



FlexNet Manager Suite 2023 R2

Installing FlexNet Manager Suite On
Premises

Legal Information

Document Name: FlexNet Manager Suite 2023 R2 Installation Guide (for on-premises delivery)

Part Number: FMS-21.0.0-IG01

Product Release Date: November 15, 2023

Copyright Notice

Copyright © 2023 Flexera.

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. Preparation	5
Synopsis and Server Breakdown	5
Prerequisites and Preparations	8
Design the Topography.....	9
Enable MTS and MSMQ.....	16
Accounts.....	17
Configure .NET and IIS.....	22
Configure Internet Explorer.....	25
Upgrade PowerShell on Inventory Beacons.....	26
Configure Network Shares for Multi-Server.....	26
Drivers for Spreadsheet Imports	27
Download the Materials.....	27
2. Installation Details	30
Create Databases	30
Authorize the Service Account.....	39
Choosing the Installation Approach	39
Managing Scripted Installation.....	40
Prepare Encrypted Credentials.....	41
Prepare the Answer File(s).....	43
Running a Scripted Installation.....	47
Managing Installations Interactively	49
Install the Web Interface.....	49
Install the Inventory Server	52
Install the Batch Server	52
Configure the System	54
Installing Flexera Analytics	58
Configuring IIS to Use SSL/TLS Encryption	67
Reconfigure Cognos Analytics to Use Third-Party SSL Certificates	68
Reconfigure Cognos gateway to use SSL using self-signed certificates.....	72
Reconfigure Cognos components to use Cognos signed certificate	74
Import the Sample Reporting Package.....	76

Installing a Free-Standing Studio.....	79
Product Activation	81
Populate the Downloadable Libraries	81
Manual Updates of Library Data.....	83
Review Scheduled Tasks	86
Link to Flexera Service Gateway	87
Configure Beacon Connections.....	88
Set Up Initial Accounts and Access Rights	90
3. Notes on Issues	93
Password Maintenance.....	93
Identifying IIS Application Pool Credential Issues	96
Update Credentials in IIS Application Pools	97
IIS Roles/Services	98
4. Additional Information.....	100

1

Preparation

This document describes installation of FlexNet Manager Suite 2023 R2 on the central application server of an on-premises implementation.



Note: Managed service providers should reference the separate documentation available for multi-tenant environments. Partners should contact your Flexera Partner Manager.

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.

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.
3. Authorize the service account.
4. Install the web interface on the web application server.
5. In a medium-to-large system (collecting FlexNet inventory for 50,000 devices or more), install one or more inventory servers as required.
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. Product activation.
9. Download the current data libraries.
10. Optionally, install Flexera Analytics.
11. If using Flexera Analytics, import the latest reporting package.

Thereafter, you can use the web interface to deploy inventory beacons, and establish rules for inventory collection. At each inventory beacon, you will also need to configure the beacon and populate the password store with credentials if you are allowing direct inventory gathering.

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 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
- CSvr - Cognos server, if you choose to implement trend reporting
- 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	CSvr	IB
Admin acct	Y	Y	Y			Y
Service acct	Y	Y	Y	Y		Y
DBA acct				Y		
Configure IIS	Y	Y	Y		Y	
Disable WebDAV			Y			Y
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				

Tasks/Server:	App svr: Web	App svr: Batch	App svr: Inv	DBSvr	CSvr	IB
Install Flexera Analytics					Y	
PowerShell configuration scripts	Y1	Y2	Y3		Y	
Product activation						
Populate libraries						
Import trend reporting package (Cognos)					Y	
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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Web application server
A processing server (combining the inventory server and the batch server)	<ul style="list-style-type: none"> • Inventory server • Batch scheduling server
A stand-alone inventory server	<ul style="list-style-type: none"> • Inventory server
The separate batch processing machine, which must use the batch scheduling server option	<ul style="list-style-type: none"> • Batch scheduling server

Prerequisites and Preparations

It is important that you work through each stage of these preparations before commencing your implementation.

Design

Your implementation may have only one central server, or it may have several. You also need to plan for inventory beacons. For details, see [Design the Topography](#).

License

Locate your FlexNet license key, emailed to you from Flexera as part of the order confirmation process, and have it ready for use in the following process.

Microsoft Message Queuing (MSMQ)

MSMQ is fundamental to process scheduling within FlexNet Manager Suite. If it is already in use within your environment, changes are unlikely. To validate, see details in [Enable MTS and MSMQ](#).

Accounts

For installation and operation, FlexNet Manager Suite requires several different sets of account privileges. You'll find full details in [Accounts](#).

Database instance(s)

All databases for this system require a collation sequence that is both case insensitive and accent sensitive. This means that they should be installed on one or more database instances that a default collation sequence ending with the codes `_CI_AS`. For details about checking for a collation sequence, see [Create Databases](#).

Configure IIS, .NET and WebDAV

Your implementation will fail if these configurations are not completed correctly. See details in [Configure .NET and IIS](#).

Browser

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 your inventory beacon has a server operating system), the IE enhanced security provisions must be turned off on that server. For details, see [Configure Internet Explorer](#). (Alternatively, use a different browser.)

Check/upgrade PowerShell

Your inventory beacons require *at least* version 3.0 of PowerShell, and where your circumstances permit, a later version is preferred. Details are in [Upgrade PowerShell on Inventory Beacons](#).

Configure network shares

If you are about to implement a multi-server solution (for example, separating your web application server, batch server,

and inventory server), you must configure network shares accessible to all for them to access common data. The requirements and process are in [Configure Network Shares for Multi-Server](#). Conversely, in a single-server implementation, this is not required.

Drivers

If you will ever import spreadsheets in XLSX format, a specific driver type is required. For details, see [Drivers for Spreadsheet Imports](#).

Configure document security

FlexNet Manager Suite allows you to attach uploaded documents to various record-types (including assets, purchases, contracts, and licenses). By default, there is no security scanning of these documents: since they are your own documents, they may be assumed good. However, where greater security is required, you can enable on-demand scanning of every uploaded document. For full details, see the section *Preventing Uploads of Malicious Files* in the *FlexNet Manager Suite System Reference* (on-premises edition for release 2020 R2 or later), available through <http://docs.flexera.com> in either PDF or HTML format. One part of the security configuration is to set two registry keys with appropriate values: this can be done by script (for a 'silent' or scripted installation), or interactively. For manual or interactive setting, you may choose to put the required values in place during installation, or to wait until installation is completed and configure the registry again later. These settings are mentioned later in the appropriate place in the process, should you choose to include document scanning as part of your initial configuration.

Downloads

Check the *FlexNet Manager Suite System Requirements and Compatibility* documentation at <https://docs.flexera.com/> and validate your topography (server by server). When your design is validated and your hardware is prepared, download the necessary software packages to commence implementation. For details, see [Download the Materials](#).

Design the Topography

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



Note: Both the inventory server (or in smaller implementations the processing server, or the application server in a single-server implementation) and the inventory beacon(s) are expected to be members of Active Directory domains. (For test environments, consultants may see article 000017145 [How to run FlexNet Manager Suite processing server on a workgroup computer](#).) If you implement a multi-server solution (separating the web application server, the batch server, or the inventory server), it is strongly recommended that all are members of the same Active Directory domain.

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

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



Tip: An inventory beacon may be installed on the same server as the batch server (defined shortly). This allows for greater functionality in future custom business adapters, as on this inventory beacon alone business adapters may operate in "connected mode".

- An inventory server, which can also be duplicated across multiple servers if you are gathering FlexNet inventory for many tens of thousands of devices (see below)
- One (and only one) batch server (also known as a reconciliation server) that imports third-party inventory, integrates FlexNet inventory, incorporates business-related information, and reconciles everything to calculate your license position



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

- The database server (where the five underlying databases may also be split across separate database servers if required)
- The web application server that handles presentation of the interface
- A server for the business reporting option (powered by Cognos), where applicable.

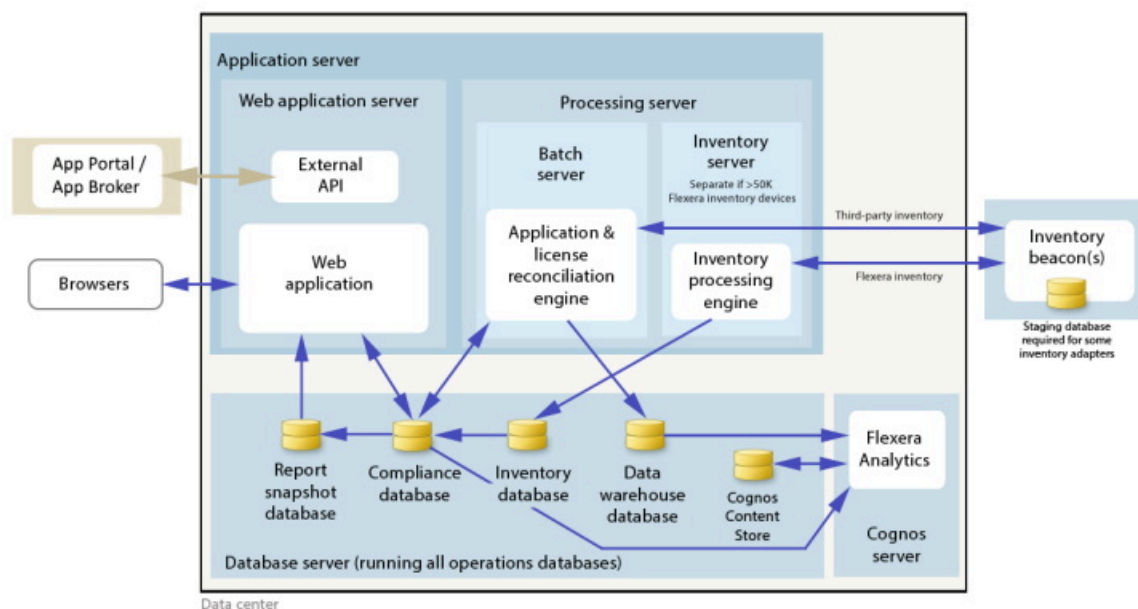


Tip: If the Cognos content store is installed on an SQL Server installation later than 2012, it should be run in SQL Server 2012 compatibility mode.

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

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

- Typically the first candidate for replication is the inventory beacon. This is often driven by network considerations as much as by simple scaling considerations.
- If your system manages more than 50,000 devices reporting FlexNet inventory alone (ignoring for the moment inventory through other third-party tools), the inventory server should be separated onto its own device. You can expect to duplicate a separate inventory server for (roughly) every 50,000 devices reporting FlexNet inventory.
- If you manage inventory from more than 100,000 devices, the batch server (or reconciliation server) may be separated from the web application server and installed separately.



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](#).

The diagram shows that:

- FlexNet inventory (from the FlexNet inventory agent) is uploaded to the inventory database by the inventory server, and then separately imported to the compliance database
- Third-party inventory imported from other tools is loaded by the batch server and stored directly in the compliance database
- Some time-based data is copied to the data warehouse database, and reports may combine trend data from here with current data from the compliance database
- Some data is copied to the snapshot database to improve presentation performance
- The web interface automatically displays a mixture of data from the snapshot database and the compliance database, as appropriate; and data manually input through the web interface is written back to the compliance database
- While Flexera Analytics can be installed on your application server, for performance reasons Flexera Analytics is best installed on a separate server (it has high memory use requirements).



Note: All servers shown inside the data center should be within a single time zone. This is particularly important if you are using Flexera Analytics, since the Flexera Analytics Operational Dashboard combines time-based data from the database server(s) and the Cognos server.

Some of the inventory adapters (such as the Citrix XenApp server adapter, BMC Discovery, and HPUD adapter) require a separate staging database to allow for manipulation and normalization of data. This staging database may be installed on any convenient SQL Server, with one of the options being your central database server hosting your compliance database. Another option is to install the staging database on an appropriate inventory beacon. Decide on the location

of this staging database as part of your design.

For more information about locating inventory beacons in your network, see [Considerations for Inventory Beacons](#).

Prepare a block diagram of the actual servers for your implementation. Don't forget the inventory beacons you intend to deploy. 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.

Considerations for Inventory Beacons

The inventory beacons in your network may be arranged in ways that meet your requirements. For example:

- You may use a flat arrangement where each inventory beacon communicates directly with the central application server
- You may arrange them in a hierarchy, where the top-level inventory beacon(s) communicate with the central application server, and further inventory beacons are arranged as 'children' that communicate with the inventory beacon(s) above them in the hierarchy.

There are no formal limits to the structure of this hierarchy. It may contain as many levels as you require. However, good network design typically means that your hierarchy has two or three (or rarely, four) levels.

The following considerations should assist in your network planning.

Fan-out

These are general guidelines. You should adjust expectations based on experience in your own environment:

- Provide one inventory beacon for every 20,000 (or so) devices with the locally-installed FlexNet inventory agent. In general, policy downloads, and inventory and usage file uploads, place negligible demands on CPU, memory and disk space on the inventory beacon. However, you may be constrained by other network throughput limitations, and by factors such as network proximity of the installed FlexNet inventory agents to at least one local inventory beacon. Here are some typical network load figures per device interacting with an inventory beacon:

Task	Network load
Inventory upload	10-200 KB per upload (low range for desktops and the like, higher range for UNIX-like servers)
Usage file uploads	5-20 KB per day (or zero when you are not tracking usage)
Policy update	10-100 KB per policy update (only occurs when policy is changed)



Remember: You cannot specify particular allocations of devices to inventory beacons: the FlexNet inventory agent is a state-based tool that manages itself to match its downloaded policy, and as part of its self-management, it chooses which inventory beacon to use for data uploads and policy downloads. The default algorithm looks first for an inventory beacon in the same site as the inventory device, then for the best ping response time, with a randomizing tie-breaker. Therefore the above guideline is about the quantitative planning; and you should use other factors to determine the placement of inventory beacons. These other factors include your network topology, including placement of firewalls, or having multiple domains without cross-trust, and the like. Any isolated subnets or the like require a dedicated inventory beacon so that all installed FlexNet inventory agents have full network access to at least one inventory beacon.

- An inventory beacon may also gather inventory from other systems, such as importing inventory gathered by Microsoft Endpoint Configuration Manager (previously Microsoft SCCM) or IBM's ILMT ('third-party inventory'). Since you control the schedule for the collection of third-party inventory, you can stagger the times for different kinds of inventory; and as a result, one inventory beacon can easily handle multiple third-party inventory sources.
- Similar considerations apply to the collection of any business information through an inventory beacon. Arrange the schedules for business importer operations to spread the load on the relevant inventory beacon.
- If you are arranging a hierarchy of inventory beacons in a very large system, you should limit the fan-out from a parent inventory beacon to less than 100 child inventory beacons.

Minimum of one per subnet

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:

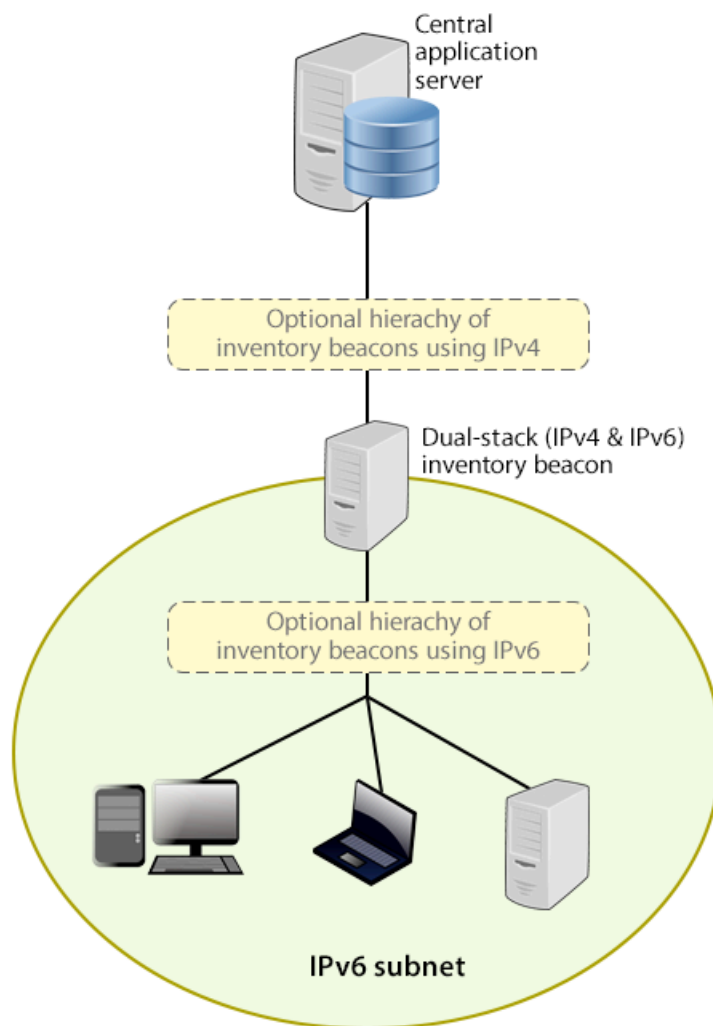
- It is possible that, across subnet boundaries, only an IP address can be found for a device (that is, the device data is missing both a MAC address and a device name).
- In this case, a central record is created for the discovered device, but because IP addresses may be dynamic (unreliable identifiers), this record is not matched (or merged) with more complete records (those which also contain either or both of the MAC address and a device name).
- As a consequence, on data import you may produce multiple discovered device records with duplicate IP addresses:
 - One record may be complete (for example, automatically created by FlexNet Manager Suite from inventory when it could not find an existing, matchable discovery device record to link to the inventory device record)
 - One or more others may be discovery records that are missing identifying data as discussed.
- Since these complete and incomplete records cannot be merged automatically, you are left with a manual task to clean up the incomplete duplicates.
- What's worse, even after that manual clean-up, if the situation persists and an applicable discovery rule is re-run, the incomplete record is recreated.

You avoid all these risks by simply having a local inventory beacon in the same subnet as target devices. Being in the same target subnet means that the inventory beacon can provide both the IP address and the MAC address, which is

sufficient for matching discovered device records. If you must do discovery across subnet boundaries *without* a local inventory beacon, ensure that there are full DNS entries visible to the inventory beacon for all devices you intend to discover. This allows the inventory beacon to report both an IP address and a device name or fully-qualified domain name (FQDN), which combination is again sufficient for record matching.

Bridging to IPv6 subnets

All inventory beacons can operate within subnets configured to use either IPv4 or IPv6 addressing; and FlexNet inventory agent can also handle all data transfers within either environment. However, the link to the central application server must use an IPv4 network protocol. The need to support the IPv4 protocol at the top level of the architecture, and the IPv6 protocol at the low level with the local FlexNet inventory agent, means that at least one inventory beacon must be a dual-stack server that provides the bridge between the two protocols, as shown in the following architectural sketch:



Reading from top to bottom, this sketch shows:

- Your application server (or in larger implementations, multiple servers) continue(s) to support HTTP or HTTPS communications over an IPv4 network layer.

- Within IPv4 zones of your network, you may deploy as many inventory beacons as required, either as a flat layer where each communicates directly with the application server, or in a hierarchy, as dictated by your network requirements. Of course, these inventory beacons provide full functionality, supporting all forms of FlexNet inventory gathering from target inventory devices within the IPv4 network (for simplicity, these devices in the IPv4 zone are not shown in the sketch above).
- At least one inventory beacon must be a dual stack device that supports both IPv4 and IPv6 network layers. It does not matter whether this is achieved using two Network Interface Cards (NICs) or a single configurable NIC. The IPv4 interface links upward to its parent (whether that be to another inventory beacon in the hierarchy or directly to the application server). The IPv6 interface links downward to those of its child devices that are in the IPv6 zone (of course, other devices in the IPv4 network could also communicate through this inventory beacon, given its dual stack architecture). As shown, these IPv6 children may optionally include a further hierarchy of inventory beacons (which child inventory beacons would then be operating entirely within the IPv6 network).
- Eventually, target inventory devices within the IPv6 zone that have locally installed FlexNet inventory agents communicate with at least one inventory beacon in the same zone; or where the lightweight FlexNet Inventory Scanner has been run on a target device, this can also communicate with the inventory beacon.

There are further restrictions and requirements to add to these general sketches:

- All inventory beacons operating within an IPv6 network (whether as single-stack IPv6 devices or dual-stack IPv4 and IPv6 devices) must utilize Microsoft IIS as the web service. The simple alternative self-hosted web server does not support the IPv6 protocol.
- Inside an IPv6 network, an inventory beacon cannot import Active Directory details. However, a dual-stack inventory beacon that can communicate with a domain name server (DNS) over IPv4 can still import Active Directory data. Alternatively, an inventory beacon *co-installed on your central application server* (which by definition must have IPv4 available to it) can still access a DNS on IPv4 and import Active Directory data.
- Inside an IPv6 network, an inventory beacon cannot do any of the following:
 - Import inventory from third-party sources
 - Import business data from other systems (such as your purchasing or HR systems)
 - Communicate with SAP systems in your IPv6 environment
 - Perform any inventory beacon-based discovery or remote inventory collection across the IPv6 subnet, including VMware host scans (such as required for special 30-minute scans for IBM PVU license management)
 - Adopt target inventory devices that can communicate only on an IPv6 subnet (instead, use third-party deployment to install the FlexNet inventory agent on target devices within an IPv6-only subnet).

However, once again, a dual-stack inventory beacon that can communicate with a DNS over IPv4, and contact the various sources also exclusively over IPv4, still supports all the above functionality on the IPv4 side. This is also true of an inventory beacon co-installed on the application server.

Take these factors into account when planning the distribution of your inventory beacons around your network. More details are available in [Configure Beacon Connections](#).

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.

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).



Important: The accounts used for administration of FlexNet Manager Suite must be mapped to SQL Server User objects in some way (depending on whether you use Windows Authentication, SQL authentication perhaps embedded in connection strings, and so on). It is critical that every relevant SQL Server user has the same default schema for each of the databases, correctly configured. (By default, Microsoft SQL Server Management Studio does not check the default schema name, so it is best entered explicitly – and without enclosing square brackets.) For more information, see [Create Databases](#).

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:

- db-admin — A database administrator (typically this is an existing database administrator within your enterprise)
- fnms-admin — An installing system administrator (account details must be made available to db-admin)
- svc-flexnet — 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.

Privileges	Required on	Purpose
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.
<p>SELECT rights to the following tables in the msdb database:</p> <ul style="list-style-type: none"> • <code>dbo.sysjobs</code> • <code>dbo.sysjobsteps</code> • <code>sysjobs_view</code>. <p>EXECUTE rights to the stored procedures from the msdb database used in the database scripts, including:</p> <ul style="list-style-type: none"> • <code>sp_add_job</code> • <code>sp_add_jobserver</code> • <code>sp_add_jobstep</code> • <code>sp_add_jobschedule</code> • <code>sp_delete_job</code>. 	Database servers	Only required if an existing installation of FlexNet Manager Suite 2015 or earlier is being migrated to a later release.




Tip: If you are installing Flexera Analytics (powered by Cognos) as part of your implementation, you also need a SQL Server account with read/write access to the Content Store database required by Cognos. The Flexera Analytics installer asks for the login name and password for this account (for details, including character set restrictions, see [Installing Flexera Analytics](#)).


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

Privileges	Required on	Purpose
Membership in the <code>db_owner</code> 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 (<code>ARITHABORT</code> , <code>QUOTED_IDENTIFIER</code>) that can only be configured by an account with <code>db_owner</code> privileges. Therefore the installing account needs membership in the <code>db_owner</code> role at least temporarily during installation.

Privileges	Required on	Purpose
Local administrator	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 installers for implementing FlexNet Manager Suite and the license from Flexera for its operation.
Internet connection to https://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
<p>Membership in the following fixed database roles:</p> <ul style="list-style-type: none"> • db_ddladmin • db_datawriter • db_datareader. <p>In addition, the account requires you to GRANT EXECUTE permissions on all operations databases (compliance data, warehouse data, snapshot data, and inventory data).</p>	Database server	Normal operation (which includes execution of SQL stored procedures).
<div>  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. </div>		
<p>Logon as a Service, and run all FlexNet services</p>	<ul style="list-style-type: none"> • 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.
<div> <div>  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. </div> <div>  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.) </div> </div>		

Privileges	Required on	Purpose
Logon as a Batch Job	<ul style="list-style-type: none"> Central application server(s) (including, where separated, web application server, batch server, and inventory server); All inventory beacons. 	<p>When the service account runs a batch job, this setting means the login is not an interactive user.</p> <hr/> <p> Tip: This is particularly important on the batch server (for authorization details, see Authorize the Service Account).</p>
Run scheduled tasks as a service account.	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Central application server(s) (including, where separated, web application server, batch server, and inventory server); Those inventory beacons that are running IIS 	Normal operations
Internet connection to https://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](#).

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

For example, if you are using adapters to connect to other systems and import data, you need appropriate accounts. For details, see documentation for the adapters you need, such as *FlexNet Manager Suite Inventory Adapters and Connectors Reference*.

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



Note: Inventory beacons have an additional requirement, that PowerShell is at least at version 3.0 (see [Upgrade PowerShell on Inventory Beacons](#) for more details).

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



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



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 4.7.2 (or later). If it is present, skip to step 4 below.
 - c. Because Microsoft .NET Framework 4.7.2 (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 4.7.2 or later. To check:
 - a. Open Windows Programs and Features.
 - b. Search the list of applications for Microsoft .NET Framework, and determine whether it is release 4.7.2 (or later).
 - If it is 4.7.2 (or later), skip to step 4 below.

- If it is an earlier release, continue here.
3. If the .NET version is less than 4.7.2, upgrade Microsoft .NET Framework to version 4.7.2 or later.
For more details, see [https://msdn.microsoft.com/en-us/library/5a4x27ek\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/5a4x27ek(v=vs.110).aspx).
 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.

If you are currently working on any of:

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

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



Tip: Although from IIS 7.0, Microsoft offered a separate download for improved WebDAV functionality, the native WebDAV functionality must also be disabled. Otherwise WebDAV intercepts HTTP processing and blocks FlexNet inventory functionality.

8. You may first check that WebDAV is installed. For example, on Windows Server 2012:
 - a. Open Server Manager (for example, **Start** > **Administrative Tools** > **Server Manager**).
 - b. Select **Dashboard**, and in the dashboard select **Add Roles and Features**.
The **Add Roles and Features Wizard** opens.
 - c. In the left-hand navigation pane, select **Installation Type**, and in the main pane, ensure that the **Role-based or feature-based installation** is selected.
 - d. Click **Next** (or select **Server Selection**), and select the server you are currently configuring.
 - e. Click **Next** (or select **Server Roles**), and in the **Roles** panel, expand **Web Server (IIS)** > **Web Server > Common HTTP Featured (Installed)**.

- f. Observe whether the check box for **WebDAV Publishing (Installed)** is selected.

If this check box is clear, WebDAV is not installed, and you may click **Cancel**, then close all relevant dialogs.

If this is not the last server on your list, loop back and restart this process on the next server. However, if the check box is selected, WebDAV is installed and *must* be disabled, as described in the following steps.

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.

15. Flexera Analytics requires installation of **URL Rewrite**.

- Open a web browser and open <https://www.iis.net/downloads/microsoft/url-rewrite>
- Select the **Install this extension** box, which will download the `urlrewrite2.exe` file. A selection of alternate language installers are also available on this page.
- Run the file which will execute the installation of this extension.
- Exit the installer.

16. Flexera Analytics also requires the installation of **Application Request Routing**.

- Open a web browser and open <https://www.iis.net/downloads/microsoft/application-request-routing>
- Select the **Install this extension** box, which will download the `ARRv3_0.exe` file.
- Run the downloaded file which will execute the installation of this extension.
- Exit the installer.



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

Configure Internet Explorer

Microsoft Internet Explorer requires 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 the *FlexNet Manager Suite System Requirements and Compatibility* documentation, available at <https://docs.flexera.com/>, 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 Inventory Beacons

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

The minimum requirement on inventory beacons is PowerShell 3.0.

You may choose to upgrade PowerShell to version 4.0, but be aware that this release has a prerequisite of .NET Framework 4.5 or later (in any case, the minimum supported version of .NET Framework for an inventory beacon is currently 4.7.2).



To check and optionally upgrade PowerShell on a candidate server:

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>.

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. 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.

Drivers for Spreadsheet Imports

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

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

- You will *import* data from spreadsheets (the export of data to spreadsheets is not relevant, and the import of data from CSV [comma-separated values] file is also not relevant)
- The spreadsheets will be Excel spreadsheets in .xlsx format (the earlier .xls format does not require the driver update; but be aware that this older format limits each spreadsheet to about 65,000 records/rows)
- The .xlsx files will be imported to the batch server (or processing server, or application server in a single server implementation); or they will be imported to an inventory beacon — obviously, drivers are needed only on servers (whether a central server or inventory beacon servers) where such imports actually occur, so that this prerequisite applies only to those relevant server(s).

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 .xlsx 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, and preferably at least some of your inventory beacons.



Important: You must download and unzip the archives to a high level folder such as `C:\Temp\FNMSDownLoads\` to avoid creating long file paths that may exceed the windows path limit of 260 characters and cause an error when running PowerShell scripts.



To download required materials:

1. Use your browser to access the Flexera Product Documentation site at <https://docs.flexera.com/>.
2. Select FlexNet Manager Suite On-Premises from the **Product** drop-down list and then select 2023 R2 from the

Version drop-down list.

3. Download and check the *FlexNet Manager Suite System Requirements and Compatibility* PDF, and validate your server plan (see [Design the Topography](#)) against the requirements for the Windows Server computer(s) you plan to use.

When your design is validated and the hardware is in place, you are ready to download the necessary files to commence your implementation.

4. Use your browser to access the Flexera Customer Community.

- a. On <https://community.flexera.com/>, 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, click the *Let's go!* button on the login page to request one. Your credentials are configured for access to content you have licensed.

- b. Select **Find My Product** and choose **FlexNet Manager** from the top menu. Now click the button **PRODUCT RESOURCES - PRODUCT INFORMATION** which will expose the **Download Products and Licenses** link. Click on this option.

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 immediately below it, click **LET'S GO**.

The Product and License Center site displays.

- 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 2023 R2](#) to access the downloads.

5. 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.

- a. Download the installer through the [FlexNet Manager Suite Installer.zip 2023 R2](#) link.

- b. If your implementation design includes Flexera Analytics also download: [Flexera Analytics 2023 R2.zip](#).

We recommend you also download the latest versions of the Flexera dashboards, data models and reports:

[FlexNet Manager Platform Data Warehouse Reports and Dashboard 2019 R2.zip](#)

[Flexera Data Models and Flexera Boards - June 2020.zip](#)

- c. If you will also install the Business Adapter Studio in connected mode (that is, on a central server with direct access to your operations databases), also download [Business Adapter Studio for FlexNet Manager Suite 2023 R2.zip](#) to the same location.
 - d. If you are collecting inventory from Citrix Virtual Apps, or from any of the other sources that require an additional adapter out of the box, also download [Adapter Tools for FlexNet Manager Suite 2023](#)


R2.zip.

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

 **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 <https://support.microsoft.com/en-au/help/3173976/fix-fatal-error-when-you-run-a-query-against-the-sys-sysindexes-view-in-sql-server-2016>.

 **Important:** If you are using Microsoft SQL Server 2019, ensure that you have installed [Cumulative Update Package 5 for SQL Server 2019](#) or later.

 **Important:** If you are using Microsoft SQL Server 2019 or Microsoft SQL Server 2022, ensure that, for all your databases used in FlexNet Manager Suite, you are **not** using the "memory-optimized tempdb metadata" feature, which was introduced in SQL Server 2019. This is because SQL Server does not allow access to these memory-optimized tables from within SQL CLR (Common Language Runtime) stored procedures, and FlexNet Manager Suite uses a signed CLR assembly (with the SAFE permission set). For this reason, if the feature is left enabled, database errors will result. The feature may be disabled on each installed SQL Server 2019 or 2022 instance prior to creating the databases for FlexNet Manager Suite on that instance. To do so:

1. Start SQL Server Management Studio.

2. Open the **New Query** window.
3. Paste either of the following queries into the window:

```
ALTER SERVER CONFIGURATION SET MEMORY_OPTIMIZED TEMPDB_METADATA = OFF
GO
```

or

```
EXEC sp_configure 'tempdb metadata memory-optimized', 0
GO
RECONFIGURE
GO
```

4. Click the **Execute** button to run your chosen query.
5. Restart SQL Server so that it loads the new configuration.

With the memory-optimized tempdb metadata now disabled on this server, you may proceed with database installation. Remember to repeat this on each SQL Server 2019 or 2022 instance where you are creating databases for FlexNet Manager Suite.

FlexNet Manager Suite uses a number of separate databases. While scripts are provided, it is typical that these scripts will be inspected and executed by a database administrator (DBA).



Important: All database scripts use Unicode character sets to allow for necessary localization. This means that:

- Any FTP transfer of these files must be in binary mode (not ASCII mode)
- The files must be edited only in editors that support Unicode character sets.

Failure to observe these precautions may result in failures in script operations.

Create the databases in the order shown below: first the inventory collection database, then the compliance database, and so on.

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.



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 [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.



Note: Database compatibility settings have a big impact on performance, especially for the nightly license reconciliation. Recommended settings are:

- For Microsoft SQL Server 2014 through 2016, set the compatibility level for each database to SQL Server 2012 (110)
- For Microsoft SQL Server 2017 you may use either the default compatibility level (such as SQL Server 2017 (140)), or set the compatibility mode to 110
- For Microsoft SQL Server 2019 or Microsoft SQL Server 2022, use the default compatibility level.

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 [Accounts](#)).



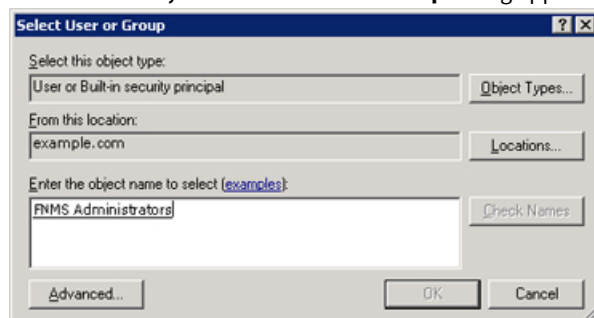
Tip: While databases are being created, you can start installing the central application servers in parallel. There are no interdependencies until you start running the PowerShell configuration scripts.



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.

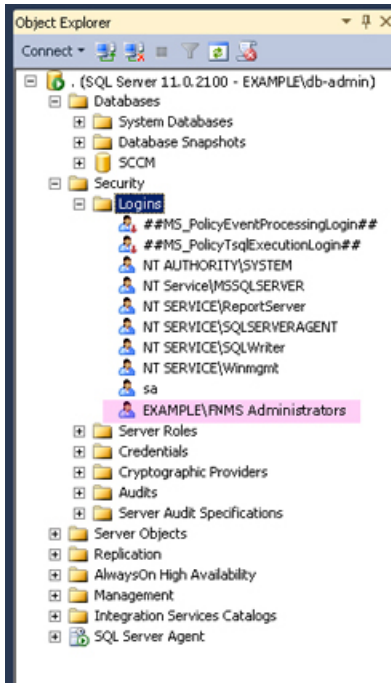


- b. Use the **Object Types...** button to ensure that `User or Built-in security principal` is selected as the object type.
- c. Use the **Locations...** button to select your Active Directory domain.
- d. As the object name, enter the name of your security group (suggested: `FNMS Administrators`), 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.

- a. For SQL Server 2017 or later, you first need to install a Flexera signed security certificate which identifies the installation as a trusted assembly.



Tip: If it happens that your various databases for FlexNet Manager Suite are on separate database servers running SQL Server 2017 or later, remember to install a copy of the certificate on each server, as follows.

- a. Download the file Flexera Signed Security Certificate for SQL Server 2017 and 2019.zip from the [Product & License Center](#). Extract the FlexeraCodeSigning.cer file from the downloaded archive to a temporary location on the host where Microsoft SQL Server is running, in a file path to which the SQL Server service account has read access.
 - b. Edit the SQLScript.sql file from the archive, and replace <location> with the path where you have copied the FlexeraCodeSigning.cer file. Save your change.
 - c. Open SQL Server Studio and execute your updated SQLScript.sql file.
- b. Enable Microsoft SQL Server Common Language Runtime (CLR) Integration by executing the following stored procedure:

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



Note: By default the CLR integration feature is disabled and must be enabled by the DB system administrator before database creation and installation. CLR is disabled by default to increase security in shared hosting contexts. However, in this context, Flexera is a known vendor supplying trusted code for an environment fully controlled by your administrators. Flexera warrants that the CLR DLL signed by Flexera does not attempt to elevate privileges or behave maliciously.

5. Create the database for FlexNet native inventory collection.



Remember: If you plan to collect both inventory data and compliance data in a single database, use the same `-d FNMSCompliance` name parameter for this and the compliance databases; or for a separate inventory database (recommended), use a different name as shown below.



Tip: To avoid typos, you may want to copy all five of the following command lines into your ASCII text editor, globally search for and replace the placeholders `DBserver-name\instance name` with the name of your SQL Server and your database instance (where that is not the default instance), and then copy/paste each modified command line when required.



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. On the database server (or the application server for a single-server implementation), 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.

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

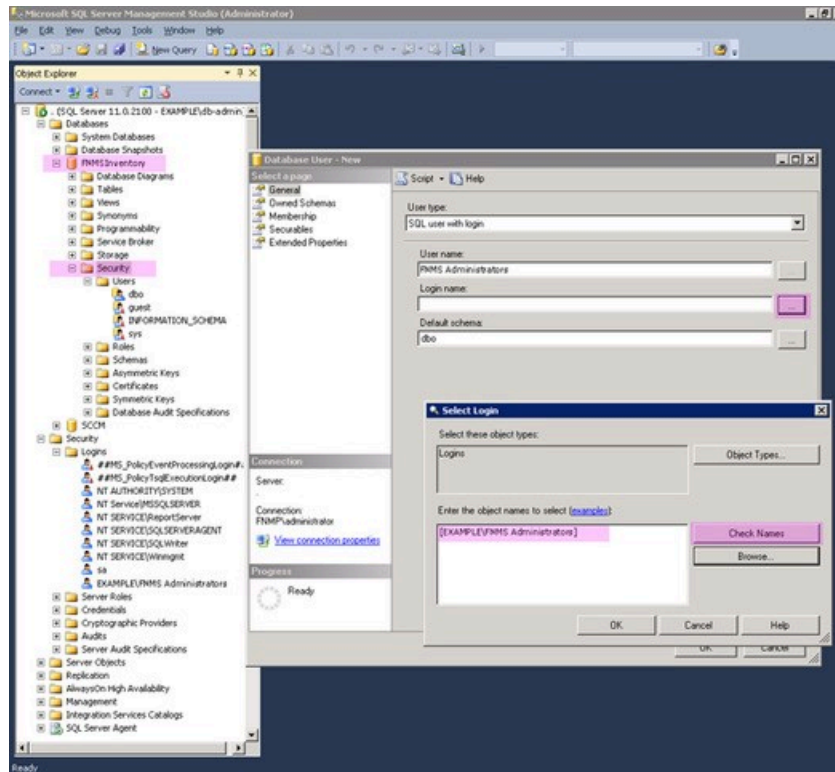
Wait for completion before proceeding.

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



Tip: To ensure that every account is guaranteed to use the same default schema, in the **Default schema** field of the **Database User - New** dialog, enter the same *dbo* schema name for each of the operations databases for FlexNet Manager Suite. Do not enclose the name in square brackets.

- e. 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).
- f. 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.



- g. For your newly-added user, right-click and select the properties, and select the Membership page. Check the db_owner role, and click **OK**.
 - h. Strongly recommended—set the compatibility level on this database:
 - For Microsoft SQL Server 2014 through 2016, set to SQL Server 2012 (110)
 - For Microsoft SQL Server 2017, either set similarly to 110, or set to the default level for the version, such as SQL Server 2017 (140)
 - For Microsoft SQL Server 2019 or Microsoft SQL Server 2022, there is no need to set the compatibility level to anything other than the default.
6. 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* and *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).
 - d. Strongly recommended—set the compatibility level on this database:
- 7. Create a data warehouse database (used for trend analysis, some product reports, and Cognos-based reporting):
 - 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—set the compatibility level on this database:
- 8. 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—set the compatibility level on this database:
- 9. Check all database log files for any errors before proceeding with any installation of FlexNet Manager Suite software.
- 10. Close the command window.
- 11. If you are also implementing Flexera Analytics, you need to create the **content store** database. The content store is a Microsoft SQL Server database used to store information about reporting models, folders, reports, and saved results, which is required by Flexera Analytics. Frequently, this database is installed separately from the other databases, so that it can be configured differently as described below. If your content store is on a separate database server, ensure that (like all the other databases for this system) it uses a case insensitive, accent sensitive collation sequence. If required, create the content store database now:
 - a. Open SQL Server Configuration Manager, expand **SQL Server Network Configuration**, select **Protocols for MSSQLSERVER**, and ensure that **TCP/IP** is Enabled, as required by Cognos to access the data it needs to populate reports.
 - b. Open the Microsoft SQL Server Management Studio, and:
 - In the **Object Explorer** panel, right-click the parent database server.
 - Select **Properties** from the context menu.
 - In the **Server Properties** dialog, select the **Security** page.
 - Ensure that the **Server authentication** is set to **SQL Server and Windows Authentication mode**, as required by Cognos.

- Close the **Server Properties** dialog.
- c. Again in the **Object Explorer** panel, expand the **Security** folder (first-level child of the top SQL Server node), right-click **Logins** and select **New Login...**
- d. Specify the login name for the IBM Cognos Service to access the content store.

This account needs the following permissions on the Cognos content store database:

- Create and Drop table privileges
 - Member of the db_ddladmin, db_datareader, and db_datawriter roles
 - Must be the owner of the default schema on this database.
- e. Select **SQL Server authentication** and enter the appropriate password in the **Password** and **Confirm password** fields.



Note: The password for the SQL Server login account used by the IBM Cognos Service must not contain any of the greater-than, less-than, or ampersand characters (< > &).

- f. Clear **Enforce password policy**.

While saving the password, this clears all three password policy check boxes.

- g. Click **OK**.

- h. Again in the **Object Explorer** panel, right-click **Databases** and select **New Database...** Provide an appropriate name for your database (such as contentstore) and configure the initial database settings (file size, location, and the like) as appropriate.

This database is typically very small, in the order of 12 MB, with potential growth depending on how many reports you store.

- i. On the **Options** page of the **New Database** dialog, ensure that the selected **Collation** ends in **CI_AS** (for example, SQL_Latin1_General_CP1_CI_AS).
- j. Click **OK** to create the database.
- k. In the **Object Explorer** panel, expand **Databases**, expand the contentstore database, then expand its **Security** folder, right-click **Schemas** and select **New Schema...**
- l. Specify the **Schema name**, and click **OK**.

Suggestion: FlexNetReportDesignerSchema

- m. With the same contentstore database selected, under its **Security** folder, right-click **Users** and select **New User...**
- n. For SQL Server 2012 and later, from the **User type** drop-down list, select **SQL user with login**.
- o. Specify a name for the database user in the **User name** field.
- p. Use the **Login name** field to browse and select the account that you created in step 11.c above.
- q. Use the **Default schema** field to browse and select the schema that you created in step 11.l.
- r. In the **Owned Schemas** list, select the same schema as specified in **Default schema**.

- s. In the **Membership** list (called **Role Members** for SQL Server 2008 R2 and earlier), select db_datareader, db_datawriter, and db_ddladmin.
- t. Click **OK**.

You can test the new login by disconnecting from SQL server, and the attempt to log in again using the account. You should be able to see the database in the object explorer.

Finally, if you have not already done so, don't forget to 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. Details for this approach start at [Managing Scripted Installation](#).

Managing Scripted Installation

Your downloaded materials include everything needed to prepare for, and then execute, scripted installations of the various server(s) needed in your implementation. This allows you to minimize interaction and reduce the likelihood of unnoticed human error that may later disrupt 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 scripted installation



Remember: *Databases must exist before you start scripted 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 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 Scripted 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 Scripted 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 [Installing Flexera Analytics](#)).
- c. Configure the application server with the URL of your Flexera Analytics server.
- d. Ensure that one or more roles have been created to permit access.
- e. Add your Flexera Analytics server to your web browser's list of trusted websites.

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 unattended 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: <ul style="list-style-type: none"> • ALL • FlexNetManagerPlatform 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
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 preparing the answer file 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
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. To configure optional security scanning of uploaded documents being attached to licenses, contracts, purchases and the like, find and edit this section in the answer file for your web application server:

```
# Enable/ Disable file scanning feature
# EnableFileUploadScan = Replace_EnableFileUploadScan_Here
# Path to Filescanner.ps1 that will be used to perform file scanning
# FileUploadScannerPath = Replace_FileUploadScannerPath_Here
```

For information about setting up on-demand anti-virus scanning of documents, see the section *Preventing Uploads of Malicious Files* in the *FlexNet Manager Suite System Reference* (on-premises edition for release 2020 R2 or later), available through <http://docs.flexera.com> in either PDF or HTML format. The two registry settings described here form only a part of the required configuration, and the values depend on your design decisions, file names and paths. Configuring these settings through the answer file is optional: if you prefer, you may return to your web application server after installation is complete, and modify the settings manually. An example of an edited section of the answer file for the web application server that turns on document scanning with the recommended anti-virus tool is:

```
# Enable/ Disable file scanning feature
EnableFileUploadScan = true
# Path to Filescanner.ps1 that will be used to perform file scanning
FileUploadScannerPath = C:\ClamAV\Filescanner_ClamAV.ps1
```

Be sure to update the example with the correct path to your PowerShell script for integrating your chosen anti-virus tool; but keep in mind that `EnableFileUploadScan = true` is a mandatory setting to allow document scanning.

11. Save your edited answer file.
12. 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 Scripted Installation

Before running the scripted 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 scripted 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 scripted 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: <div> <pre>drive-and-path\FlexNet Manager Suite\Installers\FlexNet Manager Suite\FlexNet Manager Suite Server.msi</pre> </div>
\$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: <div> <pre>drive-and-path\FlexNet Manager Suite\Support\Config\FNMS Windows Authentication Config.xml</pre> </div>

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: <ul style="list-style-type: none"> • <code>updateConfig</code> (default) — Modifies the installation only with new settings that have been changed in the answer file • <code>forceUpdateConfig</code> — 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 scripted 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 your inventory and license position. Continue this process as administrator (fnms-admin) on either your:

- application server (for a single server installation); or
- web application server (in a multi-server installation).

 **Tip:** The web interface transfers high volumes of HTML data, which may have noticeable performance impacts for operators with slow links (such as across a WAN) between their web browsers and the web application server. To maximize performance, the web.config file installed on this web application server turns on both static and dynamic content compression, with a setting of this form:

```
<urlCompression doStaticCompression="true" doDynamicCompression="true" />
```

These settings turn on compression settings for IIS, where these are available on the web application server:

- Static compression is installed by default for IIS.
- Dynamic compression requires a standard Microsoft installation to enable it. (Without this setup, the dynamic compression setting in the `web.config` file remains latent, having no possible effect.)

If you have operators on slow (WAN) links, check whether dynamic compression is already available on your web application server by examining the **Server Manager**, using the **Add Roles and Features** wizard. If it is not yet configured, see <https://docs.microsoft.com/en-us/iis/configuration/system.webServer/urlCompression#setup> for installation details.

The instructions provided here show how to install the web interface for FlexNet Manager Suite. Additionally, FlexNet Manager Suite can be installed using a scripted installation. For more information, refer to [Managing Scripted Installation](#).



To install the web interface for FlexNet Manager Suite:

1. On the (web) application server, open Windows Explorer.
2. Copy the downloaded archive `FlexNet Manager Suite 2023 R2 Installer.zip` from your staging location to a convenient location on this server (such as `C:\temp`), and unzip it.



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

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



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

5. Step through the installer until asked for the **Setup Type**, and do one of the following:
 - For a small, single server installation combining the web application, the inventory collection, and the batch processing functionality in one server, select the **Complete** option, and follow the instructions in the installation wizard to complete the standard installation.



Tip: In the page where you are asked for the batch process credentials, for **Server type**, choose either **Production** for your main server installation, or **Failover** if this is a stand-by or testing server. 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.*

- For a multi-server installation, select the **Custom** installation path, and select the **Web application server** for this installation. (If this is the *only* functionality on this server, also ensure that **Inventory server**, **Batch scheduling server**, and **Batch server** are all deselected; but in fact you can combine most servers in the way that best suits your enterprise, so make the selection that matches your server plan.)

Take note of the installation location for future reference.

6. If this is a separate installation of the web application server in a multi-server implementation, ensure that from this server you can access the network shares that you configured in [Configure Network Shares for Multi-Server](#).
7. If this server includes the batch server functionality, you are prompted for the credentials used for batch processes. Be sure that the account you enter already has Logon as a service permission (see [Authorize the Service Account](#)).
8. When successful, close the installation wizard.
9. If you have decided to configure on-demand scanning for every uploaded document, you need to turn on the capability. The setup process so far has create the two required registry keys, but has not set the values required to turn on scanning.

if you have not already done so, see details in the section *Preventing Uploads of Malicious Files* in the *FlexNet Manager Suite System Reference* (on-premises edition for release 2020 R2 or later), available through <http://docs.flexera.com> in either PDF or HTML format. If you wish to configure the registry settings now, continue as below (if not, you may defer these changes until later, as part of other changes needed to configure the on-demand scanning).

- a. Open your preferred registry editor on your web application server.

For example, in the Windows search bar, enter Registry and then open Registry Editor.

- b. Navigate in the registry editor to HKLM\Software\WOW6432Node\Flexera Software\FlexNet Manager Platform\Security\CurrentVersion.

- c. Scroll to, and double-click the value FileUploadScannerPath.

- d. Edit the **Value data** field to be the path and file name for your PowerShell integration script.

For example, the default suggested path for the ClamAV tool is

```
C:\ClamAV\Filescanner_ClamAV.ps1
```

However, ensure that your value is correct for your environment and file name. When done, click **OK**.

- e. Scroll back to, and double-click the value EnableFileUploadScan.

- f. Edit the **Value data** field to true, and click **OK**.

- g. Exit the registry editor.

The registry settings have no effect until an operator attempts to upload a document.

Install the Inventory Server

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

In a single server implementation, this step is already completed and you should skip ahead to [Configure the System](#).

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

- processing server (in a two server application installation); or
- inventory server (in a three or more server application installation).



To install the inventory server software:

1. On the inventory (or processing) server, open Windows Explorer.
2. Copy the downloaded archive `FlexNet Manager Suite 2023 R2 Installer.zip` from your staging location to a convenient location on this server (such as `C:\temp`), and unzip it.
3. Navigate in the unzipped archive to the `FlexNet Manager Suite\Installers\FlexNet Manager Suite` folder.
4. Start (double-click) `setup.exe`.



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

5. Select the **Custom** installation path, and do one of the following:
 - For a two server installation, now installing your processing server, select all of the **Inventory server** and the **Batch scheduling server** for this installation, and ensure that the **Web application server** is deselected (displaying a cross).
 - For an installation using three or more servers, now separately installing your inventory server, select only the **Inventory server** for this installation, ensuring that the other options are deselected.

Take note of the installation location for future reference.

6. If this server includes the batch server functionality, you are prompted for the credentials used for batch processes. Be sure that the account you enter already has Logon as a service permission (see [Authorize the Service Account](#)).
7. When successful, close the installation wizard.

Install the Batch Server

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

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

- A single-server implementation combining the web application server, the batch server, and the inventory server in

one; or

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

In these two cases, this step is already completed and you should skip ahead to [Installing a Free-Standing Studio](#).

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:

1. On the batch server, open Windows Explorer.
2. Copy the downloaded archive FlexNet Manager Suite 2023 R2 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. Select the **Custom** installation path, and select only the **Batch scheduling server** for this installation, ensuring that the other options are deselected (displaying a cross).

Take note of the installation location for future reference.

6. When asked to enter the credentials to be used for running batch processes, be sure that the account you enter already has Logon as a service permission (see [Authorize the Service Account](#)).
7. 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.

8. For the batch processor, you are asked to identify the folder where intermediate packages (uploaded from

inventory beacons) are saved prior to processing. The default location is %ProgramData%\Flexera Software\Beacon\IntermediateData. This default is formed by appending IntermediateData to the value of the base directory saved in HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ManageSoft Corp\ManageSoft\Beacon\CurrentVersion\BaseDirectory. This base location is also used by other processes, and should be changed only with care.



Tip: A second folder, a network share, is used for handing off files uploaded through the web interface (such as inventory spreadsheet imports) for processing by the batch server. For this share, the default path is %ProgramData%\FlexNet Manager Platform\DataImport, and the path is saved in the registry at HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ManageSoft Corp\ManageSoft\Compliance\CurrentVersion\DataImportDirectory. There is also a parallel folder for data export. For implementations that separate the web application server from the batch server, these shares must also be configured and accessible from both servers.

For more information, see [Configure Network Shares for Multi-Server](#).

9. When successful, close the installation wizard.

Configure the System

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



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

1. Your web application server
2. Your batch server (or processing server, for a two-server application implementation)
3. Your inventory server(s).

On each applicable server in turn, as administrator (fnms-admin), complete all the following steps (noticing that on different servers, different dialogs may be presented). Before executing the PowerShell scripts, you should first ensure that:

- Your administrator account is a member of the db_owner fixed database role (at least temporarily, as described in [Accounts](#))
- The scripts themselves have sufficient authorization to execute, as described in the following process.



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

- a. Open IIS Manager.
- b. In the **Connections** pane, expand the **Sites** node in the tree, and then click to select the site for which you want to add a binding.
- c. In the **Actions** pane, click **Bindings**.
- d. In the **Site Bindings** dialog box, click **Add**.
- e. In the **Add Site Binding** dialog box, add the binding information and then click **OK**.

For more information (including the set up of the required certificate), see <http://www.iis.net/learn/>

[manage/configuring-security/how-to-set-up-ssl-on-iis.](#)

4. 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.

5. 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.

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

7. 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.

8. 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`.

9. Close the PowerShell command window.

10. 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:

- Navigate to **Start > Control Panel > Administrative Tools > View local services**.

The **Services** dialog opens.

- 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.

11. As required for a multi-server implementation, loop back to step 1 and repeat across a multi-server implementation.



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

12. You now need to activate the product. Please refer to [Product Activation](#).

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 Windows 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 Flexera Analytics

Flexera Analytics provides interactive reporting for software and hardware asset management.



Important: Flexera Analytics uses IBM Cognos version 11.1.7 (or later) as the underlying technology for these reports. Your license for FlexNet Manager Suite includes terms for Flexera Analytics, by default authorizing one Analytics Administrator and 60 Analytics Users (for license installation, see [Product Activation](#)).



Note: Your license does not include usage of IBM Cognos for purposes unrelated to FlexNet Manager Suite. If you are using data from external data sources (that is, a database not related to FlexNet Manager Suite), you need a separate full license for IBM Cognos.

For supported platforms and database versions for each release, see *FlexNet Manager Suite System Requirements and*

Compatibility, available as either PDF or HTML through docs.flexera.com.

Flexera Analytics has the following components:

- **Analytics** — Flexera Analytics is an interactive means for you to explore and create customized reports and dashboards, and easily share these with anyone in your organization.
- **Content Store Database** — The Content Store is a relational database used by the Flexera Analytics to store information about reporting models, folders, reports, and saved results. You should have already completed setting up this database (see [Create Databases](#)).

Once you have confirmed that all prerequisites have been met, installation of Flexera Analytics is performed using the following steps:

1. Install and configure a supported web server
2. Copy the Flexera Analytics installation media
3. Configure Flexera Analytics by populating an answer file with settings appropriate to your environment, and then install, using PowerShell
4. Configure your web server to connect with Flexera Analytics
5. Update your Roles to enable access
6. Ensure that your web browser(s) include your web server in the list of trusted web sites
7. Optionally, you may need to configure your Security Assertion Markup Language settings.

Prerequisites

The IBM Cognos Analytics installer installs Flexera Analytics to the designated host as a service. Therefore, the account used to install this component must have administrator permissions.

Make sure of the following points:

- The installing account must have administrative privileges on the Cognos Analytics server (the server hosting Flexera Analytics).
- The Flexera Analytics server must be accessible by its host name, rather than just its IP address. Do not use IP addresses anywhere in the Flexera Analytics settings.
- For performance reasons, Flexera Analytics is best installed on a separate server (it has high memory use requirements). (Refer back to [Prerequisites and Preparations](#) for server design details.) When Flexera Analytics is installed on a server other than the database server running the content store database, Microsoft SQL Server Native Client must be installed on the server hosting Flexera Analytics. To download and install the Microsoft SQL Server Native Client installer (subject to changes in the Microsoft website):
 1. In your web browser, navigate to <https://www.microsoft.com/en-us/download/details.aspx?id=29065>.
 2. Expand **Install Instructions** to display the available components of the **Microsoft SQL Server® 2012 Connectivity Feature Pack**.
 3. Scroll approximately half-way down the page to the heading **Microsoft® SQL Server® 2012 Native Client** and install the **X64** (64-bit) version of the Native Client found there.
- The Flexera Analytics server must be in the same time zone as your database server(s).

- When you install Flexera Analytics, the required usernames and passwords can be encrypted, using a credential store. Refer to [Prepare Encrypted Credentials](#) for further information. Alternatively, you may choose to use clear text usernames and passwords in the answer file.
- Flexera Analytics can be configured to use *https*, however you will need to use *http* for installation and configuration.
- The password for the SQL Server login account used by Flexera Analytics must not contain any of the greater-than, less-than, or ampersand characters (< > &).
- Do not attempt to use Flexera Analytics (nor any related reports saved in FlexNet Manager Suite) before importing the correct license file from Flexera (see [Product Activation](#)).



Important: Do not allow consultants to use their 'normal' login when they develop reports on your behalf. A common user account should not be switched from one Flexera Analytics tenant to another. Otherwise, any reports saved under **My Folders** for that account are automatically removed by Flexera Analytics as the user account switches between tenants (or customers). For details, see <http://www-01.ibm.com/support/docview.wss?uid=swg21682369>: "For safety, ensure that each consultant uses a login that is unique to your company (such as johnEnterprise); or as a workaround, save their developed reports under **Public Folder**".

Before you start, decide whether you want the benefit of content compression for your Flexera Analytics server. By default, the `web.config` file installed on this server turns on both static and dynamic content compression, with a setting of this form:

```
<urlCompression doStaticCompression="true" doDynamicCompression="true" />
```

Static compression is installed by default for IIS, but dynamic compression requires a standard Microsoft installation to enable it. (Without this setup, the dynamic compression setting in the `web.config` file remains latent.) You can check whether dynamic compression is available in the **Server Manager**, using the **Add Roles and Features** wizard. If it is not yet configured, see <https://docs.microsoft.com/en-us/iis/configuration/system.webServer/urlCompression#setup> for installation details.

Installation



To install Flexera Analytics:

1. Install, configure, and test a supported **web server**.
 - Refer to *FlexNet Manager Suite System Requirements and Compatibility* for FlexNet Manager Suite 2023 R2 on-premises, available as either PDF or HTML through docs.flexera.com, to see the list of supported web servers. Refer to the installation, configuration, and testing documentation provided by the web-server vendor.
 - If you choose to use Microsoft IIS as your web server, the installer for Flexera Analytics includes a PowerShell script to apply appropriate configuration. (You need access to the downloaded unzipped archive of the FlexNet Manager Suite installer to access this PowerShell script.)
2. Copy the Flexera Analytics Installation file.
 - a. If you are installing FlexNet Manager Suite and Flexera Analytics on separate servers, first copy the `<FNMS Media>\FlexNet Manager Suite\Support` directory from the application server to `C:\FNMSCognosAnalytics` on the Flexera Analytics server. If you are performing a single server installation, then the support folder should already be located on the application server.

- b. From the support folder, copy the following files to a working directory on your Flexera Analytics server, such as C:\FNMSCognosAnalytics\Support:




- analytics-installer-2.2.27-win
- ca_srv_11.1.7-2304260612-winx64h.zip.





Tip: The executable from the archive automatically installs 32-bit software on 32-bit systems, and 64-bit software on 64-bit operating systems.

3. Configure the installation of Flexera Analytics by editing the file C:\FNMSCognosAnalytics\Support\CognosConfigProperties.xml using Notepad (or an equivalent text editor). Fill out the values for the parameters listed in the following table, using the guidance from the description and examples provided.

Property/Example	Description
CredentialStoreLocation C:\user\customstore.xml	A custom credential store location. If this parameter is omitted, the value defaults to fnms.password.store.xml under the profile directory of the logged-in user.
FNMSBatchServerLocation http://BatchServer1.company.com	The URL of the FlexNet Manager Suite batch server (or, in smaller implementations, the server hosting that functionality).
ContentStoreDatabaseLocation DBServer1\Instance1	When using TCP, the format for this value is hostname:port. Alternatively, the hostname\instancename format (without a port) can be used. Flexera Analytics does not allow the instance name to be Default or MSSQLServer. If using the instance name format, the SQL Server Browser service needs to be started.
ContentStoreDatabaseName ContentStore	This is the name of your Cognos Analytics content store database.

Property/Example	Description
ContentStoreDatabaseUsername Typically empty	Optional setting when providing credentials for SQL Server authentication. Leave this value blank to use Windows Authentication. <div>  Note: If you have restored a backup of your existing content store to use with a new version of Flexera Analytics, ensure that this user has the following permissions on the database: <ul style="list-style-type: none"> • Create and Drop table privileges. • Member of the <i>db_ddladmin</i>, <i>db_datareader</i>, and <i>db_datawriter</i> roles. • Must be the owner of the default schema on this database. </div> <div>  Tip: This schema usually is named FlexNetReportDesignerSchema. </div>
ContentStoreDatabasePassword Typically empty	Optional setting when providing credentials for SQL Server authentication. Leave this value blank to use Windows Authentication.
ContentStoreDatabaseStoreReference flexera://storeUser	The credential store reference for ContentStore database user identity. If the ContentStoreDatabaseStoreReference property is specified then the ContentStoreUserName and ContentStorePassword properties are not required in the answer file, as any value provided for these fields is overridden.
CognosInstallationPath C:\Program Files\ibm\cognos\analytics	Flexera Analytics installation directory. Update this path to change the default installation path.
CognosServerURI http://\$(ServerName):80	<div>  Note: The <i>\$(ServerName)</i> text should not be altered. It will be translated to the host name by the installation code. </div>

Property/Example	Description
CognosServerDispatcherURI http://\$(ServerName):9300	 Note: The \$(ServerName) text should not be altered. It will be translated to the host name by the installation code.
AppPoolUserName Company\svc-fnms	The service user, used by IIS.
AppPoolPassword (clear text)	A clear text password.
AppPoolStoreReference flexera://serviceUser	<p>The credential store reference for App Pool user identity.</p> <p>If AppPoolStoreReference property is specified then the AppPoolUserName and AppPoolPassword properties are not required in the answer file. Any value provided for these fields is overridden.</p>
CognosServiceUserName Company\svc-fnms	<p>The service user for the IBM Cognos Analytics service. This must have read access to the FNMPDatawarehouse database, as well as being a member of the local Administrators group. Ensure that the account you enter already has Logon as a service permission (see Authorize the Service Account).</p>
CognosServicePassword (clear text)	A clear text password.
CognosServiceStoreReference flexera://serviceUser	<p>The credential store reference for Cognos service user identity.</p> <p>If CognosServiceStoreReference property is specified then the CognosServiceUserName and CognosServicePassword properties are not required in the answer file. Any value provided for these fields is overridden.</p>

Property/Example	Description
CognosServiceMaxMemory 4096	<p>IBM recommends a minimum of 4GB (4096MB) for Cognos Analytics. This number is a starting point and should be adjusted upwards based on the memory usage of your system.</p> <hr/> <p> Note: This value determines the amount of memory used by the Java Virtual Machine and depends on how much memory is available. If this value is too high, the process will fail to start and no log information will be generated.</p>
MachineKeyValidationKey ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789	<p>This is taken from the web.config file on the FlexNet Manager Suite presentation server. For example: C:\Program Files (x86)\Flexera Software\FlexNet Manager Platform\WebUI\web.config.</p> <p>The required value is present in the <machineKey> element.</p>
MachineKeyDecryptionKey 0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ	<p>This is taken from the web.config file on the FlexNet Manager Suite presentation server. For example: C:\Program Files (x86)\Flexera Software\FlexNet Manager Platform\WebUI\web.config.</p> <p>The required value is present in the <machineKey> element.</p>
SmtpStoreReference flexera:\smtp	<p>The credential store reference for SMTP user identity. If SmtpStoreReference property is specified then the SmtpUserName and SmtpPassword properties are not required in the answer file. Any value provided for these fields is overridden.</p>
FNMSConfiguration op	<p>This value defines the FlexNet Manager Suite environment configuration. This value is pre-populated based on the installation media and does not require the user to change it.</p> <p>Modifying this value will cause the Flexera Analytics installation to fail.</p>



Note: If the CognosConfigProperties.xml file contains passwords in clear text, after installation this file should be cleared of passwords; or kept in a file path that is only accessible to Administrators and copied to a secure location off the host server. The file should be preserved for use in future upgrades.

- a. Open a PowerShell command-line window with Administrator privileges.

- b. Navigate to the directory where you copied the support directory. For example
C:\FNMSCognosAnalytics\Support

- c. If you have not done so already, set the PowerShell permissions with the following command:

```
set-ExecutionPolicy AllSigned -Force
```

Respond to the warning text with the default Y.

- d. Run the following command:

```
.\InstallCognos.ps1
```

- e. A dialog box opens, prompting you to run the installer. Click **Run** to proceed with the installation.



Tip: This may take some time to complete. After updating the configuration with the details you provided, the PowerShell script restarts the **IBM Cognos** service. If the script reports any difficulties restarting the service, it may be because of environmental issues, such as memory pressure. In this case, it is not necessary to run the PowerShell script again: you can try restarting the **IBM Cognos** service manually in Windows Service Manager.

4. Your web server needs to be configured for use with Flexera Analytics. The externally visible URL of the Flexera Analytics server needs to be set on the web application server so that FlexNet Manager Suite knows where to go when opening Flexera Analytics from **Reports** mode.

- a. Log into your web application server.
- b. Open a PowerShell command-line window with Administrator privileges.
- c. Navigate to the <FNMS Media>\FlexNet Manager Suite\Support directory.
- d. Execute the commands

```
Set-ExecutionPolicy AllSigned -Force
```

and

```
.\Config.ps1 ".\Config\FNMS Cognos Config.xml" updateConfig
```

You will now be asked to enter the externally visible URL of the Flexera Analytics server, in the format `http://{servername}`.



Tip: If your Flexera Analytics server is using encrypted communication over the HTTPS protocol, specify `https:` as part of this value.

Press **Ok**.

5. Before any operator can access any part of Flexera Analytics, you must have created and assigned a **Role**. This is only possible after you have imported the correct license file from Flexera):

- a. Create a role to which you have assigned the Analytics User privilege, and a second role that has the Analytics Administrator privilege (in the web interface for FlexNet Manager Suite, navigate to the system menu (⚙️ ▼ in the top right corner), select **Accounts**, select the **Roles** tab, use the **Business**

reporting portal section, and click the help button for further details).

- b. Assign the appropriate operator(s) to these roles.

If you do not complete this step before accessing Flexera Analytics, you may experience an error after you sign in.



Important: By default, no more than 60 operators may be linked to the role that grants the *Analytics User* privilege (or to all roles that grant this privilege). If you assign more than 60 operators to these roles, all operators are locked out until you reduce the count of operators to the licensed limit. If you need more than 60 operators with this privilege, contact your Flexera Consultant with your request to increase the licensed count.

6. For security reasons, a browser will not provide a user's credentials to the Flexera Analytics server unless the site (or subdomain) is on a list of trusted websites. Extra steps are required to enable silent Windows authentication.
 - **Internet Explorer or Chrome** on Windows
 - a. The Flexera Analytics server must be added under Local Intranet Zone in **Internet Options**. If not, the credentials will not be passed to the site and the user will be prompted to enter their credentials every time they navigate to Flexera Analytics from within FlexNet Manager Suite. You can either add the Flexera Analytics URL to trusted websites locally on the workstation or through your corporate group policy.
 - **Firefox** on Windows
 - a. Launch FireFox.
 - b. In the address bar type `about:config` and click **Enter**.
 - c. If prompted with the security warning choose "I'll be careful, I promise".
 - d. After the configuration page loads, in the filter box, type: `network.automatic`.
 - e. Modify `network.automatic-ntlm-auth.trusted-uris` by double-clicking the row and enter the fully qualified URL of the Flexera Analytics server. For example `http://cognos11.domain`.
7. If you wish to configure Security Assertion Markup Language (SAML) authentication for Flexera Analytics, please refer to the *Authentication* chapter in the *FlexNet Manager Suite Systems Reference* guide. Here you will find the instructions to run the **Flexera Report Designer Package Import Utility** to update your SAML authentication configuration.
8. If you wish to use the HTTPS protocol with your preferred certificates (rather than the default certificates supplied with IBM Cognos), or to configure the Transport Layer Security (TLS) protocol for Flexera Analytics, please continue with the following topics:
 - [Configuring IIS to Use SSL/TLS Encryption](#)
 - [Reconfigure Cognos Analytics to Use Third-Party SSL Certificates](#).

Optional for reinstallation

If you are ever reinstalling Flexera Analytics, you can use one of the following switches to skip specific segments of the installation process, but these cannot be used during a new installation.

Parameter	Description	Syntax
SkipApplyFiles	Skips the extraction of the authenticator, OAuth module, logging configuration and web content, as well as copying of some configuration files.	<code>.\InstallCognos.ps1 -SkipApplyFiles</code>
SkipConfigureIIS	Skips the IIS settings configuration segment of the script.	<code>.\InstallCognos.ps1 -SkipConfigureIIS</code>
SkipConfigureService	Skips the Cognos service configuration segment of the script.	<code>.\InstallCognos.ps1 -SkipConfigureService</code>

Configuring IIS to Use SSL/TLS Encryption

Before completing the following process, you must have all your SSL certificates in place to create the chain of trust on all servers. We recommend that you test that Flexera Analytics is working before proceeding with this configuration change.



Important: If you are using a Certificate Authority (CA) that is not one listed by default in Windows certificate stores, the CA's root certificate need to be imported into all user's computers to ensure secure communication between their web browsers and the Flexera Analytics server.

All servers in your FlexNet Manager Suite implementation must be configured to use Secure Sockets Layer for communication. This includes your Flexera Analytics host, and your application server for FlexNet Manager Suite itself. If you have a larger, multi-server implementation, these changes must be configured on your web application server, your batch server, and your inventory server (or the servers on which you are hosting these areas of functionality). Those FlexNet Manager Suite servers are assumed to be already configured following your installation or most recent upgrade.



To configure IIS on your Flexera Analytics server to use SSL:

1. Import all relevant certificates into the Windows Local Machine certificate stores.

Save the certificates as follows:

- If you have an unusual root certificate from a Certificate Authority (CA) not already known in the Microsoft Windows Trusted Store, save it under **Trusted Root Certification Authorities**.
- Your SSL certificate (usually .pfx) is saved under **Personal** (this is your public key certificate issued by the CA).
- Any intermediate certificates not already trusted in Windows are saved under **Intermediate Certification Authorities**.

2. Launch IIS on your Flexera Analytics server and configure it as follows:

- a. Select the web server for Flexera Analytics.
- b. Open the **SSL Certificates** feature and import your SSL certificate (usually .pfx).
- c. Add the HTTPS binding for the Flexera Analytics website (usually, this is the default website), and select

the displayed SSL certificate to use for encryption.

- d. Open **SSL Settings** for the default website, and turn on the **Require SSL** option.
- e. Under the same website, navigate to `ibmcognos/bi`, and open its **URL Rewrite** feature.
- f. Update the **Reverse Proxy** rule to use HTTPS as part of **Rewrite URL**.
- g. Restart the web server.

With IIS suitably configured on your Flexera Analytics server, you now need to reconfigure Cognos to use your preferred certificates in place of the default certificates installed with it.



Important: To enable SSL between your Flexera Analytics web server and Cognos, you must configure **one** of the following steps (you cannot configure both):

- [Reconfigure Cognos Analytics to Use Third-Party SSL Certificates](#)
- [Reconfigure Cognos gateway to use SSL using self-signed certificates.](#)

Reconfigure Cognos Analytics to Use Third-Party SSL Certificates

This process switches Cognos Analytics over from using the default certificates provided by IBM to using the certificates you have saved for your servers. IBM refers to this process as "decrypting" Cognos Analytics. The process restores the chain of trust, enabling SSL communication between various Cognos Analytics components, as well as between Cognos Analytics and the others servers for FlexNet Manager Suite.

Commence this process while logged in to your Flexera Analytics server, using an account with administrator privileges.



To decrypt Cognos Analytics to use third-party certificates:

1. Navigate to the Cognos Analytics installation directory (usually `C:\Program Files\ibm\cognos\analytics`).
2. Take a protective backup copy of the configuration folder.
3. Launch the IBM Cognos Analytics Configuration tool as administrator, and stop the Cognos Analytics service if it is running.
4. Navigate to **File > Export As** and export the decrypted content as `backup.xml` in the configuration folder. Choose **Yes** at the prompt, and save the file.
5. *Without* restarting the Cognos Analytics service, close the IBM Cognos Analytics Configuration tool.



Important: Do not re-open the IBM Cognos Analytics Configuration tool until instructed to do so.

6. Create a backup of the following directory, and move it from the `analytics` directory:
`CognosInstallationPath\temp\cam\freshness`
7. Open a command prompt as administrator, and run the following commands to delete existing content.

If you have a non-standard installation path, replace the default Cognos Analytics installation path shown here with the one from your environment.

```
cd "C:\Program Files\ibm\Cognos\analytics"
del .\configuration\cogstartup.xml
del .\configuration\caSerial
del .\configuration\certs\CAMCrypto.status
del .\configuration\certs\CAMKeystore
del .\configuration\certs\CAMKeystore.lock
del .\temp\cam\freshness
rd .\configuration\csk /S /Q
```

8. In the *CognosInstallationPath*\configuration directory, rename backup.xml to cogstartup.xml.



Remember: Do not start the IBM Cognos Analytics Configuration tool until specifically instructed to do so.

9. Open a command prompt as an administrator, and change to the directory *CognosInstallationPath*\bin.
10. Enter a command using the following syntax:

When providing details for your <domainName>, customize the following parameters: CN (set to your domain), OU, O, L, and C.

```
cd c:\Program Files\ibm\cognos\analytics\bin
ThirdPartyCertificateTool.(bat|sh) -c -e [-p <keystorePassword>]
-a <keyPairAlgorithm> -r <path/to/CertOrCSR> -d <domainName>
[-H <subjectAlternativeNameDnsNames>] [-I <subjectAlternativeIpAddresses>]
[-M <subjectAlternativeEmailAddresses>]
```

Example:

```
cd c:\Program Files\ibm\cognos\analytics\bin
ThirdPartyCertificateTool.bat -c -e -p NoPasswordSet -a RSA -r "request.csr"
-d "CN=server.domain.com,OU=Support,O=IBM,L=Ottawa,C=CA" -H "server.domain.com"
```

11. Best practice: Take a new backup of the complete *CognosInstallationPath*\configuration folder, save it in a different location/folder, and name the backup configuration.waiting_on_certs.

This backup allows you to recover the cryptographic keys from a known point where we are waiting on the certificate request being signed. This is a natural pause point if you need to bring Cognos Analytics back online, and it prevents having to redo all the steps above in case a problem arises.



Tip: If the Certificate Authority takes longer to issue certificates than your allowed downtime, then you may:

- a. Rename the current *CognosInstallationPath*\configuration directory to *CognosInstallationPath*\configuration.waiting.
- b. Restore the original, backup *CognosInstallationPath*\configuration directory that you made at step 2.
- c. Restart Cognos Analytics.

At this point, Cognos Analytics functions exactly as it did before starting this 'decrypting' process. Later, when the certificates arrive, you may:

- a. Stop the Cognos Analytics services.

-
- b. Rename the current `CognosInstallationPath\configuration` directory to `CognosInstallationPath\configuration.original`.*
 - c. Rename the `CognosInstallationPath\configuration.waiting` to `CognosInstallationPath\configuration`.*
 - d. Resume the remaining steps in this 'recrypting' process.*

- 12.** Get `encrypt.csr` signed by the Certificate Authority (such as DigiCert or Verisign), and receive back their root, intermediate (optional) and server certificates.
-



Tip: You cannot use self-signed certificates, as self-signed certificates are not trusted by IBM Cognos components.

- 13.** Download the root, intermediate, and server certificates onto the Cognos Analytics server.
- 14.** Use the following steps to convert each certificate to Base-64 encoded X.509 (.CER) format:
 - a.** In Windows Explorer, identify the certificate, and right-click and select **Open** (or simply double-click the file name).
 - b.** Click the **Details** tab.
 - c.** Click **Copy to File**.
A **Certificate Export Wizard** dialog appears.
 - d.** In the **Certificate Export Wizard** dialog, click **Next**.
 - e.** From the available options, select **Base-64 encoded X.509 (.CER)** format.
 - f.** Click **Next**.
 - g.** Enter the appropriate file name from these options, saving in the `CognosInstallationPath\bin` directory:
 - `root.cer`
 - `server.cer`
 - `intermediate.cer` (if you have an intermediate certificate).
 - h.** Click **Next**.
 - i.** Click **Finish**.
 - j.** Click **OK** to dismiss the message box and all pop-up windows.
 - k.** Loop back and repeat for each remaining certificate.
- 15.** If you did *not* receive an intermediate certificate, skip ahead to step **16**. If you *did* receive an intermediate certificate, you must also create a chain certificate, and then import all the certificates, as follows:
 - a.** In your preferred text editor, open the newly created root certificate and copy the entire text. Close the `root.cer` without saving it (so that it remains unchanged).
 - b.** In your preferred text editor, open the newly-created intermediate certificate (`intermediate.cer`), and paste the copied root certificate text below the intermediate certificate text.

- c. Save the modified file into the *CognosInstallationPath*\bin folder with the new name chain.cer.
- d. Open a command prompt as administrator, and run the following commands in the order shown to import the certificates:

```
cd c:\Program Files\ibm\cognos\analytics\bin
ThirdPartyCertificateTool.bat -i -T -r root.cer -p NoPasswordSet
ThirdPartyCertificateTool.bat -i -T -r intermediate.cer -p NoPasswordSet
ThirdPartyCertificateTool.bat -i -e -r server.cer -t chain.cer -p
NoPasswordSet
```

Continue from step 17.

- 16. Because you have no intermediate certificate (and therefore no need to create a chain certificate), open a command prompt as administrator, and run the following commands in the order shown to import your two certificates:

```
cd c:\Program Files\ibm\cognos\analytics\bin
ThirdPartyCertificateTool.bat -i -T -r root.cer -p NoPasswordSet
ThirdPartyCertificateTool.bat -i -e -r server.cer -t root.cer -p NoPasswordSet
```

Continue with the following steps.

- 17. In your preferred text editor, open *CognosInstallationPath*\configuration\FLEXnet.properties, and update the protocol in the URL to read HTTPS.
- 18. Launch the IBM Cognos Analytics Configuration tool as an administrator.
- 19. Navigate to **Cryptography**, and:
 - a. Change **Common symmetric key store password** to NoPasswordSet.
 - b. If your enterprise policy does not allow versions of TLS prior to 1.2, edit **SSL Protocols** accordingly.



Tip: We recommend using TLS 1.2. You may wish to refer to this knowledge base article for configuration details: <https://community.flexera.com/t5/FlexNet-Manager-Knowledge-Base/Analytics-Cognos-Connection-to-SQL-Server-Fails-When-Server-is/ta-p/113351>.

- 20. Navigate to **Cryptography > Cognos**, and:
 - a. Change **Key store password** to NoPasswordSet.
 - b. Change **Server common name** to the *fully-qualified domain name* (FQDN) of your Analytics server.
 - c. Change **Country or region code** to match the country code of your saved certificates.
 - d. Set **Use third party CA?** to True.
 - e. Change **Certificate Authority service common name** to match the Common Name (CN) of the CA root certificate.
 - f. Change **Certificate Authority password** to NoPasswordSet.
 - g. Change the **Certificate lifetime in days** figure to reflect time until the expiry date of the server certificate.
- 21. Navigate to **Environment**, and change all URIs (**Gateway URI**, **External dispatcher URI**, **Internal dispatcher URI**,

Dispatcher URI for external applications and **Content Manager URI**) to use the HTTPS protocol. In **Gateway URI** and **Controller URI for gateway**, also replace port 80 with 443.

22. Save the updated configuration.
23. Start the Cognos Analytics service.
24. Close the configuration tool.

Flexera Analytics, powered by Cognos Analytics, is now using the certificates in your preferred chain to certify SSL communications.

Reconfigure Cognos gateway to use SSL using self-signed certificates

This process configures Cognos server to use the certificates you have saved for your servers. IBM refers to this process as "recrypting" Cognos. The process restores the chain of trust between IIS and Cognos gateway (webserver) only. The communication between various Cognos components can be kept as non-SSL, in this case. Commence this process while logged in to your Flexera Analytics server, using an account with administrator privileges.



To recrypt Cognos to use self-certificates:

1. Launch the IBM Cognos Configuration tool as an administrator and stop the Cognos service if it is running.
2. Navigate to the Cognos installation directory (usually C:\ProgramFiles\ibm\cognos\analytics).
3. Take a protective backup copy of the configuration folder, and name it as configuration_original_datetime in a separate directory.
4. Navigate to **File > Export As** and export the decrypted content as *backup_original.xml* in a separate folder. Choose 'Yes' at the prompt and save the file.
5. Without restarting the Cognos service, close the IBM Cognos Configuration tool.



Important: Do not re-open the IBM Cognos Configuration tool until instructed to do so. The configuration and cogstartup.xml are backed up so that the configuration could be reverted to non-SSL state should there be any issues with certs.

6. Follow the web-server vendors' (Microsoft IIS, Apache) documentation to set up the web server correctly with SSL before making any changes in Cognos Analytics.



Note: In this case, we do not require the request.csr file to be generated via Cognos Analytics server. You may work with IT/networking team to generate certificates on the server directly.

7. Get a copy of the web server certificates and download all the levels that make up the full certificate.



Note: Importing the certificates ensures that there is full chain of trust between the webserver and the application (cognos analytics) install that the webserver routes the request to.

8. Download the root, intermediate, and server certificates onto the Cognos Analytics server.

9. Use the following steps to convert each certificate to Base-64 encoded X.509 (.CER) format and save them under the *CognosInstallationPath\bin* directory as *root.cer*, *server.cer*, and *intermediate.cer* respectively.
 - a. Open a certificate.
 - b. Click the **Details** tab.
 - c. Click **Copy to File**. A **Certificate Export Wizard dialog** appears.
 - d. In the **Certificate Export Wizard dialog**, click **Next**.
 - e. From the available options, select **Base-64 encoded X.509 (.CER)** format.
 - f. Click **Next**.
 - g. Enter the appropriate file name from these options, saving in the *CognosInstallationPath\bin* directory:
 - *root.cer*
 - *server.cer*
 - *intermediate.cer*.
 - h. Click **Next**.
 - i. Click **Finish**.
 - j. Click **OK** to dismiss the message and all pop-up windows.
 - k. Loop back and repeat for each remaining certificate.

10. Open a new command prompt as an administrator to import the certificates in the following order with these commands:

```
Windows Operating System:
cd c:\Program Files\ibm\cognos\analytics\bin
ThirdPartyCertificateTool.bat -i -T -r root.cer -p NoPasswordSet
ThirdPartyCertificateTool.bat -i -T -r intermediate.cer -p NoPasswordSet
ThirdPartyCertificateTool.bat -i -T -r server.cer -p NoPasswordSet
```

11. In your preferred text editor, open *CognosInstallationPath\configuration\FLEXnet.properties*, and update the protocol in the URL to read HTTPS.
12. In your preferred text editor, update the **web.config** file under *ApplicationserverinstallationPath\Program Files (x86)\Flexera Software\FlexNet Manager Platform\WEBUI* to read *biportalURL* as HTTPS.
13. Launch the IBM Cognos Configuration tool as an administrator.
14. Navigate to **Environment** and change **Gateway URI** to HTTPS protocol. Also, update the port number to 443.
Example: *https://<webserver FQDN>:443/ibmcognos/bi/v1/dispatch*.
15. Save the updated configuration.
16. Start the Cognos service and close the Configuration tool.
17. Ensure that the certificates are added to the Trusted Root Certificates and Intermediate Certificates in the MMC console.
18. Launch IIS on Flexera (Cognos) Analytics server and configure it as follows:

- a. Navigate to the website and add bindings to configure HTTPS.
- b. Add the correct server host name (FQDN) and certificate name.
- c. Restart IIS.

Reconfigure Cognos components to use Cognos signed certificate



Note: This is an optional step that enables SSL across your full Cognos estate and components. Complete this step after completing one of the above steps ([Reconfigure Cognos Analytics to Use Third-Party SSL Certificates](#) or [Reconfigure Cognos gateway to use SSL using self-signed certificates](#)).

This process configures SSL communication between Cognos components using Cognos Analytics' built-in functionality to create and sign certificate. Once the webserver (gateway) has been enabled to use SSL protocol, the following process is to be followed if there is no requirement to use third-party certificates. Commence this process while logged in to your Flexera Analytics server, using an account with administrator privileges.



To reencrypt Cognos Analytics to use Cognos signed certificate:

1. Launch the IBM Cognos Configuration tool as an administrator and stop the Cognos service if it is running.
2. Navigate to the Cognos installation directory (usually C:\ProgramFiles\ibm\cognos\analytics).
3. Take a protective backup copy of the configuration folder and save it as *configuration_withgatewaySSL_datetime* in a separate directory.
4. Navigate to **File > Export As** and export the decrypted content as *backup.xml* in the configuration folder. Choose 'Yes' at the prompt and save the file.
5. Without restarting the Cognos service, close the IBM Cognos Configuration tool.
6. Create a backup of the following directory and move them from the analytics directory:
CognosInstallationPath\temp\cam\freshness.



Important: Do not re-open the IBM Cognos Configuration tool until instructed to do so.

7. Open a command prompt as administrator and run the following commands (update Cognos installation path) to delete existing content.

If you have a non-standard installation path, replace the default Cognos installation path shown here with the one from your environment.

```
cd "C:\Program Files\ibm\Cognos\analytics"
del .\configuration\cogstartup.xml
del .\configuration\caSerial
del .\configuration\certs\CAMCrypto.status
del .\configuration\certs\CAMKeystore
del .\configuration\certs\CAMKeystore.lock
del .\temp\cam\freshness
```

```
rd .\configuration\csk /S /Q
```

8. In the *CognosInstallationPath*\configuration folder, rename 'backup.xml' to 'cogstartup.xml'.



Remember: Do not start the IBM Cognos Analytics Configuration tool until specifically instructed to do so.

9. In the *CognosInstallationPath*\configuration folder, rename 'backup.xml' to 'cogstartup.xml'.
10. Launch the IBM Cognos Analytics Configuration tool as an administrator.
11. Navigate to **Environment** and change all URIs to change all URIs to use HTTPS protocol. In Gateway URI and Controller URI for gateway, also replace port 80 with 443.
12. Navigate to **Environment > Configuration Group** and enter the fully qualified host name into the following fields:
 - a. Group contact host
 - b. Member coordination host.
13. Navigate to **Security > Cryptography > Cognos** and enter the fully qualified host name into the following fields:
 - a. Server common name
 - b. Subject Alternative Name > DNS names.
14. If an alias name is being used instead of a server host name, then update the following fields:
 - a. Under the Gateway URI (update to the alias name)
 - b. Under **Security > Cryptography > Cognos > Subject Alternative Name > DNS Name** (add the alias name next to the fully qualified domain name).
15. Save the configuration.
16. Ensure that the biportalURL under Program Files (x86)\Flexera Software\FlexNet Manager Platform\WebUI\web.config file reads as HTTPS.
17. Ensure the URL under *CognosInstallationPath*\configuration\FLEXnet.properties file, reads as HTTPS.
18. Start the IBM Cognos service.
19. To use Cognos as the certifying authority, export the Cognos root certificate and import it to trusted root certificate authorities.



Note: This ensures that IIS trusts the Cognos certificate authority that signed the certificate.

20. Launch a command prompt window selecting 'Run as Administrator' from the *CognosInstallationPath*\bin directory:
 - a. Windows Operating System: ThirdPartyCertificateTool.bat -E -T -p NoPassWordSet -r CognosCAroot.cer
 - b. This command generates the CognosCAroot.cer in the *CognosInstallationPath*\bin directory
 - c. Copy the certificate to the IIS server (within analytics server)
 - d. Right-click on the certificate and select Install Certificate
 - e. Select Local Machine for the store location

- f. Select 'Place all certificates in the following store'
- g. Under browse button, select 'Trusted Root Certification Authorities'
- h. Select **Next** and **Finish**.

21. Launch IIS on Flexera Analytics server and configure it as follows:

- a. Navigate to **website> ibmcognos/bi** and open the URL Rewrite feature
- b. Update the Reverse Proxy rule to use HTTPS
- c. Apply the changes
- d. Ensure that the bindings in IIS contain HTTPS and reference the correct certificate
- e. Restart the web server (IIS).

Import the Sample Reporting Package

This section is only for those using Flexera Analytics (powered by Cognos).



Important: Before attempting this process, be sure that you have imported the latest license for FlexNet Manager Suite, which includes new license terms for Flexera Analytics. You should have completed this license import in the topic [Product Activation](#).

If you wish to continue with custom reporting through Flexera Analytics, use the following process to update your reports package for the new release. In overview, you need to:

- Authorize the service account to complete the import
- Perform the import itself
- Restore normal operational permissions to appropriate accounts.



To import the sample reporting package:

1. In the web interface for FlexNet Manager Suite 2023 R2, add your service account (suggested: svc-flexnet) as an Analytics Administrator for the business reporting portal as follows:



Tip: You need to have administrator privileges within FlexNet Manager Suite to make these changes.

- a. Navigate through the system menu (⚙️ ▼ in the top right corner) > **Accounts**.
The **Accounts** page opens.
- b. Select the **Roles** tab, and check for the existence of the **Business Reporting Portal Admin** role.
If the role does not already exist, you can create it.
- c. Click the edit (pencil) icon at the right-hand end of the card for this role.
The properties page for this role appears.
- d. Expand the **Business reporting portal** tab of the accordion, and from the **Privileges** drop-down list, ensure

the **Analytics Administrator** feature has **Allow** permissions.

- e. Switch to the **All Accounts** tab, locate your service account (suggested: svc-flexnet) in the list, and click the account name hyperlink.

The page switches to show **Account Properties** for your account.

- f. Under the **Permissions** section, check whether your **Business Reporting Portal Admin** role is already listed against the service account. If so, you are set for upload permissions, and should continue with the next step.
- g. Click the **+** button to the right of the current **Role** to add this account to another role.

A duplicate line appears with another drop-down list of all the roles defines so far.



Tip: Each enterprise is licensed for only a single operator in the **Analytics Administrator** role. If one has already been assigned this privilege, you need to move that account out before you can add the service account.

- h. From the duplicate drop-down list, select your **Business Reporting Portal Admin** role.

The **Business reporting portal** tab of your resulting list of privileges is updated. If you expand this tab of the accordion, you see that **Analytics Administrator** now displays **Allowed** access.

- i. Scroll to the bottom of this page, and click **Save**.

Your services account is now the (only) **Analytics Administrator** for use of the Flexera Analytics.



Tip: Flexera Analytics also requires that this account is valid in Active Directory.

This privilege level allows the account to complete the import of the sample reports package. Keep this web page available for further use shortly.

2. Using the service account (suggested: svc-flexnet), log into your batch server directly.

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



Note: The following 6 steps can be completed using a package import utility as described here, or using a command-line interface (for which see the note at the end of the process).

3. Navigate in Windows Explorer to `installation-folder\Cognos\BusinessReportingAuthenticationService\bin`.

Example:

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

4. Right-click `CognosPackageImport.exe` and click **Run as Administrator**.

A window appears for the **Flexera Report Designer Package Import Utility**.

5. Click **Update...**

An **Update Value** dialog appears.

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

In a typical installation, this value has the form:

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

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



Tip: If your Flexera Analytics server is using encrypted communication over the HTTPS protocol, specify `https:` as part of this value.

7. Click **Update.**

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



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

8. Click **Install Reports Package.**

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



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

9. Restore the Analytics Administrator privilege to an appropriate interactive operator account.

- a.** Back in the web interface for FlexNet Manager Suite 2023 R2 (in the **Accounts** tab of the same page), remove your service account (suggested: `svc-flexnet`) from the `Business Reporting Portal Admin` role that includes the sole Analytics Administrator privilege (do this in the account properties, by deleting the appropriate line in the **Roles** group). Save the account properties that you have changed.
- b.** Switch to the appropriate administrator account (suggestion: `fnms-admin`), and for this account add the `Business Reporting Portal Admin` role. Save the changed account properties.

Flexera Analytics dashboards and reports are now available as baselines for your own customization and extension as required. The dashboards and reports can be accessed in a web browser through the web interface for FlexNet Manager Suite: select **Reports** in the modal bar at the very top, then select **Analytics** in the menu bar. Selecting **Analytics** will provide you with three options:

- **Software Asset Management** — This dashboard, provided by Flexera, displays information about applications, installations, and licenses
- **Hardware Asset Management** — This dashboard, provided by Flexera, displays information about assets, discovered devices, and inventory
- **My Analytics home** — This is a personal dashboard enabling the creation of a customized dashboard, populated using a variety of supplied widgets, for each operator's specific needs.

As well, the appropriate administrator's account is configured to manage Cognos rights for other users.

Remember that Flexera Analytics requires that you allow pop-ups, and that the URL for your reports (where this is separate from the URL for your web interface) must be a trusted site for your web browser. See step 6 in [Installing Flexera Analytics](#) for more details.



Note: Rather than using the **Flexera Report Designer Package Import Utility** as described above, you can use the following command-line interface:

1. Open a command line as Administrator.
2. Navigate to `installation-folder\Cognos\BusinessReportingAuthenticationService\bin`.
3. Run the following commands, replacing the `RD-Server` placeholder with the name of your server hosting Cognos Analytics:

```
CognosPackageImportConsole.exe set -d "http://RD-Server:9300/p2pd/servlet/dispatch"
CognosPackageImportConsole.exe import
```



Note: If you are using single sign-on using either a SAML-compliant identity provider or Google OAuth, change the second command by adding the `--saml` (or `-s`) switch:

```
CognosPackageImportConsole.exe import -s
```



Important: If you choose to use the command-line interface, please be advised that the following options are not supported for an on-premises installation, and will not work if they are specified as part of the install:

- `add` — Add system administrator login
- `remove` — Remove system administrator login
- `sync` — Synchronize tenants.

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 the 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 an 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 additional 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://community.flexera.com/>, 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, click the *Let's go!* button on the login page to request one. Your credentials are configured for access to content you have licensed.

 - b. Select **Find My Product** and choose **FlexNet Manager** from the top menu. Now click the button **PRODUCT RESOURCES - PRODUCT INFORMATION** which will expose the **Download Products and Licenses** link. Click on this option.

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 immediately below it, click **LET'S GO**.

The Product and License Center site displays.
 - 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 2023 R2](#) to access the downloads.
2. In the list of components to download, select **Business Adapter Studio for FlexNet Manager Suite 2023 R2 .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 the online help or *FlexNet Manager Suite System Reference*. For details about the Business Importer, see *Using FlexNet Business Adapters*.

Product Activation

Details of your license were emailed to you as part of the order confirmation process. Continue this process as administrator (fnms-admin), on the appropriate server (the one that includes the batch server):

- The application server (in a single server implementation)
- The processing server (in a two server application implementation)
- The batch server (in a three server application implementation).



To activate FlexNet Manager Suite:

1. On the appropriate server, save a copy of your license in a convenient folder (such as your installation folder), where it is accessible for this activation process.
2. From the Windows Start menu, run **Flexera Software > FlexNet Manager Suite Activation Wizard**.
3. Import your license to use FlexNet Manager Suite.

Populate the Downloadable Libraries

FlexNet Manager Suite comes with an Application Recognition Library, and a SKU (Stock Keeping Unit) Library. You may also have the End of Service Life (EOSL) product, and additional Product Use Rights Libraries (depending on whether you have licensed FlexNet Manager for Datacenters). The various libraries are updated regularly by Flexera and normally downloaded automatically.



Tip: Some product functionality updates are also delivered through the library downloads (for example, the latest version of the *InventorySettings.xml* file, containing extended functionality for the FlexNet inventory agent).



Note: If your server has Internet access controlled through a proxy server, the following URLs must be accessible:

- For the ARL: <https://www.managesoft.com:443/support/Compliance/RecognitionAfter82.cab>
- For the EOSL library: <https://www.managesoft.com:443/support/Compliance/EOSL.cab>
- For the SKU library: <https://www.managesoft.com:443/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.

For backward compatibility, the HTTP protocol is also supported, with a server-side redirect being issued to the relevant HTTPS address. If you choose to use HTTP protocols, the corresponding addresses must also be authorized through your proxy server; but HTTPS support remains a requirement.

If neither direct access nor access through a proxy server can be provided, you can use an alternative process to manage library updates manually, as described in [Manual Updates of Library Data](#).

At installation time, you need to trigger download of the libraries to create a baseline ready for product use. Library downloads check the terms of your Flexera license. That is why this task cannot be attempted before a current license is installed (see [Product Activation](#)), and must occur on the same server where your license was imported to activate the product.

In summary, the process downloads several different files to which you are entitled, saving them into staging locations on your batch server (or the server hosting that functionality). When the downloads are all completed successfully, the files are imported into the compliance database as required. The staging locations are subdirectories of %PROGRAMDATA%\Flexera Software\FlexNet Manager Platform\DataImport\Content. If necessary, you may customize this by saving your preferred path in the registry at HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ManageSoft Corp\ManageSoft\Compliance\CurrentVersion\Recognition\ContentImportDirectory.

For details of log files, see the end of the following procedure.

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



To trigger a download of the current libraries:

1. On the batch server (or application server for a single-server implementation), open the Microsoft Task Scheduler.
2. Manually trigger the **Recognition data import** scheduled task.

Given that no other processes are running at this stage of your implementation, it executes almost immediately. By default this task is run at 1am daily.



Tip: You can save considerable download time and bandwidth by editing the schedule for this task to be 1am on Sunday morning, for example. Since ARL updates are made weekly, and less frequently for other libraries, more frequent downloads are of little benefit, other than perhaps recovering from networking issues.

Whenever it is triggered, the task places a request for download in the queue of the internal batch scheduler. A utility downloads all libraries according to the terms of your license, and, when all downloads are successful, imports the contents into FlexNet Manager Suite. Depending on your network speeds, a typical download may take in the order of one-two hours, followed by the import.



Tip: Since all downloads must succeed before the import starts, a failure in any of the downloads means that the import is not attempted on this occasion. However, the process is resilient in that each download is automatically retried up to five times where necessary to work around transient network issues.

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 %ProgramData%\Flexera Software\Compliance\Logging\Content (where the asterisk in each file name is replaced with the appropriate date):

- mgsImportRecognition*.log
- recognition*.log (for the Application Recognition Library)
- importPURL*.log.



Tip: Each log file is configured through a matching .config file saved in the same directory. Note that by default, 30 dated copies of each log file are preserved, and thereafter the oldest file is automatically removed to make room for the next log file (see `maxSizeRollBackups` in the .config files). You cannot modify the file path for logging within the .config files, but you could if necessary customize the file name(s). If you really need a different file path for these logs, you can change the value used for `%property{ComplianceLoggingPath}` in the .config files by creating a `REG_SZ` registry key at `SOFTWARE\Wow6432Node\ManageSoft Corp\ManageSoft\Compliance\CurrentVersion\LoggingBaseDirectory` on your batch server (or in smaller implementations, the server hosting this functionality), and setting the registry key to your preferred path. (Removing this key again restores the default value.)

Manual Updates of Library Data

The downloadable Application Recognition Library, Product Use Rights Library, EOSL 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.

- Sign-up to receive email notifications for FlexNet Manager Suite Content Library Updates on the <https://info.flexera.com/SLO-FMS-Software-Content-Library-Updates> web page. 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 username and password for the Flexera Community website (<https://community.flexera.com>). If you do not yet have these credentials, you can apply as noted in the process below. (There is a delay for account validation.)

- Once your account is valid, subscribe to the FlexNet Manager Release blog, located on the web page, to track updates to the FlexNet Manager Suite Content Library. You can receive email notifications for this and other content by modifying the subscription and notification settings for your account.

When these preparations are completed, you can use the following process to manually update each of the downloadable libraries for your new installation, and again as new editions are released (as advised in your email notifications).

In summary, in this process you download several different files to which you are entitled, saving them into staging locations on your batch server (or the server hosting that functionality). When the downloads are all completed successfully, you import the files into the compliance database as required. The staging locations are subdirectories of %PROGRAMDATA%\Flexera Software\FlexNet Manager Platform\DataImport\Content. This default pathway is referenced throughout the description below. If necessary, you may customize the default path by saving your preferred path in the registry at HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ManageSoft Corp\ManageSoft\Compliance\CurrentVersion\Recognition\ContentImportDirectory.

For details of log files, see the end of the following procedure.



To manually download and deploy current libraries:

- Log into a computer where you are permitted to access the Internet and download files.
- Download the ARL from <https://www.managesoft.com/support/Compliance/RecognitionAfter82.cab> and save it temporarily.

Its eventual destination is %PROGRAMDATA%\Flexera Software\FlexNet Manager Platform\DataImport\Content\ARL on your batch server.

- If you have licensed the EOSL (End of Service Life) product, also download <https://www.managesoft.com/support/Compliance/EOSL.cab>.

This is eventually saved in %PROGRAMDATA%\Flexera Software\FlexNet Manager Platform\DataImport\Content\EOSL on your batch server.

- Download the SKU library from <https://www.managesoft.com/support/Compliance/PURL.cab> (despite the filename, being PURL.cab, this is not a typographical error).

Later you will save this in %PROGRAMDATA%\Flexera Software\FlexNet Manager Platform\DataImport\Content\SKU on your batch server.

- To collect your PURL entitlements, navigate to the appropriate download page in the Flexera Customer Community website:
 - On <https://community.flexera.com/>, 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, click the *Let's go!* button on the login page to request one. Your credentials are configured for access to content you have licensed.

- Select **Find My Product** and choose **FlexNet Manager** from the top menu. Now click the button **PRODUCT RESOURCES - PRODUCT INFORMATION** which will expose the **Download Products and Licenses** link. Click on this option.

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 immediately below it, click **LET'S GO**.

The Product and License Center site displays.

- d. In the **Your Downloads** panel, select one of the products that you have licensed to open the **Download Packages** page (for example, FlexNet Manager for Datacenters).

- e. Click on the *productName* **Content Libraries** link to download the related PURL file.

- f. If necessary, loop back and repeat the download for each of the products you have licensed for FlexNet Manager Suite.

All downloaded PURL files are eventually to be saved in %PROGRAMDATA%\Flexera Software\FlexNet Manager Platform\DataImport\Content\SKU (again, not a typo) on your batch server.

6. Log in to your batch server (or the server hosting that functionality, such as your application server in a single-server implementation) 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.

7. If this is not the first time you have downloaded the libraries, run the following command to clean out the disk cache on your batch server (or equivalent):

```
cd InstallDir\DotNet\bin
"ShadowHostWin.exe" "BatchProcessTask.exe" run ARLCleanup
```

8. On your batch server (or equivalent), navigate to %PROGRAMDATA%\Flexera Software\FlexNet Manager Platform\DataImport and create the Content directory and its subdirectories ARL, SKU, and EOSL.

Use exactly these names to allow for subsequent automated tasks. (These folders are all removed each cycle by the ARLCleanup task.)

9. Copy the downloaded files to your batch server, placing each one in the appropriate subdirectory under the \Content path, as identified in the downloading steps described earlier.


10. Still on your batch server, navigate to the Microsoft Task scheduler, and in the **FlexNet Manager Platform** group:

- a. Validate that the **Recognition data import** scheduled task has indeed been disabled.
- b. Create a new import scheduled task with the following command line to execute in the *InstallDir\DotNet\bin* directory:

```
"ShadowHostWin.exe" "BatchProcessTask.exe" run ARLImport
```

It is appropriate to schedule this daily at 1am. This schedules an import from the disk cache where you have placed the files into the compliance database (and on the daily schedule, if there is nothing new in the cache, exits quickly). The import is scheduled as soon as possible, and run when there are no conflicting tasks. You can also trigger this scheduled task manually if need be, without needing to memorize a command line.

When the import scheduled task is triggered, all the downloaded libraries are loaded into the compliance database by the ARLImport task. When the process is complete, you can log into the web interface of FlexNet Manager Suite, and

navigate to the system menu ( ▼ in the top right corner) and choose **System Health > System Health Dashboard**. The summary cards there display the versions and date/time of the last successful updates to the ARL, PURL, and SKU library. (The cards do not update automatically once the page is open. Use F5 to refresh the display.) Errors display an additional alert icon with some explanatory text.

Troubleshooting:

In case of errors, check the following log files, located in %ProgramData%\Flexera Software\Compliance\Logging\Content (where the asterisk in each file name is replaced with the appropriate date):

- mgsImportRecognition*.log
- recognition*.log (for the Application Recognition Library)
- importPURL*.log.



Tip: Each log file is configured through a matching .config file saved in the same directory. Note that by default, 30 dated copies of each log file are preserved, and thereafter the oldest file is automatically removed to make room for the next log file (see `maxSizeRollBackups` in the .config files). You cannot modify the file path for logging within the .config files, but you could if necessary customize the file name(s). If you really need a different file path for these logs, you can change the value used for `%property{ComplianceLoggingPath}` in the .config files by creating a REG_SZ registry key at `SOFTWARE\Wow6432Node\ManageSoft Corp\ManageSoft\Compliance\CurrentVersion\LoggingBaseDirectory` on your batch server (or in smaller implementations, the server hosting this functionality), and setting the registry key to your preferred path. (Removing this key again restores the default value.)

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.

Link to Flexera Service Gateway

Flexera Service Gateway allows interaction between separate products from Flexera.

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

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



To link to Flexera Service Gateway:

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



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

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

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

The **Your FlexNet Manager Suite License** page appears.

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

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

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



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

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

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

5. Locate the registration tool and click to open it; or

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

- b. Run `RegisterFlexeraServiceGateway.exe`.

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

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

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

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

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

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

9. Click **OK**.

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

Configure Beacon Connections

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

Remember that it is both common and helpful to install an inventory beacon on your batch server. Uniquely amongst your inventory beacons, this one has access to the operations databases, which (for example) gives extra functionality to business adapters created and run on this inventory beacon.



Important: When you install an inventory beacon on your batch server, you must manually configure that inventory beacon to use Microsoft IIS, as described in the online help. In particular, see *FlexNet Manager Suite Help* > *What Is an Inventory Beacon?* > *Configuring Inventory Collection*. Also note that if you install an inventory beacon on your batch server, you must use the default location for its distribution folder (`DATADIR`) — to protect the integrity of your central application server(s), custom locations are not permitted on this shared server. For custom locations, use a stand-

alone inventory beacon.

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



Note: Any computer on which you will install an inventory beacon must have at least version 3.0 of PowerShell installed. For more information, see [Upgrade PowerShell on Inventory Beacons](#).



To install and configure an inventory beacon:

1. Use a web browser to access the URL `server-name-or-IP-address/Suite/`.



Tip: It's convenient to do this on the machine you intend to use as your inventory beacon. However, if your inventory beacon cannot access the central application server, you may download the installer to another convenient device and then move it to the proposed inventory beacon.

2. In the **Discovery & Inventory** menu, under the **Network** group, select **Beacons**.
3. Click **Deploy a beacon**.

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

4. Click **Download a beacon**.



Tip: This button is displayed only to members of the Administrator role.

5. 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.

6. In Windows Explorer, navigate to the saved file on your inventory beacon, and double-click it to run the installer.
7. 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).



Remember: When installing an inventory beacon on your batch server, you must manually configure that inventory beacon. In the online help, see *FlexNet Manager Suite Help > What Is an Inventory Beacon? > Configuring Inventory Collection*, and be sure to select the *IIS* option.

8. When the FlexNet Beacon software is installed and configured on your inventory beacon, open Microsoft Task Scheduler and check the following tasks are correctly scheduled:

- Upload FlexNet logs and inventories
- Upload third party inventory data.

On some systems, Task Scheduler waits until midnight to start the repeating schedule for these tasks (by default, both repeat every 10 minutes). If they are not yet running, and you want them running today rather than tomorrow, edit the start times to the current time.

9. With your inventory beacon(s) configured, in the web interface for FlexNet Manager Suite, navigate to **Discovery & Inventory > Discovery and Inventory Rules** (in the **Discovery** group) to set up FlexNet inventory collection rules.

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

- *Inventory Systems Tab*
- *SAP Systems Tab*
- *Engineering Apps Agent Page*.

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 your license position.

Set Up Initial Accounts and Access Rights

The installing account (example: fnms-admin) defaults to having administrator privileges in your new implementation. An account (such as that installing account) with administrator privileges must do three things to make other operators functional in FlexNet Manager Suite:

- Gather records of users from Active Directory. For your on-premises implementation, each of your operators must first be known to FlexNet Manager Suite as a user within your enterprise. Since authentication in FlexNet Manager Suite is based on Active Directory accounts, the user must be known within the Active Directory domain where your central application server is located (or a domain that is trusted by the application server's domain).
- Create an account in FlexNet Manager Suite for each operator, referencing their Active Directory user account.
- Assign each operator account to the appropriate role(s). All access rights are controlled by roles, and individual operator accounts are assigned to the appropriate role(s) for the access rights they require.



To set up accounts and access rights:

1. Import data from Active directory:

- a. Log into an inventory beacon in the same domain as your central application server using an account that has local Windows administrator privileges, and open the FlexNet Beacon interface.



Tip: This may be a convenient time to schedule regular imports from Active Directory. For more information, see the help on *Creating a Data Gathering Schedule*.

- b. In the **Data collection** group, click **Active Directory**, and select the default connection for Current domain.



Tip: If you do not have an Active Directory connection listed, or you need to import users from a different domain, click the help button and see *Inventory Beacons > Importing from Active Directory*.

- c. Click **Execute Now**.

The Active Directory data is gathered, uploaded to your central application server, saved in the inventory database, and shortly thereafter imported into the compliance database. This process may take some time

(in the order of 30 minutes for each 10,000 users recorded in the Active Directory domain).

- d. Return to the web interface for FlexNet Manager Suite and navigate to **License Compliance > Reconcile**.

The **Reconcile** page displays.

- e. Select the **Update inventory for reconciliation** check box and click **Reconcile**.

The Reconcile pending: A license reconcile has been scheduled for processing message displays and the manual reconcile commences.

- f. Press F5 or use your browser's refresh control to update the display until the **Status** field displays the Success message.
- g. Navigate to **Enterprise > All Users**, and validate that the user accounts have been imported from Active Directory.

Once displayed, this listing is not refreshed automatically. Press F5 or use your browser's refresh control to update the display until the data appears.

2. Ensure that appropriate roles are ready to assign to the future operators:

- a. Navigate to the system menu (⚙️ ▼ in the top right corner), choose **Accounts**, and select the **Roles** tab.
- b. 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.

For more information, see the online help.

3. Set up the account for each operator:

- a. Switch to the **All Accounts** tab.

This tab lists all existing operator accounts permitted to log in to FlexNet Manager Suite. At this stage, you should expect to see only the installing user's operator account.

- b. Click **Create an account**.
- c. Enter part of the Active Directory user name in the search field, and click **Search**.
- d. In the search results list, select the desired user account, and click **Get account details**.

FlexNet Manager Suite populates the **Name**, **Email**, and **Job title** (if known) into the respective fields. If desired, you can add further information about this operator's account.

- e. Ensure that the **Status** is set to **Enabled**.

This setting is mandatory to allow the operator to log in. (Conversely, you can disable an account here, if necessary for any reason.)

- f. From the **Role** drop-down list, select the first role for this operator. You can add additional roles for each operator as required.

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

g. Click **Create.**

A FlexNet Manager Suite operator account is created for the existing Active Directory user. Repeat the account creation process for each operator.

3

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 Cognos server

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

On the inventory beacon

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

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



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

- *Flexera Inventory Manager installation agent*
- *Flexera Inventory Manager managed device versionNumber*
- *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.

4

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 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. You may also find the introductory matrix comparing the results of various inventory sources to be helpful.
 - Local PDF version: [Gathering FlexNet Inventory](#)
 - HTML version: <https://docs.flexera.com/FlexNetManagerSuite2023R1/EN/GatherFNInv/index.html>
- *FlexNet Manager Suite Inventory Adapters and Connectors Reference* covers standard adapters available for the system that manipulate data from external systems into a format useable by FlexNet Manager Suite; and some connectors that manage somewhat simpler imports. It also includes how to use the Inventory Adapter Studio.
 - Local PDF version: [FlexNet Manager Suite Inventory Adapters and Connectors Reference](#)
 - HTML version: <https://docs.flexera.com/FlexNetManagerSuite2023R1/EN/InvAdapConn/index.html>
- *Using FlexNet Business Adapters* covers both the Business Importer and the Business Adapter Studio. The latter builds business adapters, which the Business Importer command-line executable uses to import business-related, ancillary data into FlexNet Manager Suite. This document includes the data model common to the Business Importer and the Business Adapter Studio (called the Data Domain Interface, or DDI), as well as some sample adapters. Finally, it covers how to use the Business Adapter Studio, for those who want to create their own business adapters.
 - Local PDF version: [Using FlexNet Business Adapters](#)
 - HTML version: <https://docs.flexera.com/FlexNetManagerSuite2023R1/EN/BusnAdap/index.html>
- *FlexNet Manager Suite System Reference* collects a variety of reference materials, 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 set up in a single sign-on environment

- And much more.

Available versions include:

- Local PDF version: [FlexNet Manager Suite System Reference](#)
- HTML version: <https://docs.flexera.com/FlexNetManagerSuite2023R1/EN/SystemRef/index.html>.
- *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.
 - Local PDF version: [FlexNet Manager Suite Schema Reference](#)
 - HTML version: <https://docs.flexera.com/FlexNetManagerSuite2023R1/EN/Schema/index.html>
- *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).
 - Local PDF version: [FlexNet Manager for SAP Applications User Guide](#)
 - HTML version: <https://docs.flexera.com/FlexNetManagerSuite2023R1/EN/SAPUser/index.html>
- *Non-Commercial Software Disclosures* lists all third-party non-commercial code used in FlexNet Manager Suite, with attributions and license terms.
 - Local PDF version: [Non-Commercial Software Disclosures](#)

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