Upgrading FlexNet Manager Suite to 2015 R2 On Premises

Contents

Legal Information

Document Name: FlexNet Manager Suite 2014 Rx to 2015 R2 SP1 Upgrade Guide (for on-premises delivery)

Part Number: FMS-11.1.0-UG01

Product Release Date: 23 October 2015

Copyright Notice

Intellectual Property

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

Restricted Rights Legend

1

Upgrading FlexNet Manager Suite to 2015 R2 SP1 on Premises

Topics:

- *Process Overview*

- *Design the Final Topography*

- *Prerequisites and Preparations*

This document covers upgrading from any 2014 version of FlexNet Manager Suite (2014, 2014 R2, or 2014 R3), or the 2015 version, to FlexNet Manager Suite 2015 R2 SP1 in an on premises implementation.

Note • Migrating from earlier versions such as 9.2 or earlier is not included in this document. For that process, please see the separate document Migrating to FlexNet Manager Suite 2015 On Premises. As well, managed service providers (MSPs) should reference separate documentation covering multi-tenant environments.

This document is intended for use by:

- System engineers responsible for implementing and maintaining the system

- Network and security personnel with responsibility for infrastructure that the system relies on

- Flexera Software consultants implementing your system.

Assumptions: Readers have completed at least the appropriate training course in FlexNet Manager Suite administration, and understand basic product concepts. Readers have a technical background and are experienced with product installations and configuration.

Process Overview

Upgrading from the 2014, 2014 R2, 2014R3, or 2015 release to FlexNet Manager Suite 2015 R2 SP1 is conceptually very straight-forward:

- If you had installed any language packs for your previous implementation (localizing the user interface into, for example, German or Japanese), these should be uninstalled first. (The new 2015 release installs language support for all available languages.)

- Run the scripts provided to upgrade the underlying databases.

- Run the installer on (each of) your central application server(s) to update the product itself

- Manage your inventory beacon updates:

    - If migrating from 2014, visit each inventory beacon and run the installer (available through your updated web interface of FlexNet Manager Suite) to update the beacon. While there, you may prefer to tweak the default schedules in the new, in-built beacon scheduler; and you need to update connection details for adapters previously run as Windows Scheduled Tasks.

    - If migrating from 2014 R2 or 2014 R3, your inventory beacons are self-updating. You can manage the upgrade process (including testing, pilot groups, and roll out) as described in `FlexNet Manager Suite Help` > `What Is an Inventory Beacon?` > `Upgrading Inventory Beacons`.

At this point, your system is upgraded and functional. You may also choose, as part of the upgrade project, to extend your implementation with some of the newly supported features, as described in the release notes. In general, details about these enhanced features are not included in this document, which focuses on the upgrade process itself.

Design the Final Topography

Your existing implementation of FlexNet Manager Suite might be installed on a single central server, or on a group of servers (such as a separate database server, and you may even have a separation between the web application server and the processing server). Going forward, you might consider scaling up your implementation as your estate grows. (In any case, please study the diagram below to understand terminology in this document.)

Determine whether to implement a single server or multi-server solution, based on projected scaling. Please refer to the following diagram, where each blue box represents a potentially separate server, and where all are given the names referenced throughout this document.

Note • Both the inventory server (processing server, or application server in a single-server implementation) and the inventory beacon(s) are expected to be members of Active Directory domains. (For test environments, consultants may see article 000017145 How to run FlexNet Manager Suite processing server on a workgroup computer.) Where you have only a single batch server (also known as a reconciliation server), this is not required to be a member of an Active Directory domain (although it may be). If you split this server into a master batch scheduling server and additional, separate batch servers, the Microsoft messaging technology requires a common

account which is much simpler to provide if all these servers are members of the Active Directory domain. For this reason, domain membership is recommended, and assumed in this document.

There are six different kinds of server functionality in FlexNet Manager Suite. Your implementation may merge all this functionality onto a few servers; or for very large implementations, you may need six or more separate (virtual or physical) servers. In all cases, it is important to understand the functionality of these separate components that make up a working system:

- At least one inventory beacon, and typically more for a complex infrastructure

Tip • An inventory beacon should be installed on the same server as the batch scheduling server (defined shortly).

- An inventory server, which can also be duplicated across multiple servers if you are gathering FlexNet inventory for many tens of thousands of devices (see below)

- A batch server (also known as a reconciliation server) that imports third-party inventory, integrates FlexNet inventory, incorporates business-related information, and reconciles everything to calculate your license position

Note • Massive implementations may spread this load across multiple batch servers, in which case exactly one is the 'parent' or batch scheduling server that controls the load sharing. Here, 'massive implementations' means those with over a million devices returning inventory, or with unusually high batch processing loads. Most likely you need only a single reconciliation server here.

- The database server (where the five underlying databases may also be split across separate database servers if required)

- The web application server that handles presentation of the interface

- A server for the business reporting option (powered by Cognos), where applicable. (This server may be shared between FlexNet Manager Suite and FlexNet Manager for Engineering Applications.)

Tip • Currently the Cognos content store requires a SQL Server installation no later than 2012.

Tip • You can start with your FlexNet Manager Suite 2014 (or 2014 R2) server and upgrade it to the new system, where it can function as any of the servers described above (or indeed, for the combined servers as described next, if yours is a smaller implementation). Similarly, if you had a separate database server in your previous implementation, that same database server may host the new databases shown in the diagram.

All system servers require a 64-bit operating system. The database server (alone) may have a 32-bit operating system, but a 64-bit operating system is recommended.

In more moderately-sized implementations (the vast majority), a typical implementation might have a separate database server and Cognos server, and combine the remaining three central functions as a single "application server", as shown in the diagram. As scaling dictates, you can combine or separate the web application server, the batch server, and the inventory server in any combination required. The logical separation of presentation from processing need not drive hardware requirements. Scaling considerations may include the following:

- Typically the first candidate for replication is the inventory beacon. This is often driven by network considerations as much as by simple scaling considerations.

- If your system manages more than 50,000 devices reporting FlexNet inventory alone (ignoring for the moment inventory through other third-party tools), the inventory server should be separated onto its own device. You can expect to duplicate a separate inventory server for (roughly) every 50,000 devices reporting FlexNet inventory.

- If you manage inventory from more than 100,000 devices, the batch server (or reconciliation server) may be separated from the web application server and installed separately.

- If you manage in the order of a million inventory devices, the batch server itself may be split into multiple batch servers, controlled by one batch scheduling server that also shares in the processing load.

💡
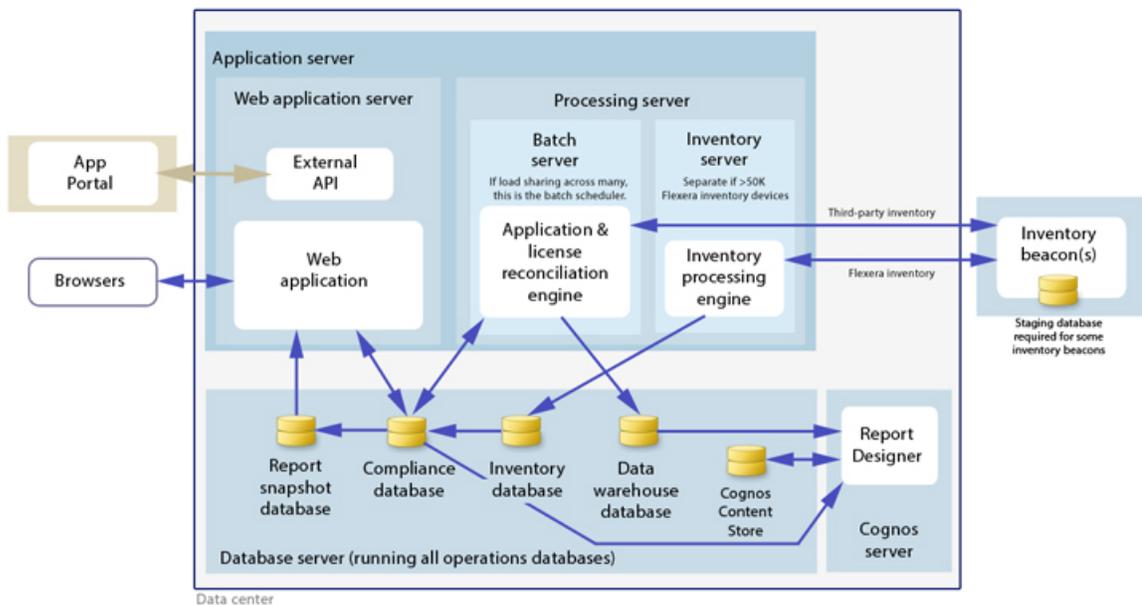
Tip • *When you implement your web application server as a separate server, or implement multiple batch servers, you must configure one or two network shares that all can access to share uploaded data between them. The shared drives are identified during the installation process. For details, see Configure Network Shares on page 20.*

The diagram shows that:

- FlexNet inventory (from the FlexNet inventory agent) is uploaded to the inventory database by the inventory server, and then separately imported to the compliance database

- Third-party inventory imported from other tools is loaded by the batch server(s) and stored directly in the compliance database

- Some time-based data is copied to the data warehouse database, and reports may combine trend data from here with current data from the compliance database

- Some data is copied to the snapshot database to improve presentation performance

- The web interface automatically displays a mixture of data from the snapshot database and the compliance database, as appropriate; and data manually input through the web interface is written back to the compliance database.

Choose your web servers per device

Web protocols are used for data transfer within the FlexNet Manager Suite infrastructure. Two alternatives are supported, and can be mixed and matched within the infrastructure of inventory beacons and servers:

- Microsoft IIS. Choose this alternative when any of the following apply:

    - The host server is one of your central application servers (web application server, batch server, or inventory server, or combinations as applicable). No web server is required on a stand-alone database server. When you install the recommended inventory beacon on the same device as the central batch scheduling server, that beacon also uses IIS (whereas other free-standing beacons on separate devices still have a choice).

    - When a particular inventory beacon is collecting inventory from (and passing back recommendations to) FlexNet Manager for SAP Applications, that inventory beacon must use IIS.

    - When you require Windows Authentication to allow transfer of data (for example, a parent inventory beacon might typically use Windows Authentication if it receives data from a child in your DMZ outside a firewall).

    - When you require the use of the HTTPS protocol to encrypt data transfers.

- FlexNet self-hosted web server. Choose this alternative when none of the previous cases apply, and:

    - You want simple administration of the web server.

    - You want to minimize the installations on your inventory beacon, so that you do not need to install Microsoft IIS.

    - Anonymous access, and use of the HTTP protocol, are adequate (for example, within your secure LAN).

Note • *After installation, more information about these web server options and how to configure them is available in the online help under Inventory Beacons > Local Web Server Page > Configuring Direct Inventory Gathering.*

Output

Prepare a block diagram of the actual servers for your implementation. Start with the central cluster of servers, depending on the scale of your implementation.

Don't forget the inventory beacons you intend to deploy. An inventory beacon on your batch server (or processing server, or application server, depending on your scaling decisions) is an option, but not mandatory if you are migrating only from the 2014 (or 2014 R2) release. Thereafter you may choose to deploy a hierarchy of inventory beacons, ensuring that every targeted device will have access (preferably high-speed LAN access) to an inventory beacon.

Label each block in your diagram with:

- The server type, either 'inventory beacon' or as named in the diagram above (for ease of reference in following instructions)

- The actual server name and IP address

- Which web server will be installed on each of these hosts.

Prerequisites and Preparations

Please ensure that you have worked through every one of the following topics.

Locate License Details (probably)

There are three possibilities for your license documentation:

- You may not need to find it. This is the case if you are upgrading with the same hardware as for your 2014 Rx implementation, and *not* adding the specialized inventory functionality in FlexNet Manager for VMware. The license installed on your server covers your upgrade (while you are under a maintenance agreement).

- You may need your existing license. If you are either upgrading to new hardware as part of this update, or scaling up your implementation with additional central servers (but not adding newly-licensed functionality), you need your original license file. A license file for your existing product(s) was sent to you with your original order confirmation. If you need and cannot locate the license file, please contact the Flexera Software order processing team, and ask for a new copy of your license file.

> 💡
> _____
>
> *Tip • One reason you might consider upgrading to new hardware is if you are still using 32-bit operating systems. FlexNet Manager Suite 2015 R2 SP1 requires 64-bit operating systems on all central application server(s). You might consider upgrading the operating system, or replacing the old servers.*

- You may need a new license. This is the case if you are upgrading from 2014 or 2014 R2, and plan to license the FlexNet Manager for VMwareoption for advanced inventory gathering in that context (2014 R3 already supported this option). Please contact your Flexera Software (or partner) account manager to request a license including this additional term.

Identify (or Set Up) Accounts

You may have accounts correctly configured from your previous implementation. If you need to adjust, here are the details.

For installation and operation, FlexNet Manager Suite requires several different sets of account privileges. While it is possible to load a single account with all these privileges, this is typically unacceptable in secure environments, which have a separation of concerns between interactive login accounts for installation and maintenance, and operational service accounts (usually with long-term and closely-guarded credentials).

The following table lists the various privilege levels, their purpose within FlexNet Manager Suite, and a suggested set of Active Directory accounts allowing for that separation of concerns.

💡

Tip • Where privileges are controlled by Active Directory Group Policy Objects (GPOs), ensure that the accounts and group(s) are added to the appropriate GPO settings prior to attempting installation. The recommended practice when creating the databases is to assign the installing administrator account (`fnms-admin`) and the service account (`svc-flexnet`) to an Active Directory group (suggested: `FNMS Administrators`) in order to grant them `db_owner` privileges; so you may choose to manage other rights through that group. Also note that these accounts and their privileges must remain active for the lifetime of the FlexNet Manager Suite environment.

Privileges	Required on	Purpose
Database administration privileges — suggested AD account: `db-admin` (Typically this is an existing database administrator within your enterprise.)		
Database administrator, with db_owner rights on all databases related to FlexNet Manager Suite.	Database servers	Provides the following accounts with database access rights as described.
Member of the **public** database role in the `model` database on the database server.	Database servers	Required so that the account can run scripts that check the database compatibility level.
SELECT rights to the `dbo.sysjobs` and `dbo.sysjobsteps` tables in the **msdb** database.	Database servers	Only required if an existing installation of FlexNet Manager Suite 2015 or earlier is being migrated to a later release.
Installing administrator privileges — suggested AD account: `fnms-admin` (Account details must be made available to `db-admin`.)		
Local administrator	• Central application server(s) (including, where separated, web application server, batch scheduling server, any separate batch servers, and inventory server); • All inventory beacons.	Installs and configures software on all servers. On inventory beacons, interactive login to the inventory beacon interface also requires local administrator privileges (that is, on inventory beacons this is an operational account as well as being required for setup).

Privileges	Required on	Purpose
Set the execution policy for, and execute, PowerShell scripts	Central application server(s) (including, where separated, web application server, batch scheduling server, any separate batch servers, and inventory server).	PowerShell scripts are used to complete the configuration of central servers during implementation.
Create tasks in Windows Task Scheduler	• Central application server(s) (including, where separated, web application server, batch scheduling server, any separate batch servers, and inventory server); • All inventory beacons.	Runs PowerShell scripts during installation that create scheduled tasks.
Internet connection to `https://flexerasoftware.` `flexnetoperations.com`	A central server (with network access to all other central application servers in a multi-server implementation).	Retrieve product downloads and licenses for implementation.
Internet connection to `http://` `www.managesoft.com` (Typically granted through membership in the `FNMS Administrators` security group in Active Directory.)	All central batch servers including the batch scheduling server (or, in smaller implementations, the processing server or application server).	Maintenance or unscheduled collection of the Application Recognition Library, the SKU libraries, and the Product Use Right Libraries.
Service account privileges — suggested AD account: `svc-flexnet` (Account details must be made available to `db-admin`.)		
Logon as a Service, and run all FlexNet services 💡 *Tip • Admin access for this account is convenient, and typically granted through membership in the `FNMS Administrators` security group in Active Directory; otherwise read, write, and execute permissions are required on all folders containing FlexNet installations, FlexNet data, and FlexNet log files.*	• Central application server(s) (including, where separated, web application server, batch scheduling server, any separate batch servers, and inventory server); • All inventory beacons.	Runs all system operations, including batch services and web services. ⚠ *Important • In a multi-server implementation, the same service account must be used on all central servers. This is required for proper functioning of Microsoft Message Queueing between the servers. (A distinct service account may be used for inventory beacons.)*

Privileges	Required on	Purpose
Logon as a Batch Job	• Central application server(s) (including, where separated, web application server, batch scheduling server, any separate batch servers, and inventory server); • All inventory beacons.	When the service account runs a batch job, this setting means the login is not an interactive user. 💡 *Tip • This is particularly important on the batch scheduling server (for authorization details, see Authorize the Service Account on page 32).*
Run scheduled tasks as a service account.	• Central application server(s) (including, where separated, web application server, batch scheduling server, any separate batch servers, and inventory server); • All inventory beacons.	Runs scheduled tasks within normal operations.
Run IIS application pools as a service account	• Central application server(s) (including, where separated, web application server, batch scheduling server, any separate batch servers, and inventory server); • Those inventory beacons that are running IIS	Normal operations
Internet connection to `http://www.managesoft.com` (Typically granted through membership in the `FNMS Administrators` security group in Active Directory.)	All central batch servers including the batch scheduling server (or, in smaller implementations, the processing server or application server).	Scheduled collection of the Application Recognition Library, the SKU libraries, and the Product Use Right Libraries.

💡

Tip • While the table above lists a single service account `svc-flexnet` on your application server(s) and inventory beacons, this may be adequate only in environments where security is not a significant concern. For greater security, consider a separate service account for each inventory beacon that has the permissions listed above on the inventory beacon, but no permissions on your central application server(s).

Note • *At implementation time, all services are configured with the correct password using the PowerShell scripts provided. If at any time the password on the service account is forced to change, the services will cease to operate. To ensure service continuity, you may either (a) allow the service account password to never expire (as normal for Windows service accounts), where permitted by your corporate policies; or (b) review the accounts listed in Password Maintenance on page 62.*

In addition to the three core accounts described in the table, your implementation may require additional accounts for special circumstances.

For example, if you are using adapters to connect to other systems and import data, you need appropriate accounts. For details, see documentation for the adapters you need, such as the *FlexNet Manager Suite Adapters Reference*, available through the title page of the online help after installation.

Important • *All accounts that will log in directly to (any part of) the application server to use FlexNet Manager Suite (excluding access through the web interface) must have db_owner permissions on all components of the operations databases: compliance data, warehouse data, snapshot data, and inventory data. A suggested method is to create either a local or Active Directory security group (such as FNMS Administrators) and add all such accounts to this group. Then you can, for example, set these permissions by opening each database in Microsoft SQL Server Management Studio, and granting db_owner privileges to the security group. The procedures are detailed in the topics covering database creation. Accounts to list in the security group minimally include:*

- *The operational service account (suggested: svc-flexnet)*

- *The installing administrator account (suggested: fnms-admin)*

- *Any operational account needing to log in to a central inventory beacon installed on your batch scheduling server (remember that, since the inventory beacon requires administrator privileges to run, this account is both a local administrator on the batch scheduling server and a db_owner)*

- *Any future back-up administrator accounts needed for the application server.*

Isolate the System

You need to protect your data from operational changes during the upgrade.

Since your FlexNet Manager Suite system receives inputs from operators, from uploads from inventory beacons, through scheduled tasks, and from its own processing of staged data, all of these should be turned off before you upgrade.

If you are upgrading a multi-server implementation, you need to repeat parts of this process for different servers. This table summarizes which tasks should be performed on which server for a multi-server implementation. (Where you have a smaller implementation that combines the functionality on fewer servers, make the changes on those servers that host the appropriate functionality. Any 'Yes' condition over-rides a 'Not required' statement.)

Tip • *In your 2014 Rx system, the column marked "Batch Svr" was previously assigned to your reconciliation server. In the 2015 R2 SP1 release, for very large implementations the reconciliation server can be split into a batch scheduling server and a number of child batch servers. The processes listed in the column below apply to any migrating batch scheduling server or batch server. (When these servers are not separated into multiple machines, but continue as a single server, the name reconciliation server may continue to appear.)*

Table 1: Isolation tasks for each server type

Task	Web App Svr	Batch Svr	Inventory Svr	Database Svr(s)
Shut down IIS	Yes	Yes	Yes	Not required
Stop related scheduled tasks	Not required	Yes	Yes	Not required
Stop services for FlexNet Manager Suite Batch Process Scheduler	Not required	Yes	Not required	Not required

1. Send out the notification (such as email), as required by your corporate processes, to alert operators that the system is going down for maintenance.

   At the appointed time, repeat the remaining steps across your central server(s) as required.

2. Log in to the server as a system administrator.

3. On your web application server, batch server, or inventory server, shut down Microsoft IIS as the most efficient way to prevent any operator from logging in, or any files from being uploaded. Use your preferred method. For example, using the user interface on Windows Server 2008:

   a) Click Start, right-click on **Computer**, and select **Manage** from the context menu.
      The **Server Manager** dialog opens.

   b) In the left-hand navigation bar, expand **Roles** > **Web Servers (IIS)**, and select **Internet Information Services**.
      The IIS page is displayed.

   c) In the **Actions** panel on the right, select **Stop**.
      A message like `Attempting to stop...` appears. Note that it can take some time before the service is stopped.

4. On your batch server or inventory server, disable all Windows scheduled tasks related to FlexNet Manager Suite.

   The scheduled tasks are different on the two different types of servers. On your batch scheduling server (also known as reconciliation server), change all tasks in the `FlexNet Manager Platform` folder:

   • Data warehouse export

   • Export to ServiceNow

   • Import SAP inventories

   • Import SAP package license

   • Inventory import and license reconcile

- Recognition data import

- Regenerate Business Import config

- Send contract notifications.

On your inventory server, change all tasks in the `FlexNet Manager Platform` folder:

- Import Active Directory

- Import application usage logs

- Import discovery information

- Import installation logs

- Import inventories

- Import Inventory Beacon activity status

- Import Inventory Beacon status

- Import remote task status information

- Import security event information

- Import system status information

- Import VDI access data.

An example process to change these tasks on Windows Server 2008:

a) Ensure that your **Server Manager** dialog is still open.

b) In the left-hand navigation bar, expand **Configuration** > **Task Scheduler** > **Task Manager Platform**, and select the **FlexNet Manager Platform** folder.

c) Select all of the relevant tasks in the list (click the first, shift+click the last), and in the **Actions** pane, in the **Select Item** section, click **Disable** (or right-click the selection, and click **Disable**).

d) Close the dialog.

5. On your batch scheduling server/reconciliation server, stop the services for FlexNet Manager Suite Batch Process Scheduler:

a) Navigate to Start > **Control Panel** > **Administrative Tools** > **View local services**.
The **Services** dialog opens.

b) In the list of services, right-click on `FlexNet Manager Suite Batch Process Scheduler`, and from the context menu, select **Stop**.

Check Database Collation Sequence

All databases for this system, including `tempdb`, require the correct collation sequence, both case insensitive and accent sensitive.

This means that they should be installed on one or more database instances that have this as the default collation sequence. If you are carrying forward the database instance that previously supported yourFlexNet Manager Suite 2014 (or 2014 R2 or R3) implementation, this already complies with the appropriate collations sequence. For any new DB instance, use this process to check the collation sequence.

1. In SQL Server Management Studio, locate the SQL Server instance in the **Object Explorer** pane.

2. Right-click the server, and select **Properties** from the context menu.

3. On the server **Properties** dialog, select the **General** tab, and check the current collation sequence.
   If the collation sequence ends with the codes `_CI_AS` (for example, `Latin1_General_CI_AS`), you may proceed with the installation. Otherwise you can set the collation sequence for each database, as you create it, by right-clicking the new database, selecting **Properties** from the context menu, and choosing the collation on the **Options** tab.

Configure .NET and IIS

ASP.NET needs patching, and IIS configuration must be modified for ASP.NET.

Detailed steps depend on the operating system and installed software. You must repeat this process in turn on each of:

• web application server

• batch server(s)

• inventory server

• each free-standing inventory beacon (the inventory beacon installed on your central batch scheduling server is covered by the configuration of the batch scheduling server).

Note • Inventory beacons have an additional requirement, that PowerShell is at least at version 3.0. Should you wish to upgrade PowerShell to release 4.0, Microsoft also requires Microsoft .NET Framework 4.5 on the same server. Take both these matters into account at the same time (see Upgrade PowerShell on Inventory Beacons on page 19 for more details).

(If your implementation combines multiple servers into a processing server, or into an application server, then complete the task once per server.)

Tip • Mark off each server on your block diagram as this process is completed for that device.

1. If the server is running Microsoft Windows Server 2012:

   a) Open Windows Programs and Features.

   b) Search the list of applications for Microsoft .NET Framework 4.5 (or later). If it is present, skip to step 4 below.

c) Because Microsoft .NET Framework 4.5 (or later) is not present, follow steps under "To install IIS and ASP.NET modules on Windows Server 2012 using the UI" in *http://technet.microsoft.com/en-us/library/ hh831475.aspx#InstallIIS*. Thereafter, continue with step 4 below.

2. If your server is running Microsoft Windows Server 2008, the original installation was Microsoft .NET Framework 4, but it may have been upgraded already to 4.5. To check:

    a) Open Windows Programs and Features.

    b) Search the list of applications for Microsoft .NET Framework, and determine whether it is release 4 or release 4.5 (or later).

        • If it is 4.5 (or later), skip to step 4 below.

        • If it is 4.0, apply the patches listed in step 3 (following).

3. In all cases where you have Microsoft .NET Framework 4.0 (and *not* 4.5) installed, ensure that both of the following patches are applied:

    • Update 4.0.3 for Microsoft .NET Framework 4 Runtime Update (KB2600211), from *http:// www.microsoft.com/en-us/download/details.aspx?id=29053*

    • Update for Microsoft .NET Framework 4 on Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows 2008 R2 - KB2836939, from *http://www.microsoft.com/en-us/ download/details.aspx?id=39257*

    • FIX: System.ArgumentOutOfRangeException exception when you run a .NET Framework 4-based application that uses the MemoryCache.CreateCacheEntryChangeMonitor method, from *https:// support.microsoft.com/en-au/kb/2346777*.

4. If you are currently patching an inventory beacon (including one co-installed with your batch scheduling server) with the previous two updates, also ensure that you have applied this third patch: Update for the .NET Framework 4, from http://support.microsoft.com/kb/2468871, and downloadable from *http:// www.microsoft.com/en-us/download/details.aspx?id=3556*.

Tip • *The installer for inventory beacons will not run until this patch has been applied on the beacon server running Microsoft .NET Framework 4. (As before, the patch is not required if the version of Microsoft .NET Framework is 4.5 or later.)*

5. Open a Command Line window on the current server (for example, **Start** > search for `cmd` > run `cmd.exe`).

6. Enter `cd %SystemRoot%\Microsoft.NET\Framework\v4.0.30319` (this folder is available only after you have correctly installed Microsoft .NET Framework 4.0).

7. Install ASP.NET (which also registers ASP.NET with IIS when present), for example with the platform-appropriate commands:

    For operating systems up to Windows Server 2008 R2, use:

    ```
    aspnet_regiis.exe -ir -enable
    ```

    For Windows Server 2012, use:

    ```
    dism /online /enable-feature /featurename:IIS-ApplicationDevelopment
    dism /online /enable-feature /featurename:IIS-ISAPIFilter
    ```

```
dism /online /enable-feature /featurename:IIS-ISAPIExtensions
dism /online /enable-feature /featurename:IIS-NetFxExtensibility45
dism /online /enable-feature /featurename:IIS-ASPNET45
```

8. `Exit` to close the command line window.

   If you are currently working on any of:

   - Your web application server

   - Your batch scheduling server

   - A free-standing inventory beacon that uses the FlexNet self-hosted web server (and not IIS)

   loop back now and restart this process for the next server on your list. For your inventory server and any inventory beacon using IIS, continue and disable WebDAV on these devices.

9. Open the IIS settings page. For example:

   - On Windows Server 2008 R2, open Server Manager (**Start** > **Administrative Tools** > **Server Manager**). In the hierarchy (on the left), expand **Roles**, then **Web Server (IIS)**, and select **Internet Information Services (IIS) Manager**.

   - On Windows 7, navigate to **Control Panel** > **System and Security** > **Administrative Tools**, and double-click **Internet Information Services (IIS) Manager**.

10. In the work pane that opens, expand **Sites**, and select **Default Web Site**.

11. In the **Home** pane for this site, in the **IIS** group, locate **WebDAV Authoring Rules**.

    Tip • If it is not present, it is likely that WebDAV is not installed on this server, and your mission is complete.

12. Right-click the icon, and select **Open Feature**. A pane opens for **WebDAV Authoring Rules**.

13. On the right, in the **Actions** group, there is an option to enable or disable WebDAV.

    - If the link currently says **Enable WebDAV**, do nothing, because your mission is complete.

    - If the link current says **Disable WebDAV**, click the link.

14. Click **OK** to close all applicable dialogs.

    If this is not the last server on your list, loop back and restart this process on the next server.

    Tip • There is additional configuration of IIS handled by PowerShell configuration scripts described later.

Configure Internet Explorer

Microsoft Internet Explorer needs configuration.

Compatibility mode must be turned off for FlexNet Manager Suite. In addition, when Internet Explorer is used on a server-based operating system to access FlexNet Manager Suite after setup is complete (for example, if you are testing from your central application server, or an inventory beacon has a server operating system), its enhanced security provisions must be turned off on that server, as follows. (Alternatively, use a different browser.)

1. Open Internet Explorer, and navigate to:

```
res://iesetup.dll/IESecHelp.htm#overview
```

2. Follow the instructions displayed there for disabling Enhanced Security Configuration.

3. FlexNet Manager Suite attempts to advise Internet Explorer that the website should not be run in compatibility mode. You need follow these steps only if you receive an alert asking you to turn off compatibility mode:

   a) In Internet Explorer, press the Alt key to display the Menu bar.

   b) Click **Tools**, then **Compatibility View Settings**.

   c) Make sure **Display all websites in Compatibility View** and **Display intranet sites in Compatibility View** are both clear.

   d) Add websites that do require compatibility mode to the list of **Websites you've added to Compatibility View**.

There are a number of other configuration requirements for whichever web browser you choose to use:

* URLs to add to your trusted locations

* Recognition of your central server as an Intranet site, and allowing automatic logon

* Javascript must be enabled

* Cookies must be enabled

* Windows authentication must be enabled

* Font download should be enabled for optimum usability of the site

* Any company proxy servers must allow browsers to access to the web application server.

Details for each of these are included in the first topic in the online help, *Configuring Your Web Browser*, available after the product is upgraded.

Upgrade PowerShell on Inventory Beacons

PowerShell is used both as part of the installation, and for operation of inventory beacons after installation.

The minimum requirement on inventory beacons is PowerShell 3.0.

You may choose to upgrade PowerShell to version 4.0, but be aware that this release has a prerequisite of .NET Framework 4.5. In summary, you may chose either of the following combinations:

* .NET 4.0, with the *three* patches required for inventory beacons installed (as in *Configure .NET and IIS* on page 16), and PowerShell 3.0

* .NET 4.5 (which requires no patches), and PowerShell 4.0.

Use this procedure to check the version installed on your candidate computer before installing an inventory beacon.

1. Within Windows PowerShell, run `$PSVersionTable.PSVersion`.

This produces output similar to the following:

```
Major       Minor       Build      Revision
-----       -----       -----      --------
3           0           -1         -1
```

2. If the `Major` value is less than 3, download your chosen version and install it.

   For example:

   - For PowerShell 3.0, see *http://www.microsoft.com/en-us/download/details.aspx?id=34595*; and after installation, continue with the patches below.

   - For PowerShell 4.0, see *https://www.microsoft.com/en-us/download/details.aspx?id=40855*. When this is installed, you have completed this procedure, as patches are not required for .NET 4.5.

3. If this inventory beacon is running .NET version 4, ensure that these three patches are installed (you may have completed this earlier, under *Configure .NET and IIS* on page 16):

   - Update 4.0.3 for Microsoft .NET Framework 4 Runtime Update (KB2600211), from *http://www.microsoft.com/en-us/download/details.aspx?id=29053*

   - Update for Microsoft .NET Framework 4 on Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows 2008 R2 - KB2836939, from *http://www.microsoft.com/en-us/download/details.aspx?id=39257*

   - Update for the .NET Framework 4, from http://support.microsoft.com/kb/2468871, and downloadable from *http://www.microsoft.com/en-us/download/details.aspx?id=3556*.

Configure Network Shares

If you have not already done so, use Windows Explorer to configure the network share drives used by all your central servers. There are two such shares in a fully-scaled up implementation:

- The data import directory for inventory collected through FlexNet inventory agent (default value: `C:\ProgramData\Flexera Software\FlexNet Manager Platform\DataImport\`). This share is required as soon as you install the web application server on a separate server; or as soon as you separate the batch server (reconciliation server) into a distinct batch scheduling server with one or more child batch servers. It may be on any of your central servers, as convenient in your implementation; and it may be on any drive and any file path.

- The staging folder for inventory beacon data upload and download (default value: `C:\ProgramData\Flexera Software\Beacon`). This second share is only required when you separate the batch server (reconciliation server) into a distinct batch scheduling server with one or more child batch servers. (On the other hand, if you have only a single batch server, the folder is on this server, and no sharing is required.) Once again, it may be on any drive and any file path; but a share (or folder) on the batch scheduling server is recommended, to optimize performance.

You may implement these shares as you see fit.

For added security, you may set up these shares so that they are available to the minimum number of accounts (rather than open to all). From *Identify (or Set Up) Accounts*, you are already acquainted with the Active Directory security group `FNMS Administrators`, which minimally contains the operational service account (suggested:

`svc-flexnet`), the installing administrator account (suggested: `fnms-admin`), and any accounts with interactive logins to any of your central servers. If you wish, you can restrict these network shares so that they are open only to members of `FNMS Administrators`, with the group providing full control for both daily operations and any required maintenance/troubleshooting.

During the installation process using the InstallShield Wizard, you identify these share drives, so keep a note now of the locations you have selected.

Drivers for Spreadsheet Imports

It is quite likely that at some stage you will need to import data from spreadsheets or CSV files. For example, you may have purchase records in spreadsheets, or inventory exported from a hard-to-reach system, or you may have a record of entitlements from a reseller in a spreadsheet format. Documentation is available for these different uses, including the chapter *Importing Inventory Spreadsheets and CSV files* in the *FlexNet Manager Suite System Reference* PDF file, available through the title page of online help after installation.

You need a driver update in the following conditions:

- You will *import* data from spreadsheets (the export of data to spreadsheets is not relevant, and the import of data from CSV [comma-separated values] file is also not relevant)

- The spreadsheets will be Excel spreadsheets in `.xlsx` format (the earlier `.xls` format does not require the driver update; but be aware that this older format limits each spreadsheet to about 65,000 records/rows)

- You are working on a batch server or the batch scheduling server (or processing server, or application server in a single server implementation); or you are working on an inventory beacon that will perform these spreadsheet imports.

In these conditions, you must install a 32-bit version of Microsoft Access Database Engine on the server. The particular release is not important: for example, Microsoft Access Database Engine 2010-32 is adequate. Drivers are supplied within the Microsoft Access Database Engine.

Important • *Only the 32-bit version is supported by the import mechanism, and this version is incompatible with the 64-bit version of Microsoft Office products installed on the same machine. This means that, when you need imports in `.xlsx` format, 64-bit Office cannot be installed on the central batch scheduling server (or processing/ application server), or on applicable inventory beacons. This limitation only prevents co-installation of the two code bases on the same computer. It does not affect which document types can be imported. For example, Office documents including spreadsheets prepared in 64-bit Office running on other machines can successfully be imported.*

Download the Materials

Collect the contents for your upgrade process.

Position yourself on a computer that is accessible from all the central servers you will implement, and preferably at least some of your inventory beacons.

1. Login to the Product and License Center at *https://flexerasoftware.flexnetoperations.com*.

   💡

   Tip • *Use the account details you have as part of your maintenance agreement.*

2. From the list of products, select <u>FlexNet Manager Platform</u>, and select the same again in the following page to differentiate elements of the Suite, if applicable.

3. Click through the link for <u>FlexNet Manager Suite 2015 R2 SP1</u> to access the downloads.

4. Depending on your login account, a click-through license may appear. If so, review the terms, and click **I Agree**.

5. Download the following archives and save to a convenient (network-accessible) location on this computer (such as `C:\temp\FNMSUpgrade\`). You may unzip all these archives here.

   • `FlexNet Manager Suite 2015 R2 SP1 Installer.zip`

   • `Database Migration to FNMS 2015 R2 SP1.zip`

6. If you are collecting inventory from Citrix XenApp, also download:

   • Tier 1 Adapter Tools.zip.

7. If your implementation design includes FlexNet Report Designer (powered by Cognos), also download:

   • Report Designer Package - Single Tenant (`FlexNetManagerPlatformReportsAndDashboard.zip`) - required even if you already have Report Designer implemented with FlexNet Manager for Engineering Applications.

8. If you will also install the Business Adapter Studio in connected mode (that is, with direct access to your operations databases), also download `Business Adapter Studio 2015 R2 SP1.zip` to the same location.

   💡

   Tip • *If you have a previously installed version of the Business Adapter Studio, it must be upgraded at this release by removing the old installation and replacing it with the new version.*

2

Upgrading FlexNet Manager Suite

Topics:

- *Remove Previous Language Packs*
- *Upgrade/Create Databases*
- *Authorize the Service Account*
- *Upgrade the Web Interface*
- *Update the Inventory Server*
- *Update the batch scheduling server*
- *Installing a Free-Standing Studio*
- *Configure the System*
- *Populate the Downloadable Libraries*
- *Update the Sample Reporting Package*
- *Link to Flexera Service Gateway*
- *Update Access Rights*
- *Update, and Deploy Additional Inventory Beacons*
- *Upgrade Connected-Mode Studios*
- *Configure Updates to Inventory Agents*
- *Activating and Using New Features*

You have completed all the prerequisites in *Prerequisites and Preparations* on page 9 (and its subsections). Only when all these tasks are complete should you move forward to the upgrade of FlexNet Manager Suite to 2015 R2 SP1.

Remove Previous Language Packs

For easier and safer maintenance, remove previous localization packs before upgrading.

FlexNet Manager Suite 2015 R2 SP1 installs all available language packs as a standard part of the installation process, so that they no longer require separate installation. There is a risk, if you attempt to remove old language packs after the upgrade is completed, that you will remove functionality you require in this release. For this reason, use this opportunity to remove previous language packs before undertaking the upgrade. (If you have not previously installed language packs, ignore this section.)

1. Open the Windows Control Panel (for example, Windows Start menu > **Control Panel**).
2. Click **Programs and Features**.
   The dialog displays the **Uninstall or change a program** page.
3. Select one of the available language packs.

   When you make a selection the **Uninstall** button appears above the list of programs.
4. Click **Uninstall**, and if necessary click **Yes** in the confirmation dialog that may appear.

   Wait while the removal process is completed.
5. If necessary, repeat the selection and uninstall process for the other language pack.
6. Close the Control Panel.

Upgrade/Create Databases

Any existing compliance databases must be upgraded, and if you are migrating from 2014, 2015 R2 SP1 uses an additional mandatory database.

You may wish to update your existing database(s) for the new release. However, you may wish to take this opportunity to scale up to multiple databases (potentially sharing the same server, of course) for inventory and compliance. Separate databases are shown in the architectural diagram in *Design the Final Topography* on page 5.

Take note of all the database names you create with the `-d` parameter in the following steps. You need the names later (if database setup is done by a separate DBA, the database names must be handed off to the installing administrator). While it is possible to rename the databases, using the default names makes it easier to follow the rest of the documented processes.

Important • All accounts that will log in directly to (any part of) the application server to use FlexNet Manager Suite (excluding access through the web interface) must have `db_owner` permissions on all components of the operations databases: compliance data, warehouse data, snapshot data, and inventory data. A suggested method is to create either a local or Active Directory security group (such as `FNMS Administrators`) and add all such accounts to this group. Then you can, for example, set these permissions by opening each database in Microsoft SQL Server Management Studio, and granting `db_owner` privileges to the security group. The procedures are detailed in the topics covering database creation. Accounts to list in the security group minimally include:

- *The operational service account (suggested: `svc-flexnet`)*

- *The installing administrator account (suggested: `fnms-admin`)*

- *Any operational account needing to log in to a central inventory beacon installed on your batch scheduling server (remember that, since the inventory beacon requires administrator privileges to run, this account is both a local administrator on the batch scheduling server and a `db_owner`)*

- *Any future back-up administrator accounts needed for the application server.*

1. Create a security group (suggested: `FNMS Administrators`), and (optionally) add to it all accounts directly logging into the central application server (or you can add accounts later).

2. In SQL Server Management Studio, ensure that the AD security group (suggested: `FNMS Administrators`) has a secure login:

   a) Under **Security** > **Logins**, Create a new login.
   The **Select User, Service Account or Group** dialog appears.
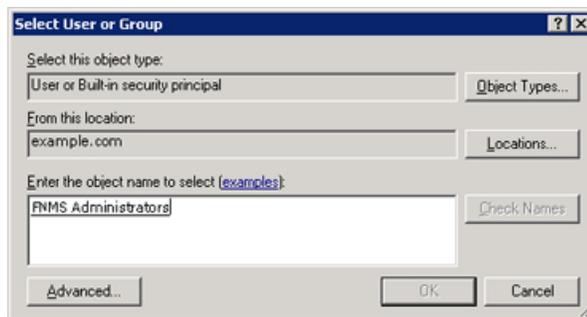
   b) Use the **Object Types...** button to ensure that `User, Group, or Built-in security principal` is selected as the object type.

   c) Use the **Locations...** button to select your Active Directory domain.

   d) As the object name, enter the name of your security group (suggested: `FNMS Administrators`), and use **Check Names** to validate that the group name is found.

   e) Click **OK**.
   The newly added group is visible under the `Security > Logins` node. (You will use this group after the creation of each database.)
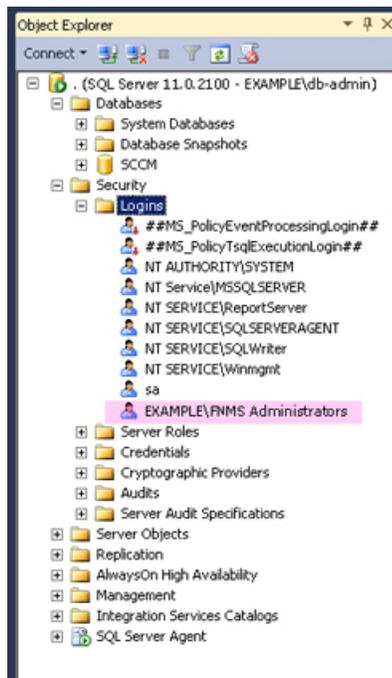
3. Back up your existing FlexNet Manager Suite database.

4. Back up any customized files to a temporary location, (for example, `C:\temp`).

   Customized files may include compliance importer procedures (XML files located by default in *installation_dir*`\Compliance\ImportProcedures` from 8.0 onwards, or for earlier releases, check in `sourceprocedures.xml`).

5. Ensure that the target database instance is set for case-insensitive and accent-sensitive collations (as required by all databases in this system, including the tempdb). To check the collation settings at the server level:

   a) In SQL Server Management Studio, locate the SQL Server instance in the **Object Explorer** pane.

   b) Right-click the server, and select **Properties** from the context menu.

   c) On the server **Properties** dialog, select the **General** tab, and check the current collation sequence.

   If the collation sequence ends with the codes `_CI_AS` (for example, `Latin1_General_CI_AS`), you may proceed with the installation. Otherwise you can set the collation sequence for each database, as you create it, by right-clicking the new database, selecting **Properties** from the context menu, and choosing the collation on the **Options** tab.

6. Use SQL Server Management Studio to ensure that the database **Recovery model** is set to `Simple` (first recording its current value before changing it if necessary).

   a) In SQL Server Management Studio, right-click the database, and select **Properties** from the context menu.

   b) Select the **Options** tab.

   c) Check that **Recovery model** is set to `Simple` (or note its current value, change it to `Simple`, and click **OK**).

Especially for large databases, this prevents the transaction log from growing to excessive proportions. Because of this growth, for databases of all sizes, the migration process will truncate the transaction log at the end of the process, and this truncation relies on the simple **Recovery model**. If the model is not currently `Simple`, note the existing value — there is a reminder below to restore this value after a successful database migration.

7. If you have not already done so, log on to the central application server with a privileged account (suggestion: `db-admin`) that has the privileges described in *Identify (or Set Up) Accounts* on page 10.

8. If you cannot access your downloaded and unzipped archives from your current login on this application server, copy `Database Migration to FNMS 2014 R3.zip` to this server and unzip it to a convenient location, such as `C:\temp\FNMSUpgrade`.

9. In the Command Prompt window, navigate to your working copy of the migration folder (such as `C:\Temp \FNMSUpdate\Database Migration\FlexNet Manager Platform\Normal`).

Tip • *If your console window is in **QuickEdit** mode (visible in the **Properties** for the window), simply clicking in the window when it already has focus puts it into Mark or Select mode. In such a mode, a process that is writing to the window is paused, awaiting your input. Beware of unintentionally pausing database migration by extra clicking in this command prompt. A process that has been paused in this way is resumed when the window already has focus and you press any key.*

10.

Remember • *For a single database, use the same* `-d FNMSCompliance` *parameter as for the compliance database; or for a separate inventory database (recommended), use a different name such as* `FNMSInventory` *(shown here).*

Update the database for FlexNet native inventory collection by running the `mgsDatabaseUpdate.exe` program, using the following syntax:

Important • *Be very careful with copy and paste. Some tools "helpfully" convert a pasted minus (dash, or hyphen) character to something else, perhaps from an extended character set. Such substitutions will cause the command line to fail.*

```
mgsDatabaseUpdate.exe -i InventoryManagerMigration.xml -nsu -d FNMSInventory
                      [-l logFile]
                      [-s serverName\instanceName]
                      [-u userName]
                      [-p password]
```

where:

-d <databaseName>	The name of the database to connect to. A suggested name is FNMSInventory.

	Note • If you are currently operating from a new application server that has not previously connected to the database server, this parameter is mandatory. If you are upgrading an existing application server that has separately run your compliance product (not in co-location with Inventory Manager), the registry entry listed below for the `-s` option is normally set. In this case, if you omit the `-d` option, the database name is taken from the registry key.
`-i InventoryManagerMigration.xml`	This is the configuration file describing the migration tasks, and is of course mandatory.
`-l <logFile>`	Identifies the path and name of the file to receive a log of the migration tasks that occurred. If this option is not specified, a log file called `InventoryMigration.log` is created in the same folder where the executable is running.
`-nsu`	Run the database update without putting the database into single user mode. (The steps to perform migration require that multiple connections are made.)
`-p <password>`	The password for the username specified with `-u`. This is only required if the database server is configured to use SQL Server authentication.
`-s <serverName>` or `-s <serverName>\<instanceName>`	The name of the database server to connect to. If `-s` is not specified, the value at `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node \ManageSoft Corp\ManageSoft \Reporter\CurrentVersion \DatabaseConnectionString` is used. The registry key is present on the compliance and inventory servers. (If you have chosen to run this script on the database server itself, the registry entry is not available, and you must therefore specify the server name, or use the dot notation [.] to refer to the current server.) If the database is in a named instance (and not in the default database on the server), the instance name must be specified as well.
`-u <userName>`	The username with which to connect to the database. This is only required if the database server is configured to use SQL Server authentication. If not specified, Windows Integrated Authentication is used to connect to the database server using the current user's credentials.

Example: The following command performs the migration using the standard configuration file. Instead of recording the log in the default log file, it will be written to the `mig.log` file specified in the command. Because the upgrade is running on a new server, the database server name (and, if required, instance name) and database name must be specified, and Windows Authentication is used to log in as the account name running the executable.

```
mgsDatabaseUpdate.exe -i InventoryManagerMigration.xml -nsu -l mig.log -s MyDBServer
\thisInstance -d FNMSInventory
```

Check messages on the command line to confirm that the database migration was successful. If any error messages occur, check the log file to troubleshoot the problem. Do not proceed to the next step until the database migration is successful. For more information about database validation and remedies, see *Database Validation* on page 31.

💡

Tip •   If, after migration is complete, the database size still seems much larger than before, ask your database administrator to check whether there is a significant amount of unused space in the database files (using Microsoft SQL Server Management Studio). If so, a database `shrink` operation can reclaim this unused space.

11. On this database, grant `db_owner` privileges to the security group (suggested: `FNMS Administrators`):

   a) Open this database in Microsoft SQL Server Management Studio, expose the `Security > Users` node, right-click and choose to create a new user.

   b) In the **Database User - New** dialog, set the **User type** to `SQL user with login`, and enter a **User name** (for example, call it `FNMS Administrators` as well).

   c) Next to the **Login name** field, click the ellipsis (**...**) button, and use the **Select Login** dialog to select your Active Directory security group (suggested: `FNMS Administrators`). Click **OK** to close both dialogs.
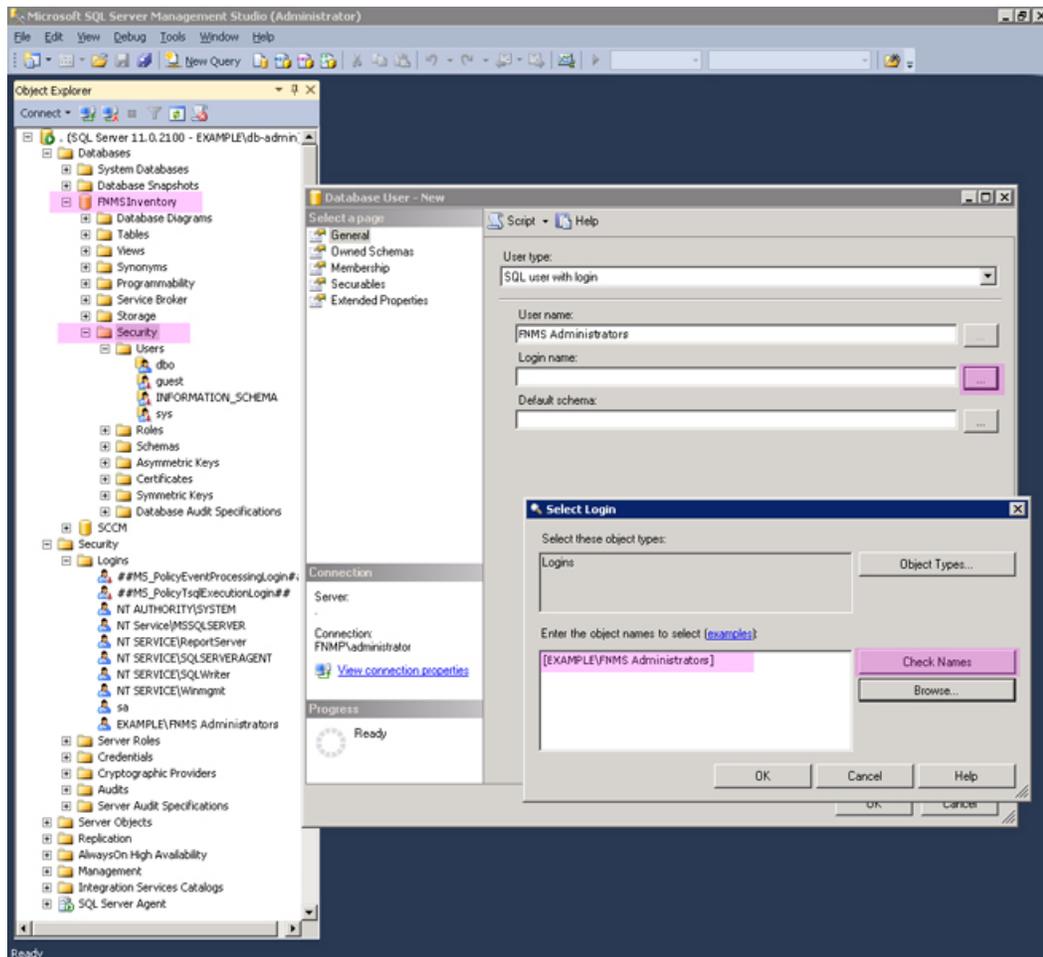
d) For your newly-added user, right-click and select the properties, and select the `Membership` page. Check the `db_owner` role, and click **OK** .

12. Similarly, update the compliance database.

a) Still in the command window on the database server, using the administrative account (`db-admin`), and in the same folder of the unzipped archive, execute:

```
mgsDatabaseUpdate.exe -i ComplianceMigration.xml -nsu -d FNMSCompliance
                      [-l logFile]
                      [-s serverName\instanceName]
                      [-u userName]
                      [-p password]
```

b) Open this database in Microsoft SQL Server Management Studio, and grant `db_owner` privileges to the security group (suggested: `FNMS Administrators`).

For more information about database validation and remedies, see *Database Validation* on page 31.

13. If you previously changed the setting for the database **Recovery model**, restore the original value now.

14. Optionally, re-index the database. Consider the following factors:

- Re-indexing increases data access speed and recovers wasted disk space.

- On large databases, **this process can take more than 24 hours**. You can proceed with the rest of your upgrade and perform this step at a later, convenient time if required.

Tip • It is a good idea to re-index your database at least once a year. In SQL Server, tables that do not have clustered indexes do not automatically reclaim space from deleted records. Re-indexing will reclaim this space.

If you decide to re-index at this time:

a) Start SQL Server Management Studio.

b) Open `ReIndexAll.sql` (**File** > **Open...** and browse in the unzipped archive to your migration folder, such as `C:\temp\FNMSUpate\Database Migration\FlexNet Manager Platform\Normal`, and select the file).

c) Click the **Execute Query** tool, or press `F5` to run the script.

15. Migrate your data warehouse database, running the `mgsDatabaseUpdate.exe` program again with different parameters:

```
mgsDatabaseUpdate.exe -i DataWarehouseMigration.xml -nsu -d FNMPDataWarehouse
                      [-l logFile]
                      [-s serverName\instanceName]
                      [-u userName]
                      [-p password]
```

Important • In this instance, the database name (`-d` parameter) is mandatory. (The suggested value is shown, which you should customize if your database name is different.)

Check messages on the command line to confirm that the warehouse migration was successful. If any error messages occur, check the log file to troubleshoot the problem. Do not proceed to the next step until the migration is successful. For more information about database validation and remedies, see *Database Validation* on page 31.

Note • The snapshot database does not require migration.

Database Validation

Database migration includes a number of checks on the quality of the resulting database.

The first of these is a check of database constraints that may have been either enabled or disabled without data checks. if constraint errors are detected, the migration process corrects them. Where a constraint is enabled, the process also attempts to ensure that the data it covers is appropriate for the constraint. Generally, this succeeds

without issue, and the change is simply noted in the migration log. However, if it fails, the migration process also fails with an error similar to:

```
ERROR: One or more constraints cannot be enabled (step number 99).
```

If this occurs, the names of the constraints that cannot be enabled are listed in the migration log. Restarting the migration at this time does not help this issue, and the database is unusable for production work. First, a database administrator or a Flexera Software support engineer must manually correct the issue with the underlying data. Once the data has been corrected, the migration process will be able to be restarted safely.

At the end of the migration process, there is a final schema check of the upgraded database to ensure that the upgrade has been successful. Messages from this database check may appear in your console towards the end of the process, after the migration itself is completed.

This check is included for the three main system databases: the compliance database, the inventory database, and the data warehouse database.

When these checks are run, the upgrade has already been completed without errors, and the database is likely to be usable. These are additional checks to look for irregularities in the database that may cause future operational problems. These kinds of irregularities may occur because:

- The earlier database had previously been changed (either by database administrators or by a Flexera Software consultant) in ways that are not supported by the product

- A previous migration updated the database in ways that were not entirely correct, but not previously detected

- Something has occurred in the present migration that did not raise an error in the migration, but leaves the database in a less than perfect condition.

Such causes can produce a range of possible issues, including:

- Missing tables, indexes, columns, or foreign keys

- Extra indexes, columns or foreign keys

- Incorrectly configured columns (the size differs, or their nullability)

- An index configured in unexpected ways, either in its uniqueness, its clustering status, or in the columns it covers.

For the above cases, assistance from a database administrator or Flexera Software support engineer is also required to correct the schema. In many cases, the issues described in the log can be remedied in place, without requiring that the database migration process is restarted.

Authorize the Service Account

The account used to run processing services requires permission to run as a service. Prior to installing anything, perform this process on:

- Your batch scheduling server/reconciliation server (in a large-scale implementation with three or more servers)

- Your processing server (in a two server application implementation)

- Your application server (in a single server implementation)

- Any independent batch servers.

> *Tip • You should use a single account (that is, the same Active Directory user) for communications between the batch scheduling server and any child batch servers. If you do not do this, you instead need to modify permissions on the Microsoft Message Queuing configuration on the batch scheduling server (which modifications are beyond the scope of this document). Assuming use of a single account, it is most convenient if this is the same service account used on all your central server(s).*

1. On the appropriate server, log in as an administrator (suggested: `fnms-admin`).
2. Go to:

   - On Windows Server 2012, **Start** > **Administrative Tools** > **Local Security Policy**

   - On earlier releases of Windows Server, **Start** > **All Programs** > **Administrative Tools** > **Local Security Policy**.

3. Select the **Local Policies** node, and choose **User Rights Assignment**.
4. Open the policy `Log on as a service`, and add the service account (example: `svc-flexnet`).
5. Open the policy `Log on as a batch job`, and add the service account (example: `svc-flexnet`).
6. Click **OK**.

> *Tip • A Microsoft error dialog* `Security Templates - An extended error has occurred. Failed to save Local Policy Database`*. may appear. This error is described at* http://support.microsoft.com/kb/2411938*, and may safely be ignored.*

Upgrade the Web Interface

Continue this process as administrator (`fnms-admin`) on either your

- application server (for a single server installation) or

- web application server (in a multi-server installation).

> *Note • Are you installing on the same server that was previously your application server for FlexNet Manager Suite 2014 (the 10.0 release) (an in-place upgrade)? If so, you should now uninstall the previous version of the product so that you remove the MMC interface, deprecated from version 2014 R2. To do so:*
>
> *1. On the application server, open **Program and Features** (**Control Panel** > **Uninstall a Program**).*
>
> *2. Uninstall FlexNet Manager Platform (or your earlier compliance product, such as Compliance Manager), and then close **Program and Features**.*

To update the web interface for FlexNet Manager Suite 2015 R2 SP1:

1. On the (web) application server, open Windows Explorer.

2. Copy the downloaded archive `FlexNet Manager Suite 2015 R2 SP1 Installer.zip` from your staging location to a convenient location on this server (such as `C:\temp`), and unzip it.

> *Tip •* *Unzipping the archive locally on each of your servers simplifies running the configuration scripts later in the process. After running the installers, PowerShell scripts need to be* `Run as Administrator`*. Notice that the entire archive must be present, as scripts reference other elements from the archive.*

3. Navigate in the unzipped archive to the `FlexNet Manager Suite\Installers\FlexNet Manager Suite` folder.

4. Start (double-click) `setup.exe`.

> *Tip •* *You must start the installation by running* `setup.exe`*, rather than running the MSI by any other means. The setup file also installs Visual C++ 2010 Redistributable (if it is not already present), which is a prerequisite for integration with FlexNet Manager for SAP Applications.*

5. Step through the installer until asked for the **Setup Type**, and do one of the following:

    • For a small, single server installation combining the web application, the inventory collection, and the batch processing functionality in one server, select the **Complete** option, and follow the instructions in the installation wizard to complete the standard installation.

    • For a multi-server installation, select the **Custom** installation path, and select the **Web application server** for this installation. (If this is the *only* functionality on this server, also ensure that **Inventory server**, **Batch scheduling server**, and **Batch server** are all deselected; but in fact you can combine most servers in the way that best suits your enterprise, so make the selection that matches your server plan, keeping in mind that the batch scheduling server and batch server are never installed together.)

    Take note of the installation location for future reference.

6. If this server includes the batch scheduling server functionality, you are prompted for the credentials used for batch processes. Be sure that the account you enter already has `Logon as a service` permission (see *Authorize the Service Account* on page 32).

7. When successful, close the installation wizard.

Update the Inventory Server

The inventory server processes all inventory collected (or augmented) by the FlexNet inventory agent.

In a single server implementation, this step is already completed and you should skip ahead to *Configure the System*.

For a multi-server implementation, continue this process as administrator (`fnms-admin`) on either your

• processing server (in a two server application installation)

• inventory server (in a three or more server application installation).

1. On the inventory (or processing) server, open Windows Explorer.

2. Copy the downloaded archive `FlexNet Manager Suite 2015 R2 SP1 Installer.zip` from your staging location to a convenient location on this server (such as `C:\temp`), and unzip it.

3. Navigate in the unzipped archive to the `FlexNet Manager Suite\Installers\FlexNet Manager Suite` folder.

4. Start (double-click) `setup.exe`.

   💡

   Tip • You must start the installation by running `setup.exe`, rather than running the MSI by any other means. The setup file also installs Visual C++ 2010 Redistributable (if it is not already present), which is a prerequisite for integration with FlexNet Manager for SAP Applications.

5. Select the **Custom** installation path, and do one of the following:

   • For a two server installation, now installing your processing server, select all of the **Inventory server** and the **Batch scheduling server** for this installation, and ensure that the **Web application server** is deselected (displaying a cross).

   • For an installation using three or more servers, now separately installing your inventory server, select only the **Inventory server** for this installation, ensuring that the other options are deselected.

   Take note of the installation location for future reference.

6. If this server includes the batch scheduling server functionality, you are prompted for the credentials used for batch processes. Be sure that the account you enter already has `Logon as a service` permission (see *Authorize the Service Account* on page 32).

7. When successful, close the installation wizard.

Update the batch scheduling server

💡

Tip • Massive implementations may spread the batch processing load across multiple batch servers, whose processing is controlled by the batch scheduling server (which itself also includes the batch server functionality and contributes to the batch processing effort). Installation of any batch server is identical; and for the batch scheduling server, the only difference is the choice selected in the custom installation as described below. You may follow this process for either the batch scheduling server or for any batch server.

The batch scheduling server is the integration point that correlates all your entitlement records and your consumption revealed in inventory to work out your reconciled license position.

You do *not* need this process if you have either of:

• A single-server implementation combining the web application server, the batch scheduling server, and the inventory server in one; or

• A two-server application implementation where you have combined the batch server and inventory server functionality on one computer and kept the web application server as a second server.

In these two cases, this step is already completed and you should skip ahead to *Installing a Free-Standing Studio* on page 36.

For a three server implementation (or larger), continue this process as administrator (`fnms-admin`) on your batch scheduling server.

1. On the batch scheduling server (or, where applicable, a separate child batch server), open Windows Explorer.

2. Copy the downloaded archive `FlexNet Manager Suite 2015 R2 SP1 Installer.zip` from your staging location to a convenient location on this server (such as `C:\temp`), and unzip it.

3. Navigate in the unzipped archive to the `FlexNet Manager Suite\Installers\FlexNet Manager Suite` folder.

4. Start (double-click) `setup.exe`.

   💡

   Tip • You must start the installation by running `setup.exe`, rather than running the MSI by any other means. The setup file also installs Visual C++ 2010 Redistributable (if it is not already present), which is a prerequisite for integration with FlexNet Manager for SAP Applications.

5. Select the **Custom** installation path, and make one of the following choices:

For a single batch scheduling server that performs all your batch calculations and does not manage any further 'child' batch servers	Select only the **Batch scheduling server** for this installation (ensuring that the other options are deselected). 💡 *Tip • Do not also select the **Batch server** option. Remember that the installed batch scheduling server also includes the batch server functionality.*
For a batch scheduling server that performs some batch calculations, and also manages further batch processing on 'child' batch servers	As above, select only the **Batch scheduling server** for this installation (ensuring that the other options are deselected).
For a child batch server	Select only the **Batch server** (ensuring that the other options are deselected).

   Take note of the installation location for future reference.

6. When asked to enter the credentials to be used for running batch processes, be sure that the account you enter already has `Logon as a service` permission (see *Authorize the Service Account* on page 32).

7. When successful, close the installation wizard.

Installing a Free-Standing Studio

You can install additional copies of the Business Adapter Studio.

There are two kinds of Studio. Adapters can be created or modified using either the Inventory Adapter Studio or Business Adapter Studio (each for its appropriate type of adapter). Each time that you install an inventory beacon, copies of each of the Business Adapter Studio and the Inventory Adapter Studio are installed ready for use on the inventory beacon. These versions are configured exclusively for disconnected mode, where they cannot directly access your central database.

However, sometimes you want to work in connected mode, with direct access to your central database (for example, to write data into stages tables and manipulate it). For these cases:

- The Inventory Adapter Studio is also available on the web application server (or, in smaller implementations, the server providing that function). This works in connected mode.

- You can co-install an inventory beacon on your web application server. As always, this also installs the Business Adapter Studio, giving it (and adapters built there) additional privileges to access your central database in connected mode.

In addition, it is also possible to install a free-standing copy of the Business Adapter Studio (only) on your central application server. (If you have scaled up to several central servers, such as installation can be on whichever server suits you. The default location is indicated below.) Business adapters installed directly on your central server(s) operate in connected mode, with full access to your central database. Obviously, attempt this only if you are very confident and well informed about details of the database schema.

Tip • *It is not possible to install addition free-standing copies of the Inventory Adapter Studio.*

Start this procedure using a web browser on the server where you will install the Business Adapter Studio, or a computer that provides easy and fast network access from your central server.

1. Using the credentials supplied by Flexera Software with your order confirmation (or as renewed since), log into the Product and License Center at *https://flexerasoftware.flexnetoperations.com*.

2. On the first page, select `FlexNet Manager Platform`, and on the resulting second page, select the product again.

3. In the list of versions, click the product name for the version you are using (typically the most recent version).

4. In the list of components to download, select `Business Adapter Studio` *releaseNumber*`.zip`, and download and save it to a convenient location (such as `C:\Temp`).

5. In Windows Explorer, navigate to the downloaded archive, right-click, and choose **Extract All**.

6. Navigate into the unzipped archive, and double-click `setup.exe`, following the instructions in the installation wizard.

The Business Adapter Studio may be installed on any of your central servers (in a multi-server implementation). The installer assesses the installation paths, and installs itself in the installation folder of FlexNet Manager Suite. The defaults are as follows:

- The Business Adapter Studio executable: `BusinessImporterUI.exe`

- Default installation path (in connected mode on central server): `C:\Program Files (x86)\Flexera Software\FNMP Business Adapter Studio`

- No template file storage is required for the Business Adapter Studio in connected mode, as it validates the database schema directly. Your custom business adapters may be saved in the folder(s) of your choice.

When you have completed the remainder of your product installation, the Business Adapter Studio can be run from the Windows start menu on this server; and the Business Importer, which is also installed automatically with the Business Adapter Studio, is also available for execution on the command line. For details about the Business Adapter Studio, see online help or the *FlexNet Manager Suite System Reference* PDF file; and for details about the Business Importer, see the *Using the FlexNet Business Importer* PDF file. Both PDF files are available through the title page of the online help.

Configure the System

PowerShell scripts are provided to complete configuration of the central application server(s), including the connections to the databases, and then store appropriate values in the database.

Important • *For a single server implementation, run the PowerShell scripts on the application server (if you have a separate database server, you do not run the PowerShell scripts on that.) If the logical application server has been separated into multiple servers, the PowerShell scripts must be run on each of these servers, and must be run in the following order:*

1. *Your web application server*

2. *Your batch scheduling server (or processing server, for a two-server application implementation)*

3. *Any separate batch servers*

4. *Your inventory server(s).*

On each applicable server in turn, as administrator (`fnms-admin`), complete all the following steps (noticing that on different servers, different dialogs may be presented). Before executing the PowerShell scripts themselves, you should first ensure that these scripts have sufficient authorization to execute, as described in this process.

Also notice that, to complete this configuration process, you restore IIS, the scheduled tasks, and the batch processing service to prepare your system for operations.

1. On your web application server, batch server, or inventory server, ensure that Microsoft IIS is running again:

    a) Ensure that your **Server Manager** dialog is still open.

    b) In the left-hand navigation bar, expand **Roles** > **Web Servers (IIS)**, and select **Internet Information Services**.
       The IIS page is displayed.

    c) In the **Actions** panel on the right, select **Start**.
       A message like `Attempting to start...` appears. Note that it can take some time before the service is started. When the service is running, the PowerShell scripts can update the IIS configuration as required.

2. If you require that the URLs for your central server(s) use the HTTPS protocol, confirm that site bindings have been configured to allow this:

    a) Open IIS Manager.

      b) In the **Connections** pane, expand the **Sites** node in the tree, and then click to select the site for which you want to add a binding.

      c) In the **Actions** pane, click **Bindings**.

      d) In the **Site Bindings** dialog box, click **Add**.

      e) In the **Add Site Binding** dialog box, add the binding information and then click **OK**.

         For more information, see *https://technet.microsoft.com/en-us/library/cc731692%28v=ws.10%29.aspx*.

3. Run PowerShell as administrator (use the 64-bit version where available):

      a) Locate PowerShell. For example:

          • On Windows Server 2012, **Start** > **Windows PowerShell**

          • On earlier releases, in the Windows Start menu, find **All Programs** > **Accessories** > **Windows PowerShell** > **Windows PowerShell** (this is the 64-bit version; the 32-bit version is `Windows PowerShell (x86).`).

      b) Right-click, and choose **Run as Administrator**.

Important • It is critical that you run the PowerShell scripts with administrator privileges. Otherwise, scripts will fail.

4. In the PowerShell command window, execute:

```
set-executionpolicy AllSigned
```

Respond to the warning text with the default `Y`.

5. In the PowerShell command window, navigate through the unzipped downloaded archive to the **Support** folder.

6. On each server, execute:

```
.\Config.ps1 "Config\FNMS Windows Authentication Config.xml" updateconfig
```

(This script determines the type of server installation, and applies appropriate configuration. See also server-specific comments below.)

*Tip • If your PowerShell window is in its default **QuickEdit** mode (visible in the **Properties** for the window), simply clicking in the window when it already has focus puts it into Mark or Select mode. In such a mode, a process that is writing to the window is paused, awaiting your input. Beware of unintentionally pausing the configuration scripts by extra clicking in this PowerShell window. A process that has been paused in this way is resumed when the window already has focus and you press any key.*

On each server, on first run PowerShell asks whether to trust the publisher of this script. You may allow **Run always** for a certificate signed by Flexera Software LLC.

7. In each case, allow the script to run once, completing the requested details.

Tip • Helpful notes:

- *Use the service account details you created earlier (example: `svc-flexnet`).*

- *Separately on each dialog, the check box **Use the same credentials for all identities** copies the account details from the upper section to the lower section of the dialog.*

- *For externally visible URLs, you can specify either HTTP or HTTPS protocol, and either the flat server name or the fully qualified domain name is supported. Any port number is optional. Remember that site bindings may be required if you are using the HTTPS protocol (see above). Valid examples:*

  ```
  http://servername
  https://www.servername.mydomain:8080
  ```

- *The PowerShell script asks for appropriate database connection details, depending on the configuration of the current server (for example, if the current server includes inventory server functionality, the script asks for the Inventory Management database). In each case, supply the host server name (and, if the database instance is not the default instance, the instance name, separated by a backslash character); and the database name for each kind of database. In a small-to-medium implementation, all the operations databases may be on the same host and instance combination; but in larger implementations may be separated onto distinct servers. In either case, each database has a distinct database name, for which the suggested values are:*

  - *The main compliance database: `FNMSCompliance`*

  - *The database for inventory collected by the FlexNet inventory agent: `FNMSInventory`*

  - *The data warehouse for trend reporting: `FNMSDataWarehouse`*

  - *The snapshot database for performance improvement: `FNMSSnapshot`.*

8. Close the PowerShell command window.

9. If this is your batch scheduling server (or the server hosting that functionality), ensure that the services for FlexNet Manager Suite Batch Process Scheduler are running:

    a) Navigate to Start > **Control Panel** > **Administrative Tools** > **View local services**.
        The **Services** dialog opens.

    b) In the list of services, ensure that both `FlexNet Manager Suite Batch Process Scheduler` and `FlexNet Manager Suite Batch Processor` are both running. If not, right-click each stopped service in turn, and from the context menu, select **Start**.

        Note • These services are critical to the operation of FlexNet Manager Suite. It is best practice to set up your service monitoring to alert you any time either of these services is stopped.

10. On your batch server or inventory server, enable all Windows scheduled tasks related to FlexNet Manager Suite.

The scheduled tasks are different on the two different types of servers. On your batch scheduling server (also known as reconciliation server), change all tasks in the `FlexNet Manager Platform` folder:

* Data warehouse export

* Export to ServiceNow

* FlexNet inventory data maintenance

* Import SAP inventories

* Import SAP package license

* Inventory import and license reconcile

* Recognition data import

* Regenerate Business Import config

* Send contract notifications.

On your inventory server, change all tasks in the `FlexNet Manager Platform` folder:

* Import Active Directory

* Import application usage logs

* Import discovery information

* Import installation logs

* Import inventories

* Import Inventory Beacon activity status

* Import Inventory Beacon status

* Import remote task status information

* Import security event information

* Import system status information

* Import VDI access data.

An example process to change these tasks on Windows Server 2008:

a) Open your **Computer Management** dialog (for example, clickStart, right-click on **Computer**, and select **Manage** from the context menu).

a) In the left-hand navigation bar, expand **Configuration** > **Task Scheduler** > **Task Manager Platform**, and select the `FlexNet Manager Platform` folder.

b) Select all of the relevant tasks in the list (click the first, shift+click the last), and in the **Actions** pane, in the **Select Item** section, click **Enable** (or right-click the selection, and click **Enable**).

c) Close the dialog.

Configuration by the PowerShell scripts is now complete. Although not needed now, at other times it is possible to re-run the PowerShell scripts with the following flags for the use cases shown. You do not need to re-run the scripts unless, at some later stage, one of these use cases applies to you:

- Use without a flag to add a configuration file to a new installation; or on an existing implementation, to remove all customizations and replace the `web.config` file with the default version:

  ```
  .\Config.ps1 "Config\FNMS Windows Authentication Config.xml"
  ```

- Add the `updateConfig` flag to insert any new parameters added by Flexera Software, leaving all settings (including customizations) unchanged for existing parameters:

  ```
  .\Config.ps1 "Config\FNMS Window Authentication Config.xml" updateConfig
  ```

- Add the `forceUpdateConfig` flag to insert any new parameters added by Flexera Software, and restore the default values for all factory-supplied settings, but leaving any custom parameters unchanged:

  ```
  .\Config.ps1 "Config\FNMS Windows Authentication Config.xml" forceUpdateConfig
  ```

- Add the `removeConfig` flag to remove the `web.config` file before using Windows Programs and Features to uninstall FlexNet Manager Suite:

  ```
  .\Config.ps1 "Config\FNMS Windows Authentication Config.xml" removeConfig
  ```

Populate the Downloadable Libraries

FlexNet Manager Suite comes 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). These are updated regularly by Flexera Software and normally downloaded automatically.

Note • The automated updates, and the following process, both assume that your server has access to the Internet. Alternatively, if your server has Internet access controlled through a proxy server, the following URLs must be accessible:

- *For the ARL: http://www.managesoft.com/support/Compliance/RecognitionAfter82.cab*

- *For the SKU library: http://www.managesoft.com/support/Compliance/PURL.cab*

- *For the PURLs: https://update.managesoft.com:443/ProductUseRights, including access to any sub-directories of this that may be returned to your server in response to its initial request.*

If neither direct access nor access through a proxy server can be provided, you can use an alternative process to managed library updates manually (see Manual Updates of Library Data on page 43).

At installation time, you need to trigger download of the libraries to create a baseline ready for product use.

Tip • *New functionality in the 2015 release, including the recognition of some Microsoft Server applications, relies on the latest updates of the downloadable libraries.*

Complete this procedure as administrator (`fnms-admin`), having database rights as described in earlier sections.

1. On the batch scheduling server (or application server for a single-server implementation), open the Microsoft Task Scheduler.

Tip • *Library downloads check the terms of your Flexera Software license. That is why this task cannot be attempted before Product Activation, and must occur on the same server where your license was imported to activate the product.*

2. Manually run the **Recognition data import** scheduled task.

   By default this task is run at 1am daily. The task places a request for download in the queue of the internal batch scheduler. Given that no other processes are running at this stage of your implementation, it executes almost immediately. A utility downloads all libraries according to the terms of your license, and imports them into FlexNet Manager Suite. Typically for a first download, this may take in the order of a half an hour.

3. Thereafter, in the web interface for FlexNet Manager Suite, navigate to the system menu (⚙ ▼ in the top right corner), select **System Health** >**System Health Dashboard**, and check the cards for:

   • **ARL**

   • **SKU Library**

   • **PURL**.

Tip • *The cards do not refresh automatically. Use* `F5` *to refresh the display from time to time.*

Each card shows the currently installed version of the relevant library, and the date of the last successful download and import of these libraries. Errors display an additional alert icon with some explanatory text. In case of errors, check the following log files, located in `%APPDATA%\Local\Temp` for the service account running the batch processor (suggested: svc-flexnet):

• `ImportPURL-*.log`

• `PURL-*-log.txt`

• `Recognition*.log` (for the Application Recognition Library).

Manual Updates of Library Data

The downloadable Application Recognition Library, Product Use Rights Library, and SKU Library are intended for automated updates delivered directly to your application server (or, in a multi-server implementation, the server hosting the batch scheduling server functionality). This automated process naturally relies on the server having direct Internet access.

However, in some secure environments, the applicable server may not be permitted to have Internet access. For such environments, the process of updating these critical libraries must be maintained manually. The manual process is outlined below; but first there are the following preparations.

- Subscribe to the *Mgs-CM-Announce Mailing List* (`http://maillist.managesoft.com/mailman/listinfo/mgs-cm-announce_maillist.managesoft.com`). This is the FlexNet Manager Suite library release advisory mailing list, whose members receive email notifications when updates to library data are published.

- Contact *Flexera Software Support* (`https://flexeracommunity.force.com/customer/apex/SupportSFCaseInsert?rt=sf`) and ask for your Product Use Rights Library content to be published at a private location for you to download when updates are published. You also need to supply an email address, so that you can be notified of any changes to this service.

Tip • Your Product Use Rights Library content is customized according to the options you have licensed.

- On your applicable server, navigate to the Microsoft Task scheduler and disable the **Recognition data import** task (in the **FlexNet Manager Platform** group).

  This prevents the server from attempting to connect to the Internet to start downloads.

When these preparations are completed, you can use the following process to manually update each of the downloadable libraries as new editions are released.

1. When the Application Recognition Library content is updated:

   a) On a computer with Internet access, download the file `http://www.managesoft.com/support/Compliance/RecognitionAfter82.cab`.

   b) Log in to your application server (or the server hosting the batch scheduling server functionality) as a user in the `FNMS Administrators` security group.

      This is the security group recommended during installation. A suggested account to use is fnms-admin.

   c) Copy the downloaded `cab` file to a convenient directory (for example, `C:\Temp`) on this server.

   d) Install the Application Recognition Library content using this command:

      ```
      InstallDir\DotNet\bin\MgsImportRecognition.exe -ia C:\Temp\RecognitionAfter82.cab
      ```

      (replacing *InstallDir* with the installation folder for FlexNet Manager Suite on this server, which by default is `C:\Program File (x86)\Flexera Software\FlexNet Manager Platform`.)

      Important • The update to the Application Recognition Library asserts locks on various database tables, and other transactions that are queued may time out. You should therefore execute this command only in off-peak times.

      ---

2. When SKU Library content is updated:

   a) On a computer with Internet access, download the file `http://www.managesoft.com/support/Compliance/PURL.cab`.

b) Log in to your application server (or the server hosting the batch scheduling server functionality) as a user in the `FNMS Administrators` security group, such as fnms-admin.

c) Copy the downloaded `cab` file to a convenient directory (for example, `C:\Temp`) on this server.

d) Install the SKU Library content using this command:

```
InstallDir\DotNet\bin\MgsImportRecognition.exe -is C:\Temp\PURL.cab
```

(replacing *InstallDir* with the installation folder for FlexNet Manager Suite on this server, which by default is `C:\Program File (x86)\Flexera Software\Flexera Manager Platform`.)

Important • The update to the SKU Library asserts locks on some database tables, and other transactions that are queued may time out. Although this has less impact than updates to the Application Recognition Library, best practice is to execute this command only in off-peak times.

3. When Product Use Rights Library content is updated, multiple files may be added to the location supplied for you by Flexera Software Support. These include `PURL.cab` (for basic functionality), and others with the naming convention `PURL-vendor.cab` for different vendor options you may have purchased. Process these one at a time:

a) On a computer with Internet access, download the files available to you.

b) Log in to your application server (or the server hosting the batch scheduling server functionality) as a user in the `FNMS Administrators` security group, such as fnms-admin.

c) Copy the downloaded `cab` files to a convenient directory (for example, `C:\Temp`) on this server.

d) Install each Product Use Rights Library in turn using commands like the following:

```
InstallDir\DotNet\bin\MgsImportRecognition.exe -is C:\Temp\PURL.cab
InstallDir\DotNet\bin\MgsImportRecognition.exe -is C:\Temp\PURL-vendor.cab ...
```

(replacing *vendor* with the appropriate name(s), and replacing *InstallDir* with the installation folder for FlexNet Manager Suite on this server, which by default is `C:\Program File (x86)\Flexera Software\Flexera Manager Platform`.)

Tip • You must install `PURL.cab` as the first PURL library installation, before any vendor-related PURLs. If the SKU library has been released simultaneously, you should have already imported `PURL.cab` in the previous step (it completes the SKU library import as well); and if this is the case, you do not need to repeat it now.

Important • The update to the Product Use Rights Library asserts brief locks on some database tables, and other transactions that are queued may time out. Although this has less impact than updates to the Application Recognition Library, best practice is to execute this command only in off-peak times.

Update the Sample Reporting Package

This section is only for those using FlexNet Report Designer (powered by Cognos). Even if the installation of FlexNet Report Designer (and Cognos) is shared with (say) FlexNet Manager for Engineering Applications, you must still complete this process.

1. Log in to your Report Designer (Cognos) server, and navigate to `reportDesignerInstallationDirectory\c10\deployment`.

   Tip • If this folder does not already exist, create it.

2. Copy your Report Designer Package - Single Tenant (`FlexNetManagerPlatformReportsAndDashboard.zip`) to this folder.
   You downloaded this package as you worked through *Download the Materials*.

   Important • Do not change the file name. This file name and location are both requirements.

3. You may log out of the Report Designer (Cognos) server now.
   Shortly you will log into your batch scheduling server, but first there are permissions to set.

4. In the web interface for FlexNet Manager Suite 2015 R2 SP1, add your current account (suggested: `fnms-admin`) as a Web Administrator for the business reporting portal as follows:

   a) Navigate through the system menu (⚙▼ in the top right corner) > **Accounts**.
      The **Accounts** page opens.

   b) Select the **Roles** tab, and check for the existence of the `Business Reporting Portal Admin` role.
      If the role does not already exist, you can create it.

   c) Click the edit (pencil) icon at the right-hand end of the card for this role.
      The properties page for this role appears.

   d) Expand the **Business reporting portal** tab of the accordion, and from the **Privileges** option list, ensure the **Web Administrator** role has **Allow** permissions.

   e) Switch to the **All Accounts** tab, locate your current account (suggested: `fnms-admin`) in the list, and click the account name hyperlink.
      The page switches to show **Account Properties** for your account.

   f) Under the **Permissions** section, check whether your `Business Reporting Portal Admin` role is already listed against the **Role**. If so, you are set for permissions, and should continue with the next step *6*.

   g) Click the + button to the right of your current **Role** (typically, `Administrator`) to add your account to another role.
      A duplicate line appears with another option list of all the roles defines so far.

Tip • Each enterprise is licensed for only a single operator in the web administrator role. If one has already been defined, you need to move that account out before you can add yourself.

h) From the duplicate option list, select your `Business Reporting Portal Admin` role.
The **Business reporting portal** tab of your resulting list of privileges is updated. If you expand this tab of the accordion, you see that **Web Administrator** now displays `Allowed access`.

i) Scroll to the bottom of this page, and click **Save**.
Your account is now the (only) web administrator for use of the Report Designer.

Tip • Report Designer also requires that this account is valid in Active Directory.

5. Using the same account, log into your batch scheduling server directly.

Refer to your block diagram of servers to identify this machine. If you have combined servers, this may be your processing server, or your application server.

6. Navigate in Windows Explorer to *installation-folder*\Cognos
\BusinessReportingAuthenticationService\bin.
Example:

```
C:\Program Files (x86)\Flexera Software\FlexNet Manager Platform\Cognos
\BusinessReportingAuthenticationService\bin
```

7. Right-click `CognosPackageImport.exe` and **Run as Administrator**.
A window appears for the **Flexera Report Designer Package Import Utility**.

8. Click **Update...**.
An **Update Value** dialog appears.

9. In the **Value** field, enter the value for Report Designer's Dispatch URL.

In a typical installation, this has the following form:

```
http://RD-Server:9300/p2pd/servlet/dispatch
```

where you should replace *RD-Server* with the name of your server hosting Report Designer (powered by Cognos).

10. Click **Update**.
The value entered is written into the registry on this server, and the additional dialog disappears.

*Tip • If you run this import utility on the same machine in future, it displays the value stored in the registry in its read-only **Dispatch URL** field.*

11. Click **Install Reports Package**.
Progress is logged in the text window of this dialog as the package is imported into the Cognos database. When successfully completed, the last line displays `Finished publishing the Report Designer package.`

Important • *Do not close the utility until it has finished the import! This process may take several minutes.*

Link to Flexera Service Gateway

Flexera Service Gateway allows interaction between separate products from Flexera Software.

The ability to link FlexNet Manager Suite to the Flexera Service Gateway is subject to a separate license option. If you have licensed this option (you can check using the process below), you need to configure the connection as part of your configuration process.

To complete this process, you must know credentials that can log into your Flexera Service Gateway server with administrator privileges.

1. Log into the web interface for FlexNet Manager Suite.

Tip • *Either log in from a computer other than your web application server; or if running on that server, ensure that you access the full server name (and not* `localhost`*) in the URL. The URL in your web browser is taken into account in preparing the integration file, and should not include* `localhost` *if you want to integrate with other products from Flexera Software.*

2. Optionally, check that you have licensed the option to link to Flexera Service Gateway:

    a) Navigate to the system menu (⚙ ▼ in the top right corner) > **FlexNet Manager Suite License**. The **Your FlexNet Manager Suite License** page appears.

    b) Check the **License details** section.

    If you have licensed this option, `FNMP API integration enabled: Yes` appears in the list. If it is not visible, you cannot continue with this procedure.

3. Navigate to the system menu ⚙ ▼ > **System Settings**, and select the **Web API** tab.

Note • *This tab is available only if your enterprise has licensed the FNMP API integration option.*

4. Click each of the links in turn to download the two files, and save them to a convenient location (such as `C:\temp`).

    There must be network access to your Gateway server from the location where you save the files.

5. Either, in your web browser's list of recent downloads, click the registration tool to open it; or

    a) Open a Command Window, and navigate to the location where you downloaded the files.

    b) Run `RegisterFlexeraServiceGateway.exe`.

    The **Flexera Service Gateway Registration** dialog appears.

6. Identify the **Flexera Service Gateway host**, the server in your enterprise where the Gateway is installed, and the **Port** number.

You may use an IP address, a fully qualified domain name, or (if your DNS is correctly configured and accessible) the server's host name. The default port number is 9443.

7. Provide the credentials for administrator access to the Gateway account.

   In the absence of any better information, try the account `admin` with the password `password`.

8. Use the **Import** button to browse to the other downloaded file, `webapi.config`, and import it into the registration tool.

9. Click **OK**.

   Registration is complete. (You do not need to repeat this registration on others of your central servers.)

Update Access Rights

Through your processes of database migration, all the access rights that applied in your earlier compliance product are carried forward into FlexNet Manager Suite 2015 R2 SP1.

In addition, if you created a new account for installation (suggested: `fnms-admin`), this account defaults to having administrator privileges in your new implementation, in addition to the migrated access rights. This account has adequate rights to modify access rights for other operators.

If you wish to modify access rights:

1. Log in to the web interface to FlexNet Manager Suite 2015 R2 SP1.

2. Navigate through the system menu (⚙ ▼ in the top right corner) > **Accounts**, and select the **Roles** tab.

3. For each unique set of access rights, ensure that there is (or create) a distinct role, and set its rights by expanding the various headings in the accordion and using the controls inside. (For advanced combinations, start by selecting `Custom` from the option list in each section.) Remember to scroll down and click **Save** (or **Create**) when you make any changes.

4. When appropriate roles are defined, switch to the **All Accounts** tab.

5. Find each account in the list in turn, and click the hyperlinked account name to open its properties.

6. Change the roles assigned, or add additional roles, to each account as required.

   The net effect of all roles on permissions for this account is displayed in read-only mode in the accordion below as you make changes. (Remember that a 'deny' in one role over-rides an 'allow' in another role when the same account is assigned to both roles.)

7. Remember to **Save** each changed account.

Update, and Deploy Additional Inventory Beacons

Beacons must be updated to take advantage of this release.

The inventory beacon is enhanced in 2015 R2 SP1, and *must* be updated if you wish to use:

• Activity analysis through the web interface

- Log uploads from inventory beacons.

> 💡
>
> *Tip • Separate log files are now generated for all the following processes, and by default saved in* `C:\ProgramData\Flexera Software\Compliance\Logging\InventoryRule` *on the inventory beacon. These are automatically uploaded to your central application server, and accessible in the* **System Tasks** *page:*
>
> - *Device discovery*
> - *Gathering device inventory*
> - *Gathering Microsoft SQL inventory*
> - *Gathering Microsoft Hyper-V inventory*
> - *Gathering XenDesktop device inventory*
> - *Gathering VMware inventory*
> - *Gathering Oracle VM inventory*
> - *Gathering Oracle DB inventory.*

Functionality added to inventory beacons at version 2015:

- Higher frequency hardware scanning to support subcapacity licensing on IBM PVU licenses
- 64-bit tools, especially for importing SAP inventory and for inventory upload

> 💡
>
> *Tip • If you are using ILMT as an inventory source, the DB2 drivers on the inventory beacon must be upgraded to 64-bit.*

- Uploaded inventory triggering an immediate inventory import
- Secure SSL connections to Active Directory.

Functionality added to inventory beacons at version 2014 R3:

- Advanced VMware inventory collections (subject to you having licensed this option)
- Inventory collection from XenDesktop including version 7.5
- Enhanced recognition for Microsoft Server applications such as Exchange Server, Biztalk, and SharePoint.

Functionality added to inventory beacons at version 2014 R2:

- Built-in task scheduling
- Self-updating
- Co-location on your central batch scheduling server (or in smaller implementations, the processing server or application server)

- Deploying a hierarchy of inventory beacons, where some beacons can act as data concentrators for others (this can be helpful in complex network topographies).

Tip • If an inventory beacon functions as a parent to any other beacon, and is using Microsoft IIS as its web server, it must be updated as described below to grant access to the folder used for staging uploads, and to the files that must be served to a child beacon.

Because of the self-updating functionality introduced for inventory beacons at version 2014 R2, the processes are quite different for:

- Updating an inventory beacon from version 2014 R2

- Updating an inventory beacon from version 2014 or earlier.

Upgrading 2014 or earlier, or installing new inventory beacons

The process for installing and configuring inventory beacons starts from the web UI for FlexNet Manager Suite.

Note • Any computer on which you will install an inventory beacon must have at least version 3.0 of PowerShell installed. For more information, see Upgrade PowerShell on Inventory Beacons on page 19.

Use this same process for both upgrading an inventory beacon from version 2014 or earlier, and installing a new one.

1. Log in on the computer where the inventory beacon is to be installed, and start a web browser there to access the URL *server-name-or-IP-address*/**Suite**/.

2. In the **Discovery & Inventory** menu, under the **Network** group, select **Beacons**.

3. Click **Deploy a beacon**.
   The **Deploy a Beacon** page appears. Ensure that the default **Download beacon** section of the page is open.

4. Click **Download beacon**.

5. Use the web browser dialog to save the installer to a convenient directory on the inventory beacon computer (such as `C:\temp`).

6. In Windows Explorer, navigate to the saved file, and double-click it to run the installer.

7. Step through the installation wizard, using the summaries in the accordion section **Beacon setup** or the more detailed online help available through the web interface to assist as necessary.

8. Does this inventory beacon act as a parent to any other inventory beacons (lower in your hierarchy of beacons)? And if so, it is using Microsoft IIS as its local web server? If both of these are the case, you need to update parameters set for IIS as follows:

   a) In the inventory beacon interface, in the **Beacon configuration** group in the navigation bar, click **Local web server**.

The **Web Server Settings** page opens.

b) Select **No local web server (will not allow any incoming web requests)**.
This turns off the settings for IIS.

c) Select **IIS web server**.
The settings needed for child inventory beacons are now passed to IIS.

9. Is this an upgrade of an inventory beacon that previously collected third-party inventory (such as SCCM) in your 2014 system? If not, continue to the next step.

In 2014 (or earlier), third-party inventory collection was triggered by Windows Scheduled Tasks, and the account used for data access was the account running the scheduled task (often the SYSTEM account). In 2015 R2 SP1, all scheduling is managed by the inventory beacon engine (with settings controlled through the inventory beacon interface). This means that previously operating adapters will no longer work until you specify credentials under which they should run under the new scheduling system. To do this:

a) In the inventory beacon interface, navigate to the **Inventory systems** page.

b) Select a connection to update from the list, and click **Edit...**.
The **Edit SQL Source Connection** dialog appears (or a similar dialog according to your chosen connection). All details of your previous connection should be preserved, but the authentication details must be set up for the new architecture.

c) Typically, choose the **Window (specific account)** option, and provide the **Username** and **Password** that allows access to the data source.

d) Click **Save** to close the dialog (which only writes the change to the inventory beacon interface).

e) Repeat this for all other connections in the list that need updating.

f) Finally, click **Save** again on the Inventory systems page to commit all your changes.

10. When the configuration of this inventory beacon is complete, relocate to the next inventory beacon (or proposed beacon), and repeat this process.

When deployment and updating of inventory beacons is complete, remember to adjust your subnets and possibly your inventory/discovery rules in the web interface of FlexNet Manager Suite to bring the new beacons into operation.

Managing self-upgrades from 2014 R2/R3 inventory beacons

There are two settings, both controlled from the web interface for FlexNet Manager Suite, that manage the self-updating behavior of inventory beacons:

• Global settings for the overall update strategy

• Individual settings for each inventory beacon.

The combination allows you to silently upgrade all inventory beacons automatically; or to run a pilot program to test the behavior of one new inventory beacon before allowing all others to automatically update. The following procedure covers both strategies.

1. First check the global settings for inventory beacons:

    a) In the compliance browser, navigate to **Discovery & Inventory** > **Settings**.
        The **Inventory Settings** page appears.

        💡

        *Tip • Check the release details using the **View Change History for Flexera Inventory Beacon** link in the **Beacon settings** section.*

    b) In the **Beacon settings** section, make a selection from the **Beacon version approved for use** control.

        •   For fully automated updates of your inventory beacons, choose `Always use the latest version (currently` *release-number*`).` With this setting operational for all your inventory beacons, updates are silent and self-managing. (You need to check, as described below, that each inventory beacon is permitted to accept this setting.)

        •   For a pilot program, choose the latest version of self-updating FlexNet Beacon software installed in your enterprise. Currently, this must be no later than 2014 R3 (for which choose a version similar to `10.2.x`, with a trailing build number). By limiting the global automation to your last approved version, you control when the upgrades flow through your estate.

2. Now check the settings for each individual inventory beacon:

    a) In the compliance browser, navigate to **Discovery & Inventory** > **Beacons** (in the **Network** group).
        The list of your current inventory beacons is displayed. In the **Actions** column on the right-hand end of each entry, there is an edit icon (pen).

    b) For the desired inventory beacon, click its edit icon.
        The properties page for this inventory beacon is displayed. Ensure that the **General** tab is selected.

    c) In the **Overview** section of the **General** tab, make a selection from the **Upgrade mode** option list.

        •   For all operational inventory beacons (but not for your pilot test one), choose `Always use the approved version (currently` *release-number*`).` This setting makes this inventory beacon respond to the *global settings* for all your inventory beacons.

        •   For the pilot test inventory beacon, choose `Choose a specific version`: Another control appears where you can choose the **Specific version**. For release 2014 R3, choose a version `10.2.0` (plus build number).

3. After your testing period, when you are satisfied with the functionality of the upgraded pilot inventory beacon, remember to return to the global settings (step 1) and authorize the latest version.

    💡

    Tip • Remember that you cannot access the latest inventory collection functionality until all relevant inventory beacons have been upgraded (allow up to a day after you approve the latest version at your central server for all inventory beacons to self-update).

Upgrade Connected-Mode Studios

If you use the Inventory Adapter Studio or Business Adapter Studio in connected mode on your central application server, you should update them separately.

Installations of the studios on inventory beacons are automatically updated as a part of the inventory beacon self-update procedure. These installations operate in disconnected mode, and need no intervention for updates.

Separate installations on one of your central servers may operate in connected mode. These are not installed or upgraded automatically, and if you have previously installed them, you should install the latest version to overwrite your existing installation.

1. For safety's sake, make a backup copy elsewhere of any custom adapters saved in the standard storage paths used by the Inventory Adapter Studio or Business Adapter Studio.

2. Using the credentials supplied by Flexera Software with your order confirmation (or as renewed since), log into the Product and License Center at *https://flexerasoftware.flexnetoperations.com*.

3. On the first page, select `FlexNet Manager Platform`, and on the resulting second page, select the product again.

4. In the list of versions, click the product name for the version you are using (typically the most recent version).

5. In the list of components to download, select `Business Adapter Studio` *releaseNumber*`.zip`, and download and save it to a convenient location (such as `C:\Temp`).

6. In Windows Explorer, navigate to the downloaded archive, right-click, and choose **Extract All**.

7. Navigate into the unzipped archive, and double-click `setup.exe`, following the instructions in the installation wizard.

The Business Adapter Studio may be installed on any of your central servers (in a multi-server implementation). The installer assesses the installation paths, and installs itself in the installation folder of FlexNet Manager Suite. The defaults are as follows:

- The Business Adapter Studio executable: `BusinessImporterUI.exe`

- Default installation path (in connected mode on central server): `C:\Program Files (x86)\Flexera Software\FNMP Business Adapter Studio`

- No template file storage is required for the Business Adapter Studio in connected mode, as it validates the database schema directly. Your custom business adapters may be saved in the folder(s) of your choice.

When you have completed the remainder of your product installation, the Business Adapter Studio can be run from the Windows start menu on this server; and the Business Importer, which is also installed automatically with the Business Adapter Studio, is also available for execution on the command line. For details about the Business Adapter Studio, see online help or the *FlexNet Manager Suite System Reference* PDF file; and for details about the Business Importer, see the *Using the FlexNet Business Importer* PDF file. Both PDF files are available through the title page of the online help.

Configure Updates to Inventory Agents

Adjust the database settings that control automatic updates of deployed FlexNet inventory agents.

By default, an upgrade to your central application server(s) and inventory beacon(s) does not trigger any automatic updates to the FlexNet inventory agents that you have deployed on target machines for local inventory collection. In fact, the upgrade mechanism for FlexNet inventory agent is turned off after an upgrade to the central application servers. This gives you freedom to manage the upgrade of deployed FlexNet inventory agents independently of the upgrade to your central application servers.

Tip • *This procedure applies only to FlexNet inventory agents deployed on inventory targets (that is, computers that have been 'adopted'). Copies of the FlexNet inventory agent installed on inventory beacons and used for zero-touch inventory collection are updated as part of the FlexNet Beacon self-update.*

The upgrade of deployed FlexNet inventory agents is controlled by settings stored in the database. For that reason, this procedure takes place on your batch scheduling server/reconciliation server (or whichever server includes that functionality, such as your processing server, or application server in smaller implementations).

1. Log in to your batch scheduling server using the installing user account (suggestion: `fnms-admin`).

   Depending on the actions you want to take, the account requires either read or write access to the database.

2. Open *installation-folder*`\DotNet\bin`.

3. To review a list of the FlexNet inventory agent versions to which you may upgrade:

   ```
   .\ConfigureSystem.exe list-agent-versions
   ```

   Note • *Managed Service Providers (MSPs) covering multiple tenants must use:*

   ```
   .\ConfigureSystem.exe list-agent-versions --tenantuid tenantIdentifier
   ```

   This lists all versions of the FlexNet inventory agent that are stored in your database and available for use as upgrades to your currently deployed agents. The list is typically updated at each release of FlexNet Manager Suite. Versions are shown by their internal major-minor-update numbering (such as `10.3.0`).

4. To identify which version of the FlexNet inventory agent you have currently authorized as the target version for all upgrades:

   ```
   .\ConfigureSystem.exe current-agent-upgrade
   ```

   Note • *Managed Service Providers (MSPs) covering multiple tenants must use:*

   ```
   .\ConfigureSystem.exe current-agent-upgrade --tenantuid tenantIdentifier
   ```

5. To authorize a new version of the FlexNet inventory agent as the target version for all upgrades:

   ```
   .\ConfigureSystem.exe select-agent-upgrade --version versionString
   ```

Note • Managed Service Providers (MSPs) covering multiple tenants must use (all on one line):

```
.\ConfigureSystem.exe select-agent-upgrade --version versionString
                              --tenantuid tenantIdentifier
```

Replace *versionString* with the same major-minor-update numbering as is displayed by the `list-agent-versions` action. This value must be an exact match for one of the available versions listed by `list-agent-versions`. If not, no action is taken. (Notice that there is no requirement for the new version to be greater than versions previously installed: you can specify an earlier version from the available list, which causes any later FlexNet inventory agents to downgrade to the specified earlier version.)

Tip • The same version (number) of the FlexNet inventory agent is normally installed across all platforms.

6. To halt all upgrades and downgrades of the FlexNet inventory agents currently deployed in your enterprise:

```
.\ConfigureSystem.exe clear-agent-upgrades
```

Note • Managed Service Providers (MSPs) covering multiple tenants must use:

```
.\ConfigureSystem.exe clear-agent-upgrades --tenantuid tenantIdentifier
```

Tip • The result is the default state after the FlexNet Manager Suite application server(s) have been upgraded.

When your new settings are saved to the database, they are distributed to the inventory beacons at the next update, along with the installer for the currently authorized target version of the FlexNet inventory agent for each platform. The individual FlexNet inventory agents receive the setting and (if necessary) the installer when they next check in (by default, once a day), and subsequently they self-update to the specified version.

For more information about the actions available with this utility, use either of these commands:

```
.\ConfigureSystem.exe help
.\ConfigureSystem.exe help action-name
```

Activating and Using New Features

Some new features in the 2015 R2 SP1 release are available now that you have:

• Updated the inventory server (see *Update the Inventory Server* on page 34)

• Updated the Application Recognition Library (see *Populate the Downloadable Libraries* on page 42)

• Updated your inventory beacons, including setting the global update settings to the latest release (see *Update, and Deploy Additional Inventory Beacons* on page 49 and sub-sections).

To take advantage of new features (including the increased reporting from inventory beacons), your next inventory import and license consumption calculation must include a full import. The command line to achieve this is shown below. Notice the particular use of the dash characters:

```
BatchProcessTask.exe run InventoryImport -- -f
```

Some adapters require special handling, or additional configuration or upgrade:

- ADDM adapter — If you are using this adapter and running it on your application server (rather than on a free-standing FlexNet Beacon), you should ensure that all devices are updated for sociability with FlexNet inventory. You achieve this by making your next import and compliance calculation a full import, as described above.

- XenApp adapter (see *Update the XenApp Adapter* on page 57)

- XenDesktop adapter (see *Update the XenDesktop Adapter* on page 58).

These last two adapters require upgrading to match the new architecture that Citrix has released since version 7 of those products.

Update the XenApp Adapter

The updated XenApp adapter requires updates to the XenApp server agent, the staging database, and the method of collecting Active Directory data.

1. Check the inventory beacon update is complete (see *Update, and Deploy Additional Inventory Beacons* on page 49 and sub-sections).

2. Be sure that you have completed an import from Active Directory from all relevant domains.

   For set-up details refer to *FlexNet Manager Suite Help > Inventory Beacons > Active Directory Page*.

3. If you did not already update your staging database for this adapter in your central database server (as described in *Upgrade/Create Databases* on page 24):

   a) Locate your downloaded archive `Tier 1 Adapter Tools.zip` (perhaps in `C:\temp\FNMSUpgrade\`), and in your unzipped archive, navigate into the `\Citrix XenApp Server Agent` subdirectory.

   b) Further navigate into the appropriate sub-folder for your version of XenApp:

      - `XenAppAgent6`

      - `XenAppAgent65`

      - `XenAppAgent75`.

   c) From your chosen folder, collect a copy of the database creation/update script `SetupXenAppAgentStagingDatabase.sql`.

   d) Drop this SQL script on the database server hosting your staging database, and execute it in SQL Server Administration Studio against your chosen database instance.

Tip •   If you have more than one of these staging databases, repeat this process until they are all updated.

---

4. Ensure that the appropriate inventory beacon(s) has/have a connection configured for the staging database(s), and that the connection is scheduled for regular operation.

   For details, check the *Create Connections for Data Upload* section of the *XenApp Server Adapter* chapter in `FNMSAdaptersReferencePDF.pdf`, available through the title page of online help.

5. On each of your XenApp controlling servers where `FNMPXenAppAgent.exe` is installed, replace the executable with the correct version from the unzipped archive.

   For details, check the *Installing the XenApp Server Agent* section in the above-mentioned chapter.

6. As required, create or update a scheduled task to execute the upgraded XenApp server agent.

   See the adjacent topic *Create a Scheduled Task* in the same chapter.

   💡

Tip •   Pay particular attention to the schedule for the agent, and the schedule of the inventory beacon import from the staging table. These two activities must not overlap.

The XenApp adapter is now ready for operation. On schedule, the agent populates the staging database; on the later schedule, the staged data is collected by the inventory beacon and uploaded to the central server; finally, when the next inventory import and compliance calculation is run, the XenApp applications and the users who can access them are available, at least as installer evidence and file evidence, within FlexNet Manager Suite. You may additionally need to link the evidence to applications, and to ensure these applications are licensed. For more information, see the other online help topics under *FlexNet Manager Suite Help > Adapters Supplied by Default > XenApp Server Adapter*.

Update the XenDesktop Adapter

The best practice configuration for the XenDesktop adapter is to allow direct network access from the appropriate inventory beacon to the XenDesktop broker. (Where this is not permitted, you can copy the appropriate PowerShell script to the XenDesktop broker, execute it locally, and copy the generated .vdi and .ndi files to the Incoming folder on the relevant inventory beacon.)

As this adapter relies on PowerShell scripts run from the inventory beacon and executing on the XenDesktop broker, both these servers must allow at least `RemoteSigned` execution policy for PowerShell, as described below.

If you are upgrading from an earlier version of the XenDesktop adapter, notice that you *must* run the Active Directory import separately, and prior to exercising the adapter, as listed below. Failure to do this risks the removal of previously-gathered inventory of VDI access to applications.

1. Check the inventory beacon update is complete (see *Update, and Deploy Additional Inventory Beacons* on page 49 and sub-sections).

2. Be sure that you have completed an import from Active Directory from all relevant domains.

   For set-up details refer to *FlexNet Manager Suite Help > Inventory Beacons > Active Directory Page*.

3. On each of the inventory beacon and the XenDesktop broker, check the execution policy for PowerShell scripts:

    a) On each machine in turn, open a PowerShell window.

    b) At the prompt, enter `Get-ExecutionPolicy`.

    Usable settings include `RemoteSigned`, `AllSigned`, or `Unrestricted` (although the latter is not recommended).

    a) If the current policy setting is `Restricted`, run the following command to set it to `RemoteSigned`:

```
Set-ExecutionPolicy RemoteSigned
```

4. Create (or update) discovery and inventory gathering rules to target your XenDesktop brokers:

    a) In the web interface for FlexNet Manager Suite, navigate to **Discovery & Inventory** > **Discovery** group > **Discovery and Inventory Rules**.

    b) Select the **Targets** tab, click **Create a target**, and complete the details to target your XenDesktop broker(s). Click **Save** to add your new target to the list of available targets. (If necessary, repeat to create multiple targets.)

    c) Select the **Actions** tab, click **Create an action**, and give your new action a useful name and description.

    d) Expand the **XenDesktop environments** heading in the accordion list, and select both **Discover XenDesktop environments** and **Also gather XenDesktop environment inventory**. Then click **Create** to record your new action.

    a) Select the **Rules** tab, click **Create a rule**, and in the rule builder that appears, click the `View Actions...` hyperlink.

    b) For the rule you just created, click **Add to rule builder**, and in the rule builder, click the `View Targets...` hyperlink.

    c) For the target(s) you defined, click **Add to rule builder**, and in the rule builder, click **Schedule**.

    d) Complete the scheduling details, and click **Save as**.

    e) Give your rule a meaningful name, and click **Save**.

      Tip • *After a little time (say, 30 minutes) to allow for the relevant inventory beacon to collected its updated rules, you can inspect the rule on the applicable inventory beacon, in its **Rules** page. (If it hasn't updated yet, click **Update now**.)*

5. After the XenDesktop adapter runs (according to the schedule you just created), and after the subsequent inventory import and compliance calculation, you can inspect the inventory from your XenDesktop broker:

    a) In the web interface for FlexNet Manager Suite, navigate to **Discovery & Inventory** > **Discovery** group > **All Discovered Devices**.

    a) Locate your XenDesktop broker in the list of devices.

Tip • *Adding the **VDI broker** column from the column chooser, and then filtering on* `Yes`*, may help you locate this server.*

a) Click the device's name to open its properties, select the **Status** tab, and expand the **XenDesktop environment inventory** section of the accordion.

This is also the location where any PowerShell script errors from the inventory beacon are reported. Should you need additional troubleshooting:

- Inspect the log file on the inventory beacon for errors relating to XenDesktop discovery. This file is located at `%PROGRAMDATA%\Flexera Software\Compliance\Logging\BeaconEngine`.

- Should you need to prepare a trace file to submit to Flexera Software Support, turn on the `Scheduling/RemoteExecution` tracing options by editing this file on your inventory beacon: `InstallationDirectory\Flexera Software\Inventory Beacon\etdp.trace`

6. As required, you may need to link the file evidence imported from XenDesktop to application records, and ensure that those application records are linked to license records. Wherever possible, link the license records to purchase records to identify the number of your license entitlements.
Once all the links are in place, the next compliance calculation reflects your compliance position for applications accessible through XenDesktop.

3

Notes on Issues

Topics:

- *Password Maintenance*
- *Identifying IIS Application Pool Credential Issues*
- *IIS Roles/Services*

This chapter includes a few brief guidelines for dealing with common issues. If you discover additional issues not described here, please contact Flexera Software Support for assistance.

For help on problems uploading inventory data, access the online help through the web interface for FlexNet Manager Suite, and navigate to **FlexNet Manager Suite Help** > **Inventory Beacons** > **Inventory Beacon Reference** > **Troubleshooting: Inventory Not Uploading**.

Password Maintenance

When a password on the service account expires, services cease to operate. At password refresh time, ensure that the password is updated for all of the following.

📋
_____

Note • For accuracy, the changes are listed for distinct servers. In smaller implementations:

- *If you have only a web application server and a processing server, then combine the lists for the batch scheduling server and inventory server for use on your processing server.*

- *In a single server implementation, combine all three lists on your application server.*

The configuration scripts used during product installation cannot be re-run simply to update passwords. The following passwords must all be maintained manually.

On the web application server

- The identity configured on the following IIS application pools:
    - **FlexNet Manager Platform**
    - **ManageSoftWebServiceAppPool**
    - **SAP Optimization**
    - **SAPServiceAppPool**

On the batch scheduling server

- The identity configured on the IIS application pool: **Flexera Beacon**
- In Services:
    - **FlexNet Manager Suite Batch Process Scheduler**
    - **FlexNet Manager Suite Batch Processor** (if you have separated out to multiple batch servers, this is also found on each batch server, and the password must be updated there as well)
- In the **FlexNet Manager Platform** folder for Microsoft Scheduled Tasks:
    - Data warehouse export
    - Export to ServiceNow
    - FlexNet inventory data maintenance
    - FNMP database support task
    - Import Active Directory
    - Import application usage logs
    - Import discovery information

- Import installation logs

- Import inventories

- Import Inventory Beacon activity status

- Import Inventory Beacon status

- Import remote task status information

- Import security event information

- Import SAP inventories

- Import SAP package license

- Import SAP user and activity information

- Import system status information

- Import VDI access data

- Inventory import and license reconcile

- Recognition data import

- Regenerate Business Import config

- Send contract notifications.

On the inventory server

- The identity configured on the following IIS application pools:

  - **Flexera Importers**

  - **Flexera Package Repository**

- In the **FlexNet Manager Platform** folder for Microsoft Scheduled Tasks:

  - Import Active Directory

  - Import application usage logs

  - Import discovery information

  - Import installation logs

  - Import inventories

  - Import Inventory Beacon activity status

  - Import Inventory Beacon status

  - Import remote task status information

  - Import security event information

  - Import system status information

- Import VDI access data.

On the Cognos server

The password on the IBM Cognos service also needs to be maintained.

On the inventory beacon

By default, the FlexNet Beacon Engine service and scheduled tasks run as the local SYSTEM account. If these defaults have been modified:

- The following service in the **Services (local)** folder of Component Services (this may have been modified to run as a service account with administrator privileges):

  - FlexNet Beacon Engine.

  Note • The following services are also present, but must be running as the local SYSTEM account:

  - *Flexera Inventory Manager installation agent*

  - *Flexera Inventory Manager managed device vversionNumber*

  - *Flexera Inventory Manager peer-to-peer download service*

  - *Flexera Inventory Manager security service.*

- In the **FlexNet Inventory Beacon** folder for Microsoft Scheduled Tasks (by default, these tasks run as the local SYSTEM account, but you may have modified the installation to run these as a named user account in order to manage proxy access):

  - Upload Flexera logs and inventories

  - Upload third party inventory data

Identifying IIS Application Pool Credential Issues

A password change on (any of the) application server(s) may require an update of the IIS configuration.

Background

During installation of an on-premises implementation, PowerShell scripts run on the application server (or, in a multi-server implementation, on each of the component servers in turn) ask you to provide credentials for the application pools used within IIS for FlexNet Manager Suite. The scripts save these as part of the IIS configuration.

Note • If, as recommended, you have used a service account (suggested: `svc-flexnet`) for this purpose, it is very unusual to require a password change for such an account. If you used a normal user account, you require this additional maintenance each time that the password on that account is changed.

If, at any time after installation, the password for this user account is updated, the IIS configuration is now out of date, and IIS will refuse to run the application pools for FlexNet Manager Suite.

Tip • In this case, as well as IIS configuration, you may also need to update passwords on scheduled tasks and on services. For a complete list, see Password Maintenance on page 62.

Diagnosis

First symptom: The web interface for FlexNet Manager Suite will not load, producing the following error:

```
HTTP Error 503 - Service unavailable
```

Investigation: If you examine the Microsoft IIS application pools, you will find that the application pool for FlexNet Manager Platform is disabled after any attempt to run the web interface. An examination of the IIS log file shows entries like the following:

```
server-name  5057  Warning Microsoft-Windows-WAS  System  date time
Application pool FlexNet Manager Platform has been disabled. Windows Process Activation
Service (WAS)did not create a worker process to serve the application pool because the
application pool identity is invalid.

server-name  5059  Error  Microsoft-Windows-WAS  System  date time
Application pool FlexNet Manager Platform has been disabled. Windows Process Activation
Service (WAS) encountered a failure when it started a worker process to serve the
application pool.

server-name  5021  Warning Microsoft-Windows-WAS  System  date time
The identity of application pool FlexNet Manager Platform is invalid. The user name or
password that is specified for the identity may be incorrect, or the user may not have
batch logon rights. If the identity is not corrected, the application pool will be
disabled when the application pool receives its first request.  If batch logon rights
are causing the problem, the identity in the IIS configuration store must be changed
after rights have been granted before Windows Process Activation Service (WAS) can
retry the logon. If the identity remains invalid after the first request for the
application pool is processed, the application pool will be disabled. The data field
contains the error number.
```

Repair

Update the credentials for the applications pool on each of your application servers, using the process in *Update Credentials in IIS Application Pools* on page 65.

Update Credentials in IIS Application Pools

To update the password for the FlexNet Manager Suite application pools within Microsoft IIS, complete the following process on each of your servers in turn:

Tip • Servers are here named in a series from most specific (in large scale implementations) to most general (for small scale implementations). Use the first-listed server type that applies to you. For example, if the list item says 'on the inventory server/processing server/application server', and you have a separate inventory server, make the change there. If you do not have a separate inventory server, but you have scaled to a separate processing server (that combines your inventory server and your batch server), make the change on your processing server. For a single-server implementation, you make this change on your application server.

1. Open IIS Manager (**Start** > **Administrative Tools** > **Internet Information Service (IIS) Manager**).

2. In the navigation area on the left, expand the ***SERVER-NAME (account-name)*** node, and select **Application Pools**.
   Any application pool accessed since the user account password was changed displays a status of `Stopped`. On each server type, the relevant application pools are:

   • **Flexera Beacon** on the batch scheduling server/processing server/application server

   • **Flexera Importers** on the inventory server/processing server/application server

   • **Flexera Package Repository** on the inventory server/processing server/application server

   • **FlexNet Manager Platform** on the web application server/application server

   • **ManageSoftWebServiceAppPool** on the web application server/application server

   • **SAP Optimization** on the web application server/application server

   • **SAPServiceAppPool** on the web application server/application server.

3. Select the appropriate application pool, and in the **Actions** list on the right, click **Advanced Settings**.
   The **Advanced Settings** dialog appears.

4. In the **Process Model** section, select **Identity**, and click the ellipsis button next to the account name.

5. Next to **Custom Account**, click **Set**.
   The **Set Credentials** dialog appears.

6. Enter the full **User name** for the account and enter the updated password in the two required fields.

7. Click **OK** to close all the open dialogs and save the new settings.

8. With the appropriate application pool still selected, in the **Actions** list on the right, click **Start**.

IIS Roles/Services

Below are the Microsoft Internet Information Services (IIS) roles and services utilized by FlexNet Manager Suite. In the event of misbehavior, it is often helpful to validate that all of the following are enabled on all your central servers (depending on the scale of your implementation, the ones that you have implemented from the application server, the web application server, the processing server, the batch scheduling server, and the inventory server). The process for checking whether the services are enabled is summarized below the list.

• `Web Server > Application Development > .NET Extensibility`

• `Web Server > Application Development > ASP.NET`

• `Web Server > Application Development > CGI`

- `Web Server > Application Development > ISAPI Extensions`

- `Web Server > Application Development > ISAPI Filters`

- `Web Server > Common HTTP Features > Default Document`

- `Web Server > Common HTTP Features > Directory Browsing`

- `Web Server > Common HTTP Features > HTTP Errors`

- `Web Server > Common HTTP Features > HTTP Redirection`

- `Web Server > Common HTTP Features > Static Content`

- `Web Server > Health and Diagnostics > HTTP Logging`

- `Web Server > Performance > Dynamic Content Compression`

- `Web Server > Performance > Static Content Compression`

- `Web Server > Security > Basic Authentication`

- `Web Server > Security > Request Filtering`

- `Web Server > Security > Windows Authentication`

To check whether these services are enabled in the Windows Server operating system:

1. Starting from the Windows start menu, navigate to **Control Panel** > **Administrative Tools** > **Server Manager**.

2. In the navigation bar on the left, under the **Server Manager** node, select the **Roles** node.

3. Locate the **Web Server (IIS)** section, and within that, identify the **Role Services** section.
   This section lists the status for each service. All of those in the list above should be both installed and enabled on all your central servers.