSoftServices/ComplianceAPIService/ComplianceAPIService.asmx`

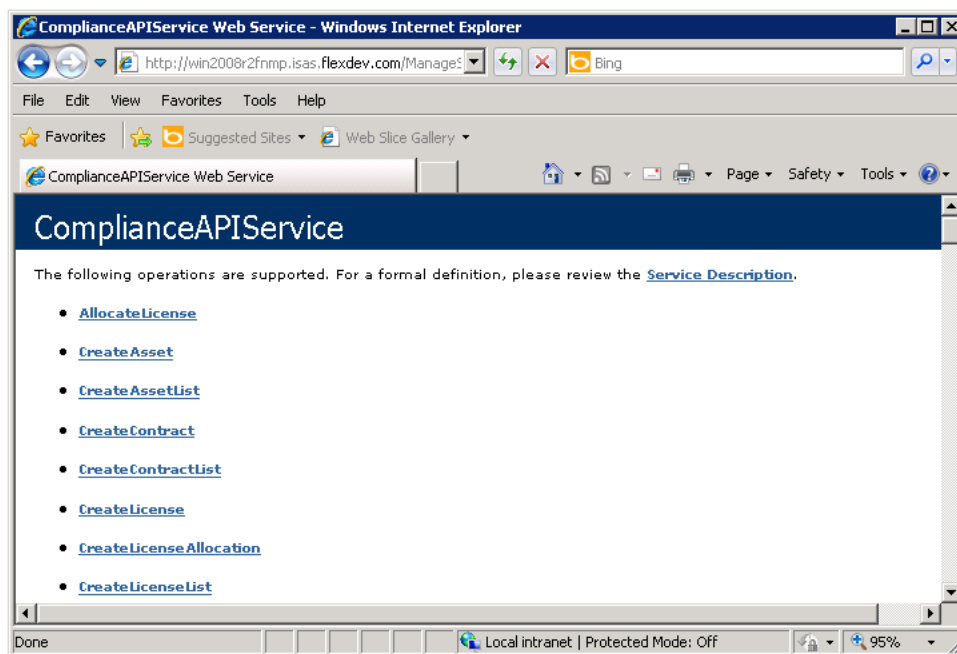
such as:

`http://win2008r2fnmp/ManageSoftServices/ComplianceAPIService/ComplianceAPIService.asmx`



**Tip** • When identifying the FlexNet Manager Suite / FlexNet Manager Platform server in this URL, you can enter either the application server name or the server IP address.

The **ComplianceAPIService** page on the FlexNet Manager Suite / FlexNet Manager Platform server should open **without** prompting you to enter network credentials:



If you **are** prompted to enter network credentials, then Windows Authentication is not set up correctly on the FlexNet Manager Suite / FlexNet Manager Platform server and you will need to modify its authentication settings.



**Note** • If Windows Authentication is not enabled on the FlexNet Manager Platform server, App Portal will be unable to communicate with FlexNet Manager Suite / FlexNet Manager Platform.

2. To modify the FlexNet Manager Suite/ FlexNet Manager Platform server authentication settings, see [Verify FlexNet Manager Suite On Premises Application Server Authentication Settings in IIS](#).

## Invoke GetCategories API

On the App Portal server, once you are able to browse to the ComplianceAPIService without being prompted to log in (as described in [Testing App Portal Server Authentication Settings](#)), try to invoke the GetCategories API. You should be able to invoke it without encountering any issues.



### Task

#### To invoke GetCategories API:

1. On the App Portal server machine, enter the following URL in a web browser:

`http://<AppPortalServer>/ESD/WS/Integration.asmx`

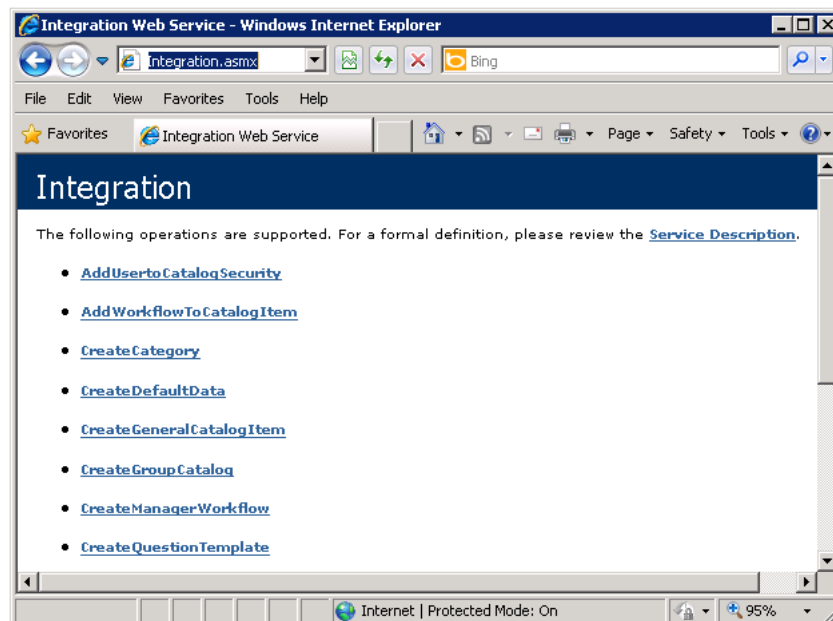
such as:

`http://Win2008R2AppPortal/ESD/WS/Integration.asmx`

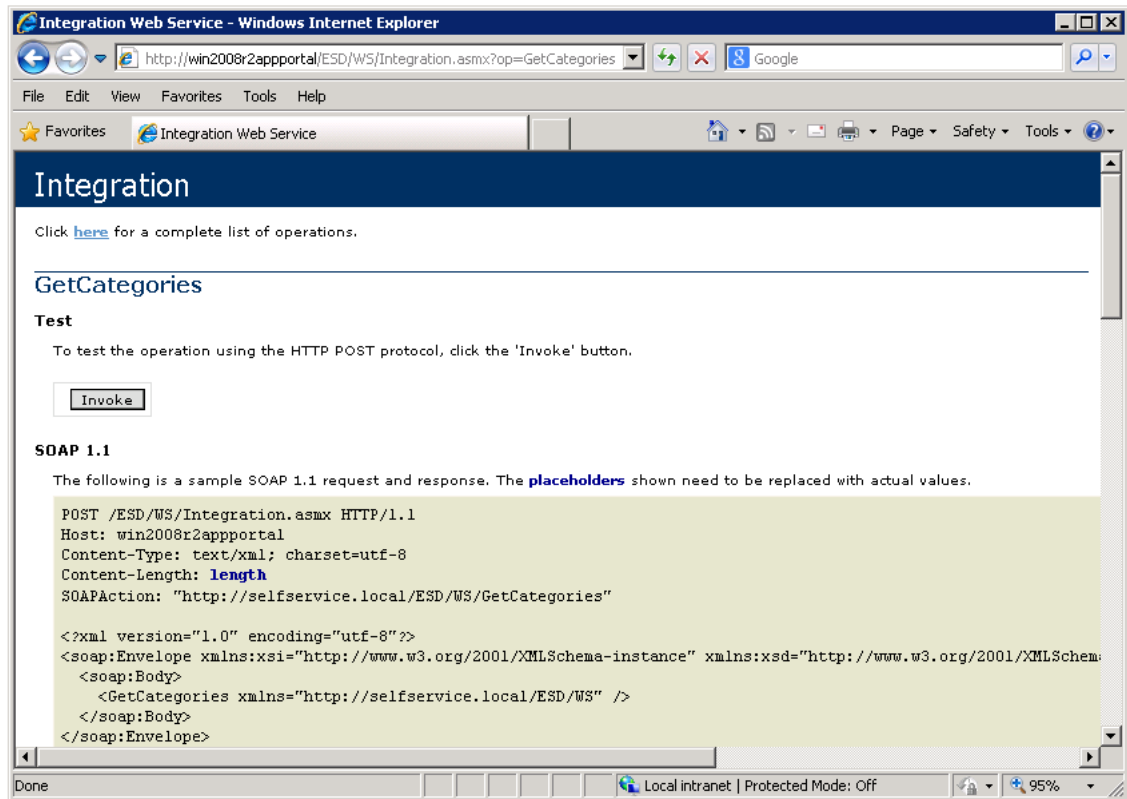


**Tip** • When identifying the App Portal server in this URL, you can enter either the application server name or the server IP address.

The **Integration** documentation page on the App Portal server should open **without** prompting you to enter network credentials:



2. Click on **GetCategories** in the list. If this API is working correctly, the following page should be displayed:



If an error message is displayed instead, App Portal is not configured properly. One of the following could be causing this problem:

- **Prevented by Active Directory policy**—This type of error usually means that the System Administrator has changed the Active Directory policy so that it prevents the Flexera Software services from working.
- **User does not have access to IIS**—The user who is testing the connection may not have access to IIS if they are in the wrong security groups.

## Error After Installation on X64 Server with WSUS Role

The App Portal website fails after installation on an X64 Server with WSUS role and generates the following error message:

HTTP 500.19 - Internal Server Error: The requested page cannot be accessed because the related configuration data for the page is invalid

To resolve this error, run the following command:

```
%windir%\system32\inetsrv\appcmd.exe set config -section:system.webServer/httpCompression /-
[name='xpress']
```



**Note** • You are only required to run this command one time, not each time App Portal is launched.



**Note** • The resolution to this error is documented in the following KB article:

*Q207028: ERRDOC: WSUS and X64 - HTTP Error 500.19 - Internal Server Error*

## Troubleshooting App Portal Integration Issues

The following topics may assist you when troubleshooting App Portal integration issues:

- [App Portal Catalog Item Not Automatically Created When AdminStudio Publishes an Application](#)
- [Preventing App Portal From Possibly Displaying False “Install Failed” Status for Application Deployment on SCCM 2012](#)

### App Portal Catalog Item Not Automatically Created When AdminStudio Publishes an Application

There could be several reasons why an App Portal catalog item is not automatically created when AdminStudio publishes an application to System Center Configuration Manager or Symantec Altiris Management Suite.

- [AdminStudio 2013 R2 App Portal Settings Not Specified](#)
- [AdminStudio 2013: App Portal Default Category Not Specified](#)
- [Symantec Endpoint Protection Blocking Notification of App Portal](#)

#### AdminStudio 2013 R2 App Portal Settings Not Specified

If you are using AdminStudio 2013 R2 or later, an App Portal catalog item is automatically created when AdminStudio publishes an application *only if* the following App Portal settings on the **App Portal Information** tab of the **Application View** in Application Manager have been set:

- The **Categories** property must be specified.
- The **Notify Flexera Software App Portal on publish of current Application** option on the **Categories** dialog box must be selected.

For more information, see [Enabling Automatic Creation of App Portal Catalog Item](#) in the AdminStudio 2014 Help Library.

#### AdminStudio 2013: App Portal Default Category Not Specified

If both AdminStudio (11.5 SP2 or 2013) and App Portal are connected via the Flexera Service Gateway, when you publish an application from AdminStudio to System Center 2012 Configuration Manager, a catalog item for that application should automatically be created in App Portal (in the default catalog category). Both the App Portal catalog item and the AdminStudio application will be identified by the same Flexera Identifier.

If a catalog item fails to be created, it may be because App Portal no longer has a **Default Category** specified. This can occur if the existing default category is deleted in App Portal. If the existing default category is deleted, the **Default Category** field on the **Settings > Web Site > General** tab is set to -Select-:

Default Workflow	Default Workflow ▼
Default Workflow Group	Default Workflow Group ▼
Default Category	- Select - ▼

**Figure 6-1:** Default Category Field on Web Site > General Tab

In order for AdminStudio to automatically create an App Portal catalog item during publication, App Portal's default category must be set to a valid category. To attempt to resolve this issue, select an existing category from the **Default Category** list.



**Note** • Starting with AdminStudio 2013 R2, you can choose whether or not to automatically create a catalog item for an application when you publish it to System Center 2012 Configuration Manager or Symantec Altiris Management Server. You can also specify the destination App Portal category for the new catalog item. These settings are made on the **App Portal Information** tab of the Application Manager **Application View**. For more information, see:

- [Enabling Automatic Creation of App Portal Catalog Item](#)
- [Specifying Catalog Item Categories](#)

## Symantec Endpoint Protection Blocking Notification of App Portal

In some instances, an App Portal catalog item is not created when AdminStudio publishes a package to System Center Configuration Manager.

### Cause

This could be because Symantec Endpoint Protection blocked the notification of App Portal. If this is the case, the following error messages would be generated:

```
17:26:47 ERROR: AdminStudio.ESB.Integration.IntegrationService.LogException - NotifyAppPortalForGroup :  
The ConnectionString property has not been initialized.
```

```
17:26:47 ERROR: AdminStudio.ESB.Integration.IntegrationService.LogException - NotifyAppPortalForGroup :  
at System.Data.SqlClient.SqlConnection.PermissionDemand()
```

An anti-virus program (do not know which one yet) caused running tests in Test Center to fail. It prevented extraction of CAB files from MSI files thus stopping the correct execution of tests

### Resolution

To resolve this issue, try to disable SEP (Symantec Endpoint Protection).

## Preventing App Portal From Possibly Displaying False “Install Failed” Status for Application Deployment on SCCM 2012

When deploying an application from App Portal to System Center 2012 Configuration Manager, in some instances it is possible that App Portal will display an **Install Failed** status message in the **Status** column on the **My Requests** tab when, in fact, the deployment was successful.

This issue arises because System Center 2012 Configuration Manager returns different values to indicate failure for packages vs. applications, and App Portal is incorrectly interpreting the value returned from System Center 2012 Configuration Manager when an application is deployed as if a package was deployed.

If you have specified that you want System Center 2012 Configuration Manager to return the failure status of **Rejected** for package deployments, App Portal will incorrectly apply the “package” return value to “applications” and display an **Install Failed** status.

To resolve this issue, perform the following steps:



### Task

#### To prevent false “Install Failed” status for applications:

1. Perform one of the following steps:
  - **App Portal 2013 R2**—On the **Admin** tab, select **Settings > Deployment > SCCM 2012**.
  - **App Portal 7.3.1 or 7.5.x**—On the **Admin** tab, select **Settings > SCCM**.
2. Locate the **SCCM Status ID Mapping** area.

#### SCCM Status ID Mapping

Success Status ID's	Select Status IDs	▼
Failure Status ID's	Select Status IDs	▼
Program Collection Cleanup Status ID's	Select Status IDs	▼
Task Sequence Collection Cleanup Status ID's	Select Status IDs	▼
Enable Rerun Advertisement for Status ID's	Select Status IDs	▼



**Important** • The selections you make in the **Success Status ID's** and **Failure Status ID's** lists should only apply when deploying packages; they should be ignored when deploying applications.

3. From the **Failure Status ID's** list, clear the selection of **Rejected**.
4. To confirm that everything is set correctly, run the SQL below in the App Portal database and make sure that you do not see the value 2 in the comma-separated list of return values:

```
select * from WD_AppSettings where KeyName = 'FailureStatusIDs'
```

## Upgrading the App Portal Web Site

To upgrade an existing installation of App Portal to Enterprise Product Integration Enterprise Product Integration, first review the [About Upgrading](#) section and then perform the upgrade.



- [About Upgrading](#)
- [Performing the Upgrade](#)



**Important** • If you are upgrading from a previous release of App Portal and you are using Symantec Altiris as your deployment technology, you cannot use the App Portal Upgrader to perform an upgrade. Instead, you need to perform a complete installation and point to your existing Altiris database.

## About Upgrading

When upgrading an existing version of App Portal to App Portal Enterprise Product Integration, 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 Enterprise Product Integration from the following previous versions:

- App Portal 2015 R2
- App Portal 2015
- App Portal 2014
- App Portal 2013 R2

To upgrade from one of these supported versions to App Portal Enterprise Product Integration, use the **App Portal Enterprise Product Integration Upgrader**, which can be downloaded from the Flexera Software Product and License Center, as described in [Performing the Upgrade](#).



**Important** • If you want to upgrade an installation of App Portal 2013 or earlier to App Portal Enterprise Product Integration, contact a member of the Flexera Software Global Consulting Services team for assistance.

## Planning Your Upgrade

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

- **Step 1: Review the Release Notes**—Thoroughly review the Enterprise Product Integration Release Notes.
- **Step 2: 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.
- **Step 3: 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.

## Performing the Upgrade

The instructions for upgrading App Portal vary depending upon the version of App Portal you are upgrading to:

- **App Portal 2017 and later**—For instructions on how to upgrade to App Portal 2017 and later, see [Using the App Portal Installer to Perform an Upgrade](#).
- **App Portal 2016 SP2 and earlier**—For instructions on how to upgrade to App Portal 2016 and earlier, see [Running the App Portal Upgrader](#).

# Configuring AdminStudio

AdminStudio 11.5 SP2 or later can be integrated with App Portal and FlexNet Manager Suite / FlexNet Manager Server via the Flexera Service Gateway. When AdminStudio is integrated, the following occurs:

- **AdminStudio obtains the Flexera Identifier from FlexNet Manager Suite / FlexNet Manager Server**—When an application is imported into the Application Catalog, AdminStudio will automatically query the FlexNet Manager Suite / FlexNet Manager Server ARL and obtain the application's Flexera ID.
- **AdminStudio creates catalog item in App Portal**—When an application is published from AdminStudio to System Center Configuration Manager (2012 or Current Branch), a catalog item for that application will automatically be created in App Portal.

The following sections explain how to configure AdminStudio:

- [Connecting AdminStudio to the Flexera Service Gateway](#)
- [Testing AdminStudio's Connection to the Flexera Service Gateway](#)
- [Configuring Authentication in Internet Explorer](#)
- [Upgrading AdminStudio](#)

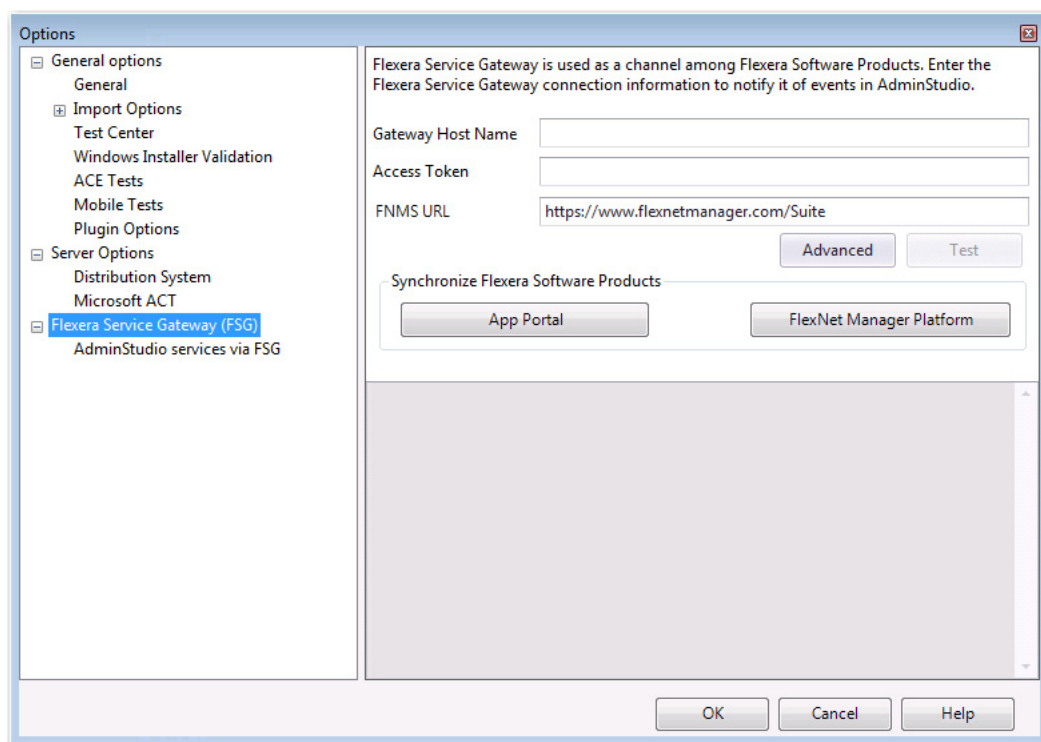
# Connecting AdminStudio to the Flexera Service Gateway

To enable AdminStudio to communicate with App Portal and FlexNet Manager Suite / FlexNet Manager Server via the Flexera Service Gateway, perform the following steps:




**Task**      **To enter Flexera Service Gateway connection settings:**

1. Open Application Manager.
2. On the **Application Manager** tab menu, select **Options**. The **Options** dialog box opens.
3. Select **Flexera Service Gateway (FSG)**. The **Flexera Service Gateway (FSG)** tab opens.



**Important** • Make sure that you select the **Flexera Service Gateway (FSG)** tab, not the **AdminStudio services via FSG** subtab.

4. Enter the following information:

Field	Description
<b>Gateway Host Name</b>	<p>Enter the name or URL of your Flexera Service Gateway server.</p> <ul style="list-style-type: none"> <li>• <b>Port number</b>—If your System Administrator has installed Flexera Service Gateway using a different port than the default port, enter the appropriate port number at the end of the URL, preceded by a colon, such as:  172.300.40.501:8484</li> <li>• <b>DNS name vs. IP address</b>—You can use a DNS name or an IP address. You should specify a DNS name if all clients are on the same domain and can resolve it; otherwise, use an IP address.</li> <li>• <b>HTTPS</b>—You should always use https.</li> </ul>  <p><b>Note</b> • The Flexera Service Gateway installer is downloaded from the Flexera Software Product &amp; License Center.</p>
<b>Access Token</b>	<p>If you are connecting to an installation of FlexNet Manager Suite Cloud, enter the access token that was provided by your system administrator.</p> <p>If you are connecting to an installation of FlexNet Manager Suite On Premises, leave this field blank.</p>
<b>FNMS URL</b>	To easily configure your connection to FlexNet Manager Suite, enter the FlexNet Manager Suite URL.

5. If you need to enter the Flexera Service Gateway login credentials, click **Advanced** to open the **Credentials** dialog box, where you can enter the Flexera Service Gateway login credentials.



**Important** • By default, the default credentials (admin, admin) are already entered. Unless your system administrator has informed you that these credentials have been changed, you do not need to open the **Credentials** dialog box.

6. Click **Test** to validate and save the Flexera Service Gateway connection information.



**Tip** • The Flexera Service Gateway will not appear as registered within AdminStudio. The only place to confirm the current integrated gateway is to check the AdminStudio database for the `cssysconnectioninfo` table.

7. Under **Synchronize Flexera Products**, click the **FlexNet Manager Platform** button to search the FlexNet Manager Suite Application Recognition Library (ARL) to locate and obtain the Flexera Identification Number for the Application Catalog's existing applications.



**Note** • After valid Flexera Service Gateway connection information is entered, each time you import an application into the Application Catalog, the Flexera Identification Number for that application will be automatically obtained from FlexNet Manager Suite / FlexNet Manager Server.

8. Click the **App Portal** button to create a catalog item in App Portal for all of the applications in the Application Catalog that were published to System Center Configuration Manager before the Flexera Service Gateway connection information was entered.



**Note** • After valid Flexera Service Gateway connection information is entered, each time you publish an application to System Center 2012 Configuration Manager, a catalog item for that application will automatically be created in App Portal.

9. Click **OK**.

## Testing AdminStudio's Connection to the Flexera Service Gateway

If AdminStudio is successfully connected to the Flexera Service Gateway (as described in [Connecting AdminStudio to the Flexera Service Gateway](#)), and if FlexNet Manager Suite / FlexNet Manager Server is also connected, a **Flexera Identification Number** will be displayed on the **General Information** tab of an application's **Application View**. Also, messages related to the Flexera Identification Number will be displayed during application import and publication to System Center 2012 Configuration Manager.

- [View Flexera Identification Number in Application View](#)
- [View Flexera Service Gateway Messages During Import and Distribution to SCCM](#)

## View Flexera Identification Number in Application View

If AdminStudio is successfully connected to the Flexera Service Gateway (as described in [Connecting AdminStudio to the Flexera Service Gateway](#)), and if FlexNet Manager Suite / FlexNet Manager Server is also connected, a **Flexera Identification Number** will be displayed on the **General Information** tab of an application's **Application View**.



### Task

#### To view an application's Flexera Identification Number:

1. Open Application Manager.
2. On the **Catalog** tab, select an application in the tree. The **Application View** opens.

Salesforce for Outlook Application View		
General Information	Deployment Types	References
Property	Value	
Administrator comments	Contact: Your local administrator	
Manufacturer	salesforce.com	
Software version	1.5.178.214	
Date published		
Install from Install Application task sequence	True	
Distribution priority	Medium	
Distribute to preferred DP	False	
Prestaged DP settings	Manually copy the content in this package to the DP	
Display supersedes information to user	False	
Localized description	Contact: Your local administrator	
User documentation		
Icon file	sync_ico	
Classification	Desktop	
Flexera Identification Number	arl://MGS-APP-00000125196	

- Note that an ID number is displayed in the **Flexera Identification Number** field, such as:

arl://MGS-APP-00000125196

## View Flexera Service Gateway Messages During Import and Distribution to SCCM

When AdminStudio is connected to the Flexera Service Gateway, additional output messages appear each time you import an application into the Application Catalog or publish an application to System Center 2012 Configuration Manager. To view these messages, perform the following steps:



### Task

#### To view Flexera Service Gateway messages during import and distribution to SCCM:

- Using Application Manager, import an application into the Application Catalog. The following messages will be listed on the **Import** tab of the Output Window:

Extracting Flexera Identification Number from FlexNet Manager Platform...

Done with extracting Flexera Identification Number from FlexNet Manager Platform

- Using Distribution Wizard, publish an application to System Center 2012 Configuration Manager. The following messages will be listed on the **Distribution Output** panel of the Distribution Wizard:

Sending publish notification to Flexera Gateway Service.

Publish notification result from Flexera Gateway Service: Success.

# Configuring Authentication in Internet Explorer

To configure authentication in Internet Explorer so that you can access FlexNet Manager Suite / FlexNet Manager Server from AdminStudio, perform the following steps:



## Task

### To configure authentication in Internet Explorer:

1. On the AdminStudio machine, enter the following URL in the Internet Explorer web browser:

`http://<FNMPServer>/ManageSoftServices/ComplianceAPIService/ComplianceAPIService.asmx`

such as:

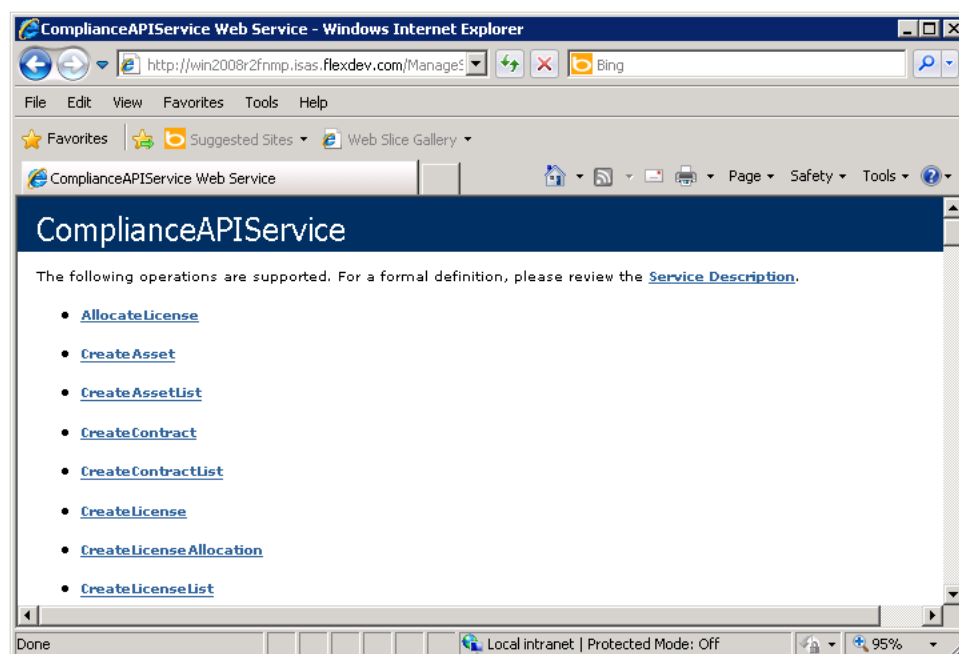
`http://win2008r2fnmp/ManageSoftServices/ComplianceAPIService/ComplianceAPIService.asmx`



**Tip** • When identifying the FlexNet Manager Suite / FlexNet Manager Server server in this URL, you can enter either the application server name or the server IP address.

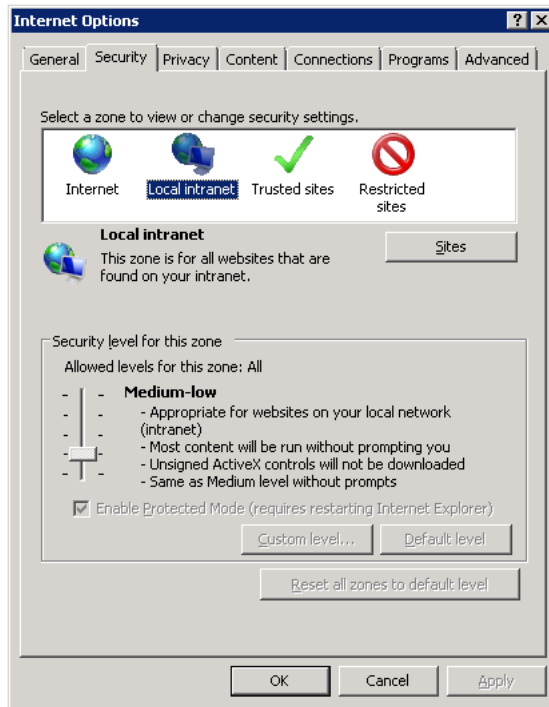
You will then be prompted to login to this server.

2. Enter the login credentials for this server and click **OK**. The **ComplianceAPIService** page on the FlexNet Manager Suite / FlexNet Manager Server server opens:

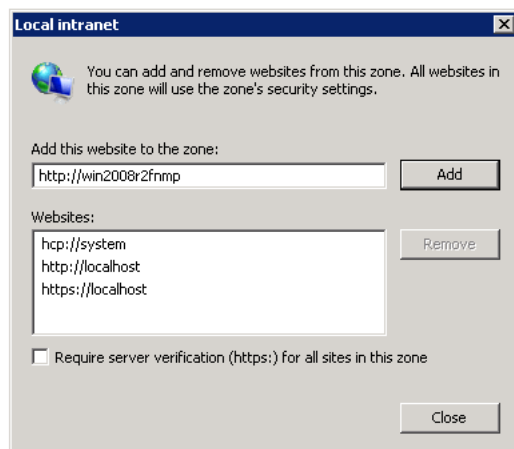


3. Select **Tools > Internet Options**. The **Internet Options** dialog box opens.
4. Open the **Security** tab.
5. Select the **Local intranet** zone.





6. Click **Sites**. The **Local intranet** dialog box opens, with the current site (<http://win2008r2fnmp>) listed in the **Add this website to the zone** field.



7. Click **Add**. The site name is now listed in the **Websites** list.
8. Click **Close** to close the **Local intranet** dialog box and click **OK** to close the **Intranet Options** dialog box.

## Upgrading AdminStudio

Upgrading an existing Application Catalog to AdminStudio 2013 is a two step process. You first need to use the user interface to upgrade the database. Then you need to change the Application Catalog database's collation setting to SQL\_Latin1\_General\_CP1\_CI\_AS.

- [Upgrading an Application Catalog](#)

- [Changing the Database Collation of the Upgraded Application Catalog](#)

## Upgrading an Application Catalog

When you attempt to open an existing Application Catalog in the AdminStudio 2013 client tools interface, you are prompted to upgrade the Application Catalog to the latest AdminStudio schema. This section explains this procedure.



**Important** • Before you upgrade the Application Catalog database from a previous AdminStudio version, it is strongly recommended that you create a backup of the original database. This is a standard precaution that is recommended to prevent possible data loss. If you are using the Application Catalog Software Repository feature, you may also want to make a backup copy of your Software Repository directories before upgrading.



### Task

#### To upgrade an existing Application Catalog:

1. Launch Application Manager.
2. On the Application Manager tab menu, select **Connect**. The **Connect Application Catalog** dialog box opens.
3. Open the **Standalone** tab. The **Standalone** tab opens, prompting you to enter database connection information.
4. If you want this Application Catalog to be the default shared Application Catalog used in your organization, select the corresponding option at the bottom of the dialog box.
5. Select the **Server** where the Application Catalog is stored.
6. Specify how the database server should verify the authenticity of the login—either using **Windows Authentication** or **Server Authentication**. If you selected **Server Authentication**, enter the appropriate **Login ID** and **Password**.
7. In the **Catalog** box, enter the name of the Application Catalog you want to open.
8. Click **Test** to test the connection to the database.
9. Click **OK**. A message opens stating that the Application Catalog needs to be upgraded, and asking Do you want to upgrade now?.
10. Click **Yes**. The **Welcome** panel of the Upgrade Wizard opens.
11. Click **Next**. The **Upgrade Progress** panel opens and the upgrade begins.  
  
When the upgrade is complete, the message Upgrade Completed is listed, and the **Finish** button is enabled.
12. Click **Finish**. The upgrade is now complete and all of your Application Catalog data has been preserved.



**Note** • When an SQL Server Application Catalog database is upgraded, the old tables are not dropped from the Application Catalog.

# Changing the Database Collation of the Upgraded Application Catalog

Generally, an Application Catalog database obtains its collation setting from the SQL Server collation setting, unless one specifies a different collation setting. Therefore, if an SQL Server is running with the collation setting of `Latin1_General_CI_AS`, then any database created on this SQL Server will have the collation setting of `Latin1_General_CI_AS` by default.

However, AdminStudio 2013 or later requires the database collation to be `SQL_Latin1_General_CP1_CI_AS`. If a new Application Catalog is created using AdminStudio 2013 or later, that Application Catalog database is created with the correct collation setting, irrespective of the SQL Server collation setting. However, if you upgrade an Application Catalog database from a previous version to the AdminStudio 2013 or later schema using the Upgrade Wizard or using scripts, the collation setting is not changed, so you must perform the steps below to change it.



**Note** • In the United States, the default collation for any SQL Server is `SQL_Latin1_General_CP1_CI_AS`. However, in other geographies such as the United Kingdom and Europe, the default collation is set to something else. Therefore, this topic is more relevant to users located in geographies outside of the United States.



**Important** • If the collation setting of an AdminStudio 2013 or later Application Catalog is not set to the correct collation setting, you will be able to connect to it, but it will cause Application Manager to periodically crash. An error message such as the following will appear in the log file (`ISCMIDE.Log`):

*'Exception 'System.Data.SqlClient.SqlException (0x80131904): Cannot resolve the collation conflict between "Latin1\_General\_CI\_AS" and "SQL\_Latin1\_General\_CP1\_CI\_AS" in the equal to operation.'*

To change the collation setting of an AdminStudio Application Catalog database to `SQL_Latin1_General_CP1_CI_AS`, perform the following steps:



## Task

### To change the collation setting of an AdminStudio Application Catalog database:

1. Download the following ZIP file and extract the files to a temporary folder:  
<http://helpnet.flexerasoftware.com/adminstudio2013/CollationChange.zip>
2. Open SQL Management Studio and run the `Pre_Collation_Change.sql` file against the AdminStudio 2013 Application Catalog database.
3. Open the `Collation_Change.sql` file in an editor and replace the `AS_DATABASE_NAME` string with the name of the Application Catalog database that you are upgrading.
4. Run the `Collation_Change.sql` file against the AdminStudio 2013 Application Catalog database.
5. Run the `Post_Collation_Change.sql` file against the AdminStudio 2013 Application Catalog database.

The collation setting of the AdminStudio Application Catalog database will now have been changed to `SQL_Latin1_General_CP1_CI_AS`.



# 8

## Configuring Workflow Manager

When Workflow Manager is connected to the Flexera Service Gateway, you can connect an App Portal catalog item to a Workflow Manager workflow request.

- [Connecting Workflow Manager to the Flexera Service Gateway](#)
- [Testing Workflow Manager's Connection to the Flexera Service Gateway](#)
- [Upgrading Workflow Manager](#)
- [Troubleshooting Workflow Manager Issues](#)

# Connecting Workflow Manager to the Flexera Service Gateway

The Flexera Service Gateway is a component that enables AdminStudio, Workflow Manager, App Portal, and FlexNet Manager Platform to communicate. When Workflow Manager is connected to the Flexera Service Gateway, you can connect an App Portal catalog item to a Workflow Manager workflow request.

In App Portal, you select an event that you want to trigger a Workflow Manager workflow (such as **On Submit Approval**) and the Workflow Manager project that you want to use. A workflow request is then created in Workflow Manager. When Workflow Manager completes the workflow request, the status in App Portal changes to **Complete**.

The method used to connect Workflow Manager to the Flexera Service Gateway varies by version:

- [Workflow Manager 2015 and 2016](#)
- [Workflow Manager 2013 or 2014](#)

## Workflow Manager 2015 and 2016

To connect Workflow Manager to the Flexera Service Gateway, perform the following steps:



---

### Task

#### **To connect to the Flexera Service Gateway:**

1. Launch the following file on the machine where you installed Workflow Manager:  
`C:\AdminStudioWebComponents_[VERSION]\Support\Config\Config.exe`  
The AdminStudio Configuration Wizard Welcome panel opens.
2. Select **Configure Flexera Service Gateway** and click **Next**. The **Configuration Settings: Flexera Service Gateway** panel opens.
3. In the **Gateway Host Name** field, enter the name of your Flexera Service Gateway Server.
4. By default, the user name and login to the Flexera Service Gateway is admin / admin. If your organization is using a different user name and password, click **Advanced** and enter the appropriate credentials.
5. Leave the **Access Token** and **Application Recognition Service URL** fields blank.
6. Click **Test** to test the connection. You should receive the following message:  
  
Connection to Flexera Service Gateway successful!  
  
Testing WorkflowManager was successful at http://SERVER\_NAME:81/WebServicesroot/authentication.asmx  
  
The configuration begins and messages are displayed.
7. When the configuration steps are complete, click **Finish** to close the wizard.

## Workflow Manager 2013 or 2014

To connect Workflow Manager to the Flexera Service Gateway, perform the following steps:



### Task

#### To connect to the Flexera Service Gateway:

1. In Workflow Manager, open the **System Settings** subtab of the **Administration** tab.
2. Under **Register With Flexera Service Gateway**, enter the following information:
  - **Workflow Manager Portal Server**—Enter the IP address of your Workflow Manager portal server. Do not enter an http:// prefix.
  - **Flexera Service Gateway Server**—Enter the name of your Flexera Service Gateway Server.

**Register With Flexera Service Gateway**  
Services in Flexera Service Gateway only works with Windows Authentication. Please enter the Workflow Manager portal host name to register with Flexera Service Gateway  

<b>Workflow Manager Portal Server:</b>	<input type="text" value="111.200.33.444"/>
<b>Flexera Service Gateway Server:</b>	<input type="text" value="myserver.3535.mycompany.com"/>

Update

3. Click **Update**.



# Testing Workflow Manager's Connection to the Flexera Service Gateway

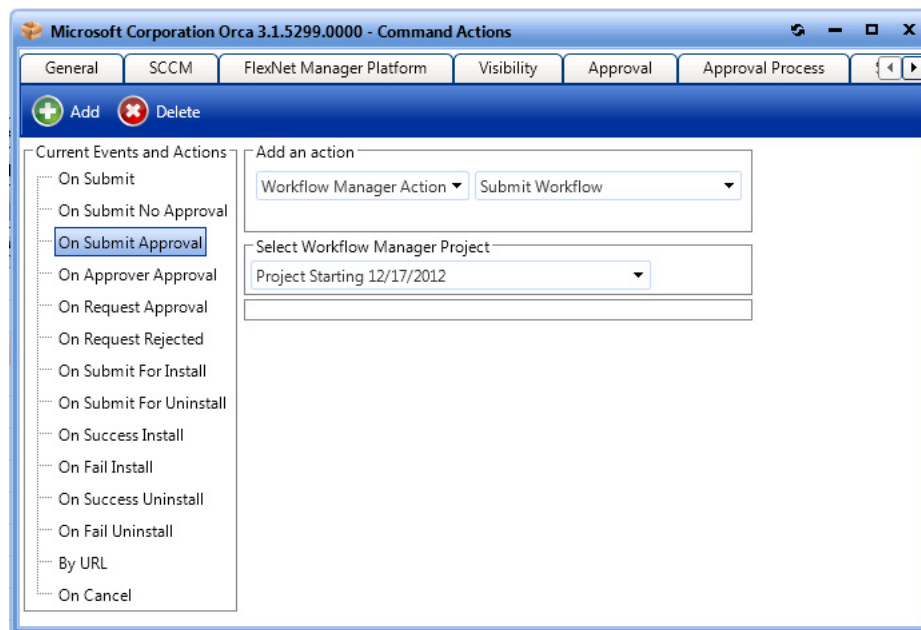
To test Workflow Manager's connection to the Flexera Service Gateway, perform the following steps:



## Task

### **To test Workflow Manager's connection to the Flexera Service Gateway:**

1. In App Portal, open the **Actions** tab of a catalog item's **Catalog Item Properties** dialog box.
2. Under **Current Events and Actions**, select an event that you want to trigger a Workflow Manager workflow (such as **On Submit Approval**).
3. Under **Add an action**, select **Workflow Manager Action** from the first list and **Submit Workflow** from the second list.
4. Under **Select Workflow Manager Project**, select a project from the list.



5. Click **Add**.
6. On the **Browse Catalog** tab, submit a workflow request for this catalog item.
7. Open Workflow Manager to see if a workflow request was automatically created for this catalog item.
8. In Workflow Manager, complete the workflow request.
9. Open App Portal and confirm that the status of the catalog item request has changed to **Complete**.

## Upgrading Workflow Manager

To upgrade an existing version of Workflow Manager to a new version, perform the following steps.

**Task****To upgrade a previous version of Workflow Manager:**

1. On the Workflow Manager web server, launch the Workflow Manager installer. The **Welcome** panel opens and states that it has detected an existing version of Workflow Manager.
2. Click **Next**. The **License Agreement** panel opens.
3. Select the **I accept the terms of the license agreement** option and click **Next**. The **Ready to Upgrade the Program** panel opens.
4. Click **Install**. The upgrade of the installation of Workflow Manager begins. When the upgrade is complete, the **Completed** panel opens.
5. Click **Finish** to exit the wizard.



**Note** • A log file has been created to help you identify any customizations that you may have made since the original installation of the previous version. You may need to take additional manual steps to port over these customizations to the latest version.

# Troubleshooting Workflow Manager Issues

You may encounter the following issues when running Workflow Manager in an integrated environment.

- [Test Center Testing Fails When Triggered by Workflow Manager](#)

## Test Center Testing Fails When Triggered by Workflow Manager

### Problem

When a Workflow Manager workflow request triggers testing in Application Manager Test Center, the testing fails.

### Cause

If Test Center testing fails when testing is triggered by Workflow Manager, it could be because an anti-virus program is installed and running on the machine where AdminStudio is installed, and is blocking the functionality required to test Windows Installer packages. Testing could fail because the anti-virus software prevents the extraction of CAB files from the Windows Installer packages, thus stopping the correct execution of tests.

### Resolution

To resolve this issue, turn off the anti-virus software program on the machine where AdminStudio is installed.



# Index

## A

- access token [32](#)
- accounts [16](#)
  - required permissions [16](#)
- Active Directory
  - resolving "double hop" issues [74](#)
- AdminStudio [10](#)
  - account permissions [17](#)
  - changing database collation of upgraded Application Catalog [107](#)
  - configuring [99](#)
  - configuring Internet Explorer authentication to connect to FlexNet Manager Platform [104](#)
  - connecting to the Flexera Service Gateway [100](#)
  - installing [13](#)
  - specifying required database permissions to user or group [17](#)
  - testing ability to obtain Flexera Identifier [71](#)
  - testing connection to Flexera Service Gateway [102](#)
  - troubleshooting App Portal connection [94](#)
  - unable to create App Portal catalog item [94](#)
  - Upgrade Wizard [106](#)
  - upgrading [105](#)
  - upgrading an Application Catalog [106](#)
  - viewing application's Flexera Identifier [102](#)
  - viewing Flexera Service Gateway messages [103](#)
- AdminStudio user account [17](#)
  - permissions on App Portal [17](#)
  - permissions on FlexNet Manager Platform [17](#)
  - permissions on SQL Server [17](#)
  - permissions on System Center 2012 Configuration Manager [17](#)
- AMS\_SYSTEM account
  - required privileges [33](#)
- App Portal
  - account permissions [30](#)
  - checking Default Category setting [94](#)
  - checking the ESDService service [89](#)
  - checking the SelfService service [89](#)
  - configuring [81, 82](#)
  - connecting to the Flexera Service Gateway [83](#)
  - error on X64 server with WSUS role [93](#)
  - ESD Service Account permissions required to access FlexNet Manager Platform [30](#)
  - ESD Service Account permissions required to access System Center 2012 Configuration Manager [30](#)
  - FlexNet Manager Platform tab of Catalog Item Properties dialog box [84](#)
  - installing [14](#)
  - permissions required by AdminStudio user account [17](#)
  - testing by invoking GetCategories API [92](#)
  - testing FlexNet Manager Platform server authentication settings [91](#)
  - testing server authentication settings [82](#)
  - testing the connection to the Flexera Service Gateway [84](#)
  - troubleshooting [86](#)
  - upgrading to App Portal 2015 [96](#)
  - verifying IIS settings [86](#)
  - verifying server authentication settings [86](#)
  - viewing catalog item's Flexera Identifier [84](#)
  - website failure after installation on X64 server with WSUS role [93](#)
  - Workflow Manager Action [113](#)
- App Portal App Pool identity account
  - permissions on FlexNet Manager Platform [30](#)
  - permissions on System Center 2012 Configuration Manager [30](#)
- App Portal Web Server [10](#)
- Application Catalog
  - changing database collation setting [107](#)

- specifying required database permissions [17](#)
- upgrading the collation setting [107](#)

application life cycle [11](#)

Application Recognition Library (ARL) [64](#)

## C

collation setting [107](#)

configuring

- Workflow Manager [109](#)

## D

database

- assigning required permissions [17](#)
- collation setting [107](#)

database collation issues [107](#)

database collation setting [107](#)

db\_reader permission [33](#)

db\_writer permission [33](#)

domains

- establishing two-way trusts between domains [34](#)

double hop issues

- resolving [74](#)
- temporary resolution for lab scenario [78](#)

## E

ESD Service Account

- permissions required to access FlexNet Manager Platform [30](#)
- permissions required to access System Center 2012 Configuration Manager [30](#)

ESDServices [89](#)

- checking in IIS [89](#)

execute permission [33](#)

## F

Flexera ID [79](#)

- viewing in Application Manager [102](#)
- viewing in FlexNet Manager Platform [79](#)

Flexera Identifier

- viewing in App Portal [84](#)

Flexera Service Gateway [10](#)

- connecting AdminStudio to [100](#)
- connecting App Portal to [83](#)
- connecting FlexNet Manager Suite to [63](#)
- connecting Workflow Manager to [110](#)
- installing [41](#)
- testing App Portal's connection to [84](#)
- testing Workflow Manager's connection to [113](#)
- viewing messages in AdminStudio [103](#)

FlexNet Manager Platform [10](#)

"trusted for delegation" requirement [31](#)

App Pool Identity account [31](#)

assigning permissions to App Portal account [30](#)

checking to see if ManageSoftWebServiceAppPool service is running [67](#)

Compliance API Service documentation page [62](#)

configuring [61](#)

configuring Internet Explorer authentication settings on AdminStudio machine [104](#)

creating Custom View to display Flexera ID [79](#)

enabling a trusted delegation [74](#)

enabling Kerberos authentication [76](#)

FlexNet Manager System account [31](#)

importing the Application Recognition Library (ARL) [64](#)

importing the ARL [15](#)

invoking GetTenants and GetFlexeraIDForApplication API [68](#)

permissions required by AdminStudio user account [17](#)

permissions required by App Portal [30](#)

permissions required on FlexNet Manager Platform machine [31](#)

resolving problems that occur when installed on a separate machine from its SQL server [74](#)

Service Principal Names (SPNs) [76](#)

temporarily resolving "double hop" issues for P.O.C. [78](#)

testing configuration [71](#)

testing GetFlexeraIDForApplication API [71](#)

testing server authentication settings [62](#)

testing server authentication settings from App Portal [91](#)

troubleshooting communication issues [65](#)

upgrading Compliance Console [80](#)

verifying server authentication settings in IIS [66](#)

viewing application's Flexera ID [79](#)

when FlexNet Manager Platform is installed on separate computer than its SQL Server [31](#)

Windows Authentication problems [74](#)

FlexNet Manager Suite

- connecting to Flexera Service Gateway [63](#)

FlexNet Manager Suite Cloud

- access token [32](#)
- creating a service account [32](#)
- service account [32](#)

FlexNet Manager System Account

- permissions required on AdminStudio and App Portal [31](#)

FNMP. See *FlexNet Manager Platform*.

## G

GetFlexeraIDForApplication API [68](#)

- testing [71](#)

GetTenants API [68](#)

## I

IIS

- Service Principal Names (SPNs) 76
- IIS\_WPG group member 33
- installation 13
  - AdminStudio 13
  - App Portal 14
  - Flexera Service Gateway 41
  - Workflow Manager 16
- integrated environment
  - overview 10
- integrated solution
  - outline 10
  - prerequisites 9

## K

- Kerberos authentication 76

## L

- Latin1\_General\_CI\_AS 107

## O

- overview diagram 10

## P

- permissions 16
  - AdminStudio 17
  - AdminStudio user account 17
  - App Portal 30
  - assigning to Application Catalog user 17
  - by account 16
  - FlexNet Manager Platform 31
  - System Center 2012 Configuration Manager 34
  - Workflow Manager 33

## S

- SCCM 2012. *See System Center 2012 Configuration Manager.*
- SelfService service 89
  - checking in IIS 89
- server authentication settings
  - verifying in App Portal 86
- Service Principal Names (SPNs) 76
- SQL Server
  - permissions required by AdminStudio user account 17
- SQL\_Latin1\_General\_CP1\_CI\_AS 107
- System Center 2012 Configuration Manager 10
  - App Pool Identity account 34
  - permissions required by AdminStudio 17
  - permissions required by App Portal 30

## T

- token 32
- troubleshooting
  - App Portal 86
  - communication issues with FlexNet Manager Platform 65
- trusted delegation
  - enabling to resolve "double hop" issues 74
- trusts
  - establishing two-way trusts between domains 34
- two-way trusts between domains 34

## U

- upgrading
  - AdminStudio 105
  - App Portal 96
  - collation setting of database 107
  - FlexNet Manager Platform 80
  - Workflow Manager 113

## W

- Windows Authentication
  - enabling a trusted delegation 74
  - problems in FlexNet Manager Platform 74
- Windows NT authentication 34
- Workflow Manager 10
  - Active Directory query permission 33
  - AMS\_SYSTEM account privileges 33
  - App Pool Identity account 33
  - configuring 109
  - connecting to Flexera Service Gateway 110
  - creating a Workflow Manager action in App Portal 113
  - db\_reader, db\_writer, execute permissions 33
  - IIS\_WPG group member 33
  - installing 16
  - Local Administrators group member 33
  - permissions required on SQL Server 33
  - SQL Server permissions required when using Windows Authentication 33
  - testing connection to Flexera Service Gateway 113
  - upgrading 113
- Workflow Manager Action 113
- WSUS role 93

## X

- X64 Server 93

