Installing FlexNet Manager Suite for a Managed Service

Legal Information

Document Name: Installing FlexNet Manager Suite 2018 R1 for a Managed Service

Part Number: FMS-13.0.0-MIG01

Product Release Date: March 30, 2018

Copyright Notice

Copyright © 2018 Flexera. All Rights Reserved.

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

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

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, see http://www.flexera.com/intellectual-property. All other brand and product names mentioned in Flexera products, product documentation, and marketing materials are the trademarks and registered trademarks of their respective owners.

Restricted Rights Legend

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

Contents

1

Installing FlexNet Manager Suite 2018 R1 for a Managed Service

This document describes installation of a multi-tenant version of FlexNet Manager Suite 2018 R1 on the central application server(s) of a managed service provider (MSP). It includes some notes about managing the deployment of FlexNet Beacon software to servers on your customer sites ("inventory beacons"). These inventory beacons are the information-gathering arms of the system that make possible your central management of multiple tenants.

There are significant code and behavioral differences between the single tenant version of FlexNet Manager Suite (for installation on the premises of a single customer) and this multi-tenant version (for installation on the premises of managed service providers supporting multiple customers). If you have prior experience installing the single-tenant version, be sure to read these instructions carefully. A summary of differences is available in What Is Special?.

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 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.

What Is Special?

Installations for MSPs are unique in several ways.

Perhaps you have previously implemented single tenant systems for some of your customers. There are several differences in the processes for a multi-tenant system. The differences are summarized here, with details provided in the following pages as required.

Database server: higher prerequisites, special scripts

The database schema is now partitioned to ensure data separation for your different customers. As a result:

- The minimum database requirement for a multi-tenant system is Microsoft SQL Server Enterprise Edition (since this supports partitioning).
- The installation of databases requires the use of special scripts that support partitioning and multi-tenant data.

> ***Warning:*** *To set up your MSP implementation, you must use the partitioned scripts provided in all cases. Using the scripts in Normal (non-partitioned) mode will result in strange and unrecoverable errors. These can be remedied only removing the failed installation and commencing a new database installation with the correct scripts.*

Special licensing required

The license from Flexera to operate FlexNet Manager Suite is different for a multi-tenant environment. Each tenant must be separately licensed, and activated by the import of the appropriate license issued by Flexera. It is not possible to run a multi-tenant (MSP) system on a single-tenant (on-premises) license. Ensure that your order clearly identifies that you are running a multi-tenant system, and that you require a license for the tenant(s) within that system.

More Active Directory accounts

Running an MSP system requires that you are using Active Directory. In addition to the accounts needed to run the in-house aspects of your system, you also need, within your own Active Directory domain (where your central application servers are running), a separate Active Directory account for each tenant. This account:

- Must be unique for each tenant (it is not possible to reuse the same account for multiple tenants, and attempting to do so results in all those tenants being locked out without warning). This also means that each account must be registered in a Role for exactly one tenant, never more.
- Is used to correlate FlexNet Beacons with each individual tenant (a single account per tenant can authenticate access by multiple inventory beacons within each tenant, if desired).
- Is the account with which the appropriate inventory beacon(s) authenticate access to your central application server(s), allowing inventory beacon uploads of inventory and business data.
- Within your central domain, requires no privileges, since it only uses the HTTPS protocol to transfer data to/from your central application server.
- Must be registered as an account within FlexNet Manager Suite, and that registration process requires that it is assigned to a Role. However, it does not require administrative permissions within FlexNet Manager Suite — membership in a read-only Role in the application is sufficient.
- Is registered on the inventory beacon at installation time, along with its password (so that you might consider creating this account with the “Password never expires” setting).

The installing user is administrator

It is very strongly recommended that a special (and enduring) account is used for installation. In a multi-tenant installation, the account that runs the installation is automatically added as the first operator in the system, as

administrator. As each new tenant is activated (through the import of the appropriate license), this same installing account is also present as the only operator in that tenant's environment.

Therefore, as each new tenant is created and activated, this same installing account must log in to that tenant's environment, and:

- Add accounts for all operators who will access this tenant's system.
- Add the unique Active Directory account for this tenant's inventory beacon(s) to authenticate with the central server.

Operators are not users

With single-tenant systems, operators are created from user records, usually after an import of Active Directory to establish those user records. This has no parallel in your multi-tenant system. (You do not need to import your Active Directory unless you are acting as one of your own tenants, for managing your own software licensing.)

For your multi-tenant system, operator accounts are created directly by the installing user, as described in Identify (or Set Up) Accounts.

No support for Flexera Service Gateway

Flexera Service Gateway allows interaction between separate enterprise products from Flexera in a single-tenant environment. However, Flexera Service Gateway does not support passing a tenant UID when using Windows authentication, and is therefore not supported in a multi-tenant environment as used by managed service providers. The impact is that, if you have customers who already have enterprise products from Flexera installed on their own sites, those systems cannot integrate with your implementation of FlexNet Manager Suite.

All inventory beacons must be free-standing

By way of contrast, in a single-tenant environment, it is recommended to co-install an inventory beacon on the same computer as provides your batch server/reconciliation server functionality.

In a multi-tenant environment (such as for your managed service), this is not supported, and all inventory beacons must be free-standing, installed on servers other than your central application server machines. In the main, each inventory beacon is installed on a customer site, collecting data there and uploading to your application server. The one exception to this if you also want to manage your own licensed software entitlements, in which case you need at least one inventory beacon within your own enterprise; and this must be free-standing, separate from your application server machines.

Managing your own licenses

Your primary goal is to manage license compliance for your customers; but you may also want to use the same system to manage your own license entitlements. To do this, treat your own company as a tenant, including installing your own internal (free-standing) inventory beacon(s) to gather your inventory.

Synopsis and Server Breakdown

The major steps in the installation process are:

1. Verify all prerequisites, including the installing (administrator) account and operational services account.

2. Install all required databases using the multi-tenant scripts, on SQL Server Enterprise Edition.
3. Authorize the service account.
4. Install the web interface on the web application server.
5. Install one or more inventory servers (each can collect FlexNet inventory for around 50,000 devices).
6. If you are implementing a large system, install a separate batch server. (The order of server installation is important.)
7. Use the provided PowerShell scripts to configure the system.
8. Activate one or more tenants on the system.
9. Download the current data libraries.

Thereafter, on a tenant-by-tenant basis, you need remote access to each inventory beacon. With this, you can install FlexNet Beacon software, configure the inventory beacon, and populate the password store with credentials for direct inventory gathering. Finally, using the web interface on your central application server, you establish rules for inventory collection for each tenant.

The following table summarizes which of the tasks in the installation details (from the following chapter) apply to which servers in a multi-server implementation (servers are identified and discussed in Design the Final Topography). A blank means not required; a Y means required, and Y1, Y2, Y3 and Y4 mean required in that order. When the functionality of several of these columns is rolled up in smaller implementations, then a Y in any relevant column means to perform the task on the server covering that functionality. The breakdown of servers in the columns is:

- Web - web application server
- Batch - batch server (sometimes called a reconciliation server)
- Inv - inventory server
- App svr - the application server (when all of the above are combined on a single server, in which case a **Y** in any of the three columns means perform the task on your single server)
- DBSvr - database server
- IB - inventory beacon.

Installation tasks (from following pages) for each type of server:

Tasks/Server:	App svr: Web	App svr: Batch	App svr: Inv	DBSvr	IB
Admin acct	Y	Y	Y		Y
Service acct	Y	Y	Y	Y	Y
DBA acct				Y	
Patch .NET	Y	Y	Y		
Configure IIS	Y	Y	Y		
Disable WebDAV			Y		Y

Tasks/Server:	App svr: Web	App svr: Batch	App svr: Inv	DBSvr	IB
MS ADE (for Excel imports)		Y			Y
Create databases				Y	
Authorize Service acct	Y	Y	Y		
Install web interface	Y				
Install inventory server			Y		
Install batch server		Y			
PowerShell configuration scripts	Y1	Y3	Y4		
Product activation					
Populate libraries					
Set up access rights	Y				
Deploy/configure inventory beacon(s)					Y
Populate password store					Y

The installation processes for each server are fully documented in the following sections. The table below summarizes which *custom* installation options are required for different server configurations. For each installation type, ensure that *only* the options listed are selected when you take the custom installation path.

Tip: *For custom installations, the batch server is called the batch scheduling server in the installer. Regardless of the name, this server includes both the batch scheduling and the batch processing functionality.*

Installation type	Select these custom installation options
Single (full) application server	• **Inventory server** • **Web application server** • **Batch scheduling server**  ***Tip:*** *This is the same configuration as if you step straight through the standard installer without taking the custom installation path.*
A stand-alone web application server	• **Web application server**
A processing server (combining the inventory server and the batch server)	• **Inventory server** • **Batch scheduling server**
A stand-alone inventory server	• **Inventory server**

Installation type	Select these custom installation options
The separate batch processing machine, which must use the batch scheduling server option	• **Batch scheduling server**

Design the Final Topography

If you plan to support a number of customers (tenants), in combination managing large numbers of computer systems, you will need a multi-server installation. If you are starting with a smaller implementation, you could combine the functionality of several servers together for economy; and perhaps you might consider scaling up your implementation as your customer base grows. In any case, it is important to understand the separate functionality available for different servers, and to understand terminology in this document, as explained in this section and the diagram below. Each blue box represents a separate server, and all are given the names referenced throughout this document. Included are some inclusive terms. For example, *application server* means the combination of all the servers inside that box.

Of course, all your central servers are within your MSP Active Directory domain.

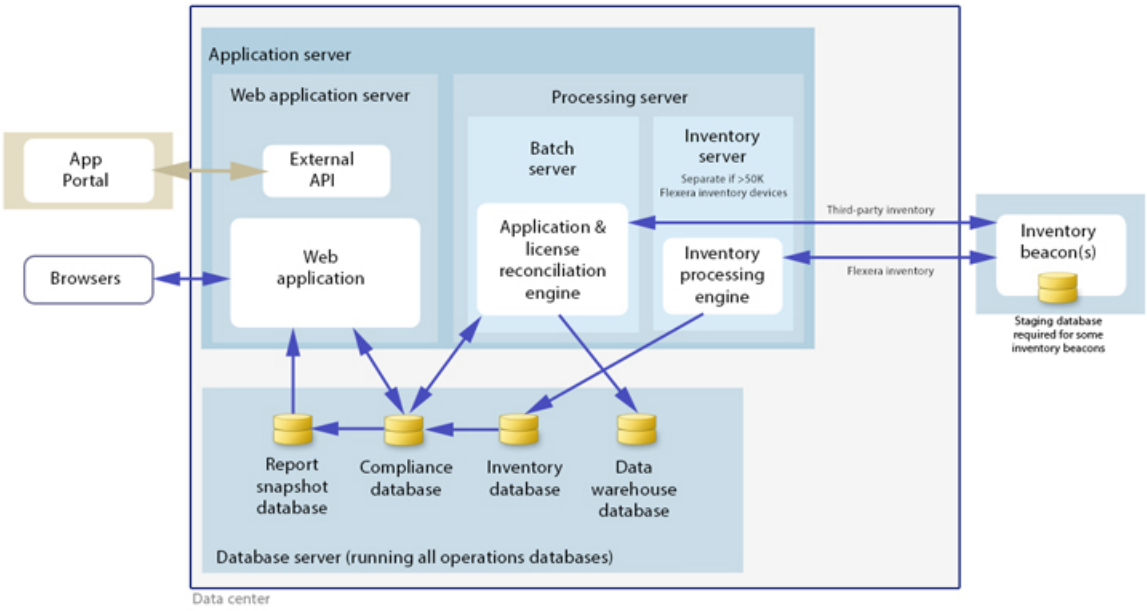
In contrast, the tenant's inventory beacons are located inside the Active Directory domains of each of your customers. This greatly simplifies the access and authentication that each inventory beacon needs to connect to other systems within your customers' sites to collect data.

There are six different kinds of server functionality in a working implementation of FlexNet Manager Suite, shown in the diagram below:

Server type	Scaling	Purpose and notes
inventory beacon (An inventory beacon is a server with FlexNet Beacon software installed.)	Minimum of one for each tenant (customer). ***Tip:*** *If you intend to manage your own software licenses on the same system, you must also install a free-standing inventory beacon within your own domain. Here, "free-standing" means that FlexNet Beacon is installed on a separate device, and not on any of your central application servers.*	An inventory beacon is the data collecting arm of the system. If a customer has a complex computing infrastructure, you may need multiple inventory beacons within that environment. Within each customer, inventory beacons may be deployed in a hierarchy, ensuring that every targeted device will have access to an inventory beacon. For more information, see Considerations for Inventory Beacons.
inventory server	One for (roughly) every 50,000 devices reporting FlexNet inventory.	Collects inventory reported by the FlexNet inventory agent. (Specifically excludes inventory collected by third-party tools like Microsoft SCCM, ILMT, and so on.)

Server type	Scaling	Purpose and notes
batch server (previously known as a reconciliation server.)	Schedules tasks taking into account constraints between process types, and efficiently executes from the resulting queue.	Imports third-party inventory, integrates FlexNet inventory, incorporates business-related information, and reconciles everything to calculate your license position. ***Tip:*** *Currently MSMQ limits the hostname of the batch server to 15 characters (excluding the domain qualifier).*
database server	The four underlying databases may be split across separate database servers if required.	Known collectively as the operations databases, these are: • The inventory database for staging the import of FlexNet inventory • The compliance database where all other imports are stored, and license consumption calculations are conducted • The snapshot database, for performance improvements especially in relation to reporting • The data warehouse, storing time-based content for trend reporting.
web application server		Handles presentation of the web interface to FlexNet Manager Suite.

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



Tip: *When you implement your web application server as a separate server, you must configure one or two network shares that all servers can access to share uploaded data between them. The shared drives are identified during the installation process. For details, see Configure Network Shares for Multi-Server.*

Inventory adapters are elements of the system that connect to other inventory sources, collect data, and map it to the database tables within FlexNet Manager Suite. Some inventory adapters (such as the XenApp adapter, ADDM adapter, and HPUD adapter) require a staging database for preliminary data manipulation. Because of networking and firewall restrictions, such staging databases are typically located within your customer's site. These may be installed on any convenient SQL Server, with one of the options being to install the staging database on an appropriate inventory beacon (increasing the prerequisites for the inventory beacon to include a SQL Server database). If you are using any such adapters to collect your internal inventory, decide on the location of any necessary staging databases as part of your design. For each tenant, this forms part of the planning discussion with the customer.

Choose your web servers per device

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

- Microsoft IIS. Choose this alternative when any of the following apply:
  - The host server is one of your central application servers (web application server, batch server, or inventory server, or combinations as applicable). No web server is required on a stand-alone database server.
  - When 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
  - When you require the use of the HTTPS protocol to encrypt data transfers.
- FlexNet self-hosted web server. Choose this alternative when none of the previous cases apply, and:

- You want simple administration of the web server.
- You want to minimize the installations on your inventory beacon, so that you do not need to install Microsoft IIS.
- Anonymous access, and use of the HTTP protocol, are adequate (for example, within your secure LAN).

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

Output

Prepare a block diagram of the actual servers for your implementation. Start with the central cluster of servers, depending on the scale of your implementation. Also identify the location of the shared network drive that a multi-server implementation uses for file sharing between the central servers.

Don't forget the inventory beacons you intend to deploy on your customer sites.

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

Tip: *Keep in mind that an underscore character is not valid in a host name referenced by a DNS. If you have a host name that includes an underscore, you may need to set up a DNS alias for the server; or else use its IP address during the installation process.*

- 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.

Software Components Summarized

In addition to your installation of FlexNet Manager Suite itself, the following software components are required for your multi-tenant application server(s):

- **Microsoft SQL Server Management Studio**
  This is required only if your database server is separate from your application server *and* you have access permissions to the operations databases. It is helpful for inspecting content at the database level for tracing and debugging.
- **Microsoft Access Database Engine 2010**
  This is required only if:
  - Your batch server or inventory beacon needs to import any spreadsheets in `.xslx` format

- The same server does not already have a 32-bit version of Microsoft Office 2007 or later installed.

  For full details (including the fact that the Excel drivers cannot be the 64-bit version), see Drivers for Spreadsheet Imports.

- **Microsoft PowerShell 3.0 (or higher)**
  This is a requirement for installation of FlexNet Beacon, so that if you are implementing an inventory beacon within your domain for collecting your own internal inventory (not including inventory collected from customer sites), you need to have a recent version of PowerShell. For full details, see Upgrade PowerShell on Local Inventory Beacons. (Remember, an inventory beacon for collecting your own inventory must be installed on a separate (free standing) server, not co-located on your batch server as is possible in single-tenant installations.)

The following software components are suggested for your multi-tenant application server(s):

- **Adobe Reader** for viewing additional PDF documentation (available through the title page of the online help, after the system is installed).
- **Microsoft Office Viewers** and the free `FileFormatConverters.exe` are useful for viewing Microsoft `.xlsx` documents on the application server before importing them.

Secure the Licenses

Each tenant that you will manage must be separately licensed by Flexera. You activate the tenant in a process that includes importing the license file supplied in response to your order.

When preparing your order for each new tenant, be sure to specify that this is a license for a tenant (or an additional tenant) in your multi-tenant system, identifying both the tenant company and your own company.

Order your tenant license(s) now so that they arrive in good time for the activation stage.

Identify (or Set Up) Accounts

There are five types of accounts to consider within your own environment; and additional accounts are necessary within your customer sites, with the number depending on functionality required.

Important: *Correct account privileges (as discussed below) are critical to a successful implementation.*

In-house accounts

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

The following tables list the various privilege levels, their purpose within FlexNet Manager Suite, and a suggested set of Active Directory accounts allowing for that separation of concerns. The three account types described are:

- A database administrator (typically this is an existing database administrator within your enterprise)

- An installing system administrator (account details must be made available to db-admin)
- A service account for normal operations (account details must be made available to db-admin).

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

Table 1: Database administration privileges — suggested AD account: db-admin

Privileges	Required on	Purpose
Database administrator, with `db_owner` rights on all operations databases related to FlexNet Manager Suite (compliance data, warehouse data, snapshot data, and inventory data).	Database servers	Provides the following accounts with database access rights as described.
Member of the **public** database role in the `model` database on the database server.	Database servers	Required so that the account can run scripts that check the database compatibility level.
SELECT rights to the following tables in the **msdb** database: • `dbo.sysjobs` • `dbo.sysjobsteps` • `sysjobs_view`. EXECUTE rights to the stored procedures from the **msdb** database used in the database scripts, including: • `sp_add_job` • `sp_add_jobserver` • `sp_add_jobstep` • `sp_add_jobschedule` • `sp_delete_job`.	Database servers	Only required if an existing installation of FlexNet Manager Suite 2015 or earlier is being migrated to a later release.

Table 2: Installing administrator privileges — suggested AD account: fnms-admin

Privileges	Required on	Purpose
Membership in the `db_owner` role on all operations databases (compliance data, warehouse data, snapshot data, and inventory data).	Database server.	Post-installation, for continuing administration, this account can be reduced to the same privileges as for the service account (described below). However, the standard installation scripts set some database properties (`ARITHABORT`, `QUOTED_IDENTIFIER`) that can only be configured by an account with `db_owner` privileges. Therefore the installing account needs membership in the `db_owner` role at least temporarily during installation.
Local administrator	• Central application server(s) (including, where separated, web application server, batch server, and inventory server); • All inventory beacons.	Installs and configures software on all servers. On inventory beacons, interactive login to the inventory beacon interface also requires local administrator privileges (that is, on inventory beacons this is an operational account as well as being required for setup).
Set the execution policy for, and execute, PowerShell scripts	Central application server(s) (including, where separated, web application server, batch server, and inventory server).	PowerShell scripts are used to complete the configuration of central servers during implementation. Includes an attempt to enable Microsoft Message Queuing, where this is not already enabled.
Create tasks in Windows Task Scheduler	• Central application server(s) (including, where separated, web application server, batch server, and inventory server); • All inventory beacons.	Runs PowerShell scripts during installation that create scheduled tasks.
Internet connection to `https://flexerasoftware.flexnetoperations.com`	A central server (with network access to all other central application servers in a multi-server implementation).	Retrieve product downloads and licenses for implementation.

Privileges	Required on	Purpose
Internet connection to `http://www.managesoft.com` (Typically granted through membership in the `FNMS Administrators` security group in Active Directory.)	The batch server (or, in smaller implementations, the processing server or application server).	Maintenance or unscheduled collection of the Application Recognition Library, the SKU libraries, and the Product Use Right Libraries.

Table 3: Service account privileges — suggested AD account: svc-flexnet

Privileges	Required on	Purpose
Membership in the following fixed database roles: • `db_ddladmin` • `db_datawriter` • `db_datareader`. In addition, the account requires you to `GRANT EXECUTE` permissions on all operations databases (compliance data, warehouse data, snapshot data, and inventory data). ***Tip:*** *In less stringent environments, it may be convenient to give this account membership in the `db_owner` role for the operations databases, which supersedes all of the above.*	Database server	Normal operation (which includes execution of SQL stored procedures).

Privileges	Required on	Purpose
Logon as a Service, and run all FlexNet services ***Tip:*** *Admin access for this account is convenient, and typically granted through membership in the* `FNMS Administrators` *security group in Active Directory; otherwise read, write, and execute permissions are required on all folders containing FlexNet installations, FlexNet data, and FlexNet log files.*	• Central application server(s) (including, where separated, web application server, batch server, and inventory server); • All inventory beacons.	Runs all system operations, including batch services and web services. ***Important:*** *In a multi-server implementation, the same service account must be used on all central servers, and it must be a Windows domain account. This is required for proper functioning of Microsoft Message Queueing between the servers. (A distinct service account may be used for inventory beacons.)*
Logon as a Batch Job	• Central application server(s) (including, where separated, web application server, batch server, and inventory server); • All inventory beacons.	When the service account runs a batch job, this setting means the login is not an interactive user. ***Tip:*** *This is particularly important on the batch server (for authorization details, see Authorize the Service Account).*
Run scheduled tasks as a service account.	• Central application server(s) (including, where separated, web application server, batch server, and inventory server); • All inventory beacons.	Runs scheduled tasks within normal operations.
Run IIS application pools as a service account	• Central application server(s) (including, where separated, web application server, batch server, and inventory server); • Those inventory beacons that are running IIS	Normal operations

Privileges	Required on	Purpose
Internet connection to `http://www.managesoft.com` (Typically granted through membership in the `FNMS Administrators` security group in Active Directory.)	The batch server (or, in smaller implementations, the processing server or application server).	Scheduled collection of the Application Recognition Library, the SKU libraries, and the Product Use Right Libraries.

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

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

As a managed service provider, you must also set up the following accounts within your Active Directory:

1. A minimum of one additional account for every tenant you activate. It is useful to name these accounts by the tenant (say, `FNMS-`*`tenantName`*`-Beacons`).
   - Each such account must be unique to its tenant, and never used for any other. Failure to observe this restriction means that inventory beacons from all affected tenants fail to authenticate. Repairing this situation requires a support call to Flexera; so a careful naming convention is well worthwhile.
   - If a tenant has multiple inventory beacons, you may use the same tenant account for all of these inventory beacons within the one tenant. However, there is no limit to the number of these accounts you create within each tenant, so that you may choose to have a separate account for each inventory beacon if you wish (say, `FNMS-`*`tenantName-beaconName`*).
   - Within your central domain, requires no privileges, since it only uses the HTTPS protocol to transfer data to/from your central application server (consider using a special security group for these accounts to restrict their privileges).
   - Each account's credentials are registered in the appropriate inventory beacon at installation time (along with the URLs the inventory beacon uses to access your application servers), and thereafter the account is used for data transfers from the inventory beacon to the appropriate application server. For this reason, consider creating these accounts with the "Password never expires" setting. (This means that the account is used both for authentication to access your system, and authorization to access data for the particular tenant.)
   - Each account must be registered through the web interface for FlexNet Manager Suite, which requires that they are assigned to a Role. They can be assigned to a read-only Role.

Important: *The service account described previously (say, svc-flexnet) must not be used to authenticate any inventory beacon.*

2. An account for each operator who will interact through the web interface for FlexNet Manager Suite.
   - Each operator account must also be registered within the web interface for FlexNet Manager Suite by the global administrator (suggested: fnms-admin), and assigned to a Role (which sets access rights and permissions).
   - An operator account may be authorized to work on more than one tenant account, and may be assigned to different roles in different tenants, if required.

As an MSP, you also have some additional requirements for the installing administrator account (suggested name: fnms-admin) described in the table above. During installation, this account is automatically registered in the central `Administrator` role within FlexNet Manager Suite, and thereafter *must* be used to set up operators for each of your tenants over time. While the account must therefore be preserved, its privilege levels within Active Directory may change over time:

- During installation of the central system, it needs significant privileges as described in the table above.
- When installation is completed, the account itself must be preserved, but you may (if you wish) remove its elevated privileges within Active Directory. Although it continues as the main member of the `Administrator` role within FlexNet Manager Suite, it no longer requires Active Directory privileges as an administrator on the various central servers.

Tip: *There may be several accounts needing to log in directly to the application server for tasks related to FlexNet Manager Suite, such as manipulating log files, scheduling tasks, and the like (this excludes access through the web interface, which is not relevant to this discussion.) It is often convenient for these accounts to have the same database permissions as the services account on all components of the operations databases: compliance data, warehouse data, snapshot data, and inventory data. A suggested method is to create either a local or Active Directory security group (such as `FNMS Administrators`) and add all such accounts to this group. Then you can, for example, set these permissions by opening each database in Microsoft SQL Server Management Studio, and granting the appropriate privileges to the security group. The procedures are detailed in the topics covering database creation. Accounts to list in the security group minimally include:*

- *The operational service account (suggested: svc-flexnet)*
- *The installing administrator account (suggested: fnms-admin) for post-installation on-going administration (remembering that `db_owner` membership is required temporarily during installation, as described in Identify (or Set Up) Accounts)*
- *Any operational account needing to log in to a central inventory beacon installed on your batch server (remember that, since the inventory beacon requires administrator privileges to run, this account is both a local administrator on the batch server and a `db_owner`)*
- *Any future back-up administrator accounts needed for the application server.*

Accounts within customer sites

Depending on what functionality you wish to offer to your customers, you may also need to arrange for accounts within your customer's infrastructure.

1. On each inventory beacon, you must have an administrator-level account for configuration and management. Several functions (such as connection configuration for data gathering, management of the Password Manager, and the like) can be controlled only locally on the interface to the FlexNet Beacon software. If there is a staging database on the inventory beacon, your administrator account will likely require `db_owner` privileges on this database. Most likely you will want to remotely log in to the inventory beacon, so this account may also need special access through your customer's firewall.
2. Most connections to third-party systems require authentication to collect data. In the main, these credentials are encrypted and stored on the applicable inventory beacon (that is, they stay, and are used, exclusively within the customer's environment). Some customers may provide existing account details for you; others may prefer to set up accounts for the specific purpose of data gathering.

Enable MTS and MSMQ

Microsoft Task Scheduler (MTS) must be enabled on your central application server. If you have a multi-server implementation, Microsoft Task Scheduler must be enabled on at least the batch server and the inventory server. If Microsoft Task Scheduler is disabled, the PowerShell configuration script fails when attempting to create a scheduled task folder, and of course the scheduled task required for server operation are not created. To correct this, enable Microsoft Task Scheduler, and re-run the `Config.ps1` configuration script.

Microsoft Message Queuing (MSMQ) is a messaging service widely available as a component of various Microsoft operating systems. It allows applications running in separate processes, even on separate servers, to enjoy failsafe communications. MSMQ is used as foundational infrastructure for the batch scheduler and batch processor on the central application server (or, in larger systems, the batch server) of FlexNet Manager Suite. Its operation is mandatory on all central servers (whether a single server, or scaled up to separate web application server, batch server, and inventory server) to allow the interactions necessary for batch processing tasks. Where the database server is separate, it is not required on the database server.

FlexNet Manager Suite makes use of the standard facilities of MSMQ, with no customization required. For example, MSMQ may make use of the following ports in operation:

- TCP: 1801, and 389 for version 3.0 and later
- RPC: 135, 2101*, 2103*, 2105* (Port 135 is queried to check availability of the remaining ports. The port numbers marked * may be incremented by 11 if the initial choices are not available when MSMQ initializes.)
- UDP: 3527, 1801.

FlexNet Manager Suite makes no special demands on, nor adjustments to, the use of ports for MSMQ, and uses whatever ports are operational. Please check Microsoft documentation for more information about when various ports are required (for example, https://support.microsoft.com/en-us/kb/178517).

The system requirements for integration with MSMQ are:

- In a multi-server implementation, each server must know the URL of all others (or, on a single-server implementation, `localhost` may be used). This is normally configured by the PowerShell configuration script, described later.
- MSMQ imposes a 15-character limit on the batch server hostname (as noted in the section on design, and elsewhere).

- A single service account should be used in common across all central servers to facilitate the operations of MSMQ. This is also noted in the following section on accounts.

Where MSMQ is already operational on your central servers, no customization is required. Where MSMQ has been disabled or removed:

- When the feature is not installed or is not enabled, the PowerShell configuration script (described later) will attempt to install (if necessary) and enable the Windows feature. This requires that the installing user (see section on accounts, below) has sufficient permissions to allow these actions if required. It also requires that the Windows CAB files are still available to the server.

Tip: *After installing MSMQ, the PowerShell configuration script attempts to create the message queue. If the installation process requires a reboot, this attempt fails, and the script reports* `Message Queueing has not been installed on this computer`. *If you see this message, reboot the server and re-run the same PowerShell configuration script.*

- Alternatively, if the CAB files are still in place, an administrator can manually enable the Windows feature before running (or re-running) the PowerShell configuration script.
- Where CAB files have been removed as part of server hardening for security, MSMQ must be installed following the instructions from Microsoft available through MSDN. The PowerShell scripts can be run (or re-run) thereafter.

FlexNet Manager Suite has been tested with multiple versions of MSMQ, up to and including version 6.3, which is part of Windows Server 2012 R2.

Check Database Collation Sequence

All databases for this system require a collation sequence that is both case insensitive and accent sensitive. This is easiest if they are installed on one or more database instances that have a default collation sequence matching these properties.

Tip: *Remember that the operations databases for a multi-tenant implementation of FlexNet Manager Suite 2018 R1 require Microsoft SQL Server Enterprise Edition. If you have not already implemented this edition, please do so before attempting the rest of the implementation.*

To validate the server's default database collation sequence:

1. In SQL Server Management Studio, locate the SQL Server instance in the **Object Explorer** pane.
2. Right-click the server, and select **Properties** from the context menu.
3. On the server **Properties** dialog, select the **General** tab, and check the current collation sequence.

   If the collation sequence includes the codes `_CI_AS` (for example, `SQL_Latin1_General_CP1_CI_AS`), you may proceed with the installation.

Tip: *Other suffixes like* `_KS` *or* `_WS` *are optional.*

If the server's default collation does not include `_CI_AS`, you can set the collation sequence for each database, as you create it, by right-clicking the new database, selecting **Properties** from the context menu, and choosing the collation on the **Options** tab. Remember that the collation sequence must be *identical* for:

- The compliance database (suggested name: FNMSCompliance)
- The reporting snapshot database (suggested: FNMSSnapshot)
- The data warehouse database (suggested: FNMSDataWarehouse).

For example, if the first of these has the collation sequence called `SQL_Latin1_General_CP1_CI_AS`, then all of them must have the exact same collation sequence. In contrast, the inventory database, when separate (suggested: FNMSInventory), and the Cognos content store may have different collation sequences, provided that these also include the same `_CI_AS` codes. The `tempdb` database (alone) may have any collation sequence, since FlexNet Manager Suite creates the required tables here with the appropriate collation sequence.

Configure .NET and IIS

ASP.NET needs patching, and IIS configuration must be modified for ASP.NET. As well, you must prevent WebDAV from blocking functionality.

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

- web application server
- batch server
- inventory server
- each free-standing inventory beacon that your are installing on your own premises for managing your own inventory collection.

Note: *Inventory beacons have an additional requirement, that PowerShell is at least at version 3.0. Should you wish to upgrade PowerShell to release 4.0, Microsoft also requires Microsoft .NET Framework 4.5 on the same server. Take both these matters into account at the same time.*

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

To configure .NET and IIS on a server:

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 Network Shares for Multi-Server.

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

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

   a. Open Windows Programs and Features.

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

      - If it is 4.5 (or later), skip to step 4.
      - If it is 4.0, continue here.

3. If the .NET version is less than 4.5, upgrade Microsoft .NET Framework to version 4.5 or later.

   For more details, see .

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

5. Change directory to the Microsoft .NET Framework installation folder.

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

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

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

   For Windows Server 2012, use:

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

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

8. On your batch server or inventory server, configure certificates on IIS to enable HTTPS communications from the inventory beacons on your tenants' sites.

   If you are currently working on any of:

   - Your web application server
   - Your batch server
   - A free-standing local inventory beacon (for your own premises) that uses the FlexNet self-hosted web server (and not IIS)

   loop back now and restart this process for the next server on your list. For your inventory server and any local inventory beacon (for your own premises) that is using IIS, continue and disable WebDAV on these devices.

9. Open the IIS settings page. For example:

- On Windows Server 2016, open Server Manager (**Start** > **Administrative Tools** > **Server Manager**). On the Server Manager dashboard, click **IIS** to reveal the server name in the right-hand pane. Right-click the server name, and select **Internet Information Services (IIS) Manager**.
- On Windows 7, navigate to **Control Panel** > **System and Security** > **Administrative Tools**, and double-click **Internet Information Services (IIS) Manager**.

10. In the work pane that opens, expand the server name node (if required), expand **Sites**, and select **Default Web Site**.
11. In the **Home** pane for this site, in the **IIS** group, locate **WebDAV Authoring Rules**.

    Tip: *If it is not present, it is likely that WebDAV is not installed on this server, and your mission is complete.*
12. Right-click the icon, and select **Open Feature**. A pane opens for **WebDAV Authoring Rules**.
13. On the right, in the **Actions** group, there is an option to enable or disable WebDAV.
    - If the link currently says **Enable WebDAV**, do nothing, because your mission is complete.
    - If the link current says **Disable WebDAV**, click the link.
14. Click **OK** to close all applicable dialogs.

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

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

Configure Network Shares for Multi-Server

If you have not already done so, use Windows Explorer to configure the network share drives used by your central servers.

There are two such shares required when you install the web application server on a separate server:

- The data import directory used for handing off any content imported through the web interface of FlexNet Manager Suite (such as one-off inventory spreadsheets) to the batch server for processing (default value: `%ProgramData%\Flexera Software\FlexNet Manager Platform\DataImport\`). It may be on any of your central servers, as convenient in your implementation; and it may be on any drive and any file path. You must configure the share manually in Microsoft Windows.
- The parallel data export folder used to stage data for integration with other systems like FlexNet Manager for Engineering Applications. This is typically located as a peer of the above (default value: `%ProgramData%\Flexera Software\FlexNet Manager Platform\DataExport\`).

You may implement these shares as you see fit.

For added security, you may set up these shares so that they are available to the minimum number of accounts (rather than open to all). From the process of setting up accounts, you are already acquainted with the Active Directory security group `FNMS Administrators`, which minimally contains the operational service account (suggested: svc-flexnet), the installing administrator account (suggested: fnms-admin), and any accounts with

interactive logins to any of your central servers. If you wish, you can restrict these network shares so that they are open only to members of `FNMS Administrators`, with the group providing full control for both daily operations and any required maintenance/troubleshooting.

Configure Internet Explorer

Microsoft Internet Explorer needs configuration.

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

Tip: *Check release notes for supported versions. For example, Microsoft Internet Explorer releases up to and including release 9 are deprecated for FlexNet Manager Suite from 2016 R1.*

To configure Microsoft Internet Explorer:

1. Open Internet Explorer, and navigate to:

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

2. Follow the instructions displayed there for disabling Enhanced Security Configuration.
3. FlexNet Manager Suite attempts to advise Internet Explorer that the website should not be run in compatibility mode. You need follow these steps only if you receive an alert asking you to turn off compatibility mode:
   a. In Internet Explorer, press the Alt key to display the Menu bar.
   b. Click **Tools**, then **Compatibility View Settings**.
   c. Make sure **Display all websites in Compatibility View** and **Display intranet sites in Compatibility View** are both clear.
   d. Add websites that do require compatibility mode to the list of **Websites you've added to Compatibility View**.

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

- URLs to add to your trusted locations
- Recognition of your central server as an Intranet site, and allowing automatic logon
- Javascript must be enabled
- Cookies must be enabled
- Windows authentication must be enabled
- Font download should be enabled for optimum usability of the site
- Any company proxy servers must allow browsers to access to the web application server.

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

Upgrade PowerShell on Local Inventory Beacons

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

Use this procedure now for any inventory beacons you are installing locally, in your own enterprise (not customer sites), to manage your own data gathering for internal license management.

Tip: *This information is repeated later for configuration of inventory beacons in your customer sites.*

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.

To upgrade PowerShell (on your own inventory beacon):

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

   This produces output similar to the following:

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

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

   For example:

   - For PowerShell 3.0, see http://www.microsoft.com/en-us/download/details.aspx?id=34595.
   - For PowerShell 4.0, see https://www.microsoft.com/en-us/download/details.aspx?id=40855.

Drivers for Spreadsheet Imports

You need a driver update if all of the following conditions apply to your future use of FlexNet Manager Suite:

- Your customers (or your own enterprise) will *import* data from spreadsheets (the export of data to spreadsheets is not relevant, and the import of data from CSV [comma-separated values] file is also not relevant)
- The spreadsheets will be Excel spreadsheets in `.xlsx` format (the earlier `.xls` format does not require the driver update; but be aware that this older format limits each spreadsheet to about 65,000 records/rows)
- The `.xlsx` files will be imported to the batch server (or processing server, or application server in a single server implementation).

Tip: *If you are working on an internal inventory beacon that will perform these spreadsheet imports within your own enterprise, you also need updated drivers as described here.*

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

Important: *Only the 32-bit version is supported by the Business Importer 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 batch server (or application server), or on applicable inventory beacons. Naturally, Office documents including spreadsheets prepared on other machines running 64-bit Office can successfully be imported. The limitation is only on co-installation on the same computers.*

Download the Materials

Position yourself on a computer that is accessible from all the central servers you will implement.

To download the installation materials:

1. Use your browser to access the Flexera Customer Community.
   a. On https://flexeracommunity.force.com/customer/CCLanding, use the account details emailed to you with your order confirmation from Flexera to log in (using the **Login** link in the top right).

      Tip: *Access requires your Customer Community user name and password. If you do not have one, use the* `Request Community Access` *link on the login page to request one. Your credentials are configured for access to content you have licensed.*

   b. Select the **Downloads** tab from the row across the top of the page.

      A routing page appears to let you `Access Product and License Center`, displaying lists of products from Flexera.

   c. In the lists of products, identify FlexNet Manager Platform, and click the **Access Above Products** button that is *below* that product name.

      The `Product and License Center` site is displayed.

   d. In the `Your Downloads` section of the `Home` page, click the link for FlexNet Manager Platform.

   e. In the `Download Packages` page, click the link for FlexNet Manager Platform 2018 R1 to access the downloads. (You may need to repeat this action on a second page to access the downloadable files.)
2. Depending on your login account, a click-through license may appear. If so, review the terms, and click **I Agree**.
3. Download the following archives and save to a convenient (network-accessible) location on this computer (such as `C:\temp\FNMSDownloads\`). You may unzip all these archives here.

- FlexNet Manager Suite 2018 R1 `Installer.zip`
- `Adapter Tools.zip`

Tip: *Adapters are ways of connecting to, and importing data from, third party systems. You can build your own adapters as required. Tier 1 adapters are adapters tested and verified by Flexera.*

2

Installation Details

Please work through the following sections *in order*. The database must be installed first, and thereafter for a multi-server installation, the order is important: the batch server/reconciliation server must be installed last in this set, as the scripts here finalize account details across all the servers:

1. The web application server
2. The inventory server(s)
3. The batch server/reconciliation server.

Important: *It is critical that you have attended to all the matters raised in Prerequisites and Preparations before attempting installation.*

Create Databases

FlexNet Manager Suite uses a number of separate databases. While it is possible in smaller implementations to co-install the database server on the application server, an MSP typically installs these on one or more separate database servers.

Important: *If you are using Microsoft SQL Server 2016, ensure that at least SP1 has been installed. This update addresses a defect in SQL Server that triggers a fatal error, as documented in .*

Two important data sets are:

- The main compliance information
- Staging data for inventory collected by FlexNet inventory agents (only, distinct from other third-party inventory sources).

An MSP must install these as separate databases, as described in the steps below. (This contrasts with small, single-tenant implementations, where it is possible to combine these into a single database.) Databases should be created in the order described below, running scripts sequentially and waiting for each one to complete before starting the next.

While scripts are provided, it is typical that these scripts will be inspected and executed by a database administrator (DBA).

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

Important: *There may be several accounts needing to log in directly to the application server for tasks related to FlexNet Manager Suite, such as manipulating log files, scheduling tasks, and the like (this excludes access through the web interface, which is not relevant to this discussion.) It is often convenient for these accounts to have the same database permissions as the services account on all components of the operations databases: compliance data, warehouse data, snapshot data, and inventory data. A suggested method is to create either a local or Active Directory security group (such as `FNMS Administrators`) and add all such accounts to this group. Then you can, for example, set these permissions by opening each database in Microsoft SQL Server Management Studio, and granting the appropriate privileges to the security group. The procedures are detailed in the topics covering database creation. Accounts to list in the security group minimally include:*

- *The operational service account (suggested: svc-flexnet)*
- *The installing administrator account (suggested: fnms-admin) for post-installation on-going administration (remembering that `db_owner` membership is required temporarily during installation, as described in Identify (or Set Up) Accounts)*
- *Any future back-up administrator accounts needed for the application server.*

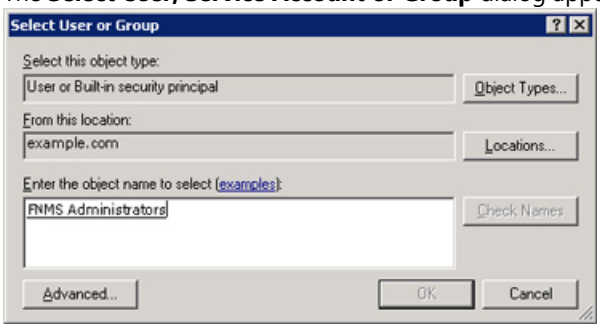
After the first step, the rest of this procedure (creating the databases) must be completed using a database administrator account (suggestion: db-admin, and see the required privileges in Identify (or Set Up) Accounts).

Tip: *While databases are being created, you can start installing the central application servers in parallel. There are no interdependencies until you start running the PowerShell configuration scripts.*

To create all required databases:

1. Create a security group (suggested: `FNMS Administrators`), and (optionally) add to it all accounts directly logging into the central application server (or you can add accounts later).
2. In SQL Server Management Studio, ensure that the AD security group (suggested: `FNMS Administrators`) has a secure login:
   a. Under **Security > Logins**, Create a new login.

   The **Select User, Service Account or Group** dialog appears.



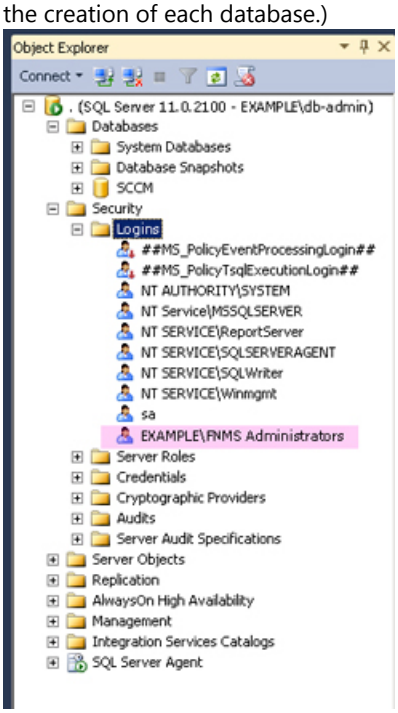
b. Use the **Object Types...** button to ensure that `User, Group, or Built-in security principal` is selected as the object type.

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

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

e. Click **OK**.

The newly added group is visible under the `Security` > `Logins` node. (You will use this group after the creation of each database.)



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

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

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

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

If the collation sequence includes the codes `_CI_AS` (for example, `SQL_Latin1_General_CP1_CI_AS`), you may proceed with the installation.

Tip: *Other suffixes like `_KS` or `_WS` are optional.*

If the server's default collation does not include `_CI_AS`, you can set the collation sequence for each database, as you create it, by right-clicking the new database, selecting **Properties** from the context menu, and choosing the collation on the **Options** tab. Remember that the collation sequence must be *identical* for:

- The compliance database (suggested name: FNMSCompliance)
- The reporting snapshot database (suggested: FNMSSnapshot)

- The data warehouse database (suggested: FNMSDataWarehouse).

For example, if the first of these has the collation sequence called `SQL_Latin1_General_CP1_CI_AS`, then all of them must have the exact same collation sequence. In contrast, the inventory database, when separate (suggested: FNMSInventory), and the Cognos content store may have different collation sequences, provided that these also include the same `_CI_AS` codes. The `tempdb` database (alone) may have any collation sequence, since FlexNet Manager Suite creates the required tables here with the appropriate collation sequence.

4. Enable Microsoft SQL Server Common Language Runtime (CLR) Integration by executing the following stored proceedure:

```
sp_configure 'show advanced options', 1;
                        GO
                        RECONFIGURE;
                        GO
                        sp_configure 'clr enabled', 1;
                        GO
                        RECONFIGURE;
                        GO
```

Note: *By default CLR integration feature is disabled and must be enabled by the DB system administrator before database creation and installation.*

5. On the database server, open a command prompt.

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

6. Navigate in the unzipped archive to the `FlexNet Manager Suite\Database\Partitioned\FlexNet Manager Platform` folder. (The database creation scripts can be run from a mapped network drive.)

Warning: *It is critical that you use the `Partitioned` path. This brings you to the scripts for creating a multi-tenant database.*

7. Create the database for FlexNet native inventory collection.

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

   a. Execute the following (replacing the placeholders *DBserver-name**instance name* with the name of your SQL Server and your database instance):

Note: *The command-line switches (as usual), and the `WindowsNT` argument, are case sensitive.*

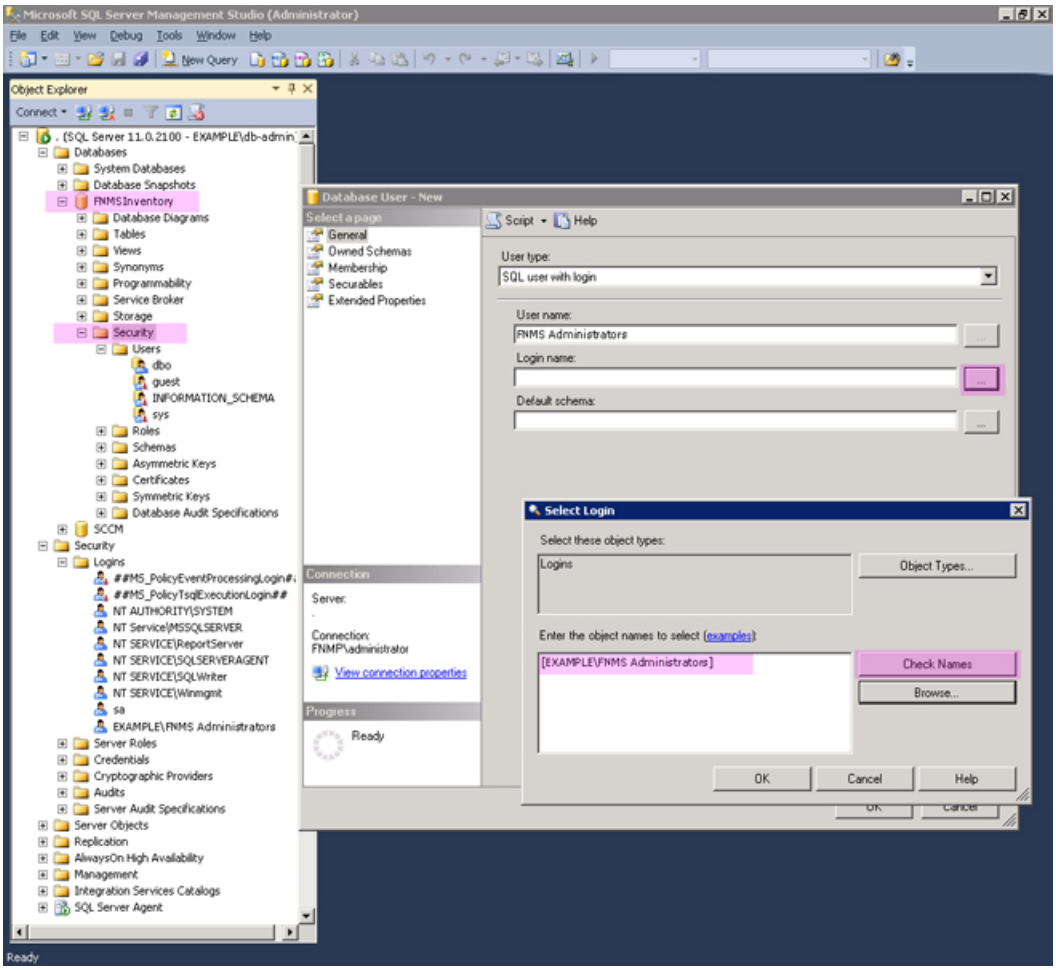
```
mgsDatabaseCreate -a WindowsNT -s DBserver-name\instance name -d
FNMSInventory -i InventoryManagerDatabaseCreation.xml
```

Wait for completion before proceeding.

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

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

d. Next to the **Login name** field, click the ellipsis (**...**) button, and use the **Select Login** dialog to select your Active Directory security group (suggested: `FNMS Administrators`). Click **OK** to close both dialogs.



e. For your newly-added user, right-click and select the properties, and select the `Membership` page. Check the `db_owner` role, and click **OK** .

8. Create the operations database for compliance data (a two-part creation process):

a. Still in the Command Prompt window on the database server, using the administrative account (db-admin), and in the same folder of the unzipped archive, execute the following (replacing the

placeholders *DBserver-name\instance name* with the name of your SQL Server and your database instance, and paying attention to case sensitivity):

```
mgsDatabaseCreate -a WindowsNT -s DBserver-name\instance name -d
FNMSCompliance -i ManageSoftDatabaseCreation.xml
```

(and wait for completion).

b. Execute:

```
mgsDatabaseCreate -a WindowsNT -s DBserver-name\instance name -d
FNMSCompliance -i ComplianceDatabaseCreation.xml
```

c. Repeat the steps outlined for the inventory database to grant `db_owner` privileges to the security group (suggested: `FNMS Administrators`).

9. Create a data warehouse database (used for trend analysis and some product reports):

a. In the same archive folder, execute:

```
mgsDatabaseCreate -a WindowsNT -s DBserver-name\instance name -d
FNMSDataWarehouse -i DataWarehouseCreation.xml
```

b. Repeat the steps outlined for the previous databases to grant `db_owner` privileges to the security group (suggested: `FNMS Administrators`).

c. Strongly recommended for SQL Server 2016 SP1 or later: Set the compatibility level on this database to `SQL Server 2012 (110)` or `SQL Server 2014 (120)`.

10. Create a snapshot database (used for performance optimization):

a. In the same archive folder, execute:

```
mgsDatabaseCreate -a WindowsNT -s DBserver-name\instance name -d
FNMSSnapshot -i SnapshotDatabaseCreation.xml
```

b. Repeat the steps outlined for the previous databases to grant `db_owner` privileges to the security group (suggested: `FNMS Administrators`).

c. Strongly recommended for SQL Server 2016 SP1 or later: Set the compatibility level on this database to `SQL Server 2012 (110)` or `SQL Server 2014 (120)`.

11. Check all database log files for any errors before proceeding with any installation of FlexNet Manager Suite software.

12. Close the command window.

Finally, if you have not already done so, don't forget the add the necessary accounts, including the operational service account (suggested: svc-flexnet) and the installing administrator account (suggested: fnms-admin), to the `FNMS Administrators` security group.

Authorize the Service Account

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

- Your batch server/reconciliation server (in a large-scale implementation with three servers)
- Your processing server (in a two server application implementation)
- Your application server (in a single server implementation).

To authorize the service account:

1. On the appropriate server, log in as an administrator (suggested: fnms-admin).
2. Go to:
   - On Windows Server 2012, **Start** > **Administrative Tools** > **Local Security Policy**
   - On earlier releases of Windows Server, **Start** > **All Programs** > **Administrative Tools** > **Local Security Policy**.
3. Select the **Local Policies** node, and choose **User Rights Assignment**.
4. Open the policy `Log on as a service`, and add the service account (example: svc-flexnet).
5. Open the policy `Log on as a batch job`, and add the service account (example: svc-flexnet).
6. Click **OK**.

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

Choosing the Installation Approach

The materials you have downloaded for your implementation (see Download the Materials) support two broad approaches to installing the server(s) that form the core of your implementation:

- You may step through the installation processes manually, maximizing your control over each step (but perhaps increasing the risk of manual error). For step-by-step instructions for each kind of server, start at Managing Installations Interactively.
- You may prepare a detailed answer file for (each of) your server(s), and then use a provided script to complete the installation(s) for you. This is especially helpful if you want a repeatable process, such as installing first in a test environment and then again in a production environment; or even holding your answer file(s) for re-use with future releases of FlexNet Manager Suite. Because this approach does not require constant interaction during the process, it is called "silent installation", and details start at Managing Silent Installation.

Managing Silent Installation

Your downloaded materials include everything needed to prepare for, and then execute, "silent" or scripted installations of the various server(s) needed in your implementation.

One script (and its support files) may either be used for a single-server implementation, or used repeatedly for a multi-server implementation with only a small configuration difference for each server.

A separate script can also implement Flexera Analytics as part of your implementation.

The instructions in this section assume that you have unzipped the downloaded installer and support files to a file share that is accessible from all the servers you want to configure (as described in Download the Materials). If this is not the case, make a local copy of the *entire* unzipped archive on each server.

Typical workflow for silent installation

Remember: *Databases must exist before you start silent installation (see Create Databases for details).*

Keep in mind the block diagram of servers you planned for your logical application server, as discussed in Design the Final Topography. The summary workflow is:

1. Optionally, set up encryption for credentials to be referenced in the answer file(s) (see Prepare Encrypted Credentials). If you choose not to do this, the relevant account name and password appear in the answer file(s) in plain text.
2. Create an answer file containing all configuration details, based on the sample FlexNet Manager Suite answer file provided (see Prepare the Answer File(s)).
3. Make a copy of the answer file for each server in your block diagram (such as the web application server, the batch server, and the inventory server), and modify the `FEATURES` setting appropriately in the answer file for each server. Of course, if you have designed a single-server implementation, you require only the one answer file.
4. On each of your servers:
   a. Optionally, save the required command-line parameters as PowerShell variables (see Running a Silent Installation).
   b. Provide the correct answer file for this server's functionality.
   c. Run the supplied script with the appropriate command line (see Running a Silent Installation).

   The script completes both the installation and configuration required for each server.
5. For Flexera Analytics, use a similar process:
   a. Customize the answer file, which in this case is an `.xml` file.
   b. Run the specialized script on your Cognos server (see).

Prepare Encrypted Credentials

This task is optional: if you do not wish to encrypt credentials used in the answer file during installation, you may enter them in plain text in the answer file itself (see Prepare the Answer File(s)).

For encrypted credentials, you may use either of two approaches:

- You may use your own RSA or ECDH certificate. The RSA certificates used with this module must allow `Key Encipherment` in their `Key Usage` extension. ECDH certificates must allow the `Key Agreement Key Usage` extension. If you want to use your own certificate, follow the first steps in the process below to validate that the certificate is usable for both encryption and decryption before attempting any installation.
- You can use the process here, along with a supplied PowerShell module, to create both a certificate and a store, along with all the identities required. Provided that you use the same identities on each of your core application servers, you can simply copy the certificate and store to each server as appropriate, where they can be accessed using your configured answer file.

Once credentials are saved in your store, you configure the answer file with store references that allow use of the credentials, without needing to include any password values in the answer file.

Important: *The account that prepares these encryption details in this process must be the same account that subsequently runs the silent installation script.*

To prepare encrypted credentials for the installation process:

1. On the first of your target servers, with mapped share or local access to the downloaded and unzipped installation archive, log in using the account that will complete the installation (suggested: `fnms-admin`).
2. Launch an elevated PowerShell window (that is, in the Windows start menu, right-click PowerShell and select `Run as administrator`).
3. In the PowerShell window, import the supplied `Encryption.psm1` module to this PowerShell session:

   ```
   cd path-to-resources\FlexNet Manager Suite\Support
   Import-Module Modules\Encryption.psm1
   ```

4. If you are using your own RSA or ECDH certificate, verify that your certificate is usable for encryption and decryption:

   For example, the following command works for the certificate we will create in this process, and for your own certificate the command should be similar.

   ```
   Get-KeyEncryptionCertificate -RequirePrivateKey
   ```

   To check on parameters for your own certificate, enter the following at your PowerShell prompt:

   ```
   help Get-KeyEncryptionCertificate -full
   ```

5. If you are not using a certificate prepared earlier, create one now that can be used to encrypt and later decrypt the credentials. Use the following command (indented lines append to the first command, all on one line), which shows recommended values:

   ```
   $thumbprint = New-CredentialCertificate
       -Subject 'CN=FNMS Installation, OU=FNMS, O=Flexera'
       -FriendlyName 'FNMS_Silent_Install'
   $thumbprint
   ```

The first command saves the certificate thumbprint in a PowerShell variable called `$thumbprint`. The last line displays the value of the variable. The newly-created certificate can now be used to generate a certificate store.

6. Use the newly-created certificate to create a new credential store for encrypted identities.

   The command line is:

   ```
   New-CredentialStore -Certificate $thumbprint
   ```

   where `-Certificate` identifies your new certificate by way of its thumbprint saved in the PowerShell variable.

   Tip: *It is possible to specify an optional `-PathToStore` parameter (for example `C:\Credential\fnms.password.store.xml`), but this is not recommended. The default behavior is to save a file named `fnms.password.store.xml` in the secure profile directory of the logged-in user (running the PowerShell session). If you vary either of these, you must continue to specify your custom path/file name in all subsequent commands.*

7. Create the credentials needed in the credential store.

   For each identity in turn, use the following command (all on one line):

   ```
   New-StoredCredential
       -Name 'friendly-name'
       -Username 'username'
       -Password 'password'
   ```

   Each use of this command echoes the `Username` and `Name` values, along with a `StoreReference` of the form `flexera://friendly-name`. Copy the value of each `StoreReference`, and save them for use in the answer file (as described in Prepare the Answer File(s)). You might choose to create separate credentials for each of the following identities; but more common practice is to create one identity for the service account you have created (suggested: `svc-flexnet`, for which see Authorize the Service Account), and then reference that same identity in each of the following set:

   - `SuiteAppPoolUser`
   - `ExternalAPIAppPoolUser`
   - `BeaconAppPoolUser`
   - `BusinessReportingAuthUser`
   - `ReconciliationScheduledTaskUser`
   - `RLAppPoolUser`
   - `DLAppPoolUser`
   - `InventoryScheduledTaskUser`.

8. If you are preparing a multi-server implementation, and you wish to use the same encrypted credentials on each of your servers:

a. Export your certificate with the following command that references its thumbprint:

```
Export-CredentialCertificate $thumbprint -Path c:\path-on-disk\
SilentInstall.pfx
```

where the `-Path` parameter is optional to identify the file path and file name for saving the certificate. If omitted, the path defaults to the working directory of the current PowerShell session.

b. Copy both the exported certificate (suggested: `SilentInstall.pfx`) and credential store (default: `fnms.password.store.xml`) together to a temporary location on the other target servers.

c. On each server in turn, install the certificate into the Windows certificate store by providing the path to the local copy:

```
Install-CredentialCertificate -Path
C:\temporary-path-on-disk\SilentInstall.pfx
```

d. Validate that you are able to retrieve credentials from the store using the following command:

```
Get-StoredCredential -PathToStore
C:\temporary-path-on-disk\fnms.password.store.xml
```

This command lists all the credentials in the store. The `Username` field is only populated if the certificate is safely located on the same server.

e. Relocate the store in the correct working directory (the local application data store under the profile directory for the installing account).

In PowerShell, the shorthand way to do this is:

```
mv C:\temporary-path-on-disk\fnms.password.store.xml $env:LOCALAPPDATA
```

When the credential store and certificate are correctly installed, and identifying all credentials required on each of your servers, you are ready to customize your answer file.

Prepare the Answer File(s)

An answer file provides all the details required for installation of your server(s).

Tip: *If you miss a setting from the answer file that is required for one of your servers, a dialog box appears during the installation process to request the missing value.*

To customize your answer file:

1. From your downloaded and unzipped archive, and using a flat text editor, open the following file:

```
drive-and-path\FlexNet Manager Suite\Support\sample-fnms-answer.txt
```

2. Save a working copy on your local drive for editing.

It may be helpful in a multi-server implementation to use a file naming convention that identifies which server this answer file copy is intended for.

3. If you have set up encryption for credentials used in this answer file, uncomment (by removing the leading hash or pound character) both the `Security` section header and the `Store` parameter, providing the path and file name for your credential store on this server:

   Example:

   ```
   [Security]
   Store = drive:\path-to-file\fnms.password.store.xml
   ```

4. Adjust the `FEATURES` parameter to suit the type of server being installed and configured. (Come back and adjust this value for each server in a multi-server implementation, saving a separate answer file for each server type.)

   Use one (or more) of the following values, depending on the server type:

Server type	Value
Single-server implementation	Use either of: • `ALL` • `FleNetManagerPlatform` Alternatively, you may list all of the following component identifiers, separating each with a comma and space.
The web application server	`WebUI`
The batch server	`BatchScheduler, BatchProcessor` (Use both labels on your batch server.)
The inventory server	`InventoryServer`

Tip: *Although these notes continue to provide guidance about which parameters apply to which server type, the remaining values in the answer file may all be completed in a single editing pass. The controlling script extracts only the parameters required for each server type, as declared by the `FEATURES` parameter that you have just customized. Therefore, other than configuring the `FEATURES` parameter for each server type, the remainder of the answer file is portable across the various types of server that you may be installing.*

5. The four settings for directories (in the middle of the `[Installation]` section) may be left commented out if you are satisfied with the default values; or else you may uncomment the parameter and add a fully qualified path.

   The parameters, the server type applicable for each one, and the default values are as follows:

Parameter	Applies to	Default/Comments
INSTALLDIR	All server types	C:\Program Files (x86)\Flexera Software\FlexNet Manager Platform\
DATAIMPORTDIR	The batch server, and web application server	C:\ProgramData\Flexera Software\FlexNet Manager Platform\DataImport\
WAREHOUSEDIR	Inventory server	C:\ProgramData\Flexera Software\Warehouse\
INCOMINGDIR	Inventory server	C:\ProgramData\Flexera Software\Incoming\

6. When prepare the answer file is for your batch server, do one of the following:
   - If you have implemented a credential store, uncomment the `BatchProcessStoreReference` parameter and provide the store reference for this credential. (When you provide a store reference, any values in the `BATCHPROCESSUSERNAME` and `BATCHPROCESSPASSWORD` are ignored.)
   - Otherwise, complete the values for the `BATCHPROCESSUSERNAME` and `BATCHPROCESSPASSWORD` parameters, identifying the service account (example: `svc-flexnet`) you already configured (see Authorize the Service Account).
7. For the following set of identities, do one of the following for each separate `[Identity]`:
   - If you have implemented a credential store, uncomment the `StoreReference` parameter and add the store reference for the credential. (When you provide the store reference, any values for `Username` and `Password` are ignored. Be certain not to modify the `Name` parameter that specifies the purpose for each identity.)
   - Otherwise, insert the account name and password for each identity. This is normally the service account (example: `svc-flexnet`) you already configured (see Authorize the Service Account). Recommended format for the `Username` parameter is *`domain\username`*, such as:

     ```
     Username = exampleDomain\svc-flexnet
     ```

All the identities for which the name includes "Pool" are used to configure Microsoft IIS on the respective server. Two others are used to run scheduled tasks. The identities and the server type to which they apply are:

Identity names	Apply to
SuiteAppPoolUser ExternalAPIAppPoolUser	The web application server

Identity names	Apply to

`BeaconAppPoolUser`
`BusinessReportingAuthUser` (also for IIS configuration)
`ReconciliationScheduledTaskUser`
	The batch server

`RLAppPoolUser`
`DLAppPoolUser`
`InventoryScheduledTaskUser`
	The inventory server

8. The `[Parameters]` section gives the servers in a multi-server implementation information about accessing each other, and are also used with Microsoft Message Queueing (MSMQ). In a single server implementation, you still need to provide these values, even though they refer to functionality on the same physical server. You do not need to specify the web application server here, as this is the component that manages intercommunication, once it receives these other values.

   For `ReconciliationServer`, enter the fully qualified hostname of your batch server ("reconciliation server" is a legacy name for the batch server); and enter a full URL for the same server in `ReconciliationServerURL`. For your inventory server, only the URL version is required.

   Tip: *In a single server implementation, in the URL versions you may use `Localhost` within the URL.*

9. Identify the database server and database names with which each of your implementation servers must communicate. For your on-premises implementation, use the "single database group setup".

   In all but the largest implementations, the databases all run on the same database server, so that the values for these four "DatabaseServer" names are identical. (You may, of course, vary the values if you have implemented multiple separate database servers.) Use the same format for identifying your database server as would appear inside a connection string. For example, if your database server hosts multiple database instances, and your operations databases are not in the default instance, use a format like:

   ```
   serverName\instanceName
   ```

   The suggested database names proposed in Create Databases are:

   ```
   FNMSDatabaseName = FNMSCompliance
   IMDatabaseName = FNMSInventory
   DWDatabaseName = FNMSDataWarehouse
   SnapshotDatabaseName = FNMSSnapshot
   ```

10. Save your edited answer file.

11. For a multi-server implementation, re-edit the values for the `FEATURES` parameter (near the top of the file) to suit each different target server, and save a renamed copy that follows your file naming convention linking the answer file with the target server type. Ensure that each answer file is accessible from its intended target server.

Important: *The supplied sample answer file does not contain an* `ADDLOCAL` *parameter, because this parameter is now deprecated. Do not re-insert this parameter into your answer file, since this forces legacy behavior which limits the flexibility of multi-server implementations.*

Running a Silent Installation

Before running the silent installation:

- All related database must exist (see Create Databases)
- If you are encrypting identities needed in the installation, you must have configured and distributed both the certificate store and the certificate validating those identities (see Prepare Encrypted Credentials)
- You must have prepared the local copy of the answer file, correctly configured for the type of server undergoing installation (see Prepare the Answer File(s))
- From the current server, you must have access (either through a network share, or using a local copy) to the *complete* unzipped archive of the installation resources (do not attempt to extract portions, as many scripts and files interact in this process).

When all is ready, triggering a silent installation is a simple matter of invoking the supplied PowerShell script with the correct parameters. The command line can optionally be simplified by first declaring some PowerShell variables to contain those parameters.

To configure variables and trigger silent installation:

1. Ensure that you are running an elevated PowerShell session (that is, started with the `Run as administrator` option).
2. Optionally, declare PowerShell variables to contain the various parameters.

   This simplifies the final command line. Declaring PowerShell variables is as simple as identifying them (with a leading dollar sign) and their values at the command prompt. All parameters for this script default to the string type; but if you are cautious, you can also enforce the cast to the string type by prepending the `[string]` literal before the variable name. Therefore both of the following forms of variable declaration are acceptable:

   ```
   $greet = "Hello"
   [string]$greet = "Hello"
   ```

   The following parameters are mandatory for the command line you will use later, and may be declared as string variables in the above manner. Of course, the suggested variable names can be modified to suit your preferences, as long as you reference them accurately in the command line. Remember to enclose the path values in double quotation marks:

Required Argument	Description
`$FnmpInstallerMsi`	Fully qualified path to the installation `.msi` for FlexNet Manager Suite. This is typically: `drive-and-path\FlexNet Manager Suite\Installers\FlexNet Manager Suite\FlexNet Manager Suite Server.msi`
`$AnswerFile`	Fully qualified path to the answer file that you have customized and saved for this server. Once again, check that this answer file has the correct setting for the `FEATURES` parameter, as this entirely determines the kind of server that is installed on this device.
`$FNMSConfigFile`	Fully qualified path to the Configuration file to be passed to `Config.ps1`. This is typically: `drive-and-path\FlexNet Manager Suite\Support\Config\FNMS Windows Authentication Config.xml`

In addition, the following parameter is optional, and is relevant only for second and subsequent attempts at installation on this server:

Optional Parameter	Description
`$configMode`	If present, must have one of the following two string values: • `updateConfig` (default) — Modifies the installation only with new settings that have been changed in the answer file • `forceUpdateConfig` — Overwrite all settings for this installation.

3. Enter the command line to trigger the installation script.

Caution: *The order of parameters is critical. There are no keys or labels to indicate which parameter is which.*

This example uses the three mandatory parameters as saved in the PowerShell variables suggested above:

```
cd drive-and-path\FlexNet Manager Suite\Support
.\InstallFNMS.ps1 $FnmpInstallerMsi $AnswerFile $FNMSConfigFile
```

This example shows the full text for the paths used in the correct order (normally all on the same line, but here formatted for easier reading):

```
cd drive-and-path\FlexNet Manager Suite\Support
.\InstallFNMS.ps1
     "drive-and-path\FlexNet Manager Suite\Installers\FlexNet Manager Suite\
FlexNet Manager Suite Server.msi"
     "drive-and-path\FlexNet Manager Platform\Support\answerfile.txt"
```

```
    "drive-and-path\FlexNet Manager Suite\Support\Config\FNMS Windows
Authentication Config.xml"
```

The installation is triggered, and immediately followed by configuration appropriate to this server type.

Remember: *If a required parameter is missing from the answer file, a dialog appears during the process to request the missing value.*

Managing Installations Interactively

The following topics provide step-by-step instructions for interactively managing installations of the server(s) you have planned to configure in your implementation of FlexNet Manager Suite. (Obviously, if you have already completed silent installations of your servers, skip this entire section and all the topics it contains.)

Instructions for a single-server implementation are included in the first topic, Install the Web Interface. For multi-server implementations, continue through the following topics as appropriate.

Install the Web Interface

The web interface provides the user interface to manage the inventory and license positions for your customers. Continue this process as administrator (fnms-admin) on your web application server.

To install the web interface:

1. On the (web) application server, open Windows Explorer.
2. Copy the downloaded archive `FlexNet Manager Suite 2018 R1 Installer.zip` from your staging location to a convenient location on this server (such as `C:\temp`), and unzip it.

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

3. Navigate in the unzipped archive to the `FlexNet Manager Suite\Installers\FlexNet Manager Suite` folder.
4. Start (double-click) `setup.exe`.

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

5. Step through the installer. When asked for the **Setup Type**, select the **Custom** installation path, and select the **Web Application Server** for this installation.

(If, as usual for an MSP, this is the *only* functionality on this server, also ensure that **Inventory Server**, **Reconciliation Server**, and **Batch Processor** are all deselected; but in fact you can combine the servers in the way that best suits your business requirements, so make the selection that matches your server plan.) Take note of the installation location for future reference.

6. When asked for the staging folder, or the data import directory, provide the locations for these two shares that you determined in Configure Network Shares for Multi-Server.
7. When successful, close the installation wizard.

Install the Inventory Server

The inventory server processes all inventory collected (or augmented) by the FlexNet inventory agent, and uploaded through inventory beacons on your customers' sites.

Continue this process as administrator (fnms-admin) on your inventory server.

To install the inventory server software:

1. On the inventory server, open Windows Explorer.
2. Copy the downloaded archive `FlexNet Manager Suite 2018 R1 Installer.zip` from your staging location to a convenient location on this server (such as `C:\temp`), and unzip it.
3. Navigate in the unzipped archive to the `FlexNet Manager Suite\Installers\FlexNet Manager Suite` folder.
4. Start (double-click) `setup.exe`.

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

5. Select the **Custom** installation path, and 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 for the staging folder, or the data import directory, provide the locations for these two shares that you determined in Configure Network Shares for Multi-Server.
7. When successful, close the installation wizard.

Install the Batch Server

The batch server is the integration point that correlates all the license entitlement records you collect from your customers with the consumption revealed in inventory to work out their reconciled license positions.

For an MSP that services multiple customers, at least a separate batch server is recommended. However, if you have chosen a two-server application implementation, where you have combined the batch server and inventory server functionality on one computer and kept the web application server as a second server, you do not need

this process. In this unusual case, this step is already completed and you should skip ahead to Installing a Free-Standing Studio.

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

Tip: *Currently MSMQ limits the hostname of the batch server to 15 characters (excluding the domain qualifier).*

To install the batch server software:

1. On the batch server, open Windows Explorer.
2. Copy the downloaded archive `FlexNet Manager Suite 2018 R1 Installer.zip` from your staging location to a convenient location on this server (such as `C:\temp`), and unzip it.
3. Navigate in the unzipped archive to the `FlexNet Manager Suite\Installers\FlexNet Manager Suite` folder.
4. Start (double-click) `setup.exe`.

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

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

   Take note of the installation location for future reference.
6. When asked for the staging folder, or the data import directory, provide the locations for these two shares that you determined in Configure Network Shares for Multi-Server.
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).
8. On the same page of the wizard, for **Server type**, choose either **Production** for your main server installation, or **Failover** if this is a stand-by or testing server.

   Tip: *On your **Production** server, the batch scheduler and batch processor are automatically started as part of the installation process, while on a **Failover** server, both are disabled by default. If you need to switch between your production and stand-by servers, you must manually:*

   - *Disable the batch scheduler and processor on the product batch server*
   - *Enable the batch scheduler and processor on the standby batch server.*

   *These adjustments are made in the **Microsoft Services** control panel.*
9. When successful, close the installation wizard.

Configure the System

PowerShell scripts are provided to complete configuration of the central application servers, including their connections to the databases, and then store appropriate values in the database. Do not run the PowerShell scripts on your separate database server. Run them on your central application servers, and they MUST be run in the following order:

1. web application server
2. batch server (or reconciliation server)
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.

To configure the system using PowerShell scripts:

1. Check that Active Directory domain policy, and (where domain policy is correctly set) local machine policy, both have the security setting `Network access: Do not allow storage of passwords and credentials for network authentication` set to `Disabled`.

   This check is required for:

   - Your batch server (or server hosting that functionality)
   - Your inventory server(s)
   - Later, any inventory beacons that you will operate using a service account (rather than running them as local SYSTEM).

   This setting is available in either domain policy or local security policy under **Security Settings > Local Policies > Security Options**. By default, the majority of Windows installations leave this setting disabled; but it may be enabled in tightly-secured environments. However, please note the following mandatory requirements:

   - This setting *must* be disabled to allow the PowerShell scripts to configure the scheduled tasks and the accounts that run them during operation (or, on inventory beacons, to allow storing credentials for any service account). If it is not disabled, the PowerShell scripts fail at `Executing step Configure scheduled tasks` with the error `Exception has been thrown by the target of an invocation`.
   - Furthermore, the setting must *remain* disabled for normal operation. If this setting is re-enabled, scheduled tasks with saved credentials will fail to run, showing the error `Logon failure: unknown username or bad password. (0x8007052E)` in the Task Scheduler interface. (However, saved credentials are not lost: disabling the setting again allows the scheduled tasks to resume as normal.)
   - Therefore, in any environment where it is mandatory for this setting to be enabled, an alternative task scheduling technology must be provided to allow operation of FlexNet Manager Suite (such as BMC Control-M, or other alternatives).

Note: *If you make this change to policy, a reboot of the server is required.*

2. On your web application server, batch server, or inventory server, ensure that Microsoft IIS is running again:
   a. Ensure that your **Server Manager** dialog is still open.
   b. In the left-hand navigation bar, expand **Roles** > **Web Servers (IIS)**, and select **Internet Information Services**.

      The IIS page is displayed.
   c. In the **Actions** panel on the right, select **Start**.

      A message like `Attempting to start...` appears. Note that it can take some time before the service is started. When the service is running, the PowerShell scripts can update the IIS configuration as required.
3. Run PowerShell as administrator (use the 64-bit version where available):
   a. Locate PowerShell. For example:
      - On Windows Server 2012, **Start** > **Windows PowerShell**
      - On earlier releases, in the Windows Start menu, find **All Programs** > **Accessories** > **Windows PowerShell** > **Windows PowerShell** (this is the 64-bit version; the 32-bit version is `Windows PowerShell (x86).`).
   b. Right-click, and choose **Run as Administrator**.

      Important: *It is critical that you run the PowerShell scripts with administrator privileges. Otherwise, scripts will fail.*
4. If you have not already done so, in the PowerShell command window, execute:

   ```
   set-executionpolicy AllSigned
   ```

   Respond to the warning text with the default `Y`.
5. In the PowerShell command window, navigate through the unzipped downloaded archive to the **Support** folder.
6. On each server, execute:

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

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

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

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

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

Tip: *Helpful notes:*

- *Use the service account details you created earlier (example: svc-flexnet).*
- *Separately on each dialog, the check box* ***Use the same credentials for all identities*** *copies the account details from the upper section to the lower section of the dialog.*
- *For externally visible URLs, you can specify either HTTP or HTTPS protocol, and either the flat server name or the fully qualified domain name is supported. Any port number is optional. Remember that site bindings may be required if you are using the HTTPS protocol (see above). Valid examples:*

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

- *If you have a single-server implementation, when asked for the hostname of the different server functionality, use* `localhost`.
- *Remember that in a multi-server implementation, MSMQ limits the hostname of the batch server to 14 characters. Of course, this limit applies to the hostname itself, and not to the fully-qualified domain name of the host. (If your batch server is already implemented with a longer hostname, consider using a DNS alias that satisfies this limitation.)*

Important: *Remember to use the fully-qualified domain name (in the style of* `serverName.example.com`*) when identifying servers in a multi-server implementation. Do not use a URL.*

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

8. Close the PowerShell command window.
9. If this is your batch server (or the server hosting that functionality), ensure that the services for FlexNet Manager Suite Batch Process Scheduler are running:
   a. Navigate to Start > **Control Panel** > **Administrative Tools** > **View local services**.

The **Services** dialog opens.

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

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

10. As required for a multi-server implementation, loop back to step 1 and repeat across your remaining servers.

Tip: *On each central application server, 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.*

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

- Use without a flag to add a configuration file to a new installation; or on an existing implementation, to remove all customizations and replace the `%ProgramFiles(x86)%\Flexera Software\FlexNet Manager Platform\WebUI\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, 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, 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 `%ProgramFiles(x86)%\Flexera Software\FlexNet Manager Platform\WebUI\web.config` file before using Windows Programs and Features to uninstall FlexNet Manager Suite:

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

Installing a Free-Standing Studio

You can install additional copies of the Business Adapter Studio.

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

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

- The Inventory Adapter Studio is also available on the web application server (or, in smaller implementations, the server providing that function). This works in connected mode.
- You can co-install an inventory beacon on your web application server. As always, this also installs the Business Adapter Studio, giving it (and adapters built there) additional privileges to access your central database in connected mode.

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

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

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

To download and install an additional instance of the Business Adapter Studio:

1. Use your browser to access the Flexera Customer Community.
   a. On https://flexeracommunity.force.com/customer/CCLanding, use the account details emailed to you with your order confirmation from Flexera to log in (using the **Login** link in the top right).

      Tip: *Access requires your Customer Community user name and password. If you do not have one, use the* `Request Community Access` *link on the login page to request one. Your credentials are configured for access to content you have licensed.*

   b. Select the **Downloads** tab from the row across the top of the page.

      A routing page appears to let you `Access Product and License Center`, displaying lists of products from Flexera.

   c. In the lists of products, identify FlexNet Manager Platform, and click the **Access Above Products** button that is *below* that product name.

      The `Product and License Center` site is displayed.

   d. In the `Your Downloads` section of the `Home` page, click the link for FlexNet Manager Platform.

   e. In the `Download Packages` page, click the link for FlexNet Manager Platform 2018 R1 to access the downloads. (You may need to repeat this action on a second page to access the downloadable files.)

2. In the list of components to download, select `Business Adapter Studio releaseNumber.zip`, and download and save it to a convenient location (such as `C:\Temp`).
3. In Windows Explorer, navigate to the downloaded archive, right-click, and choose **Extract All**.
4. Navigate into the unzipped archive, and double-click `setup.exe`, following the instructions in the installation wizard.

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

- The Business Adapter Studio executable: `BusinessImporterUI.exe`
- Default installation path (in connected mode on central server): `C:\Program Files (x86)\Flexera Software\FNMP Business Adapter Studio`
- No template file storage is required for the Business Adapter Studio in connected mode, as it validates the database schema directly. Your custom business adapters may be saved in the folder(s) of your choice.

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

Product Activation

In a multi-tenant implementation, each tenant must be separately licensed by Flexera. You activate each tenant by importing the appropriate license issued by Flexera. Ensure that each order for a tenant license clearly identifies that you are running a multi-tenant system, and that you require a license for a specified tenant within that system. Details of the tenant's license are emailed to you as part of the order confirmation process.

Tip: *To activate your implementation for testing and validation, prior to working directly with any of your tenant customers, you can either:*

- *Use the tenant license for your own company (where you will manage your own software licensing as a tenant company within your managed service)*
- *Ask your Flexera partner manager to secure a test license key.*

Enter the licenses you are currently holding now. You can re-run this process later to load additional tenants as you receive the licenses for them.

Tip: *Certain product options may be activated by the licenses available in your multi-tenant system. For example, if tenant A is not licensed for the FlexNet Manager for IBM option, but tenant B is, this option becomes available on your system only after the license for tenant B is imported. Further, the licensed options determine which libraries are downloaded and made available on your system (as described in Populate the Downloadable Libraries). For these reasons, it is convenient to import all available tenant licenses at this time.*

Continue this process as administrator (fnms-admin), on the batch server.

To activate FlexNet Manager Suite:

1. On the batch server, save a copy of each license in a convenient folder (such as your installation folder), where it is accessible for this activation process.
2. In Windows Explorer, navigate to the *Installation-Dir*\DotNet\bin folder.

   Replace *Installation-Dir* with your installation folder. The default location is `C:\Program Files (x86)\Flexera Software\FlexNet Manager Platform\DotNet\bin`.
3. Execute (double-click) `ManageSoft.Activation.Wizard.exe`.
4. In the **License and Tenant Management** window, click **New Tenant...**.

   The **Product Activation Wizard** appears.
5. Click **Import License...**, and browse to and select the `.license` file.
6. In the confirmation dialog, click **Yes**.

   The license is imported, and the **Product Activation Wizard** displays the key details. Click **Details...** for further information, including licensed product options and the `MaxManagedDevices` value.

Repeat this process for each tenant license. Use the same process to replace a license to extend the end date, or for licensed feature upgrades.

Populate the Downloadable Libraries

FlexNet Manager Suite comes with an Application Recognition Library, a SKU (stock keeping unit) Library. You may also have AppAtlas Service Life product and several Product Use Rights Libraries (depending on which products you have purchased for the suite). These are updated regularly by Flexera and normally downloaded automatically.

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

- *For the ARL:* `https://www.managesoft.com/support/Compliance/RecognitionAfter82.cab`
- *For the EOSL:* `https://www.managesoft.com/support/Compliance/EOSL.cab`
- *For the SKU library:* `https://www.managesoft.com/support/Compliance/PURL.cab`

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

If neither direct access nor access through a proxy server can be provided, you can use an alternative process to managed library updates manually (see the following topic).

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

***Tip:** The downloaded library data is global, available in common for all of your tenants alike. Each tenant's product options (such as access to FlexNet Manager for IBM, FlexNet Manager for Oracle and others) are enabled by the terms of the individual tenant license. Separate libraries support different product options, and are downloaded only when the license terms for those options have already been imported (see Product Activation). If you later activate more tenants for additional product options not previously included in your implementation, the new options are available only after the next library download. To avoid delay, you may re-run this process after the import of any new tenant licenses.*

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

To initialize the downloadable libraries:

1. On the batch server, open the Microsoft Task Scheduler.
2. Manually run the **Recognition data import** scheduled task.

   By default this task is run at 1am daily. The task places a request for download in the queue of the internal batch scheduler. Given that no other processes are running at this stage of your implementation, it executes almost immediately.The utility downloads all libraries required by the union of all terms of the tenant licenses so far installed (see Product Activation), and imports them into FlexNet Manager Suite. Typically for a first download, this may take in the order of a half an hour.
3. Thereafter, in the web interface for FlexNet Manager Suite, navigate to the system menu (▼ in the top right corner), select **System Health > System Health Dashboard**, and check the cards for:
   - **ARL**
   - **SKU Library**
   - **PURL**.

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

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

Manual Updates of Library Data

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

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

- Subscribe to the Content Library Updates email list through the webpage http://learn.flexerasoftware.com/SLO-FMS-Software-Content-Library-Updates. List members receive email notifications when updates to library data are published.
- On your applicable server, navigate to the Microsoft Task scheduler and disable the **Recognition data import** task (in the **FlexNet Manager Platform** group).
  This prevents the server from attempting to connect to the Internet to start downloads.
- Ensure that you have a User Name and Password for the Flexera Customer Community. If you do not yet have these credentials, you can apply as noted in the process below. (There is a delay for account validation.)

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

To manually update downloadable libraries:

1. Navigate to the libraries download page in the Flexera Customer Community website:
   a. On https://flexeracommunity.force.com/customer/CCLanding, use the account details emailed to you with your order confirmation from Flexera to log in (using the **Login** link in the top right).

      Tip: *Access requires your Customer Community user name and password. If you do not have one, use the* `Request Community Access` *link on the login page to request one. Your credentials are configured for access to content you have licensed.*

   b. Select the **Downloads** tab from the row across the top of the page.

      A routing page appears to let you `Access Product and License Center`, displaying lists of products from Flexera.

   c. In the lists of products, identify FlexNet Manager Platform, and click the **Access Above Products** button that is *below* that product name.

      The `Product and License Center` site is displayed.

   d. In the `Your Downloads` section of the `Home` page, click the link for FlexNet Manager Platform.

   e. In the **FlexNet Manager Platform** page, in the **New Versions** tab, click **FlexNet Manager Platform Content Libraries**.

   f. If this is your first time accessing the libraries this way, accept the End-User License Agreement by clicking **I agree**.

A **Download List** for the content libraries is displayed.

2. When the Application Recognition Library content is updated:

   a. On a computer with Internet access, download the file `RecognitionAfter82.cab` (click its name in the **Download List**).

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

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

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

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

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

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

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

3. When the Service Life Data Pack content is updated:

   Note: *When the Service Life Data Pack content is updated: The matching Application Recognition Library content must be imported prior to the Service Life Data Pack library. Please follow the process mentioned above, and import the Application Recognition Library content first.*

   On a computer with Internet access, download the file `EOSL.cab` (click its name in the **Download List**.

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

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

   d. Install the Service Life Data Pack content using this command

      ```
      InstallDir\DotNet\bin\MgsImportRecognition.exe -ie c:\Temp\EOSL.cab
      ```

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

      Important: *The update to the Service Life Data Pack content places locks on various database tables, and other transactions that are queued may time out. You should therefore execute this command only in off-peak times.*

4. When SKU Library content is updated:

a. On a computer with Internet access, download the file `PURL.cab` from the **Download List**.

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

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

d. Install the SKU Library content using this command:

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

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

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

5. When Product Use Rights Library content is updated, multiple files may be added to the **Download List**. These include `PURL.cab` (for basic functionality), `PURL-Desktop.cab`, and others with the naming convention `PURL-`*`vendor`*`.cab` for different vendor options you may have purchased. Process these one at a time:

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

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

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

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

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

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

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

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

Review Scheduled Tasks

The PowerShell configuration scripts have created a number of scheduled tasks on the batch server, in the **FlexNet Manager Platform** folder for Microsoft Scheduled Tasks. These are 'wrappers' which trigger activities in the internal batch scheduler within FlexNet Manager Suite.

You may review these tasks, and disable any that you are certain you do not need. For example, if you never require SAP license reconciliation, you could disable the three Windows scheduled tasks that relate to SAP licensing.

Scheduled tasks across all central servers are listed in Password Maintenance. On the batch server, the Windows scheduled tasks include:

- Data warehouse export
- Export to ServiceNow
- FlexNet inventory data maintenance
- FNMP database support task
- Import Active Directory
- Import application usage logs
- Import discovery information
- Import installation logs
- Import inventories
- Import Inventory Beacon activity status
- Import Inventory Beacon status
- Import remote task status information
- Import security event information
- Import SAP inventories
- Import SAP package license
- Import SAP user and activity information
- Import system status information
- Import VDI access data
- Inventory import and license reconcile
- Recognition data import
- Regenerate Business Import config
- Send contract notifications.

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.

To locate instructions for configuring various web browsers:

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.

3

Setup for Each Tenant

This chapter collects the processes that must be completed to implement each of your tenant's connections to your managed service using FlexNet Manager Suite. As business grows over time, you may revisit this chapter to add further tenants.

Set Up Accounts and Access Rights

The installing account (example: fnms-admin) has global administrator privileges in your new implementation.

Initially, this is the only account that can set up access rights for other operators. It remains the only account that can control operators' roles *across all tenants*. Once the installing account (example: fnms-admin) gives an operator administrator privileges within a tenant, that operator can also assign accounts to roles, but only within the tenant where s/he has been given administrator privileges.

Apart from the installing account (example: fnms-admin), all other operators must be assigned to roles separately for each tenant. Of course, you can assign multiple operators who can access the system on behalf of any individual tenant. Equally, you may have individual operators who are assigned for multiple tenants (by completing the assignment for one tenant at a time): when they log in, they identify which tenant to work on for the current session. In summary, tenants and operators are in a many-to-many relationship.

All operators are employees of your own MSP company. (The MSP architecture is not designed for your customers to have access to your central servers through the web interface for FlexNet Manager Suite.) Each operator must have a unique user account in your local Active Directory before being registered for FlexNet Manager Suite (the Active Directory accounts must either be in the same domain as your central application server, or in a domain trusted by your application server's domain).

Tip: *An Active Directory user account is used for this creation of the related operator record; and at each subsequent login by the operator to FlexNet Manager Suite, the account is validated against the user account in Active Directory. However, after creation, the editing/deletion of the two accounts is handled separately. Specifically, if an employee leaves your company and the relevant user account is removed from Active Directory, this does not automatically close the operator account within FlexNet Manager Suite (although future login attempts using that operator account will fail, since the Active Directory validation against the missing AD user account will fail). Once created, operator accounts must be managed separately, and of course can only be accessed from within FlexNet Manager Suite. Furthermore, once the new account is first saved (when the*

*account is created in FlexNet Manager Suite), the **Account** value is non-editable, and the account cannot be deleted (although it can be disabled). So be sure to get these details correct during the creation process.*

Once these Active Directory user accounts are in place, there is a two-stage process within the web interface of FlexNet Manager Suite:

- The operator's account must be defined. You may do this when you are logged in to manage any individual tenant: the operator's account is then visible across all tenants.
- Within each tenant, each operator must be enabled, and assigned to a role (or perhaps a few roles, depending on how you structure the roles). It is the role (or net effect of several roles) that determine the access rights available to each operator within each tenant. Roles are unique to tenants, so that if you wish, you may have the one operator Sam who has full administrator rights for one tenant, and read-only access to another tenant.

In addition to the accounts for your operators, you also need to register the Active Directory account you have established for use by the inventory beacon(s) within each tenant site to access your central application server (for details, refer back to Identify (or Set Up) Accounts.) Within FlexNet Manager Suite, each of these read-only "operator" accounts can be assigned to the read-only role within the appropriate tenant.

***Remember:** It is critical that you register and assign each of these Active-Directory-related operator accounts to exactly one tenant. If one of these accounts is accidentally added to multiple tenants, all the inventory beacons associated with all the affected tenants will fail to authenticate. There is no way to repair this through the web interface: it will require a support call and specialized repairs to your database to remedy the situation.*

For this reason, it is *strongly recommended* that you establish a spreadsheet or check list to guide your work as you loop through setting up multiple tenants, helping to ensure that you assign each inventory beacon authentication account to exactly one tenant, and also that you map your operators to the appropriate roles for each tenant.

It is convenient to set up roles first, so that they can be set for multiple operator accounts at once. To set up accounts and roles, you must be logged in as the installing account (example: fnms-admin):

To set up accounts and access rights:

1. Using the installing account (example: fnms-admin), log into the web interface to FlexNet Manager Suite 2018 R1, selecting the first tenant for which operator roles and accounts are to be registered.
2. Navigate to the system menu (▾ in the top right corner), choose **Accounts**, and select the **Roles** tab.
3. For each *unique* set of access rights that you need to assign to operators, ensure that there is (or create) a distinct role, and set its rights by expanding the various headings in the accordion and using the controls inside. (For advanced combinations, start by selecting `Custom` from the drop-down list in each section.) Remember to scroll down and click **Save** (or **Create**) when you make any changes.

   ***Tip:** A default role for an operator to access all the data for a particular tenant is `Operator`. This is one of the standard roles available by default. For an inventory beacon authentication account, the typical role is `read only`. (Remember, this account is used both for authentication and for authorization to access data for a given tenant. This means it must be registered within FlexNet Manager Suite, and the registration process requires that it is assigned to a role.)*
4. When appropriate roles are defined, switch to the **All Accounts** tab.

5. If the operator account has not yet been registered within FlexNet Manager Suite:

   a. Click **Create an account**.

      The tab changes its appearance, and displays the properties for the individual operator account.

      Tip: *When you create a new account in any tenant, that account is also made available in all tenants (although, of course, not assigned to any role in other tenants). This saves you repeatedly setting up accounts for a person needing to access several of your customers' data.*

   b. For **Account**, enter the Windows (Active Directory) domain and account name in the form `domain\account`.

      Tip: *Both the domain name and the account are validated against Active Directory for the current domain (where your web application server is running) or a trusted domain. You cannot save this account's details unless the domain and account are validated. The domain flat name is adequate.*

   c. Enter the person's name in the **Name** field, and a current email address in **Email**.

      While these fields are not validated against Active Directory, it may be good practice to make them consistent with the details saved in Active Directory, for easier management.

   d. Optionally, enter a **Job title** for this operator.

      Don't make the job title specific to this one tenant, as this property of the operator is also visible across all tenants.

      Tip: *You can also set the **Status** and **Role** for this operator with the current tenant while creating this new account. These steps are common to new and existing accounts, and are described below. Roles are not shared across tenants.*

   e. Click **Create**.

      The list of accounts reappears, with the new account included in the list (on the appropriate page of the list for the current sort order).

6. In the list of **All Accounts**, find each account in the list in turn, and click the hyperlinked account name to open its properties.

   The tab changes its appearance, and displays the properties for the individual operator account.

7. Ensure that the account **Status** is set to `Enabled`.

   When an operator's account is `Disabled` for this tenant, it cannot be used to log in or work on this tenant's data.

8. Select the role for this operator (within the current tenant) from the **Role** drop-down list.

   Tip: *If this operator needs membership in multiple roles within the current tenant, click the **+** button (to the right of the **Role** drop-down list) to display a duplicate of the drop-down list, and choose another role.*

   The net effect that all roles have on permissions for this operator account (within the current tenant) 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 operator account is assigned to both roles.) Each title bar in the accordion has a summary term on the right-hand end. For full details, click any title bar to expand that section; or click **Expand all** on the right above the accordion.

9. Remember to **Save** each changed account.
10. If you have additional operators to authorize for the current tenant, loop back and repeat the configuration of their accounts.

    Don't forget the unique inventory beacon authentication account for this tenant.
11. When you have configured all accounts for one tenant, click the down arrow shown to the left of the current tenant's name (on the left end of the title bar, next to the FlexNet Manager Suite logo), and select **Change tenant**.

    The tenant selection dialog (as displayed for your first login) reappears.
12. From the drop-down list **Please select a tenant**, choose the next tenant in your list for which you want to configure operator accounts, and repeat the process.

Configure Beacon Connections

Inventory beacons are the data-gathering arms of your compliance system.

Your managed service requires that you have at least one inventory beacon within each tenant's computer estate (in their local network, not in your local network). If your customer (tenant) has a complex networking environment, or specialized inventory requirements, you may require multiple inventory beacons with that environment (and if so, these may be arranged hierarchically, or may be in a flat array where each one contacts your central servers independently).

The inventory beacons collect information within each tenant's environment, and "phone home" to upload the data to your central application servers. Depending on data type, the upload goes to distinct servers within your implementation:

- Inventory collected by the FlexNet inventory agent is uploaded to your inventory server.
- Inventory collected by third-party tools (through inventory adapters) is uploaded to the staging folder, a network share accessible from your batch server. You identified this share in Configure Network Shares for Multi-Server.
- Specially-formatted inventory spreadsheets are uploaded to the shared folder and accessed by the batch server.
- Other business information (imported through business adapters) is also uploaded to the shared folder and accessed by the batch server.

It goes without saying that each inventory beacon must be located within the customer's domain where it is to collect data. If a customer has a multi-domain environment, place an inventory beacon within each domain, or at least ensure that there is domain trust for the inventory beacon to collect data across domain boundaries. But further than that: it is best practice to deploy at least one inventory beacon into each separate subnet that contains target devices for which you may want an inventory beacon to execute discovery and inventory gathering. Being within the target subnet allows the inventory beacon to reliably use ARP or `nbtstat` requests to

determine the MAC address of a discovered device (reliability of these results is reduced across separate subnets). If you do *not* place an inventory beacon in each subnet:

Installation of an inventory beacon includes registration within the central database for FlexNet Manager Suite. For this reason, the process for installing and configuring inventory beacons starts from the web UI for FlexNet Manager Suite. Each downloaded inventory beacon installer is unique, and customized to the individual tenant: do not copy the installer from one tenant to another.

Installation, and further configuration and management, of each inventory beacon requires that you can access the user interface presented on that inventory beacon. To do this, you may:

- Physically visit your customer's site, and implement and manage the inventory beacon directly
- Delegate the installation and management processes on the inventory beacon to an administrator employee of your customer, already on site (not recommended)
- Most likely, arrange to have a Remote Desktop Connection to each inventory beacon, so that you can perform the installation and future management tasks from your site. (This is assumed in the process below.)

Remember that the account to install and manage the inventory beacon requires administrator privileges on that computer. If you need to set up any adapter's staging databases on an inventory beacon, you may prefer to have SQL Server `sysadmin` rights on that machine as well. You may also need to arrange for firewall access into the customer's network. For more about this account (and also other service or similar account[s] to access other systems for inventory collection), refer back to Identify (or Set Up) Accounts.

Check the latest release notes for the physical requirements of each inventory beacon. You can also check the general prerequisites in the online help (*FlexNet Manager Suite Help* > *What Is an Inventory Beacon?* > *Prerequisites for Inventory Beacons*). Armed with this knowledge, negotiate the computer's availability, credentials, and configuration with each customer. It is very handy if there is a supported web browser installed on the proposed inventory beacon as well.

To install and configure an inventory beacon:

1. Arrange with your customer for the necessary firewall settings for network connectivity between your system and the proposed inventory beacon(s).

   In operation, the top-level inventory beacon(s) need only HTTPS access to your central inventory server and batch server. The default port for HTTPS access is port 443, but you noted any custom ports during setup of those servers. For set-up and management of all inventory beacon(s) in each tenant's site, you also need a Remote Desktop Connection (or similar) from your server to each inventory beacon.

2. Use a Remote Desktop Connection (RDC) to log into the proposed inventory beacon with a customer-specific account that has administrator privileges on this computer.

   The remainder of this process is conducted through RDC on the customer's computer.

3. If the .NET version is less than 4.5, upgrade Microsoft .NET Framework to version 4.5 or later.

   For more details, see .

4. Ensure that version 3.0 or later of PowerShell is installed on this inventory beacon.

   For details about checking and upgrading, see Upgrade PowerShell on Local Inventory Beacons, but now applying the information to the inventory beacon within your customer site.

5. Ensure that firewalls are configured to allow HTTPS access from the inventory beacon in your customer's site to your central application server(s) in your MSP site.
6. Start the web browser on this computer, and access the URL **https://*server-name-or-IP-address*/Suite/** (substituting the details of your web application server).
7. Log into the web interface of FlexNet Manager Suite using your installing account (example: fnms-admin). This account is a global administrator for all tenants.

   Important: *Be certain to select the correct tenant for which you are installing the inventory beacon. Configuration for each inventory beacon is specific to the individual tenant.*
8. In the **Discovery & Inventory** menu, under the **Network** group, select **Beacons**.
9. Click **Deploy a beacon**.

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

    Tip: *This button is displayed only to members of the* `Administrator` *role.*
11. Use the web browser dialog to save the installer to a convenient directory (such as `C:\temp`).

    Tip: *If you have not downloaded directly to your intended inventory beacon, you should now move the downloaded installer to that intended device.*
12. In Windows Explorer, navigate to the saved file on your inventory beacon, and double-click it to run the installer.
13. When the installer asks for the credentials to log into your web application server, supply the account name and password for the specific tenant account you have created in your Active Directory environment (refer back to Identify (or Set Up) Accounts for more details).

    Important: *Remember that you must keep these inventory beacon authentication accounts unique for each tenant.*
14. In the web interface for FlexNet Manager Suite, expand the accordion sections (and see the related help) for guidance on how to deploy and configure your inventory beacon(s).
15. When the inventory beacon is installed, be sure to register it (see the online help under *FlexNet Manager Suite Help* > *What Is an Inventory Beacon?* > *Register an Inventory Beacon*).

    Tip: *Each inventory beacon must be registered separately. A customized configuration file is downloaded that is specific both to the inventory beacon and to the tenant.*
16. With your inventory beacon(s) configured, in the web interface for FlexNet Manager Suite, navigate to **Discovery & Inventory > Discovery > Discovery and Inventory Rules** to set up FlexNet inventory collection rules for this tenant.

17. Refer to the online help for details about configuring your inventory beacon(s) to connect to other data sources to import third-party inventory for this tenant.

    For example, in the section *FlexNet Manager Suite Help* > *Inventory Beacons*, see (amongst others) the following topics:

    - *Inventory Systems Page*
    - *SAP Systems Page*.

    You may also wish to consult FlexNet Manager Suite Adapters Reference, a PDF file available through the title page of the online help for your system, for more information about setting up inventory adapters for this tenant.

18. When the processes are completed for this tenant, log out, close the Remote Desktop Connection, and repeat the processes for all remaining tenants.

When the inventory collections rules are established, and the connections set up on the inventory beacon(s), FlexNet Manager Suite is ready to import data and start calculating the license position for this tenant.

4

Notes on Issues

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

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

Password Maintenance

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

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

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

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

On the web application server

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

On the batch server

- The identity configured on the IIS application pool: **Flexera Beacon**
- In Services:
  - **FlexNet Manager Suite Batch Process Scheduler**
  - **FlexNet Manager Suite Batch Processor**
- In the **FlexNet Manager Platform** folder for Microsoft Scheduled Tasks:
  - Data warehouse export
  - Export to ServiceNow
  - FlexNet inventory data maintenance
  - FNMP database support task
  - Import Active Directory
  - Import application usage logs
  - Import discovery information
  - Import installation logs
  - Import inventories
  - Import Inventory Beacon activity status
  - Import Inventory Beacon status
  - Import remote task status information
  - Import security event information
  - Import SAP inventories
  - Import SAP package license
  - Import SAP user and activity information
  - Import system status information
  - Import VDI access data
  - Inventory import and license reconcile
  - Recognition data import
  - Regenerate Business Import config
  - Send contract notifications.

On the inventory server

- The identity configured on the following IIS application pools:

- **Flexera Importers**
- **Flexera Package Repository**

- In the **FlexNet Manager Platform** folder for Microsoft Scheduled Tasks:
  - Import Active Directory
  - Import application usage logs
  - Import discovery information
  - Import installation logs
  - Import inventories
  - Import Inventory Beacon activity status
  - Import Inventory Beacon status
  - Import remote task status information
  - Import security event information
  - Import system status information
  - Import VDI access data.

On the inventory beacon

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

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

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

- *Flexera Inventory Manager installation agent*
- *Flexera Inventory Manager managed device* `vversionNumber`
- *Flexera Inventory Manager security service.*

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

Identifying IIS Application Pool Credential Issues

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

Background

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

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

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

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

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.

Update Credentials in IIS Application Pools

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

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

To update credentials in IIS Application Pools:

1. Open IIS Manager (**Start** > **Administrative Tools** > **Internet Information Service (IIS) Manager**).
2. In the navigation area on the left, expand the ***SERVER-NAME*** **(*****account-name*****)** node, and select **Application Pools**.

   Any application pool accessed since the user account password was changed displays a status of `Stopped`. On each server type, the relevant application pools are:

   - **Flexera Beacon** on the batch server/processing server/application server
   - **Flexera Importers** on the inventory server/processing server/application server
   - **Flexera Package Repository** on the inventory server/processing server/application server
   - **FlexNet Manager Platform** on the web application server/application server
   - **ManageSoftWebServiceAppPool** on the web application server/application server
   - **SAP Optimization** on the web application server/application server
   - **SAPServiceAppPool** on the web application server/application server.
3. Select the appropriate application pool, and in the **Actions** list on the right, click **Advanced Settings**.

   The **Advanced Settings** dialog appears.
4. In the **Process Model** section, select **Identity**, and click the ellipsis button next to the account name.

5. Next to **Custom Account**, click **Set**.

   The **Set Credentials** dialog appears.

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

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

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

IIS Roles/Services

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

5

Additional Information

Details about installing, configuring and operating the inventory beacon are summarized directly in the web interface for FlexNet Manager Suite, and are detailed in the online help available through those pages.

Additional documentation is available through the title page of online help for your implementation:

- Gathering FlexNet Inventory provides a structured reference to the different ways of deploying and using the FlexNet inventory agent and its various components, as well as command lines and preference settings for some of the code agents that are deployed to the adopted device.
- FlexNet Manager Suite Adapters Reference covers standard adapters available for the system that manipulate data from external systems into a format useable by FlexNet Manager Suite.
- Using FlexNet Business Importer covers the use of this command-line executable, which is also the tool used by the Business Adapter Studio to drive imports from adapters defined there. This document includes the data model common to the Business Importer and the Business Adapter Studio, as well as some sample adapters (called the Data Domain Interface, or DDI).
- FlexNet Manager Suite System Reference collects a variety of reference material, including:
  - How to customize FlexNet Manager Suite
  - How to use spreadsheets (or CSV files) of inventory data for one-time or scheduled imports
  - Discovering Oracle systems and collecting inventory from them
  - How to use the Business Adapter Studio and the Inventory Adapter Studio
  - How to set up in a single sign-on environment.
- FlexNet Manager Suite Schema Reference provides a working reference to the database tables and columns for FlexNet Manager Suite. This is particularly useful if you want to prepare (or specify) customizations, or to understand more as you prepare custom adapters.
- FlexNet Manager for SAP Applications User Guide is for those who licensed the FlexNet Manager for SAP Applications product, and provides operational details. This content is more extensive than the information available in the online help (see table of contents at left).
- Non-Commercial Software Disclosures lists all third-party non-commercial code used in FlexNet Manager Suite, with attributions and license terms.

- For your convenience, the Release Notes for the current version are also available. These include issues resolved in this release, new and updated features, system requirements and the like.

Additional documentation for FlexNet Manager for SAP Applications is available through the Customer Community portal.