Upgrading FlexNet Manager Suite from 2014 to 2014 R3 On Premises

Contents

Upgrading FlexNet Manager Suite from 2014 to 2014 R3 On Premises

Legal Information

Document Name: FlexNet Manager Suite 2014 to 2014 R3 Upgrade Guide (for on-premises delivery)

Part Number: FMS-10.2.0-UG02

Product Release Date: 28 November 2014

Copyright Notice

FlexNet Manager Suite incorporates software developed by others and redistributed according to license agreements. Copyright notices and licenses for this externally-developed software are provided in the link below.

Intellectual Property

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

Restricted Rights Legend

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

1

Upgrading FlexNet Manager Suite 2014 Rx to 2014 R3 on Premises

Topics:

This document covers upgrading from FlexNet Manager Suite 2014 or 2014 R2 to FlexNet Manager Suite 2014 R3.

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 2014 R3 On Premises.*

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 an earlier 2014 release to FlexNet Manager Suite 2014 R3 is conceptually very straight-forward:

- 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.
    - If migrating from 2014 R2, 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, such as:

- Recognition of Microsoft Server applications (such as Exchange Server, BizTalk, and SharePoint), which requires the Microsoft option on your license for FlexNet Manager Suite
- Inventory of Oracle VMs
- Advanced inventory of VMware servers, which requires the VMware option on your license for FlexNet Manager Suite
- Upgrading your adapters for importing inventory from XenApp or XenDesktop for release 7.5 of those products
- Additional features if you are upgrading from version 2014:
    - Co-locating an inventory beacon on your current central reconciliation server
    - Implementing a hierarchy of inventory beacons, such that those higher in the hierarchy act as data concentrators for the import of inventory and business information
    - Adding integration with other Flexera products, such as Flexera Workflow Manager, by registering FlexNet Manager Suite with the Flexera Gateway using the installation wizard.

In general, adding these enhanced features is 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.)*

For very large implementations, six or more separate (virtual or physical) servers may be needed, including:

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

  Tip *• An inventory beacon may be installed on the same server as the reconciliation server (defined shortly).*

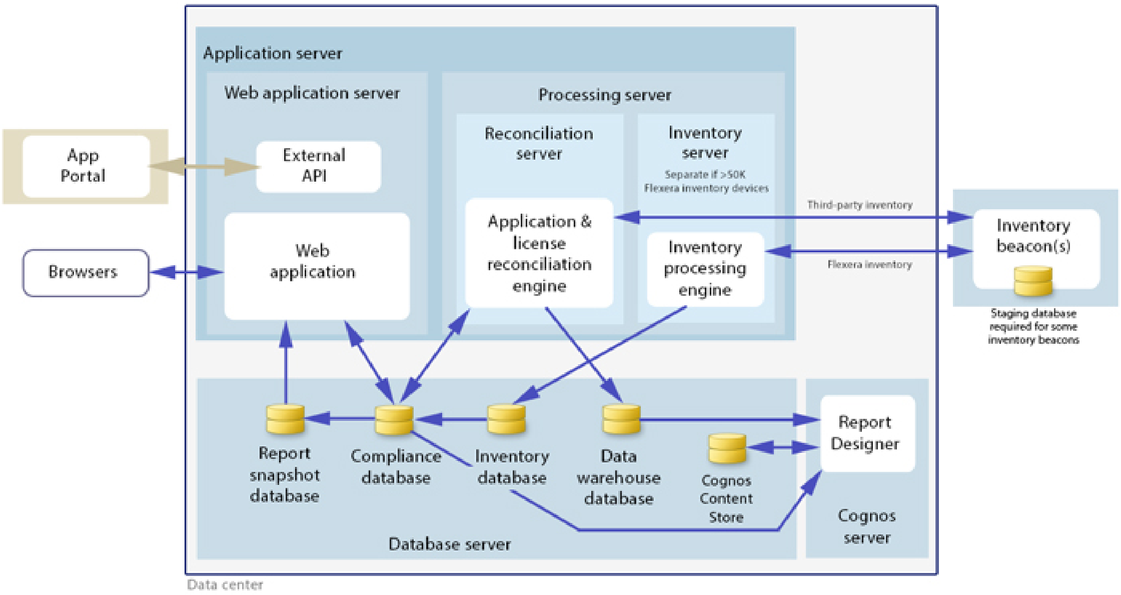
- An inventory server, which can also be duplicated across multiple servers if you are gathering FlexNet inventory for many tens of thousands of devices
- A reconciliation server that imports third-party inventory, integrates FlexNet inventory, incorporates business-related information, and reconciles everything to calculate your license position
- 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.*

While the above level of granularity may be needed only for massive implementations, it is also helpful for understanding the functionality of the different components.

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 as a single "application server", as shown in the diagram. As scaling dictates, you can combine or separate the web application server, the reconciliation server, and the inventory server in any combination required. For example, 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. (In such a case, you can choose to leave the reconciliation server and the web application server installed on the same device. The logical separation of presentation from processing need not drive hardware requirements.)



If you collect inventory from Citrix XenApp, the XenApp adapter requires a staging database. This may be installed on any convenient SQL Server, with one of the options being your central database server hosting your compliance database. Decide on the location of this staging database as part of your design.

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 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, reconciliation 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 reconciliation 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.
- Flexera 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).

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 reconciliation 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 (or 2014 R2) implementation, and not adding the specialized VMware inventory functionality. 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.
- You may need a new license. This is the case if you plan to license the new VMware option for advanced inventory gathering in that context. Please contact your Flexera Software (or partner) account manager to request a license including this additional term.

Identify (or Set Up) Accounts

In Active Directory, set up (or choose) the following accounts. At least three separate accounts are recommended as best practice:

1. It is assumed that an existing database administrator (DBA) account will be used to set up and configure the databases as described below.

2. An administrator account (say, `FNMS-Admin`, or an existing administrator account) with full admin access to all servers used for the implementation (including inventory beacons). Account details must be passed to the DBA.
3. A network service account (say, `SVC-fnmsservice`) that will run the batch services and web services in normal operations.
    - Admin access for this account is convenient; otherwise read, write, and execute permissions are required on all folders containing FlexNet installations, FlexNet data, and FlexNet log files.
    - This account must have permission to log on as a service and as a batch job on the reconciliation server (for details, see *Authorize the Service Account* on page 23).
    - The process below also includes setting up database permissions for this account, so account details are needed by the DBA.

    Tip • *If your implementation scales up to separate servers, you can use a distinct service account on each one. However, if your implementation combines web application, reconciliation, or inventory functionality on a given machine, use only a single service account per machine.*

    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 40.*

4. If you are collecting inventory from Citrix XenDesktop, you need an account with permission to execute remote PowerShell scripts on the XenDesktop server. (Typically this is an administrator account on the XenDesktop server. You may wish to register the `FNMS-Admin` described in 2. above for this purpose. Alternatively, a distinct account may be used, and must be registered in the password store on the applicable inventory beacon.)
5. Also for use with Citrix XenDesktop, you need to register (in the password store) a Citrix Readonly Administrator account, used for collecting data from the XenDesktop environment.
6. If you are collecting inventory from Citrix XenApp, you need an account with read permissions on the file system, and able to run a scheduled task, on the XenApp Delivery Controller. This account is required only on the XenApp Server (Delivery Controller), and is not registered in the password store on the inventory beacon. For further requirements for this account, refer to the *FlexNet Manager Suite Help > Adapters Supplied by Default > XenApp Server Adapter > Setting Up the XenApp Server Adapter > Installing the XenApp Server Agent*.

Tip • *If you will be setting up an inventory beacon outside your central domain (such as an Internet-facing beacon to collect inventory from travelling laptops), consider creating an additional account that is recognized, but has minimal privileges, within your central domain. This account manages the transfer of information between your inventory/application server and the inventory beacon. It has only one requirement within the central domain: the ability to use the HTTP or HTTPS protocol* *to transfer data to/from your central inventory (or application) server. The name and password for this account are entered directly in the inventory beacon interface, along with the URI it will access.*

Note • *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 its 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* `FNMSUsers`*) 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. Accounts to list in the security group minimally include:*

- *The operational service account (suggested:* `SVC-fnmsservice`*)*
- *The installing administrator account (suggested:* `FNMS-Admin`*)*
- *Any operational account needing to log in to a central inventory beacon installed on your reconciliation server (remember that since the inventory beacon requires administrator privileges to run, this account is both a local administrator on the reconciliation server and a* `db_owner`*)*
- *Any future back-up administrator accounts needed for the application server.*

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) 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 database instance in the **Object Explorer** pane.
2. Right-click the database, and select **Properties** from the context menu.
3. On the database **Properties** dialog, select the **General** tab, and in the **Maintenance** section, check the current collation sequence.
   If the collation sequence ends with the codes `_CI_AS`, you may proceed with the installation. Otherwise discuss the collation requirements with your database authorities.

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
- Reconciliation server

- Inventory server
- Each free-standing inventory beacon (the inventory beacon installed on your central reconciliation server is covered by the configuration of the reconciliation 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 .NET 4.5 on the same server. Take both these matters into account at the same time (see Upgrade PowerShell on Inventory Beacons on page 14 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, you have completed this procedure, and may skip to the next topic, *Configure Internet Explorer* on page 14.
   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*.
2. If your server is running Microsoft Windows Server 2008, the original installation was .NET 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), you have completed this procedure, and may skip to the next topic, *Configure Internet Explorer* on page 14.
      - If it is 4.0, apply the patches listed in step 3 (following).
3. On all other operating systems, 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*
4. If you are currently patching an inventory beacon (including one co-installed with your reconciliation 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 .NET Framework 4. (As before, the patch is not required if the version of .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), with the following command:

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

   If the server you are now working on is a free-standing inventory beacon that uses the Flexera self-hosted web server (and not IIS), loop back now and restart this process for the next server on your list.
8. When the installation of ASP.NET is completed, stop and restart IIS to ensure that it reads the ASP.NET registration:

   ```
   iisreset
   ```

9. `Exit` to close the command line window.
   If you are currently working on your web application server or your reconciliation server, 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.
10. 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**.
11. In the work pane that opens, expand **Sites**, and select **Default Web Site**.
12. 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.

13. Right-click the icon, and select **Open Feature**. A pane opens for **WebDAV Authoring Rules**.
14. 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.
15. 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 (step 4 below). 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. On a server operating system, open **Administrative Tools** > **Server Manager**. (On a non-server Windows operating system, skip forward to step 4.)
2. Ensure that the **Server Manager** (top) node is selected, and in the **Security Information** group, click the **Configure IE ESC** link.
3. In the **Internet Explorer Enhanced Security Configuration** dialog, ensure that the **Off** radio button is selected for both **Administrators** and **Users**.
4. Open Internet Explorer and press the `Alt` key to display the Menu bar.
5. Click **Tools**, then **Compatibility View Settings**.
6. Make sure **Display all websites in Compatibility View** and **Display intranet sites in Compatibility View** are both clear.

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 11), 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-au/download/details.aspx?id=34595*; and after installation, continue with the patches below.
   - For Powershell 4.0, see *http://technet.microsoft.com/en-au/library/hh857339.aspx*. 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 11):

   - 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*.

Drivers for Spreadsheet Imports

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 `.xslx` format (the earlier `.xsl` 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 the reconciliation 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.

***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* `.xslx` *format, 64-bit Office cannot be installed on the central reconciliation (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 FlexNet Manager Platform, and select the same again in the following page to differentiate elements of the Suite, if applicable.
3. Click through the link for FlexNet Manager Suite 2014 R3 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 archive here.
   - `FlexNet Manager Suite 2014 R3 Installer.zip`
   - `Database Migration to FNMS 2014 R3.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.

2

Upgrading FlexNet Manager Suite

Topics:

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 2014 R3.

Upgrade/Create Databases

Any existing compliance databases must be upgraded, and 2014 R3 uses mandatory databases that were not required prior to version 2014 R2.

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). With FlexNet Manager Suite 2014 R3, it is now generally recommended to install these as separate databases, and particularly so if you manage FlexNet inventory from 20,000 devices or more. Separate databases are shown in the archiectural diagram in *Design the Final Topography* on page 6.

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).

Note • *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 its 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 `FNMSUsers`) 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. Accounts to list in the security group minimally include:*

- *The operational service account (suggested: `SVC-fnmsservice`)*
- *The installing administrator account (suggested: `FNMS-Admin`)*
- *Any operational account needing to log in to a central inventory beacon installed on your reconciliation server (remember that since the inventory beacon requires administrator privileges to run, this account is both a local administrator on the reconciliation server and a `db_owner`)*
- *Any future back-up administrator accounts needed for the application server.*

1. Create a security group (suggested: `FNMSUsers`), and (optionally) add to it all accounts directly logging into the central application server (or you can add accounts later).
2. Back up your existing FlexNet Manager Suite database.
3. 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`).
4. 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).

   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.
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:

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

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

c) On the database **Properties** dialog, select the **General** tab, and in the **Maintenance** section, check the current collation sequence.

If the collation sequence ends with the codes `_CI_AS`, you may proceed with the installation. Otherwise discuss the collation requirements with your database authorities.

6. Ensure that you have sufficient disk space on the database server for a complete second copy of your database during migration.
7. If you have not already done so, log on to the central application server with a privileged account that:
   - Is a member of the domain where FlexNet Manager Suite and your database server are installed
   - Has administrator privileges on your central application server(s)
   - Has database administrator privileges. (As usual for DBAs, this account must also be in the built-in `SQLAgentUserRole`, as the scripts also create SQL jobs. If this is not already the case, the following command in SQL Management Studio adds the account to the role.)

     ```
     ALTER ROLE [SQLAgentUserRole] ADD MEMBER [accountName]
     ```
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. Open a Command Prompt window, and navigate to your working copy of the migration folder (such as `C:\Temp\FNMSUpdate\Database Migration\FlexNet Manager Platform\Normal`).
10. Run the `mgsDatabaseUpdate.exe` program, using the following syntax:

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

    where:

`-d <databaseName>`	The name of the database to connect to. *Note • If you are currently operating from a new application server that has not previously connected to the database server, this parameter is mandatory. A suggested name is `FNMP`. 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 ComplianceMigration.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

	ComplianceMigration.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\ ManageSoft Corp\ManageSoft\Reporter\CurrentVersion \DatabaseConnectionString (on a 32-bit system, or similar for 64-bit systems) 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.

Tip • *It is normal for the migration to appear to "paus"e at about the 80% mark. At this point the database is busy restructuring for local evidence for applications, and it requires time.*

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 ComplianceMigration.xml -nsu -l mig.log -s MyDBServer\thisInstance -
d FNMP
```

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 22.

11. Open this database in Microsoft SQL Server Management Studio, and grant db_owner privileges to the security group (suggested: FNMSUsers).
12. If you previously changed the setting for the database **Recovery model**, restore the original value now.
13. 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.

14. 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 default 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 22.

15. update the database for Flexera native inventory collection.

Remember • *For a single database, use the same `-d FNMP` parameter as described earlier; or for a separate inventory database (recommended), use a different name as shown below.*

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

```
mgsDatabaseUpdate.exe -i InventoryManagerMigration.xml -nsu -d IM
                      [-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: `FNMSUsers`).

For more information about database validation and remedies, see *Database Validation* on page 22.

16. Are you collecting inventory from Citrix XenApp, and are you locating the staging database on this SQL Server? If so:

a) Locate your downloaded archive `Tier 1 Adapter Tools.zip`, 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 your central database server, and execute it in SQL Server Administration Studio against your chosen database instance.

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 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 operation problems. These kinds of irregularities may occur because:

- The earlier database had previously been changed (either by database administrators or by a Flexera 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 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. Perform this process on:

- Your reconciliation server (in a three server application implementation)
- Your processing server (in a two server application implementation)
- Your application server (in a single server implementation).

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-fnmsservice`).
5. Open the policy `Log on as a batch job`, and add the service account (example: `SVC-fnmsservice`).
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 2014 R3:

1. On the (web) application server, open Windows Explorer.
2. Copy the downloaded archive `FlexNet Manager Suite 2014 R3 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. 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`.
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 reconciliation 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, ensure that **Inventory Server** and **Reconciliation Server** are both deselected; but in fact you can combine the servers in the way that best suits your enterprise.)

   Take note of the installation location for future reference.
6. When asked to enter database names, use the names of the databases you created earlier.
7. If this server includes the reconciliation 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 23).
8. When successful, close the installation wizard.

Update the Inventory Server

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

In a single server implementation, this step is already completed and you should skip ahead to *Configure the System* on page 26.

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 server application installation).

1. On the inventory (or processing) server, open Windows Explorer.
2. Copy the downloaded archive `FlexNet Manager Suite 2014 R3 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`.
5. Select the **Custom** installation path, and do one of the following:

   - For a two server installation, now installing your processing server, select both the **Inventory Server** and **Reconciliation Server** for this installation, and ensure that the **Web Application Server** is deselected (displaying a cross).
   - For a three server installation, now 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. When asked to enter database names, use the names of the databases you created earlier.
7. If this server includes the reconciliation 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 23).
8. When successful, close the installation wizard.

Update the Reconciliation Server

The reconciliation 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 reconciliation server, and the inventory server in one; or
- A two-server application implementation where you have combined the reconciliation and inventory functionality in one server 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 *Configure the System* on page 26.

For a three server implementation, continue this process as administrator (`FNMS-Admin`) on your reconciliation server.

1. On the reconciliation server, open Windows Explorer.
2. Copy the downloaded archive `FlexNet Manager Suite 2014 R3 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`.

5. Select the **Custom** installation path, and select only the **Reconciliation Server** for this installation (ensuring that the other options are deselected).

   Take note of the installation location for future reference.
6. When asked to enter database names, use the names of the databases you created earlier.
7. 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 23).
8. When successful, close the installation wizard.

Configure the System

PowerShell scripts are provided to complete configuration of the central application server(s) and 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. *Web application server*
2. *Reconciliation server (or processing server, for a two-server application implementation)*
3. *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). You should first ensure that these scripts have sufficient authorization to execute, as described in this process:

1. In the case of the reconciliation server (or processing server, or application server, depending on how your servers are consolidated), be sure that the SQL Server Agent service is running on your database server.

   ***Note* •** *By default, SQL Server Agent service is disabled on SQL Server. For on-going operation of FlexNet Manager Suite, please ask your database administrator to ensure that SQL Server Agent is up and running.*

   When this service is running during the installation process, the PowerShell scripts can create the required SQL Server job.
2. 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).

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

3. In the PowerShell command window, execute:

   ```
   set-executionpolicy AllSigned
   ```

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

4. In the PowerShell command window, navigate through the unzipped downloaded archive to the **Support** folder.
5. On each server, execute:

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

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

   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.

6. 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-fnmsservice`*).*
   - *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. Valid examples:*

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

7. Close the PowerShell command window.
8. As required for a multi-server implementation, loop back to step 1 and repeat across a multi-server implementation.

   Tip • *On the application server (or on each component server in a multi-server implementation), the PowerShell scripts configure Microsoft IIS with an application pool for FlexNet Manager Platform. This pool requires authentication, and the scripts save the current logged-in account on each server in the IIS configuration for the application pool. When the user account on any server requires a password update, you must also update the password recorded in the IIS configuration for this application pool. For more information, see Password Maintenance on page 40.*

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

Tip • New functionality in this release, including the recognition of 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 processing server (or application server for a single-server implementation), open a Command Window and navigate to `installation-folder\DotNet\bin\`.
2. Execute `MgsImportRecognition.exe`.

   The utility downloads all libraries according to the terms of your license, and imports them into FlexNet Manager Suite.

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

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 reconciliation server, but first there are permissions to set.
4. In the web interface for FlexNet Manager Suite 2014 R3, 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 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.

5. Using the same account, log into your reconciliation 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.

Configure Web Browsers

Efficient use of FlexNet Manager Suite may required adjusting your web browser settings (especially for Microsoft Internet Explorer).

Assumption: Microsoft IIS is running on your central web application server.

1. In your preferred web browser, navigate to the URL ***server-name-or-IP-address*/Suite/Help/webhelp/index.html**.
2. Expand the table of contents on the left by clicking the book icon to the left of the title.
3. Click **Configuring Your Web Browser**, and follow the guidelines in the column for your preferred web browser.

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.
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.

   a) Check the **Subscription details** on the left-hand side.

   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.
8. Us the **Import** button to browse to the other downloaded file, `FlexNet Manager Suite Web API configuration`, 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 2014 R3.

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. Open the web interface to FlexNet Manager Suite 2014 R3.
2. Navigate through the system menu (⚙ ▼ in the top right corner) > **Accounts**, and ensure that the **Roles** tab is selected.
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 unusual 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 2014 R3, and *must* be updated if you wish to use:

- 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.

In addition, if you are currently running inventory beacons earlier than 2014 R2, other benefits of upgrading to the latest version include:

- Built-in task scheduling
- Self-updating
- Co-location on your central reconciliation 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 14.*

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 accordion 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. 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 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 notes using the **View release notes** 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 Flexera Inventory Beacon software installed in your enterprise. Currently, this must be 2014 R2 (for which choose a version similar to `10.1.1`, with 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 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 `Use 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).*

Activating and Using New Features

Some new features in the 2014 R3 release are available now that you have:

- Updated the inventory server (see *Update the Inventory Server* on page 24)
- Updated the Application Recognition Library (see *Populate the Downloadable Libraries* on page 27)
- Updated your inventory beacons, including setting the global update settings to the latest release (see *Update, and Deploy Additional Inventory Beacons* on page 32 and sub-sections).

With these processes complete, you can immediately take advantage of:

- Advanced VMware inventory collections (subject to having licensed FlexNet Manager for VMware)
- Enhanced recognition for Microsoft Server applications such as Exchange Server, Biztalk, and SharePoint (subject to having licensed FlexNet Manager for Microsoft).

*Tip • Check your licensed options under the system menu (top right corner), **FlexNet Manager Suite License**.*

However, some new features require additional configuration or upgrade:

- XenApp adapter
- XenDesktop adapter.

These 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 32 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 18):

   a) Locate your downloaded archive `Tier 1 Adapter Tools.zip`, 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 *FlexNet Manager Suite Help > Adapters Supplied by Default > XenApp Server Adapter > Setting Up the XenApp Server Adapter > Create Connections for Data Upload*.

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 *FlexNet Manager Suite Help > Adapters Supplied by Default > XenApp Server Adapter > Setting Up the XenApp Server Adapter > Installing the XenApp Server Agent*.

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

   See the adjacent help topic *Create a Scheduled Task*.

   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 32 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 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:

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 the following services (in a single server implementation, all these are on the application server):

- On the web application server, in the IIS Application Pool:
    - **FlexNet Manager Platform**
    - **ManageSoftWebServiceAppPool**
    - **SAP Optimization**
    - **SAPServiceAppPool**
- On the processing server, in the IIS Application Pool: **Flexera Beacon**
- On the processing server, in the **FlexNet Manager Platform** folder for Microsoft Scheduled Tasks:
    - Data warehouse export
    - Export to ServiceNow
    - 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 system status information
    - Import VDI access data
    - Inventory import and license reconcile
    - Recognition data import
    - Regenerate Business Import config
    - Send contract notifications.
- On the processing server, in Services, **FlexNet Manager Suite Batch Process Scheduler**

- On the server where the inventory processing engine runs (typically also the processing server), in the IIS Application Pool:
  - **Flexera Importers**
  - **Flexera Package Repository**

Note that the configuration scripts cannot be run simply to update passwords. The scripts support the following (space separated) flags and use cases:

- 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
  ```

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 Network Service account 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 40.*

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 42.

Update Credentials in IIS Application Pools

To update the password for the FlexNet Manager Platform 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 serve"r, 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 reconciliation 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 reconciliation 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 reconciliation 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.