flexera

# FlexNet Manager Suite 2022 R2

## Upgrading FlexNet Manager Suite On-Premises

# Legal Information

**Document Name:** FlexNet Manager Suite 2014 Rx (or later) to 2022 R2 Upgrade Guide (for on-premises delivery)

**Part Number:** FMS-19.0.0-UG03

**Product Release Date:** December 12, 2022

## Copyright Notice



## Intellectual Property



## Restricted Rights Legend

# Contents


1. Upgrading FlexNet Manager Suite to 2022 R2 On-Premises ..... 6

**Process Overview** ..... **6**

**Design the Final Topography** ..... **7**

Considerations for Inventory Beacons ..... 11

**Prerequisites and Preparations** ..... **14**

Locate License Details (probably) ..... 14

Enable MTS and MSMQ ..... 15

Identify (or Set Up) Accounts ..... 16

Isolate the System ..... 22

Repair Database Constraint Violations ..... 24

Check Database Collation Sequence ..... 27

Enable SQL Server CLR ..... 28

Configure .NET and IIS ..... 29

Configure Internet Explorer ..... 32

Upgrade PowerShell on Inventory Beacons ..... 33

Configure Network Shares for Multi-Server ..... 33

Drivers for Spreadsheet Imports ..... 34

Scanning of Uploaded Documents ..... 34

Download the Materials ..... 35

Copy your current kentor.authservices configuration ..... 36

2. Upgrading FlexNet Manager Suite ..... 38

**Remove Previous Language Packs** ..... **38**

**Upgrade/Create Databases** ..... **39**

Re-Indexing a Database ..... 46

Database Validation ..... 47

**Authorize the Service Account** ..... **48**

**Choosing the Upgrade Approach** ..... **49**

**Managing a Scripted Upgrade** ..... **49**

Prepare Encrypted Credentials for Upgrade ..... 50

Prepare Answer File ..... 53

Running a Scripted Installation ..... 57

**Managing Upgrades Interactively** ..... **59**
Upgrade the Web Interface ..... 59
Update the Inventory Server ..... 61
Update the batch server ..... 62
Configure the System ..... 64
**Upgrading Flexera Analytics** ..... **68**
Upgrading Recent Flexera Analytics ..... 69
Upgrading Flexera Analytics from FlexNet Report Designer ..... 76
Configuring IIS to Use SSL/TLS Encryption ..... 85
Reconfigure Cognos Analytics to Use Third-Party SSL Certificates ..... 86
Reconfigure Cognos gateway to use SSL using self-signed certificates ..... 90
Reconfigure Cognos components to use Cognos signed certificate ..... 92
Importing an Updated Flexera License ..... 94
Update the Sample Reporting Package ..... 95
**Installing a Free-Standing Studio** ..... **97**
**Populate the Downloadable Libraries** ..... **98**
Manual Updates of Library Data ..... 100
**Link to Flexera Service Gateway** ..... **103**
**Update Access Rights** ..... **105**
**Update and Deploy Additional Inventory Beacons** ..... **105**
Upgrading 2014 or earlier, or installing new inventory beacons ..... 106
Managing self-upgrades from 2014 R2/R3 (or later) inventory beacons ..... 108
**Upgrade Connected-Mode Studios** ..... **109**
**Configure Updates to Inventory Agents** ..... **110**
**Optional: Perform a Full Import** ..... **112**
**Activating and Using New Features** ..... **114**
IBM PVU License Configuration ..... 116
Enhancement for Purchase Records ..... 120
Configure Updates to Inventory Agents ..... 122
Updating the ADDM Adapter ..... 124
Update the XenApp Server Adapter ..... 125
Update the Virtual Desktops Adapter ..... 126
**3. Notes on Issues** ..... **128**
**Password Maintenance** ..... **128**
**Identifying IIS Application Pool Credential Issues** ..... **131**

Update Credentials in IIS Application Pools ..... 132

**IIS Roles/Services ..... 133**

1

# Upgrading FlexNet Manager Suite to 2022 R2 On-Premises

This document covers upgrading from FlexNet Manager Suite release 2014 or later, to FlexNet Manager Suite 2022 R2 in an on-premises implementation.

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.

## Process Overview

Upgrading from the 2014 or later (web-based) releases to FlexNet Manager Suite 2022 R2 is conceptually very straight-forward:

- For any 2014 release, if you had installed any language packs (localizing the user interface into, for example, German or Japanese), these should be uninstalled first. (The current release installs language support for all available languages.)
- Run the scripts provided to upgrade the underlying databases.
- Run the installer on (each of) your central application server(s) to update the product itself.
- If you had previously implemented any custom scheduled tasks on your application server (or, in a multi-server implementation, your batch server), consider upgrading these to use the shadow copy approach that helps meet high-availability goals by allowing live updates to Windows .NET assemblies (and dependent libraries) without interrupting normal operations of FlexNet Manager Suite.
- Manage your inventory beacon updates:

- If migrating from 2014, visit each inventory beacon and run the installer (available through your updated web interface of FlexNet Manager Suite) to update the beacon. While there, you may prefer to tweak the default schedules in the new, in-built beacon scheduler; and you need to update connection details for adapters previously run as Windows Scheduled Tasks.
- If migrating from 2014 R2 or later, your inventory beacons are self-updating. You can manage the upgrade process (including testing, pilot groups, and roll out) as described in `FlexNet Manager Suite Help > What Is an Inventory Beacon? > Upgrading Inventory Beacons`.

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

# Design the Final Topography

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

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

---

***Note:*** *Both the inventory server (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.

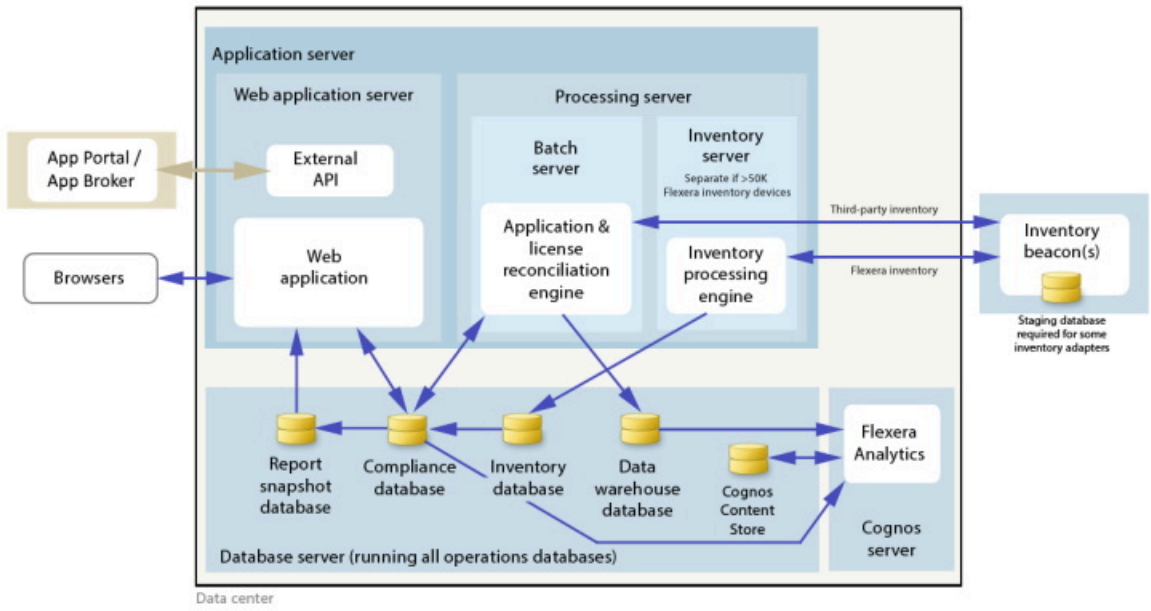
***Tip:*** *If the Cognos content store is installed on an SQL Server installation later than 2012, it should be run in SQL Server 2012 compatibility mode.*

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

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

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

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




***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.*

## Choose your web servers per device

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

- Microsoft IIS. Choose this alternative when any of the following apply:
  - The host server is one of your central application servers (web application server, batch server, or inventory server, or combinations as applicable). No web server is required on a stand-alone database server. When you install the recommended inventory beacon on the same device as the central batch server, that beacon also uses IIS (whereas other free-standing beacons on separate devices still have a choice).
  - When a particular inventory beacon is collecting inventory from (and passing back recommendations to) FlexNet Manager for SAP Applications, that inventory beacon must use IIS.
  - When you require Windows Authentication to allow transfer of data (for example, a parent inventory beacon might typically use Windows Authentication if it receives data from a child in your DMZ outside a firewall).
  - When you require the use of the HTTPS protocol to encrypt data transfers.
- FlexNet self-hosted web server. Choose this alternative when none of the previous cases apply, and:
  - You want simple administration of the web server.
  - You want to minimize the installations on your inventory beacon, so that you do not need to install Microsoft IIS.
  - Anonymous access, and use of the HTTP protocol, are adequate (for example, within your secure LAN).

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

## Placement of inventory beacons

For more information about inventory beacons, see Considerations for Inventory Beacons.

## Output

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

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

Label each block in your diagram with:

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

***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 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

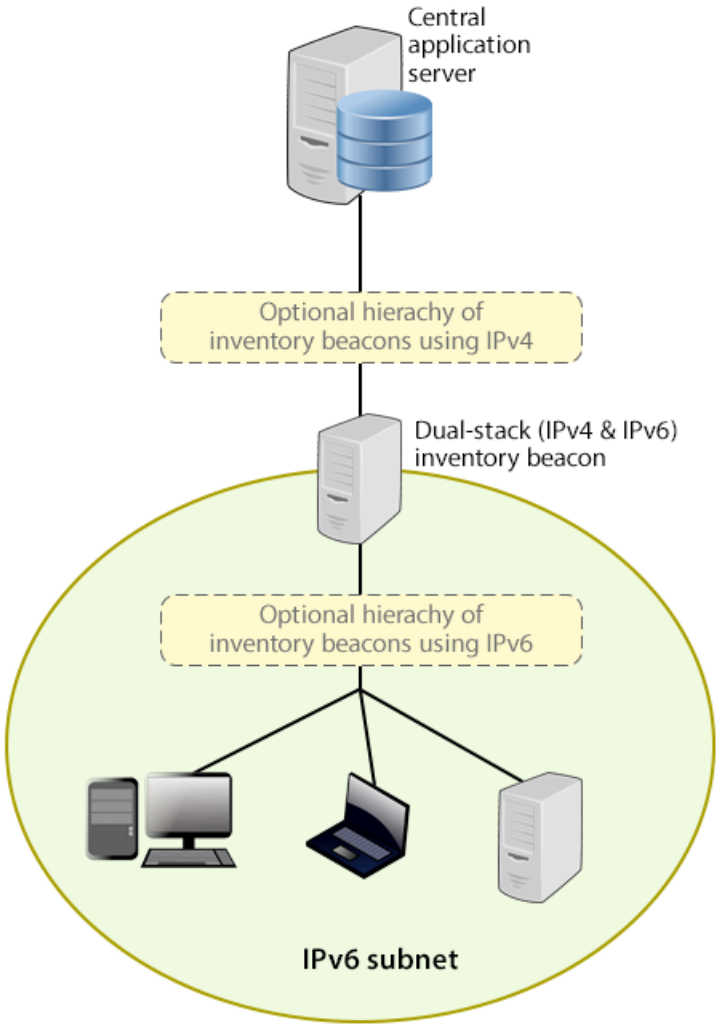
It is best practice to deploy at least one inventory beacon into each separate subnet that contains target devices for which you may want an inventory beacon to execute discovery and inventory gathering. Being within the target subnet allows the inventory beacon to reliably use ARP or `nbtstat` requests 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 Update and Deploy Additional Inventory Beacons.

# Prerequisites and Preparations

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

## Locate License Details (probably)

There are three possibilities for your license documentation:

- You may not need to find it. This is the case if you are upgrading with the same hardware as for your 2014 Rx implementation, and *not* adding the specialized inventory functionality in FlexNet Manager for Datacenters. The license installed on your server covers your upgrade (while you are under a maintenance agreement).
- You may need your existing license. If you are either upgrading to new hardware as part of this update, or scaling up your implementation with additional central servers (but not adding newly-licensed functionality), you need your original license file. A license file for your existing product(s) was sent to you with your original order confirmation. If

you need and cannot locate the license file, please contact the Flexera order processing team, and ask for a new copy of your license file.

***Tip:*** *One reason you might consider upgrading to new hardware is if you are still using 32-bit operating systems. FlexNet Manager Suite 2022 R2 requires 64-bit operating systems on all central application server(s). You might consider upgrading the operating system, or replacing the old servers.*

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

# 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.

# Identify (or Set Up) Accounts

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

For upgrade 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 Upgrade/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:

- A database administrator (typically this is an existing database administrator within your enterprise)
- An installing system administrator (account details must be made available to db-admin)
- A service account for normal operations (account details must be made available to db-admin).

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

***Important:*** *The Microsoft SQL Agent security restrictions require that any future database upgrade is performed by either:*

- *The owner of the database, being the same SQL user that creates the database in the first place; or*
- *A member of the `sysadmin` role for Microsoft SQL Server.*

*It is therefore typical for the SQL user doing the upgrade to be a member of the `sysadmin` role for the duration of the set-up process. However, since `sysadmin` privileges are not required for normal operations, the same user can be removed from the `sysadmin` role during normal operations of FlexNet Manager Suite. (If, instead, you are using the original owner for the upgrade, this SQL user requires at a minimum membership in the `SQLAgentUserRole`, or in a more privileged role such as `SQLAgentReaderRole` or `SQLAgentOperatorRole`. Privileges for any of these roles are sufficient to successfully run the scripts provided for database creation and migration.)*

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

| Privileges | Required on | Purpose |
|---|---|---|
| Database administrator, with `db_owner` rights on all operations databases related to FlexNet Manager Suite (compliance data, warehouse data, snapshot data, and inventory data). | Database servers | Provides the following accounts with database access rights as described. |
| Member of the **public** database role in the `model` database on the database server. | Database servers | Required so that the account can run scripts that check the database compatibility level. |

| Privileges | Required on | Purpose |
|---|---|---|
| SELECT rights to the following tables in the **msdb** database:<br>• `dbo.sysjobs`<br>• `dbo.sysjobsteps`<br>• `sysjobs_view`.<br>EXECUTE rights to the stored procedures from the **msdb** database used in the database scripts, including:<br>• `sp_add_job`<br>• `sp_add_jobserver`<br>• `sp_add_jobstep`<br>• `sp_add_jobschedule`<br>• `sp_delete_job`. | Database servers | Only required if an existing installation of FlexNet Manager Suite 2015 or earlier is being migrated to a later release. |

***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 Upgrading Flexera Analytics from FlexNet Report Designer).*

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

| Privileges | Required on | Purpose |
|---|---|---|
| Membership in the `db_owner` role on all operations databases (compliance data, warehouse data, snapshot data, and inventory data). | Database server. | Post-installation, for continuing administration, this account can be reduced to the same privileges as for the service account (described below). However, the standard installation scripts set some database properties (`ARITHABORT`, `QUOTED_IDENTIFIER`) that can only be configured by an account with `db_owner` privileges. Therefore the installing account needs membership in the `db_owner` role at least temporarily during installation. |

| Privileges | Required on | Purpose |
|---|---|---|
| Local administrator | • Central application server(s) (including, where separated, web application server, batch server, and inventory server);<br>• All inventory beacons. | Installs and configures software on all servers. On inventory beacons, interactive login to the inventory beacon interface also requires local administrator privileges (that is, on inventory beacons this is an operational account as well as being required for setup). |
| Set the execution policy for, and execute, PowerShell scripts | Central application server(s) (including, where separated, web application server, batch server, and inventory server). | PowerShell scripts are used to complete the configuration of central servers during implementation. Includes an attempt to enable Microsoft Message Queuing, where this is not already enabled. |
| Create tasks in Windows Task Scheduler | • Central application server(s) (including, where separated, web application server, batch server, and inventory server);<br>• 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 |
|---|---|---|
| Membership in the following fixed database roles:<br>• `db_ddladmin`<br>• `db_datawriter`<br>• `db_datareader`.<br>In addition, the account requires you to `GRANT EXECUTE` permissions on all operations databases (compliance data, warehouse data, snapshot data, and inventory data).<br>***Tip:*** *In less stringent environments, it may be convenient to give this account membership in the `db_owner` role for the operations databases, which supersedes all of the above.* | Database server | Normal operation (which includes execution of SQL stored procedures). |
| Logon as a Service, and run all FlexNet services<br>***Tip:*** *Admin access for this account is convenient, and typically granted through membership in the `FNMS Administrators` security group in Active Directory; otherwise read, write, and execute permissions are required on all folders containing FlexNet installations, FlexNet data, and FlexNet log files.* | • Central application server(s) (including, where separated, web application server, batch server, and inventory server);<br>• All inventory beacons. | Runs all system operations, including batch services and web services.<br>***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.)* |

| Privileges | Required on | Purpose |
|---|---|---|
| Logon as a Batch Job | • Central application server(s) (including, where separated, web application server, batch server, and inventory server);<br>• All inventory beacons. | When the service account runs a batch job, this setting means the login is not an interactive user.<br><br>***Tip:*** *This is particularly important on the batch server (for authorization details, see Authorize the Service Account).* |
| Run scheduled tasks as a service account. | • Central application server(s) (including, where separated, web application server, batch server, and inventory server);<br>• All inventory beacons. | Runs scheduled tasks within normal operations. |
| Run IIS application pools as a service account | • Central application server(s) (including, where separated, web application server, batch server, and inventory server);<br>• 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*.

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

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

# Isolate the System

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

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

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

***Tip:*** *In your 2014 Rx system, the column marked "Batch Svr" was previously assigned to your reconciliation server. (The name reconciliation server may continue to appear.)*

**Table 4:** Isolation tasks for each server type

| Task | Web App Svr | Batch Svr | Inventory Svr | Database Svr(s) |
|---|---|---|---|---|
| Shut down IIS | Yes | Yes | Yes | Not required |
| Stop related scheduled tasks (see note) | Not required | Yes | Yes | Not required |

| Task | Web App Svr | Batch Svr | Inventory Svr | Database Svr(s) |
|---|---|---|---|---|
| Stop services for FlexNet Manager Suite Batch Process Scheduler | Not required | Yes | Not required | Not required |

***Note:*** *Microsoft Windows may require that the Task Scheduler is completely shut down when the installer runs.*

***To isolate the system:***

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

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

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

   a. Click Start, right-click on **Computer**, and select **Manage** from the context menu.

      The **Server Manager** dialog opens.

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

      The IIS page is displayed.

   c. In the **Actions** panel on the right, select **Stop**.

      A message like `Attempting to stop...` appears. Note that it can take some time before the service is stopped.

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

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

   - Data warehouse export
   - Export to ServiceNow
   - FlexNet inventory data maintenance (only present if you are upgrading from release 2015 or later)
   - Import SAP inventories
   - Import SAP package license
   - Inventory import and license reconcile
   - Recognition data import
   - Regenerate Business Import config
   - Send contract notifications.

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

- Import Active Directory
- Import application usage logs
- Import discovery information
- Import installation logs
- Import inventories
- Import Inventory Beacon activity status
- Import Inventory Beacon status
- Import remote task status information
- Import security event information
- Import system status information
- Import VDI access data.

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

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

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

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

d. Close the dialog.

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

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

      The **Services** dialog opens.

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

# Repair Database Constraint Violations

After past upgrades, Flexera Support has identified cases where database constraints have been relaxed, and unexpected data inserted; and these changes have subsequently caused issues with license compliance outcomes. For reasons like this, the database migration scripts have been made more rigorous, ensuring that all database constraints are (re)activated, and stopping (failing the upgrade process) if unexpected data is found in tables of the following FlexNet databases:

- Compliance database (suggested name `FNMSCompliance`)
- Inventory database (suggested name `FNMSInventory`)

- Data warehouse database (suggested name `FNMSDataWarehouse`).

You can avoid having your upgrade fail because of any such database issues by running the following process against each of those databases in turn, before you start the upgrade process. To run this process, you need to be familiar with Microsoft SQL Server Management Studio, and your login must be mapped to users with (at least) `Select` permissions on all of the above databases.

---

***Note:*** *This process does not make any changes to the data in your databases, because any such changes (if required) need inspection and assessment. However, it does reactivate any database constraints that have been disabled. For this reason, it is strongly recommended that, now that your system is isolated (see Isolate the System), you start with a full backup of all your FlexNet databases.*

---

***To identify issues with database constraint violations:***

1. Log into Microsoft SQL Server Management Studio using an account with adequate mappings to database users.
2. Make full backups of all your existing FlexNet databases:
   - Compliance database (suggested name `FNMSCompliance`)
   - Inventory database (suggested name `FNMSInventory`)
   - Data warehouse database (suggested name `FNMSDataWarehouse`)
   - Reporting snapshot database (suggested: FNMSSnapshot).
3. Select the first database to validate (such as `FNMSCompliance`), and copy the following script and paste it into the execution window, select it, and run it.

   ---

   ***Note:*** *Long lines in this script have been wrapped for publication. You may choose to correct the wrapping before execution.*

   This script generates SQL statements to test data in tables that database migration will also check. A query is output for each database constraint that appears as 'untrusted' to Microsoft SQL Server.

```
SELECT
    N'IF EXISTS (SELECT * FROM ' + QUOTENAME(SCHEMA_NAME(c_o.schema_id))
                                 + N'.' + QUOTENAME(c_o.name) + N' AS a'
                                 + N' WHERE ' +
    (
        SELECT CASE WHEN fkc.constraint_column_id = 1
                                 THEN N''
                                 ELSE N' AND ' END + N'a.'
                                 + QUOTENAME(c.name) + N' IS NOT NULL'
        FROM sys.foreign_key_columns AS fkc
        INNER JOIN sys.columns AS c
            ON c.object_id = fkc.parent_object_id
            AND c.column_id = fkc.parent_column_id
        WHERE fkc.constraint_object_id = fk.object_id
        ORDER BY fkc.constraint_column_id
```

```
        FOR XML PATH ('')
    ) +
    N' AND NOT EXISTS (SELECT * FROM ' + QUOTENAME(SCHEMA_NAME(p_o.schema_id))
                                + N'.' + QUOTENAME(p_o.name) + ' AS b WHERE ' +
    (
        SELECT CASE WHEN fkc.constraint_column_id = 1
                                THEN N''
                                ELSE N' AND ' END + N'a.' + QUOTENAME(c.name)
                                + N' = b.' + QUOTENAME(cr.name)
        FROM sys.foreign_key_columns AS fkc
        INNER JOIN sys.columns AS c
            ON c.object_id = fkc.parent_object_id
            AND c.column_id = fkc.parent_column_id
        INNER JOIN sys.columns AS cr
            ON cr.object_id = fkc.referenced_object_id
            AND cr.column_id = fkc.referenced_column_id
        WHERE fkc.constraint_object_id = fk.object_id
        ORDER BY fkc.constraint_column_id
        FOR XML PATH ('')
    ) +
    N')) RAISERROR (''' + REPLACE(N'Data exists in ' + SCHEMA_NAME(c_o.schema_id)
                                + N'.' + c_o.name + N' which will break foreign
key '
                                + fk.name, '''', '''''') + N''', 18, -1)' AS
TestQueries
FROM sys.foreign_keys AS fk
INNER JOIN sys.objects AS p_o
    ON p_o.object_id = fk.referenced_object_id
INNER JOIN sys.objects AS c_o
    ON c_o.object_id = fk.parent_object_id
WHERE fk.is_not_trusted = 1
ORDER BY p_o.name
```

If there are no SQL statements printed when you run this script, the database constraints are all trusted by SQL Server, and you may loop back and repeat this step for the remaining databases in turn. If no statements are created for any of the three databases under test, this process is complete, and you may skip forward to the next topic.

An untrusted database constraint produces an output SQL statement such as the following example (here wrapped for publication, and of course the table names and column names vary according to each case):

```
IF EXISTS (SELECT * FROM [dbo].[PaymentScheduleDetail_MT] AS a
         WHERE a.[ActualAmountRateID] IS NOT NULL AND NOT EXISTS
         (SELECT * FROM [dbo].[CurrencyRate_MT] AS b
         WHERE a.[ActualAmountRateID] = b.[CurrencyRateID]))
         RAISERROR ('Data exists in dbo.PaymentScheduleDetail_MT which will
         break foreign key FK_PaymentScheduleDetail_ActualAmountRate', 18, -1)
```

4. Select any (or all) of the output SQL statements, and run them.

Each statement either:

- Produces no output, in which case the data is clean, and the previously untrusted constraint has now been reactivated
- Produces a two-line output of this form:

```
Msg 50000, Level 18, State 1, Line nn
Data exists in dbo.tableName which will break foreign key FK_Name
```

You may choose to check details of the *tableName* and *FK_Name* in your pre-upgrade version of the *FlexNet Manager Suite Schema Reference*. However, identifying and cleaning up the problematic data is likely to require specialized insight and expertise, so that the steps below are recommended.

5. Copy all such output, and paste into a document for safekeeping. Identify this set with the database name.
6. Loop back to step 3, repeating the process for all three databases in turn until all are completed.
7. Ask your registered support contact (a designated person within your enterprise who has access rights and login details) to open a new support case at https://community.flexera.com/t5/forums/postpage/board-id/@support, including a clear description of the issue. Be sure to attach the document listing affected tables and foreign keys.

   A useful title might be something like "Upgrade stalled by DB constraint violations".

In due course, Flexera personnel will be in touch to assist with your data clean-up. Clearly, access to your data will be required, so you may plan for that (for example, you may support a conference call with a system allowing shared screens so that you can collaborate on the data clean-up).

---

***Tip:*** *Since you cannot proceed with the upgrade until these data issues are repaired, you may consider resuming normal operations with FlexNet Manager Suite until after the data cleanups are resolved.*

# Check Database Collation Sequence

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

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

---

***To validate the server's default database collation sequence:***

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

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

---

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

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

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

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

# Enable SQL Server CLR

FlexNet Manager Suite requires Microsoft's SQL Server Common Language Runtime (CLR) Integration to be enabled prior to upgrading for increased performance.

***Important:*** *Failure to move the database to the new SQL Server instance prior to running the database upgrade scripts, can lead to Common Language Runtime (CLR)/Flexera certificate issues.*

***To enable SQL Server CLR:***

1. In SQL Server Management Studio, locate the SQL Server instance to be used by FlexNet Manager Suite.
2. 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 FlexeraCodeSignining.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.*

# 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.
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**.

a. Open a web browser and open https://www.iis.net/downloads/microsoft/url-rewrite

b. 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.

c. Run the file which will execute the installation of this extension.

d. Exit the installer.

16. Flexera Analytics also requires the installation of **Application Request Routing**.
    a. Open a web browser and open https://www.iis.net/downloads/microsoft/application-request-routing
    b. Select the **Install this extension** box, which will download the `ARRv3_0.exe` file.
    c. Run the downloaded file which will execute the installation of this extension.
    d. 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 `.xslx` format, 64-bit Office cannot be installed on the central batch server (or application server), or on applicable inventory beacons. Naturally, Office documents including spreadsheets prepared on other machines running 64-bit Office can successfully be imported. The limitation is only on co-installation on the same computers.*

# Scanning of Uploaded Documents

FlexNet Manager Suite allows you to attach uploaded documents to various record-types (including assets, purchases,

contracts, and licenses). Historically, there has been no security scanning of these documents: since they are your own documents within your own environment, they may perhaps be assumed to be safe. However, this is not always sufficient.

From the 2020 R2 release of FlexNet Manager Suite, you can configure on-demand scanning of every uploaded document, for those environments where greater security is required. The default behavior is that there is [still] no scanning of uploaded documents; so you need to decide whether to continue in this trusting manner, or turn on security scanning for all uploaded documents.

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. It may be worth reading that short section and making an informed decision before starting your upgrade, so that your design/plan for the upgrade is complete.

One part of the required security configuration is to set two registry keys with appropriate values: this can be done by script (for a 'silent' or scripted upgrade), or interactively. For manual or interactive setting, you may choose to put the required values in place during the upgrade process, or to wait until upgrade 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 upgraded configuration.

# 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 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 2022 R2 to access the downloads.

2. Download the following archives and save to a convenient (network-accessible) location on this computer (such as C:\temp\FNMSDownloads\). You may unzip all these archives here.
   - FlexNet Manager Suite Installer 2022 R2.zip
   - Database Migration for FlexNet Manager Suite 2022 R2.zip
3. If you are collecting inventory from Citrix Virtual Apps, also download:
   - Adapter Tools for FlexNet Manager Suite 2022 R2.zip
4. If your implementation design includes Flexera Analytics (powered by Cognos), also download:
   - Report Designer for FlexNet Manager Suite.zip (this contains the default report structures within FlexNetManagerPlatformReportsAndDashboard.zip)
5. 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 2022 R2.zip to the same location.

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

# Copy your current kentor.authservices configuration

***Note:*** *This prerequisite is for those customers that integrate FlexNet Manager Suite with SAML Service Provider for SSO authentication.*
*If you wish to configure Security Assertion Markup Language (SAML) authentication, please refer to the Authentication chapter in the FlexNet Manager Suite Systems Reference guide.*

For FlexNet Manager Suite 2022 R1, the **kentor.autherservices** section has been deleted and replaced with a new **sustainsys.saml2** section. This means, you will lose all details pertaining to the current mechanism you have authenticated for your identity provider.

Prior to upgrading, you will need to make a copy of your current **kentor.authservices** configuration from the web.config file. After the upgrade is complete, the current **kentor.authservices** configuration needs to be applied to the new **sustainsys.saml2** section in the web.config file.

Attributes and properties remain the same, and no values need to be updated. All that is required, is a copy and paste of the **kentor.authservices** configuration from the FlexNet Manager Suite version you upgraded from, to the new **sustainsys.saml2** section in the web.config file after upgrade.

By default, the web.config file is located on your web application server (or, in a single-server implementation, your application server) in *drive*:\\Program Files (x86)\Flexera Software\FlexNet Manager Platform\

WebUI.

Below is an example of the values entered into the **kentor.authservices** section of the web.config file, when using the identity provider Okta. Note: All instances of **kentor.authservices** are replaced with **sustainsys.saml2** after upgrading to FlexNet Manager Suite 2022 R1.

```
<kentor.authServices entityId="http://localhost:62500/AuthServices"
  returnUrl="http://localhost:62500/"
  authenticateRequestSigningBehavior="Always">
  <identityProviders>
   <add entityId="http://www.okta.com/exk8cq8c02Kg1OVRl0h7"
    signOnUrl="https://dev-271049.oktapreview.com/app/
flexerasoftwaredev717079_markslocalfnms_1/exk8cq8c02Kg1OVRl0h7/sso/saml/"
    allowUnsolicitedAuthnResponse="true"
    binding="HttpRedirect"
    loadMetadata="true"
    metadataLocation="https://dev-271049.oktapreview.com/app/exk8cq8c02Kg1OVRl0h7/sso/
saml/metadata">
    <signingCertificate fileName="~/App_Data/okta.cert"/>
   </add>
  </identityProviders>
  <serviceCertificates>
    <add fileName="~/App_Data/Kentor.AuthServices.Tests.pfx"/>
  </serviceCertificates>
</kentor.authServices>
```

***Note:*** *After upgrading, the authentication method in the web.config file is reset to "Default". Ensure that the authenticationType attribute in the signOn element is set to Saml.*
*Original:* `<signOn authenticationType="Default" allowSelfSigned="true">`

*Updated:* `<signOn authenticationType="Saml" allowSelfSigned="true">`

# 2

# Upgrading FlexNet Manager Suite

You have completed all the prerequisites in Prerequisites and Preparations (and its subsections). Only when all these tasks are complete should you move forward to the upgrade of FlexNet Manager Suite to 2022 R2.

## Remove Previous Language Packs

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

FlexNet Manager Suite 2022 R2 installs all available language packs as a standard part of the installation process, so that they no longer require separate installation. There is a risk, if you attempt to remove old language packs after the upgrade is completed, that you will remove functionality you require in this release. For this reason, use this opportunity to remove previous language packs before undertaking the upgrade. (If you have not previously installed language packs, ignore this section.)

***To remove previous language packs:***

1. Open the Windows Control Panel (for example, Windows Start menu > **Control Panel**).
2. Click **Programs and Features**.

   The dialog displays the **Uninstall or change a program** page.
3. Select one of the available language packs.

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

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

# Upgrade/Create Databases

Any existing compliance databases must be upgraded.

***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, please ensure that you have installed Cumulative Update Package 25 for SQL Server 2019 or later. Also ensure that, for all your databases used in FlexNet Manager Suite, you are **not** using the feature newly introduced in SQL Server 2019: memory-optimized `tempdb` metadata. 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 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 instance where you are creating databases for FlexNet Manager Suite.*

You may wish only to update your existing database(s) for the new release. However, if you have previously been running a single combined database, you may wish to take this opportunity to scale up to separate databases (potentially sharing the same server, of course) for inventory and compliance. Separate databases are shown in the architectural diagram in Design the Final Topography.

***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 please use the default compatibility level (`SQL Server 2019 (150)`).*

***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.*

***Important:** If you have been using Flexera Analytics (powered by Cognos), be aware that Cognos may acquire schema locks on objects within the operations databases of FlexNet Manager Suite. For this reason it is important to stop the Cognos server before updating databases, and to restart it afterwards.*

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:*

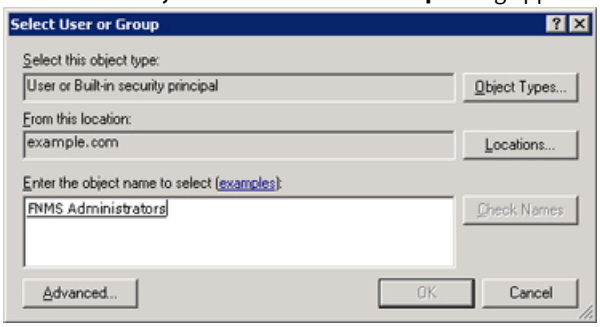
- *The operational service account (suggested: svc-flexnet)*
- *The installing administrator account (suggested: fnms-admin) for post-installation on-going administration (remembering that `db_owner` membership is required temporarily during installation, as described in Identify (or Set Up) Accounts)*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

***To upgrade databases and extend where required:***

1. If your previous implementation included Flexera Analytics (powered by Cognos), stop the Cognos server.
2. 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).
3. 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.



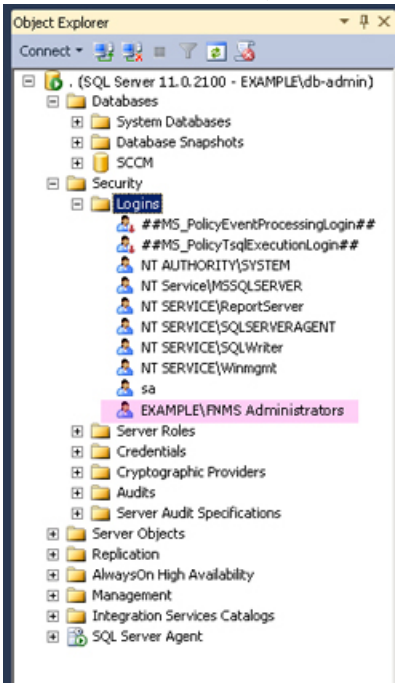

b. Use the **Object Types...** button to ensure that `User or Built-in security principal` is selected as the object type.

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.)




4. Do a full backup your existing FlexNet Manager Suite database(s).

This is very important, especially as you may interrupt transaction logging in a few steps time.

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

Customized files may include compliance importer procedures (XML files located by default in *`installation_dir`*`\Compliance\ImportProcedures`.

6. 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.

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

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

   b. Select the **Options** tab.

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

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

   ***Note:*** *In some cases it is not possible to set the **Recovery model** to `Simple`, such as when you are using Availability Groups. In these cases, it is critical to allow sufficient space for the transaction logs to expand dramatically — as a general guideline, to 2-3 times the disk space currently used by your FlexNet databases. It is also important to remain vigilant during database migration, monitoring both the remaining available space as well as the rate at which the logs are growing. Finally, after processing each individual database, consider truncating the transaction logs before proceeding to the next one; and truncate again after the final database is processed.*

8. If you have not already done so, login to the central application server with a privileged account (suggestion: db-admin) that has the privileges described in Identify (or Set Up) Accounts.

9. If you cannot access your downloaded and unzipped archives from your current login on this application server, copy `Database Migration to FNMS 2022 R2.zip` to this server and unzip it to a convenient location, such as `C:\Temp\FNMSDownloads\Database Migration\`.

   The archive unzips two subdirectories of your chosen path, `Normal` and `Partitioned`.

10. In the Command Prompt window, navigate to your working copy of the migration folder (such as `C:\Temp\FNMSDownloads\Database Migration\Normal`).

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

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

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

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

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

where:

| | |
|---|---|
| `-d <databaseName>` | The name of the database to connect to. A suggested name is `FNMSInventory`.<br><br>  ***Note:*** *If you are currently operating from a new application server that has not previously connected to the database server, this parameter is mandatory. If you are upgrading an existing application server that has separately run your compliance product (not in co-location with Inventory Manager), the registry entry listed below for the `-s` option is normally set. In this case, if you omit the `-d` option, the database name is taken from the registry key.* |
| `-i InventoryManagerMigration.xml` | This is the configuration file describing the upgrade tasks, and is of course mandatory. |

| | |
|---|---|
| `-l <logFile>` | Identifies the path and name of the file to receive a log of the upgrade tasks that occurred. If this option is not specified, a log file called `InventoryMigration.log` is created in the same folder where the executable is running. |
| `-nsu` | Run the database update without putting the database into single user mode. (The steps to perform migration require that multiple connections are made.) |
| `-p <password>` | The password for the username specified with `-u`. This is only required if the database server is configured to use SQL Server authentication. |
| `-s <serverName>` or `-s <serverName>\<instanceName>` | The name of the database server to connect to. If `-s` is not specified, the value at `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ManageSoft Corp\ManageSoft \Reporter\CurrentVersion\DatabaseConnectionString` is used. The registry key is present on the compliance and inventory servers. (If you have chosen to run this script on the database server itself, the registry entry is not available, and you must therefore specify the server name, or use the dot notation `[.]` to refer to the current server.)<br>If the database is in a named instance (and not in the default database on the server), the instance name must be specified as well. |
| `-u <userName>` | The username with which to connect to the database. This is only required if the database server is configured to use SQL Server authentication. If not specified, Windows Integrated Authentication is used to connect to the database server using the current user's credentials. |

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

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

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

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

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

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

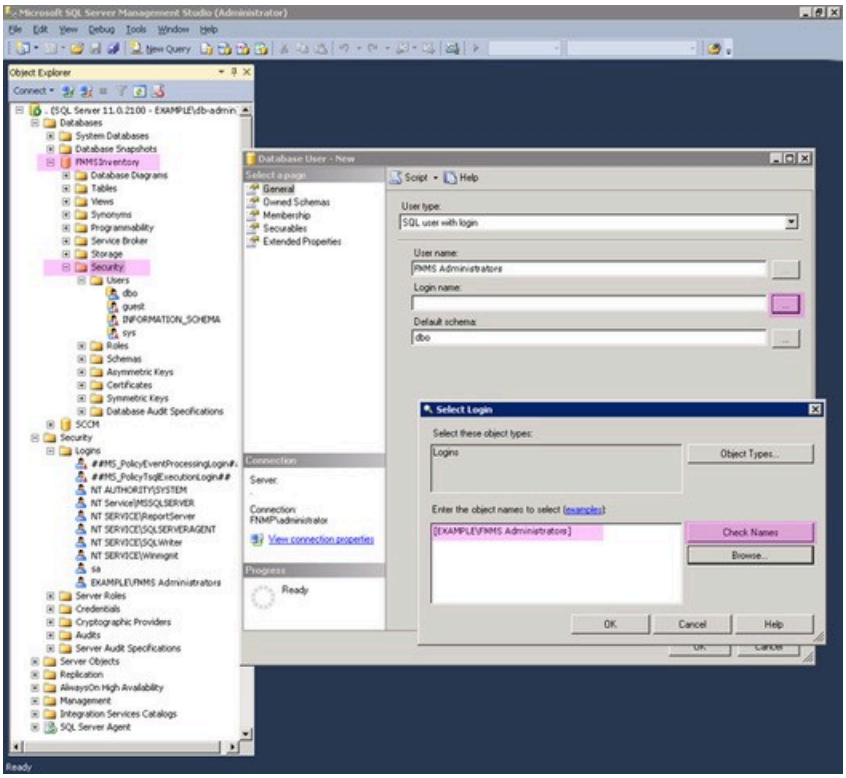
---

*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.*

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

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

---




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

e. Strongly recommended—set the compatibility level on this database:

13. Optionally, re-index the inventory database.

    For details, see Re-Indexing a Database.

14. Similarly, update the compliance database.

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

```
mgsDatabaseUpdate.exe -i ComplianceMigration.xml -nsu -d FNMSCompliance
```

```
                        [-l logFile]
                        [-s serverName\instanceName]
                        [-u userName]
                        [-p password]
```

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

   For more information about database validation and remedies, see Database Validation.

c. Strongly recommended—set the compatibility level on this database:

15. If you previously changed the setting for the database **Recovery model**, restore the original value now.
16. Optionally, re-index the compliance database.

    For details, see Re-Indexing a Database.

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

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

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

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

18. Strongly recommended—set the compatibility level on this database:
19. If you began this process by stopping your Cognos server, you may restart it now.

***Note:*** *The snapshot database does not require migration.*

# Re-Indexing a Database

When updating the databases used by FlexNet Manager Suite, consider whether this is also the time to re-index the databases. Take into account the following factors:

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

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

- Re-indexing is especially important if you have a lot of records in history tables. For example, in the inventory

database, check the `Installation` and `InstallationHistory` tables.

- Re-indexing is very demanding for SQL Server. You should only ever attempt a re-indexing of one database at a time. It is also good practice to schedule this out of production times, such as overnight or on a weekend.
- On large databases, **this process can take more than 24 hours**.

There is no requirement that you *must* re-index at this time: you may prefer to complete the current processes and schedule re-indexing at appropriate times soon. However, your current process is an excellent trigger for planning a regular schedule for re-indexing, say one or twice a year.

FlexNet Manager Suite provides a re-indexing script that can be applied to the following databases:

- The compliance database (suggested name: FNMSCompliance)
- The inventory database (suggested name: FNMSInventory)
- The data warehouse database (suggested name: FNMSDataWarehouse).

(There is little benefit in re-indexing the snapshot database (suggested name: FNMSSnapshot), as this is effectively cleaned up each time a snapshot is saved.)

---

***Important:*** *Do* ***not*** *apply the script to the Report Writer Content Store. This is a database designed by Cognos and not aligned with the reindexing script from Flexera.*

---

***To re-index one of the FlexNet Manager Suite operations databases (optional):***

1. Start SQL Server Management Studio (or your preferred tool).
2. Select *one* of the above three databases to reindex.
3. Open the `ReIndexAll.sql` reindexing script from your unzipped archive (for example, `C:\temp\FNMSDownloads\Database Migration\Normal`).
4. Click the **Execute Query** tool, or press `F5` to run the script.

Keep in mind that the re-indexing of each database may take a considerable time, depending on the size of your database. Wait until each process has completed before looping back to repeat for another of the three applicable databases.

# Database Validation

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

The first of these is a check of database constraints that may have been either enabled or disabled without data checks. If constraint errors are detected, the migration process corrects them. Where a constraint is enabled, the process also attempts to ensure that the data it covers is appropriate for the constraint. Generally, this succeeds without issue, and the change is simply noted in the migration log. However, if it fails, the migration process also fails with an error similar to:

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

If this occurs, the names of the constraints that cannot be enabled are listed in the migration log. Restarting the

migration at this time does not help this issue, and the database is unusable for production work. First, a database administrator or a Flexera support engineer must manually correct the issue with the underlying data. Once the data has been corrected, the migration process will be able to be restarted safely.

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

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

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

- The earlier database had previously been changed (either by database administrators or by a Flexera consultant) in ways that are not supported by the product
- A previous migration updated the database in ways that were not entirely correct, but not previously detected
- Something has occurred in the present migration that did not raise an error in the migration, but leaves the database in a less than perfect condition.

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

- Missing tables, indexes, columns, or foreign keys
- Extra indexes, columns or foreign keys
- Incorrectly configured columns (the size differs, or their nullability)
- An index configured in unexpected ways, either in its uniqueness, its clustering status, or in the columns it covers.

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

# Authorize the Service Account

The account used to run processing services requires permission to run as a service. 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 Upgrade Approach

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

- You may step through the upgrade 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 Upgrades Interactively.
- You may prepare a detailed answer file for (each of) your server(s), and then use a provided script to complete the upgrade(s) for you. This is especially helpful if you want a repeatable process, such as upgrading 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 a Scripted Upgrade.

# Managing a Scripted Upgrade

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

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

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

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

***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.*

## Typical workflow for scripted upgrade

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

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

1. Optionally, set up encryption for credentials to be referenced in the answer file(s) (see Prepare Encrypted Credentials for Upgrade). 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 Answer File).
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 Managing a Scripted Upgrade).
   b. Provide the correct answer file for this server's functionality.
   c. Run the supplied script with the appropriate command line (see Managing a Scripted Upgrade).

   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 Upgrading Flexera Analytics from FlexNet Report Designer).
   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 for Upgrade

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

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 upgrade 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 Answer File). 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 Answer File

An answer file provides all the details required for upgrade 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 upgrade 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:<br>• `ALL`<br>• `FleNetManagerPlatform`<br>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`<br>(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`<br>`ExternalAPIAppPoolUser` | The web application server |
| `BeaconAppPoolUser`<br>`BusinessReportingAuthUser` (also for IIS configuration)<br>`ReconciliationScheduledTaskUser` | The batch server |
| `RLAppPoolUser`<br>`DLAppPoolUser`<br>`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 Upgrade/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 upgrade:

- All related database must exist (see Upgrade/Create Databases)
- If you are encrypting identities needed in the upgrade, you must have configured and distributed both the certificate store and the certificate validating those identities (see Prepare Encrypted Credentials for Upgrade)
- You must have prepared the local copy of the answer file, correctly configured for the type of server undergoing upgrade (see Prepare Answer File)
- 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 upgrade resources (do not attempt to extract portions, as many scripts and files interact in this process).

When all is ready, triggering a scripted upgrade 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:<br>*drive-and-path*`\FlexNet Manager Suite\Installers\FlexNet Manager Suite\FlexNet Manager Suite Server.msi` |

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

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

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

3. Enter the command line to trigger the upgrade 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 upgrade 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 Upgrades Interactively

The following topics provide step-by-step instructions for interactively managing the upgrade of server(s) in your implementation of FlexNet Manager Suite. (Obviously, if you have already completed the scripted upgrade 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, Upgrade the Web Interface. For multi-server implementations, continue through the following topics as appropriate.

## Upgrade the Web Interface

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

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

---

***Note:*** *Are you installing on the same server that was previously your application server for FlexNet Manager Suite 2014 (the 10.0 release) (an in-place upgrade)? If so, you should now uninstall the previous version of the product so that you remove the MMC interface, deprecated from version 2014 R2. To do so:*

1. *On the application server, open* ***Program and Features*** *(****Control Panel*** *>* ***Uninstall a Program****).*
2. *Uninstall FlexNet Manager Platform (or your earlier compliance product, such as Compliance Manager), and then close* ***Program and Features****.*

---

***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.*

To update the web interface for FlexNet Manager Suite 2022 R2, follow this standard installation process.

---

***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 2022 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.

# Update the Inventory Server

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

In a single server implementation, this step is already completed and you should skip ahead to Upgrade PowerShell on Inventory Beacons.

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 2022 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.

# Update 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 2022 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 Identify (or Set Up) Accounts)
- The scripts themselves have sufficient authorization to execute, as described in the following process.

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

***To configure the system using supplied PowerShell scripts:***

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

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

      A message like `Attempting to start...` appears. Note that it can take some time before the service is started. When the service is running, the PowerShell scripts can update the IIS configuration as required.
2. If you require that the URLs for your central server(s) use the HTTPS protocol, confirm that site bindings have been configured to allow this:
   a. Open IIS Manager.
   b. In the **Connections** pane, expand the **Sites** node in the tree, and then click to select the site for which you want to add a binding.
   c. In the **Actions** pane, click **Bindings**.
   d. In the **Site Bindings** dialog box, click **Add**.

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

For more information (including the set up of the required certificate), see http://www.iis.net/learn/manage/configuring-security/how-to-set-up-ssl-on-iis.

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

a. Locate PowerShell. For example:

- On Windows Server 2012, **Start** > **Windows PowerShell**.
- On earlier releases, in the Windows Start menu, find **All Programs** > **Accessories** > **Windows PowerShell** > **Windows PowerShell** (this is the 64-bit version; the 32-bit version is `Windows PowerShell (x86).`).

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

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

4. If you have not already done so, in the PowerShell command window, execute:

```
set-executionpolicy AllSigned
```

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

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

6. On each server, execute:

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

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

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

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

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

***Tip:*** *Helpful notes:*

- *Use the service account details you created earlier (example: svc-flexnet).*
- *Separately on each dialog, the check box* ***Use the same credentials for all identities*** *copies the account details from the upper section to the lower section of the dialog.*
- *For externally visible URLs, you can specify either HTTP or HTTPS protocol, and either the flat server name or*

*the fully qualified domain name is supported. Any port number is optional. Remember that site bindings may be required if you are using the HTTPS protocol (see above). Valid examples:*

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

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

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

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

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

      The **Services** dialog opens.

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

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

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

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

- Data warehouse export
- Export to ServiceNow
- FlexNet inventory data maintenance
- Import SAP inventories
- Import SAP package license
- Inventory import and license reconcile
- Recognition data import
- Regenerate Business Import config
- Send contract notifications.

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

- Import Active Directory
- Import application usage logs
- Import discovery information
- Import installation logs
- Import inventories
- Import Inventory Beacon activity status
- Import Inventory Beacon status
- Import remote task status information
- Import security event information
- Import system status information
- Import VDI access data.

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

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

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

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

d. Close the dialog.

Configuration by the PowerShell scripts is now complete. Although not needed now, at other times it is possible to re-run the PowerShell scripts with the following flags for the use cases shown. You do not need to re-run the scripts

unless, at some later stage, one of these use cases applies to you:

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

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

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

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

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

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

- Add the `removeConfig` flag to remove the `%ProgramFiles(x86)%\Flexera Software\FlexNet Manager Platform\WebUI\web.config` file before using Windows Programs and Features to uninstall FlexNet Manager Suite:

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

# Upgrading Flexera Analytics

Once you have upgraded FlexNet Manager Suite to 2022 R2, you can upgrade Flexera Analytics. Flexera Analytics relies on IBM Cognos Analytics, and from the 2020 R1 release of FlexNet Manager Suite, it supported IBM Cognos Analytics version 11.0.13.

---

***Tip:*** *At the same time as the 2020 R1 release, backward compatible packages for Flexera Analytics were released that provided updated dashboards for any release of FlexNet Manager Suite from 2018 R2 forward (that is, relying on IBM Cognos Analytics version 11.0.11). This made it optional to upgrade the IBM Cognos Analytics product at that time, since you could choose to use the backward-compatible packages instead.*

From the 2020 R2 release of FlexNet Manager Suite, it is strongly recommended that you upgrade the underlying IBM Cognos Analytics version to take advantage of current and future functionality. Which process you should follow depends on your starting point – that is, from what version of FlexNet Manager Suite you are upgrading.

---

***Tip:*** *You can validate which version of IBM Cognos Analytics is currently installed on your system in either of these ways:*

- *Navigate to* ***Control Panel > All Control Panel Items > Programs and Features****, find IBM Cognos Analytics in the listing and note the contents of the* ***Version*** *column*
- *Navigate to the installation location for IBM Cognos Analytics (the default location is `C:\Program Files\ibm\cognos\analytics`), open the file `cmplst.txt` in your preferred text editor (such as Notepad), and near the top of the file, find the value for `kit_version`.*

Choose the appropriate topic based on your existing release of FlexNet Manager Suite that you are upgrading:

- If you currently use FlexNet Manager Suite 2020 R1, *and* you updated IBM Cognos Analytics when you installed/upgraded to that version, there is no further update of Flexera Analytics required. You have already upgraded to IBM Cognos Analytics release 11.0.13.
- If *either:*
  - You currently use FlexNet Manager Suite 2020 R1, *but* you have not yet upgraded your installation of IBM Cognos Analytics; *or*
  - You currently use any other release of FlexNet Manager Suite from 2017 R3 *forward*,

  then please refer to Upgrading Recent Flexera Analytics and use the process documented there.
- If you currently use FlexNet Manager Suite release 2017 R2 or *earlier*, please use Upgrading Flexera Analytics from FlexNet Report Designer.
- If you do not have Flexera Analytics or FlexNet Report Designer previously installed, but you are planning to add Flexera Analytics as part of this upgrade, please refer to *Installing Flexera Analytics* in *Installing FlexNet Manager Suite On-Premises*.

In any of the above cases, your new version of Flexera Analytics supports the use of the HTTPS protocol (with your preferred certificates), as well as the Transport Layer Security (TLS) 1.2 protocol. To take advantage of either of these security features, see Configuring IIS to Use SSL/TLS Encryption and Reconfigure Cognos Analytics to Use Third-Party SSL Certificates below.

---

***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.*

# Upgrading Recent Flexera Analytics

This topic is for use when upgrading Flexera Analytics from FlexNet Manager Suite 2017 R3 or later to 2022 R2. If you are upgrading from an earlier release using **FlexNet Report Designer**, please refer to Upgrading Flexera Analytics from FlexNet Report Designer.

Upgrading **Flexera Analytics** replaces earlier versions of IBM Cognos Analytics with IBM Cognos Analytics 11.0.13.

Once you have confirmed that all prerequisites have been met, an upgrade of **Flexera Analytics** can be summarized as follows:

1. Take a full backup of your Cognos Analytics content store database.
2. Upgrade Cognos Analytics.
3. Re-start the services.
4. Re-configure Flexera Analytics by populating an answer file with settings appropriate to your environment, and then implement the configuration, using PowerShell.
5. Run the package import tool by following the instructions in the section Update the Sample Reporting Package.
6. Optionally, you may need to configure your Security Assertion Markup Language settings.

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.

***Tip:*** *It is not necessary to back up the configuration and data files on a Microsoft Windows operating system. These files are preserved during the uninstallation.*

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 Upgrade 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 Importing an Updated Flexera License).

***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**".*

***To upgrade Flexera Analytics:***

1. Best practice is to take a full backup of your existing Flexera Analytics content store database, and save it securely. If there are any database problems in your upgrade, you can restore this protective copy to recover.
2. Upgrade IBM Cognos Analytics as follows:
   a. You will need to stop the **IBM Cognos** service and ensure that the **IBM Cognos Configuration** program is not running.
   b. Stop your Microsoft IIS web server that is running your Flexera Analytics website.
   c. If you are upgrading FlexNet Manager Suite and Flexera Analytics on separate servers, you will need to copy the `Support` folder from your application server to your Flexera Analyticsserver. Find the `Support` folder in `<drive path>\FlexNet Manager Suite\Support` from your application server and copy under the existing `<drive path>\FNMSCognosAnalytics` directory on your Flexera Analytics server. If you are performing a single server installation, then the support folder should already be located on the application server.
   d. Once downloaded from the Product and Licensing Center, you can unzip `Flexera Analytics 2022 R2.zip` and extract the following file to your Flexera Analytics server:

      ```
      ca_svr_win64_11.0.13.buildNumber.exe
      ```

      ***Tip:*** *The build number may vary. An example is 19121917.*
   e. Double-click on this executable file to launch it, and work through the installation wizard panels as described in the following table.

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

| Panel | Details |
|---|---|
| **Splash screen** | Select **Installation language**, then click **Next**. |
| **Product Install** | Select the **IBM Cognos Analytics** radio button option, then click **Next**. |
| **License Agreement** | • If you agree to be bound by its terms, select the **I accept the terms of the license agreement** check box.<br>• If you do not accept the terms of the license, you must stop the installation process. Do not proceed further in this case. |

| Panel | Details |
|---|---|
| **Location** | Specify the location of your existing Flexera Analytics instance. You can enter a path manually in the **Installation Folder** field, or browse for a location using the **Choose...** button.<br>Once an installation folder has been specified, click **Next**.<br>Click **Yes** to confirm you are installing in the same location and are overwriting a previous installation.<br>  ***Note:*** *Spaces in the installation path are acceptable in the command line; but if you are scripting the installation, be sure to enclose the entire path-with-spaces in double quotation marks.* |
| **Summary** | Click **Yes** to install, and **Done** when complete |

3. Save the configuration, and restart IIS:

   a. Open the **IBM Cognos Configuration** program. You will be prompted that older versions of **Configuration files were found and configuration files have been upgrade to the latest version**. Click **OK** and **Save** your configuration.

    ***Tip:*** *You do not need to restart the **IBM Cognos** service at this time, since there will shortly be additional configuration changes, and the service is then restarted by the PowerShell script described below.*

   b. Navigate to the root of the Cognos Analytics installation directory and open the `cmplst.txt` file in a text editor and verify that the **kit_version** has changed to **11.0.13.%**.

   c. Re-start your Microsoft IIS web server.

4. 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**<br>`C:\user\customstore.xml` | A custom credential store location.<br>If this parameter is omitted, the value defaults to `fnms.password.store.xml` under the profile directory of the logged-in user. |
| **FNMSBatchServerLocation**<br>`http://BatchServer1.company.com` | The URL of the FlexNet Manager Suite batch server (or, in smaller implementations, the server hosting that functionality). |

| Property/Example | Description |
|---|---|
| **ContentStoreDatabaseLocation**<br>`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**<br>`ContentStore` | This is the name of your Cognos Analytics content store database. |
| **ContentStoreDatabaseUsername**<br>Typically empty | Optional setting when providing credentials for SQL Server authentication. Leave this value blank to use Windows Authentication.<br><br>***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:*<br>• *Create and Drop table privileges.*<br>• *Member of the `db_ddladmin`, `db_datareader`, and `db_datawriter` roles.*<br>• *Must be the owner of the default schema on this database.*<br><br>***Tip:*** *This schema usually is named* ***FlexNetReportDesignerSchema****.* |
| **ContentStoreDatabasePassword**<br>Typically empty | Optional setting when providing credentials for SQL Server authentication. Leave this value blank to use Windows Authentication. |
| **ContentStoreDatabaseStoreReference**<br>`flexera://storeUser` | The credential store reference for ContentStore database user identity.<br>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**<br>`C:\Program Files\ibm\cognos\analytics` | Flexera Analytics installation directory. Update this path to change the default installation path. |

| Property/Example | Description |
|---|---|
| **CognosServerURI**<br>`http://$(ServerName):80` |  ***Note:*** *The `$(ServerName)` text should not be altered. It will be translated to the host name by the installation code.* |
| **CognosServerDispatcherURI**<br>`http://$(ServerName):9300` |  ***Note:*** *The `$(ServerName)` text should not be altered. It will be translated to the host name by the installation code.* |
| **AppPoolUserName**<br>`Company\svc-fnms` | The service user, used by IIS. |
| **AppPoolPassword**<br>(clear text) | A clear text password. |
| **AppPoolStoreReference**<br>`flexera://serviceUser` | The credential store reference for App Pool user identity.<br>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. |
| **CognosServiceUserName**<br>`Company\svc-fnms` | 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). |
| **CognosServicePassword**<br>(clear text) | A clear text password. |
| **CognosServiceStoreReference**<br>`flexera://serviceUser` | The credential store reference for Cognos service user identity.<br>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. |

| Property/Example | Description |
|---|---|
| **CognosServiceMaxMemory**<br>`4096` | IBM recommends a minimum of 4GB (`4096`MB) for Cognos Analytics. This number is a starting point and should be adjusted upwards based on the memory usage of your system.<br><br>***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.* |
| **MachineKeyValidationKey**<br>`ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789` | 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`.<br>The required value is present in the **<machineKey>** element. |
| **MachineKeyDecryptionKey**<br>`0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ` | 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`.<br>The required value is present in the **<machineKey>** element. |
| **SmtpStoreReference**<br>`flexera:\\smpt` | The credential store reference for SMTP user identity.<br>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. |
| **FNMSConfiguration**<br>`op` | 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.<br>Modifying this value will cause the Flexera Analytics installation to fail. |

***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.*

5. To complete the upgrade, you will need to perform the instructions in the section Update the Sample Reporting Package. This is required to apply any updated user permissions.
6. 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.

# Upgrading Flexera Analytics from FlexNet Report Designer

This topic is for use when upgrading to Flexera Analytics from **FlexNet Report Designer**. If you are upgrading from FlexNet Manager Suite release 2017 R3 or later, with Flexera Analytics already installed, please refer to Upgrading Recent Flexera Analytics.

When performing this upgrade, you will be replacing your earlier implementation with **Flexera Analytics** using Cognos Analytics 11.0.13.

Once you have confirmed that all pre-requisites have been met, an upgrade from **Report Designer** to **Flexera Analytics** can be summarized as follows:

1. Take a full backup of your existing Cognos Analytics content store database
2. Remove FlexNet Report Designer
3. Fix any inconsistencies in the Cognos Analytics Content Store database
4. Remove Notice Cast (NC) tables from your Content Store database
5. Backup and then restore your Content Store to a new database
6. Remove your previous installation of FlexNet Report Designer

7. Copy the Flexera Analytics Installation file
8. Configure Flexera Analytics by populating an answer file with settings appropriate to your environment, and then install Flexera Analytics, using PowerShell
9. Configure your web application server to connect with Flexera Analytics
10. Update your Roles to enable access
11. Ensure that your web browser(s) include your web server in the list of trusted web sites
12. Run the package import tool by following the instructions in the section Update the Sample Reporting Package
13. Optionally, you may need to configure your Security Assertion Markup Language settings.

You may require an updated license for FlexNet Manager Suite that includes new terms for Flexera Analytics. For details about applying your new license, see Importing an Updated Flexera License.

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.

---

***Tip:*** *It is not necessary to back up the configuration and data files on a Microsoft Windows operating system. These files are preserved during the uninstallation.*

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 Upgrade 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 Importing an Updated Flexera License).

---

***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.

---

***To upgrade FlexNet Report Designer to Flexera Analytics:***

1. Best practice is to take a full backup of your existing Flexera Analytics content store database, and save it securely. If there are any database problems in your upgrade, you can restore this protective copy to recover.
2. Remove FlexNet Report Designer by removing the existing installation of IBM Cognos Analytics. Navigate to the **Add or remove programs** wizard and uninstall FlexNet Report Designer.

   The existing content store database is not affected by this process.

   ---

   ***Tip:*** *Uninstallation of* ***FlexNet Report Designer*** *does not remove the* ***IBM Cognos*** *program group from the Start Menu (remaining shortcuts are not functional). It is safe to remove the entire program group. Furthermore, the uninstallation process also generates a log file in the Report Designer's installation directory (usually* `C:\Program Files\ReportDesigner`*), and this can be safely archived for removal of the entire directory.*
3. To fix any inconsistencies in the Cognos Content Store database, perform the following steps:
   a. Request your database administrator to take a full backup of the Content Store as these steps will alter your database.

      ---

      ***Tip:*** *You can find the Content Store location by launching IBM Cognos Configuration on the server hosting your* ***FlexNet Report Designer****. On the left tree list, click on the "Data Access > Content Manager > Content Store" node.*

**b.** Launch SQL Server Management Studio and login to the database server with a user that owns the default schema on Content Store database (usually 'FlexNetReportDesigner').

**c.** Log on to the server hosting the FlexNet Report Designer and then open Windows Explorer and navigate to

```
<drive>:\Program Files\ReportDesigner\c10_64\configuration\schemas\content\
sqlserver.
```

**a.** Run `dbCheckConsistency_mssqlserver.sql` on your Cognos Content Store database.

**b.** If you receive the following errors, you can safely ignore them as these procedures may not exist at this stage of the upgrade:

- `Cannot drop the procedure 'getInconsistentCMIDs', because it does not exist or you do not have permission.`
- `Cannot drop the procedure 'printInconsistentCMIDs', because it does not exist or you do not have permission.`

**c.** If you encounter any other errors, ensure that you have logged in with a user who has DDL permissions on the schema (dbo, etc.) that owns the Cognos Content Store database.

**d.** Run `dbMakeConsistent_mssqlserver.sql` on your Cognos content store database.

**4.** You will need to remove **Notice Cast** (NC) tables from your Content Store database. Notice Cast is used to manage the scheduling, delivery and notification of content.

---

***Note:*** *The following instructions are based on IBM knowledge Center article: https://www.ibm.com/support/knowledgecenter/SSEP7J_10.2.2/com.ibm.swg.ba.cognos.inst_cr_winux.10.2.2.doc/t_rundatabasecleanupscripts.html*

**a.** Stop the IBM Cognos service from Cognos Configuration

**b.** Locate the file `NC_DROP_MS.sql` in the following directory:

```
C:\Program Files\ReportDesigner\c10_64\configuration\schemas\delivery\
sqlserver
```

**c.** In SQL Server Management Studio, open the `NC_DROP_MS.sql` file

**d.** Change database connection to the FlexNet Report Designer content store database and execute the script

**e.** Check that there are no errors from the script execution

**f.** Start the IBM Cognos service using Cognos Configuration to ensure that it starts successfully, with no critical errors.

**5.** Backup and restore your Content Store to a new database

**a.** Request your database administrator to take a full backup of your FlexNet Report Designer's Content Store database

**b.** Restore the backup Content Store database to your destination server which has been set up to host the Content Store for Cognos 11.

***Note:*** *This will be a new database with a different name from the original.*

a. If you are restoring the database on a *different* server, you will need to create a login that has the following permissions on the new database:

- **Create** and **Drop** table privileges
- Membership of the `db_ddladmin`, `db_datareader`, and `db_datawriter` roles
- Must be the owner of the default schema on this database. This schema usually is `FlexNetReportDesignerSchema`.

6. 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-1.2.2-win`
- `ca_srv_11.0.13-2201052300-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.*

7. 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**<br>`C:\user\customstore.xml` | A custom credential store location.<br>If this parameter is omitted, the value defaults to `fnms.password.store.xml` under the profile directory of the logged-in user. |
| **FNMSBatchServerLocation**<br>`http://BatchServer1.company.com` | The URL of the FlexNet Manager Suite batch server (or, in smaller implementations, the server hosting that functionality). |
| **ContentStoreDatabaseLocation**<br>`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. |

| Property/Example | Description |
|---|---|
| **ContentStoreDatabaseName**<br>`ContentStore` | This is the name of your Cognos Analytics content store database. |
| **ContentStoreDatabaseUsername**<br>Typically empty | Optional setting when providing credentials for SQL Server authentication. Leave this value blank to use Windows Authentication.<br><br>***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:*<br>• *Create and Drop table privileges.*<br>• *Member of the `db_ddladmin`, `db_datareader`, and `db_datawriter` roles.*<br>• *Must be the owner of the default schema on this database.*<br><br>***Tip:*** *This schema usually is named* ***FlexNetReportDesignerSchema****.* |
| **ContentStoreDatabasePassword**<br>Typically empty | Optional setting when providing credentials for SQL Server authentication. Leave this value blank to use Windows Authentication. |
| **ContentStoreDatabaseStoreReference**<br>`flexera://storeUser` | The credential store reference for ContentStore database user identity.<br>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**<br>`C:\Program Files\ibm\cognos\analytics` | Flexera Analytics installation directory. Update this path to change the default installation path. |
| **CognosServerURI**<br>`http://$(ServerName):80` | ***Note:*** *The `$(ServerName)` text should not be altered. It will be translated to the host name by the installation code.* |

| Property/Example | Description |
|---|---|
| **CognosServerDispatcherURI**<br>`http://$(ServerName):9300` |  ***Note:*** *The `$(ServerName)` text should not be altered. It will be translated to the host name by the installation code.* |
| **AppPoolUserName**<br>`Company\svc-fnms` | The service user, used by IIS. |
| **AppPoolPassword**<br>(clear text) | A clear text password. |
| **AppPoolStoreReference**<br>`flexera://serviceUser` | The credential store reference for App Pool user identity.<br>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. |
| **CognosServiceUserName**<br>`Company\svc-fnms` | 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). |
| **CognosServicePassword**<br>(clear text) | A clear text password. |
| **CognosServiceStoreReference**<br>`flexera://serviceUser` | The credential store reference for Cognos service user identity.<br>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. |

| Property/Example | Description |
|---|---|
| **CognosServiceMaxMemory**<br>`4096` | IBM recommends a minimum of 4GB (`4096`MB) for Cognos Analytics. This number is a starting point and should be adjusted upwards based on the memory usage of your system.<br><br>***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.* |
| **MachineKeyValidationKey**<br>`ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789` | 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`.<br>The required value is present in the **<machineKey>** element. |
| **MachineKeyDecryptionKey**<br>`0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ` | 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`.<br>The required value is present in the **<machineKey>** element. |
| **SmtpStoreReference**<br>`flexera:\\smpt` | The credential store reference for SMTP user identity.<br>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. |
| **FNMSConfiguration**<br>`op` | 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.<br>Modifying this value will cause the Flexera Analytics installation to fail. |

***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.*

8. When upgrading from **FlexNet Report Designer**, your roles and operator accounts have been migrated to the new version of Flexera Analytics. However, when upgrading from **FlexNet Report Designer**, a new license is required from Flexera to authorize use of the Flexera Analytics version. See Importing an Updated Flexera License for details. This must be completed before any operator can access any part of Flexera Analytics (and, as follows, operators must also be assigned to the appropriate roles).

9. Create a role to which you have assigned the `Analytics User` privilege, and a second role that has the `Analytics Administrator` privilege, and assign operators as required:

a. 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.

---

***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.*

10. 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`.

11. To complete the upgrade, you will need to perform the instructions in the section Update the Sample Reporting Package. This is required to apply any updated user permissions.

12. 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.

# 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 "recrypting" 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 recrypt 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 'recrypting' 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 no 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/disp*.
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 recrypt 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).

# Importing an Updated Flexera License

You may require an updated license for FlexNet Manager Suite when:

- You are upgrading from an early release that supported FlexNet Report Designer to the current version, supporting Flexera Analytics
- You are upgrading from a release prior to 2016 R1 to the current version.

It is possible that details of your license were emailed to you as part of the order confirmation process for your upgrade. If not, have your support liaison person raise a support ticket to request the license upgrade, and await its arrival in email.

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 with the upgraded license:***

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

   Replace *Installation-Dir* with your installation folder. The default location is `C:\Program Files (x86)\Flexera Software\FlexNet Manager Platform\DotNet\bin`.

3. Execute (double-click) `ManageSoft.Activation.Wizard.exe`.
4. Import your updated license to use FlexNet Manager Suite.

The terms of your updated license are now visible: navigate to the system menu ( ▼ in the top right corner) of the web interface, and select **FlexNet Manager Suite License**.

# Update the Sample Reporting Package

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

***To import the sample reporting package:***

1. In the web interface for FlexNet Manager Suite 2022 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 2022 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.

# 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 addition free-standing copies of the Inventory Adapter Studio.*

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


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

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

a. On https://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 2022 R2 to access the downloads.

2. In the list of components to download, select `Business Adapter Studio for` FlexNet Manager Suite 2022 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*.

# 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 Importing an Updated Flexera License), 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:***

1. Log into a computer where you are permitted to access the Internet and download files.
2. 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.
3. 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.
4. 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.

5. To collect your PURL entitlements, navigate to the appropriate download page in the Flexera Customer Community website:

   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** 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.)*

# 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.)

# Update Access Rights

Through your processes of database migration, all the access rights that applied in your earlier compliance product are carried forward into FlexNet Manager Suite 2022 R2.

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

---

***To modify access rights:***

1. Log in to the web interface to FlexNet Manager Suite 2022 R2.
2. Navigate to the system menu ( ▼ in the top right corner), choose **Accounts**, and select the **Roles** tab.
3. For each *unique* set of access rights that you need to assign to operators, ensure that there is (or create) a distinct role, and set its rights by expanding the various headings in the accordion and using the controls inside. (For advanced combinations, start by selecting `Custom` from the drop-down list in each section.) Remember to scroll down and click **Save** (or **Create**) when you make any changes.

   For more information, click the help button at the top left.
4. When appropriate roles are defined, switch to the **All Accounts** tab.
5. Find each account in the list in turn, and click the hyperlinked account name to open its properties.
6. Change the roles assigned, or add additional roles, to each account as required.

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

# Update and Deploy Additional Inventory Beacons

The inventory beacon is enhanced in 2022 R2, and should be updated to take advantage of the most recent functionality.

Key points to note include the following:

| Upgrading from | Notes |
|---|---|
| Any version, where you used a custom account to run the FlexNet Beacon Engine service. | The FlexNet Beacon Engine service normally runs as the local SYSTEM account on the inventory beacon (the default and recommended configuration). If you provided alternative credentials (perhaps to manage access through a proxy server), be aware that these credentials are not known to FlexNet Manager Suite, so that whenever an inventory beacon is automatically updated with a new version of the FlexNet Beacon software, the credentials for running the service are reset to SYSTEM. Hence, if you have manually configured custom credentials on an inventory beacon, you must re-configure those same credentials after each upgrade to FlexNet Beacon. |
| Any version before 2016 R1 | To take advantage of access evidence used for CAL calculations, you must upgrade inventory beacons from version 2016 R1.<br><br>***Tip:*** *For the same reason, instances of FlexNet inventory agent locally installed on devices and reporting through these inventory beacons must also be upgraded. For details, see Configure Updates to Inventory Agents.* |
| Release 2015 or earlier | If you are using ILMT for DB2 as an inventory source, the DB2 drivers on the inventory beacon must be upgraded to 64-bit. |
| Release 2014 R2 or earlier | If an inventory beacon functions as a parent to any other beacon, and is using Microsoft IIS as its web server, it must be updated as described in the following topics to grant access to the folder used for staging uploads, and to the files that must be served to a child beacon. |

Because of the self-updating functionality introduced for inventory beacons at version 2014 R2, the processes are quite different, and are covered in separate topics below, for:

- Upgrading 2014 or earlier, or installing new inventory beacons
- Managing self-upgrades from 2014 R2/R3 (or later) inventory beacons

# Upgrading 2014 or earlier, or installing new inventory beacons

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

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

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

***To upgrade or install an inventory beacon:***

1. Log in on the computer where the FlexNet Beacon is to be installed, and start a web browser there to access the URL *`server-name-or-IP-address`*/**Suite/**.
2. In the **Discovery & Inventory** menu, under the **Network** group, select **Beacons**.
3. Click **Deploy a beacon**.

   The **Deploy a Beacon** page appears. Ensure that the default **Download 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. Step through the installation wizard, using the summaries in the accordion section **Beacon setup** or the more detailed online help available through the web interface to assist as necessary.
8. Does this inventory beacon act as a parent to any other inventory beacons (lower in your hierarchy of beacons)? And if so, it is using Microsoft IIS as its local web server? If both of these are the case, you need to update parameters set for IIS as follows:

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

      The **Web Server Settings** page opens.

   b. Select **No local web server (will not allow any incoming web requests)**.

      This turns off the settings for IIS.

   c. Select **IIS web server**.

      The settings needed for child inventory beacons are now passed to IIS.
9. Is this an upgrade of an inventory beacon that previously collected third-party inventory, such as Microsoft Endpoint Configuration Manager (previously Microsoft SCCM), in your 2014 system? If not, continue to the next step.

   In 2014 (or earlier), third-party inventory collection was triggered by Windows Scheduled Tasks, and the account used for data access was the account running the scheduled task (often the SYSTEM account). In 2022 R2, all scheduling is managed by the inventory beacon engine (with settings controlled through the inventory beacon interface). This means that previously operating adapters will no longer work until you specify credentials under which they should run under the new scheduling system. To do this:

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

   b. Select a connection to update from the list, and click **Edit...**.

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

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

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

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

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

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

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

# Managing self-upgrades from 2014 R2/R3 (or later) inventory beacons

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

- Global settings for the overall update strategy
- Individual settings for each inventory beacon.

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

***To manage self-upgrades of inventory beacons:***

1. First check the global settings for inventory beacons:

   a. In the compliance browser, navigate to **Discovery & Inventory > Settings**.

   The **Inventory Settings** page appears.

   ***Tip:*** *Check the release details using the* ***View Change History for FlexNet Beacon*** *link in the* ***Beacon settings*** *section.*

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

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

already installed in your enterprise. This must be earlier than the new release that you now want to test in a pilot program. (For example, suppose you previously installed version X.3 of FlexNet Beacon, but now X.4 is available. In this example, setting the approved version to X.3 prevents the later X.4 being installed until after you approve it with your pilot program.) By limiting the global automation to your previous approved version, you control when the upgrades flow through your estate.

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

   a. In the compliance browser, navigate to **Discovery & Inventory > Beacons** (in the **Network** group).

      The list of your current inventory beacons displays. In the **Actions** column on the right-hand end of each entry, there is an edit icon (pen).

   b. For the desired inventory beacon, click its edit icon.

      The properties page for this inventory beacon displays. Ensure that the **General** tab is selected.

   c. In the **Overview** section of the **General** tab, make a selection from the **Upgrade mode** drop-down list.

      - For all operational inventory beacons (but not for your pilot test one), choose `Always use the approved version (currently release-number)` — This setting makes this inventory beacon respond to the global settings for all your inventory beacons (navigate to **Discovery & Inventory > Settings** ).
      - For the pilot test inventory beacon, choose `Choose a specific version` — Another control appears where you can choose the **Specific version**. Choose the latest version that you want to test.

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

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

# Upgrade Connected-Mode Studios

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

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

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

***To upgrade studios running in connected mode:***

1. For safety's sake, make a backup copy elsewhere of any custom adapters saved in the standard storage paths used by the Inventory Adapter Studio or Business Adapter Studio.
2. Using the credentials supplied by Flexera with your order confirmation (or as renewed since), log into

`https://flexerasoftware.flexnetoperations.com`.

3. On the first page, select `FlexNet Manager Platform`, and on the resulting second page, select the product again.
4. In the list of versions, click the product name for the version you are using (typically the most recent version).
5. In the list of components to download, select `Business Adapter Studio for` FlexNet Manager Suite `2022 R2.zip`, and download and save it to a convenient location (such as `C:\temp`).
6. In Windows Explorer, navigate to the downloaded archive, right-click, and choose **Extract All**.
7. Navigate into the unzipped archive, and double-click `setup.exe`, following the instructions in the installation wizard.

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

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

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

# Configure Updates to Inventory Agents

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

***Note:*** *Advanced inventory functionality often requires you to authorize the latest versions of FlexNet inventory agent.*

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

***Tip:*** *This procedure applies only to FlexNet inventory agents installed locally on inventory targets (either through 'adoption' or third-party deployment) and collecting policy from an inventory beacon. Other scenarios are handled differently:*

- *Copies of the FlexNet inventory core components installed on inventory beacons and used for zero footprint inventory collection are updated as part of the FlexNet Beacon self-update.*

- *If you are using copies of the lightweight FlexNet Inventory Scanner, you need to update those copies using the same techniques by which you deployed it in the first place.*
- *If you have used other techniques to deploy the FlexNet inventory core components to file shares or other locations of your choosing (where they are not automatically collecting policy), you need to use your preferred technique for deploying updated components.*

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

***Tip:*** *The database setting grants permission (through policy) to the FlexNet inventory agents to perform self-upgrades (or even downgrades) to the specified version. The setting, therefore, can only be put into effect on those platforms where the FlexNet inventory agent includes self-update functionality, and where new versions of the FlexNet inventory agent are included in the operations databases after the upgrade. Currently, FlexNet inventory agents on Debian or Ubuntu Linux do not include self-update functionality. On these platforms, you can do any of:*

- *Deploy new versions of FlexNet inventory agent manually*
- *Use your preferred third-party deployment tool to publish updates to FlexNet inventory agents*
- *Uninstall the old version(s) of FlexNet inventory agent, and once again target the devices for adoption through FlexNet Manager Suite.*

***To authorize self-update of FlexNet inventory agent through policy:***

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

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

2. In a command window, navigate to *installation-folder*\DotNet\bin.

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

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

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

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

   This lists all versions of the FlexNet inventory agent that are stored in your database and available for use as upgrades to your currently deployed agents. The list is typically updated at each release of FlexNet Manager Suite. Versions are shown by their internal major-minor-update numbering (such as `12.0.0`).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# Optional: Perform a Full Import

It is important here to distinguish two separate cases, each of which uses the term "full":

- A full *compliance calculation*, which is typically associated with inventory updates from all inventory sources, and by default happens daily. After a product upgrade, full compliance calculations resume on their normal schedule.

***Tip:*** *If you are using high-frequency inventory checks for IBM PVU licenses, with FlexNet Manager Suite as the source of truth for IBM PVU sub-capacity licensing, you must complete at least one full compliance calculation after the upgrade before consumption figures and license compliance status are once again valid for IBM PVU licenses.*

- A full (or non-differential) *import of FlexNet inventory*, discussed in this topic.

In most product upgrades, a full import of the FlexNet inventory held in your staging inventory database (suggested name: FNMSInventory) to your compliance database is unnecessary. This background helps you decide whether you wish to run the full import.

***Tip:*** *If you are upgrading from any release of FlexNet Manager Suite between 2014 and 2018R1 inclusive, a full import of FlexNet inventory and a full compliance calculation are required to correctly show relationships between your installation(s) of Oracle Enterprise Manager and the database instances (and related Oracle options) that they manage.*

Different parts of the inventory import processes behave in different ways appropriate to their context:

- All uploads from inventory beacons to the central application server are "full" inventory uploads, since the inventory beacon does not have access to your central databases nor the ability to distinguish changed from unchanged records. Every record received by the inventory beacon is uploaded. (In the case of FlexNet inventory, collected by the FlexNet inventory agent in any of its forms, this full upload is staged in the FlexNet inventory database.)
- Next, imports from the FlexNet inventory database to the operational compliance database are, by default, *differential* updates, which means that only records that were updated in the inventory database *after* the previous import into the compliance database are imported: for efficiency, unchanged records are not imported again. (The test is a simple comparison between the inventory date for the individual record and the date of the last import into the compliance database.)

This rhythm is highly efficient and works well, but in rare instances may cause a slight data delay after a product upgrade. It occurs only in the following uncommon set of circumstances:

1. Imagine that data previously staged in the FlexNet inventory database included a column (let's call it `columnX`) that was not included in imports to the compliance database, as it had been considered legacy data surplus to compliance requirements.
2. Now, in our imaginary product upgrade, to meet changing requirements `columnX` has been also added to the compliance database. (This is rare, in reality.)
3. At the next import of each inventory record from the staging inventory database to the compliance database, the last-saved value in `columnX` in the inventory database is automatically imported into the compliance database, just as you expect. This is the normal case and needs no intervention.
4. However, using the default differential update from the inventory database to the compliance database, any old and unchanged inventory record is not imported at this time, and therefore this unchanged compliance record does not receive a value in `columnX`. When you look at listings of inventory devices, the more recent imports do have a value in this column, and older imports do not.

You have options for dealing with this rare possibility:

- You can do nothing until you observe the symptoms described in 4 above, and then run a full import of FlexNet inventory. (In most upgrades, this corner case never occurs, so doing nothing is not an impractical option.)
- You can simply wait until, eventually, every inventory record is updated. As each one is imported into the compliance

database, its value for `columnX`is automatically added, so that eventually (depending on the frequency with which you collect data from your inventory devices) the data gap self-corrects.

- You can force a full import of FlexNet inventory from the staging data into the compliance database, just in case. Of course, the full import may take longer than the differential import; but you may consider this a worthwhile investment.

If you wish to force a full import of FlexNet inventory data from the staging inventory database into the compliance database, please take careful note of the following:

- Identify the connection name for your FlexNet inventory database. The default connection name is `FlexNet Manager Suite`, and the **Source Type** is `ManageSoft`.
- The full import is triggered from your batch server (or, in smaller implementations, the server hosting that functionality).
- You must be logged in as a user with administrator privileges on that server.
- The following command must be entered at the Windows Command Prompt (and specifically, this is *not* for use within a PowerShell window).
- Take careful note of the format of the command line shown below. The three dashes and the *tripled* double-quotation marks are not typographical errors, and are required. However, the command line has been broken over multiple lines for publication, and you should enter it all on one line.
- When all conditions are met, use the following command line (all on one line), replacing the placeholder *`connectionName`* with the name you gave the connection to your FlexNet inventory database:

```
BatchProcessTaskConsole.exe
     run InventoryImportReaders ---f
     -it Readers
     -s """connectionName"""
```

The full import is run (and may take some time, depending on the number of additional aged inventory records that are imported). Thereafter the additional data from the inventory database is present for all records in the compliance database, and is visible in the web interface of FlexNet Manager Suite.

# Activating and Using New Features

Some new features in the 2022 R2 release are available now that you have:

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

## Improved IBM PVU sub-capacity calculations (upgrading from 2017 R1 or earlier)

The improvements both to sub-capacity calculations for IBM PVU licenses and to the robustness of compliance calculations introduced with the 2017 R2 release are based on significant changes to the database schema. Therefore, if

you are upgrading from release 2017 R1 or earlier, the IBM PVU high-frequency mode is blocked until after your first, post-upgrade, full compliance calculation, which populates the required data in the updated schema. As these calculations are typically scheduled to happen overnight, you can either wait for the normal schedule; or, as an operator in a role granting you administrator privileges, you can trigger a full compliance calculation ahead of schedule by navigating to **License Compliance > Reconcile**, selecting **Update inventory for reconciliation**, and clicking **Reconcile**.

## Improved purchase processing (upgrading from 2015 R2 SP5 or earlier)

An important area of enhancement is around purchase processing, especially the handling of license subscriptions or maintenance purchases. To support these changes, from release 2016 R1 the **Unprocessed Purchases** listing has improved logic that checks for any **Available quantity** on each purchase (that is, any shortfall in total assignments to licenses compared with the purchased quantity). Depending on your past work practices, this enhancement may cause some historical purchase records to reappear in the **Unprocessed Purchases** listing. For full details and a remediation process, see Enhancement for Purchase Records.

## Improved inventory gathering (upgrading from 2015 R2 SP5 or earlier)

Some items of new or improved functionality requires updates to your deployed FlexNet inventory agents. These include:

- Gathering access evidence used for managing Microsoft User CALs and Device CALs
- Enhanced Oracle inventory gathering.

After an upgrade of your system, the deployed FlexNet inventory agents are not upgraded automatically, so that you can separately control the timing of this stage. Therefore, to take advantage of the new inventory functionality, you must first allow self-updates of your installed FlexNet inventory agents. For details, see Configure Updates to Inventory Agents.

## Increased reporting from inventory beacons (upgrading from any 2014 release)

If you are upgrading from a 2014 release (prior to 2015 R1), and you wish to take advantage of other new features (including the increased reporting from inventory beacons), your next inventory import and license consumption calculation must include a full (non-differential) import of FlexNet inventory. The command line to achieve this is shown below. Notice the particular use of the dash characters:

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

For more explanation, see Optional: Perform a Full Import.

## Adapter upgrades

Some adapters require special handling, or additional configuration or upgrade from earlier releases:

- BMC Discovery — If you are using this adapter and running it on your application server (rather than on a free-standing inventory beacon), you should ensure that all devices are updated for sociability with FlexNet inventory. You achieve this by making your next import and compliance calculation a full (non-differential) import, as described above.
- The ServiceNow integration package was entirely reworked in the 2016 R1 release. For details, see the relevant part in *FlexNet Manager Suite Inventory Adapters and Connectors Reference*.
- XenApp server adapter (see Update the XenApp Server Adapter).

- Virtual Desktops adapter (see Update the Virtual Desktops Adapter).

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

# IBM PVU License Configuration

The 2019 R1 release of FlexNet Manager Suite introduced substantial changes to the handling of IBM PVU licenses for those with a revised license from IBM allowing you to use FlexNet Manager Suite in "high frequency" mode (referring to the high frequency inventory check for any hardware or virtualization changes) to replace ILMT as the source of truth for sub-capacity calculations of PVU consumption. This is also sometimes referred to as "PVU mode".

If you are not in this group, and either are not using IBM PVU licenses at all, or are using them but relying on results imported from ILMT, you are unaffected by these changes, and may skip the remainder of this topic.

***To prepare for updated management processes for IBM PVU licenses:***

1. Ignore all IBM PVU license consumption figures and compliance status results in the brief period between your system upgrade and the next overnight full inventory import and license consumption calculations.

   The methods of calculating and tracking peak PVU consumption were completely revised at the 2019 R1 release. In particular, PVU points consumption is now reevaluated for the entire reporting period as part of each nightly compliance calculation. Therefore, the change-over from old methods to new methods of calculation is not complete until the next overnight compliance calculation following your upgrade. Until then, compliance status is unknown and consumption figures are deliberately not updated and may well appear inconsistent. This is automatically corrected after the next full compliance calculation.

   ***Tip:*** *The retrospective calculations for the reporting period rely on historical information about devices consuming from IBM PVU licenses. Automatic history tracking started immediately after you upgraded to release 2018 R2; or, if you skipped that release, it starts after you upgrade to 2022 R2.*

2. Rework any business adapters that make use of the `PeakConsumed` value for IBM PVU licenses.

   Although it is uncommon, you may have prepared custom business adapters (used with the Business Importer) that modify the peak values for your IBM PVU licenses. If this is the case, those business adapters no longer function until you rework them to omit references to the `PeakConsumed` property. This property has now been removed from the data model for the Business Importer, since the old method of overwriting calculated peaks is no longer supported (nor permitted).

3. If you have not already done so, create a hierarchy of locations (a type of enterprise group) that can be used to link inventory devices correctly to their IBM PVU licenses. (Even if you have a good hierarchy of locations, at least three top-level locations need to be linked to one each of the mandatory IBM regions.) You may either:

   - Navigate to the system menu ( ▼ in the top right corner), select **Data Inputs** and choose the **Business Data** tab, and follow the online help for that page to prepare a standardized spreadsheet of locations for one-time import
   - Manually create each location in the web interface, as follows:

     a. Navigate to **Enterprise > Locations**.

b. Open the online help from this page, and review both the introduction and the notes for **IBM region**.

c. For more detailed information, see the topic *Configuring Regions for IBM* in *FlexNet Manager Suite System Reference*.

d. Using that guidance, create the hierarchy of locations you desire, and assign to the appropriate IBM regions.

   This is faster if you make the regional assignments to locations that are as high as possible in your tree of corporate locations. Child locations by default inherit the region settings of their parent locations.

4. Ensure that every device consuming from an IBM PVU license is 'owned' by one of the locations that is now assigned to a region.

   Some approaches for this include:

   - **Individual edits:** On the **Consumption** tab of your IBM PVU license, `Ctrl+click` on each device name to open its properties in a new browser tab, select its location, and click **Save**. Repeat until all devices are assigned to their appropriate locations.
   - **Multi-select update:** If your enterprise has a strong naming convention for devices, you may be able to group a listing like the **Active Inventory** page by the device name, select multiple devices (of the same type) that all need the same location, and click **Open** to produce a page of shared properties. In the **Ownership** tab, select the common **Location** for all the selected devices, and **Save** the changed properties to update all the selected devices at once.
   - **Coding:** Derive a business adapter, perhaps like this:

     a. Wait until after your next overnight full compliance calculation (so that the new data model is in play).

     b. Open the license properties of your first IBM PVU license, selecting the **Consumption** tab.

     c. Use the column chooser to add (or remove) columns to get the appropriate properties displayed. In particular, display the **Location** and **IBM region** properties; and be sure to keep the **Device** name, of course.

     d. Use the download control (toward the left, just above the list) to save the consuming devices for this license (with the displayed columns) to an `.xslx` (Excel) spreadsheet.

     e. Complete the `Location` (and if you like, `Region`) columns in the spreadsheet.

     f. Build a custom business adapter to import the location assignments for each device. For details about business adapters and running the Business Importer, see *Using FlexNet Business Adapters*.

5. If necessary, merge license records to ensure correct assignments of inventory devices to a license.

   This is particularly important if you have multiple IBM PVU licenses for any given IBM product (within a region). The license reconciliation process for IBM PVU licenses (only) no longer takes account of whether there are unused points available on a license when choosing which license to link to a consuming device (for details about the remaining factors in the choice of license, see the topic *Operation in High-Frequency Mode* in *FlexNet Manager Suite System Reference*). Therefore, if you have multiple licenses (with matching **Restrictions** scope) for a single product, the reconciliation process now repeatedly chooses the *same* license for linking devices, possibly making that license over-utilized and leaving others under-consumed. In this case, then, it important to change your ratio of "licenses to products" from many-to-one (*n*:1) to one-to-one (1:1).
   On a separate point, there is no longer any need to replicate product licenses across the three mandatory IBM regions. A *single* license (per product) now correctly rolls up the consumption *per IBM region*, mapped through

the ownership of devices by locations, and the assignment of locations to IBM regions. This means that you can simplify the future administration of IBM PVU licenses long term by having only one license per product (1:1) rather than three (or more – *n*:1).

***Tip:*** *Provided that you have only one license* ***per product*** *(1:1) within each region (scoped by its* ***Restrictions*** *tab settings), it is not* ***mandatory*** *to merge your three regional licenses into a single all-region license. It remains the recommended* ***best practice*** *to merge down to only one all-region license per product, since it simplifies administration and reporting. However, if you already have a healthy structure of regional licenses (meaning one per product, within each region), the final result of PVU consumption and reporting is the same from a single all-region license or from three regional licenses. This means that, if your conditions are right, you might choose to treat license merging as a longer term project, not directly tied to your upgrade to FlexNet Manager Suite 2022 R2. Whether now or later, it's desirable to complete the merge of licenses for one individual product within one day, so that the overnight reconciliation process has a stable and correct set of licenses to work with.*

There is no convenient or automated way to merge license records, because the requirements here are unique to your enterprise. A manual process that may assist is:

**a.** Start with the record of an application that is already linked to your IBM PVU licenses.

The normal goal is to end up with a single license for each PVU-licensable application (or software bundle, which would use a single multi-product license). Therefore, if the **Licenses** tab in the application properties for this application shows only one IBM PVU license, move on to the next application, until all of your PVU-licensable applications have only one license each.

**b.** From the **Licenses** tab in the application properties, choose one of the multiple licenses for this application to become the new 'merged' license, and `Shift+Ctrl+click` that license name to open its license properties in a new browser tab.

Starting with an existing license reduces the configuration effort. Perhaps choose the license which has the most associated data, such as the most purchases linked to it, or perhaps a linked contract. (The number of linked inventory devices doesn't matter, as these will be moved automatically in the next full reconciliation.)

**c.** In the **Identification** tab of the license properties, temporarily edit the license **Name** to help manage this target during the process. For example, append `- Merged` to the license name, and **Save**.

**d.** Ensure that the properties of the merged license are set correctly:

In the **Use rights & rules** tab, expand the section **Rights on virtual machines and hosts** and ensure that **Use sub-capacity license calculations where available** is selected (normally this should be the only selection in this section).

***Tip:*** *Because you have previously been using FlexNet Manager Suite as the source of truth for PVU sub-capacity calculations, the* ***Discovery & Inventory > Settings > IBM reporting and archiving settings > Enable frequent hardware scanning for IBM sub-capacity license calculations*** *check box should currently be selected. If in doubt, validate and set.*

**e.** Check the **Restrictions** tab of the merged license. It's possible you had previously used restrictions to scope this license (say) to one of the IBM regions. In the new 'single license' model, the merged license is to apply worldwide; so remove any restrictions that work against that principle. In particular, remove any location-based restrictions.

f. In a similar way, visit the **Group assignment** tab, and (most likely) remove group assignments so that this merged license plays worldwide.

g. Typically, the **Ownership** tab of the merged license is also blank; but this requires assessment in the light of your corporate policies.

h. Be sure to **Save** the updated properties of your merged license.

i. Switch back to the application properties, and similarly open the properties of the *next* linked license in its own browser tab. We will transfer anything of importance from this license, and then delete the license record. Let's call this the 'condemned' license.

j. In the **Purchases** tab of the condemned license, `Shift+Ctrl+click` the name of the first purchase record to open *its* properties in yet another browser tab. The purchase record provides the fastest way to transfer entitlements from one license to another:

   a. In the **Licenses** tab of the purchase properties, search for the amended name of your merged license, and *add* that license to the purchase.

   b. Then identify and select the row for the condemned license, and click **Remove**.

   c. **Save** the updated purchase properties. This purchase and its entitlements have now been transferred from the condemned license to the merged license.

   d. Close the browser tab for this set of purchase properties.

   e. Back in the **Purchases** tab of the condemned license, refresh the browser tab (the transferred purchase now disappears); and repeat this process until you have transferred all purchases from the condemned license to the merged license.

k. In a similar way, in the **Contracts** tab of the condemned license, open the properties of any linked contract, and use the **Licenses** tab of the contract to switch its link from the condemned contract to the merged contract, saving and closing the amended contract properties.

l. Review other tabs of the condemned license properties for other things to transfer to the merged license:

   - Are there any **Notes** in the **Identification** tab that should be copied across, for example as defense against a possible future audit?
   - Have you saved any important data in the **Financial** tab?
   - Check the **Documents** tab for anything linked there that should be transferred to the merged license.

   Be sure to **Save** the merged license again when anything has been added to it for safekeeping.

m. Delete the condemned license:

   a. Copy the name of the condemned license from its license properties (we want to be *certain* of deleting the correct one!).

   b. Navigate to **License Compliance > All Licenses**, paste the name of the condemned license into the search field and type `Enter`. This should return exactly the one license record in the list area. (If not, investigate and identify which is your condemned license.)

   c. Click the check box at the left of this record, click **Delete**, and confirm the deletion.

n. Switch back to the browser tab displaying the **Licenses** tab of the application properties, and refresh so that the just-deleted license disappears from this page, and the merged license is visible. If there are still

multiple licenses attached to the application, choose the next old license to condemn, and loop back and repeat.

**o.** Once this application has just a single IBM PVU - `Merged` license, you can pause for the overnight reconciliation, and tomorrow inspect the peak consumption results on the **Compliance** tab of that license.

**p.** If there are other applications licensed with multiple IBM PVU licenses, choose a day when you will loop back and work through the license merging for the next application...

You may find that, after all your rework, there is some slight correction in overall points consumed after your next full inventory import and license compliance calculation. One unusual combination that may cause a downward correction when upgrading from an earlier release to 2019 R1 (or later) is as follows:

- You have devices which you have marked as `Ignored`
- Nevertheless, you have allocated entitlements from an IBM PVU license to those ignored devices
- The allocation should *force* license consumption for normal devices (either because you chose a `Permanent` allocation on the **Consumption** tab of the license, or because you set **Allocations consume license entitlements** on the **Use rights & rules** tab of the relevant license).

In previous releases, the forced consumption from the allocation was applied even to ignored devices. From release 2019 R1, IBM PVU licenses correctly ignore the device for this method of consumption, as well as for all others. As a result, overall consumption may correctly decrease by the number of points previously consumed by the ignored devices.

# Enhancement for Purchase Records

Enhanced functionality in the **Unprocessed Purchases** page (if you are upgrading from a release prior to 2016 R1) may require that you re-process some purchase records. The process is described below. These prior notes provide background understanding of causes and impacts.

The enhancement is:

- In prior releases, a purchase (of an appropriate type) appeared in this **Unprocessed Purchases** listing only when it was not *linked* to a license. The test did not take any account of *quantities* that were linked from the purchase to one or more licenses — as long as there was at least one link between the purchase record and a license, the purchase was counted as 'processed'.
- From release 2016 R1, FlexNet Manager Suite better supports splitting purchases of relevant types (including maintenance) across multiple licenses. As part of this improved functionality, it now examines each purchase to compare the quantity purchased with the quantity assigned to one or more licenses. Any time that the quantity assigned is less than the quantity purchased, the purchase is included in the **Unprocessed Purchases** listing. This allows you to use this listing as a work center for purchase processing, especially when you are splitting purchases across multiple licenses. The purchase is automatically removed from the listing as you assign the last of its purchased quantity to a license.

Depending on your previous work practices, this enhancement may cause some purchases previously processed to reappear in the **Unprocessed Purchases** listing after upgrade. This is more likely to occur for purchases of type `Software Maintenance`, and will occur if your previous practice has been to manually set the purchase quantity for a maintenance purchase to zero as you linked it to a license.*

In those cases where you had manually set the assignment from a maintenance purchase to a license to zero, there is an ongoing mismatch between the quantity purchased and the quantity assigned to the relevant license(s). After your upgrade, this mismatch correctly causes the purchase to appear in the enhanced **Unprocessed Purchases** listing. (The same is true of any other cases of historical purchases where, for any reason, the purchased quantity does not match the total assignments to licenses.) Since every purchase record is checked for this listing (no matter how old), you may rely on it catching all historical cases where the mismatch between purchased quantity and assigned quantity exists.

***To identify and reprocess purchases if required:***

1. In the web interface for FlexNet Manager Suite, navigate to **Procurement > Unprocessed Purchases** (in the **Purchases** group).

   The listing includes all historical purchases for which there is an **Available quantity** (which is the difference between the purchased quantity and the total assigned to all linked licenses).

2. Select one or more rows from the listing.
3. Click **Recalculate**.

   After a moment, unprocessed purchases may show updated values for **Recommended licenses**. In the cases described above, the recommendation is most often to link (once again) to the same license(s) you had previously linked to each purchase. Review all recommendations.

4. Select only those purchases with recommendations that you find acceptable, and click **Accept**.

   ***Tip:** The **Accept** button is enabled only when you select purchases with recommended licenses. You cannot include any rows where the **Recommended licenses** column displays `No recommendation calculated`,*

   FlexNet Manager Suite creates the appropriate links to the recommended licenses (including correcting the link types of those purchases that had been incorrectly linked before, so that their maintenance had been wrongly counted towards entitlements).

5. If there are remaining historical purchases that still require processing, select one at a time and click **Process**.

   A blue wizard area appears above the listing to assist with your processing choices. For details, click the online help button in the top right of the **Unprocessed Purchases** page.

6. Repeat as required until all the historical purchase records have been reprocessed.

The necessary reprocessing is completed, and entitlement counts and maintenance coverage correctly reflect your input data.

***Tip:** For `Software Maintenance` purchases, be sure to record the effective date and the expiry date on each maintenance purchase. This allows the system to automatically calculate coverage, alert you to forthcoming renewals, and so on.*

* One reason you may have used this approach is because of an early defect, since repaired, that incorrectly counted maintenance purchases toward license entitlements. This error only occurred when:

- The purchase was *manually* linked to the license (it did not occur when purchase automation was used)
- The link was manually made from the *purchase* properties (it did not occur when the link was made from the license end of the relationship).

(Historical purchase records affected by the old defect are visible in the **Purchases** tab of the license properties, where you can examine the **Purchase type** and **License entitlements** columns. Any linked purchase of type `Software maintenance` should have no value shown for **License entitlements**. Cases where you had adjusted the assigned quantity manually are detected and repaired as described here; and any cases where you did not notice this old error are now likely to be flagged in license listings with an alert that there is a mismatch between the software entitlements and the maintenance coverage.)

# Configure Updates to Inventory Agents

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

***Note:*** *Advanced inventory functionality often requires you to authorize the latest versions of FlexNet inventory agent.*

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

***Tip:*** *This procedure applies only to FlexNet inventory agents installed locally on inventory targets (either through 'adoption' or third-party deployment) and collecting policy from an inventory beacon. Other scenarios are handled differently:*

- *Copies of the FlexNet inventory core components installed on inventory beacons and used for zero footprint inventory collection are updated as part of the FlexNet Beacon self-update.*
- *If you are using copies of the lightweight FlexNet Inventory Scanner, you need to update those copies using the same techniques by which you deployed it in the first place.*
- *If you have used other techniques to deploy the FlexNet inventory core components to file shares or other locations of your choosing (where they are not automatically collecting policy), you need to use your preferred technique for deploying updated components.*

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

***Tip:*** *The database setting grants permission (through policy) to the FlexNet inventory agents to perform self-upgrades (or even downgrades) to the specified version. The setting, therefore, can only be put into effect on those platforms where the FlexNet inventory agent includes self-update functionality, and where new versions of the FlexNet inventory agent are included in the operations databases after the upgrade. Currently, FlexNet inventory agents on Debian or Ubuntu Linux do not include self-update functionality. On these platforms, you can do any of:*

- *Deploy new versions of FlexNet inventory agent manually*
- *Use your preferred third-party deployment tool to publish updates to FlexNet inventory agents*
- *Uninstall the old version(s) of FlexNet inventory agent, and once again target the devices for adoption through FlexNet Manager Suite.*

***To authorize self-update of FlexNet inventory agent through policy:***

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

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

2. In a command window, navigate to *installation-folder*\DotNet\bin.

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

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

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

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

   This lists all versions of the FlexNet inventory agent that are stored in your database and available for use as upgrades to your currently deployed agents. The list is typically updated at each release of FlexNet Manager Suite. Versions are shown by their internal major-minor-update numbering (such as `12.0.0`).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# Updating the ADDM Adapter

The ADDM adapter now offers increased support for BMC Atrium Discovery and Dependency Mapping. Additional features introduced with ADDM release 11 require that, if you have previously been using this adapter, you need to update the staging database used for data import.

**Note:** *If you are continuing to use ADDM release 10 or earlier, you do not need to update the staging database schema, and may skip this process. However, if you do apply this update to the staging database schema and continue to use ADDM release 10 or earlier, be sure to also use the latest version of the* `FnmpADDMStage.exe` *executable from the same* `Adapter Tools for` *FlexNet Manager Suite 2022 R2* `.zip` *archive. This executable transfers to ADDM data (for any ADDM version) to the staging database, and is schema-aware for the upgraded staging database.*

The update is a straight-forward task, once you have the latest copy of the appropriate script.

***To update the ADDM adapter:***

1. Right-click the downloaded zip archive, and choose **Extract All...**, saving the files in your working location.

   The path of interest in the unzipped archive is `Tier 1 Adapter Tools\BMC ADDM - Atrium Discovery and Dependency Mapping Tools`, which contains three folders:

   - `FnmpADDMStage`
   - `patterns`
   - `SQL`.

2. Copy the script `ADDM_staging.sql` from the `SQL\` folder to a temporary folder on your staging server.
3. 
4. 

The schema of your staging database is updated. For more information about the latest ADDM adapter, see the relevant chapter in *FlexNet Manager Suite Inventory Adapters and Connectors Reference*.

# Update the XenApp Server Adapter

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

***To update the XenApp server agent:***

1. Check the inventory beacon update is complete (see Update and Deploy Additional Inventory Beacons and sub-sections).
2. Be sure that you have completed an import from Active Directory from all relevant domains.

   For set-up details refer to *FlexNet Manager Suite Help > Inventory Beacons > Active Directory Tab*.
3. If you did not already update your staging database for this adapter in your central database server (as described in Upgrade/Create Databases):

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

   b. Further navigate into the appropriate sub-folder for your version of Citrix Virtual Apps (noting that the `C:\XenAppAgent` folder applies to Citrix Virtual Apps versions 7.5 or later):

   - `XenAppAgent6`
   - `XenAppAgent65`
   - `XenAppAgent`

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

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

   ***Tip:*** *If you have more than one of these staging databases, repeat this process until they are all updated.*
4. Ensure that the appropriate inventory beacon(s) has/have a connection configured for the staging database(s), and that the connection is scheduled for regular operation.

   For details, check the *Create Connections for Data Upload* section in *XenApp Server Adapter* chapter in the FlexNet Manager Suite Inventory Adapters and Connectors Reference.
5. On each of your Citrix Virtual Apps controlling servers where `FNMPXenAppAgent.exe` is installed, replace the executable with the correct version from the unzipped archive.

   For details, check the *Installing the XenApp Server Agent* section in the above-mentioned chapter.
6. As required, create or update a scheduled task to execute the upgraded XenApp server agent.

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

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

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

# Update the Virtual Desktops Adapter

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

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

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

---

***To update the Virtual Desktops adapter:***

1. Check the inventory beacon update is complete (see Update and Deploy Additional Inventory Beacons and sub-sections).
2. Be sure that you have completed an import from Active Directory from all relevant domains.

   For set-up details refer to *FlexNet Manager Suite Help > Inventory Beacons > Active Directory Tab*.
3. On each of the inventory beacon and the Virtual Desktops broker, check the execution policy for PowerShell scripts:
   a. On each machine in turn, open a PowerShell window.
   b. At the prompt, enter `Get-ExecutionPolicy`.

      Usable settings include `RemoteSigned`, `AllSigned`, or `Unrestricted` (although the latter is not recommended).
   c. If the current policy setting is `Restricted`, run the following command to set it to `RemoteSigned`:

      ```
      Set-ExecutionPolicy RemoteSigned
      ```
4. Create (or update) discovery and inventory gathering rules to target your Virtual Desktops brokers:
   a. In the web interface for FlexNet Manager Suite, navigate to **Discovery & Inventory > Discovery and Inventory Rules** (in the **Discovery** group).
   b. Select the **Targets** tab, click **Create a target**, and complete the details to target your Virtual Desktops broker(s). Click **Create** to add your new target to the list of available targets. (If necessary, repeat to create multiple targets.)

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

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

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

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

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

h. Complete the scheduling details, and click **Save as**.

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

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

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

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

   b. Locate your Virtual Desktops broker in the list of devices.

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

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

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

   - Inspect the log file on the inventory beacon for errors relating to Virtual Desktops discovery. This file is located at `%PROGRAMDATA%\Flexera Software\Compliance\Logging\BeaconEngine`.
   - Should you need to prepare a trace file to submit to Flexera Support, turn on the `Scheduling/RemoteExecution` tracing options by editing this file on your inventory beacon: *`InstallationDirectory`*`\Flexera Software\Inventory Beacon\etdp.trace`

6. As required, you may need to link the file evidence imported from Virtual Desktops to application records, and ensure that those application records are linked to license records. Wherever possible, link the license records to purchase records to identify the number of your license entitlements.

   Once all the links are in place, the next compliance calculation reflects your compliance position for applications accessible through Virtual Desktops.

# 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* `vversionNumber`
  - *Flexera Inventory Manager security service.*

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

# Identifying IIS Application Pool Credential Issues

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

## Background

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

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

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

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

## Diagnosis

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

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

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

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

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

server-name  5021  Warning Microsoft-Windows-WAS  System  date time
The identity of application pool FlexNet Manager Platform is invalid. The user name or
password that is specified for the identity may be incorrect, or the user may not have
batch logon rights. If the identity is not corrected, the application pool will be
disabled when the application pool receives its first request.  If batch logon rights
are causing the problem, the identity in the IIS configuration store must be changed
```

```
after rights have been granted before Windows Process Activation Service (WAS) can
retry the logon. If the identity remains invalid after the first request for the
application pool is processed, the application pool will be disabled. The data field
contains the error number.
```

### Repair

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

# Update Credentials in IIS Application Pools

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

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

***To update credentials in IIS Application Pools:***

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

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

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

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

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

   The **Set Credentials** dialog appears.

6. Enter the full **User name** for the account and enter the updated password in the two required fields.
7. Click **OK** to close all the open dialogs and save the new settings.
8. With the appropriate application pool still selected, in the **Actions** list on the right, click **Start**.

# IIS Roles/Services

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

- `Web Server > Application Development > .NET Extensibility`
- `Web Server > Application Development > ASP.NET`
- `Web Server > Application Development > CGI`
- `Web Server > Application Development > ISAPI Extensions`
- `Web Server > Application Development > ISAPI Filters`
- `Web Server > Common HTTP Features > Default Document`
- `Web Server > Common HTTP Features > Directory Browsing`
- `Web Server > Common HTTP Features > HTTP Errors`
- `Web Server > Common HTTP Features > HTTP Redirection`
- `Web Server > Common HTTP Features > Static Content`
- `Web Server > Health and Diagnostics > HTTP Logging`
- `Web Server > Performance > Dynamic Content Compression`
- `Web Server > Performance > Static Content Compression`
- `Web Server > Security > Basic Authentication`
- `Web Server > Security > Request Filtering`
- `Web Server > Security > Windows Authentication`

---

***To check available services in the Windows Server operating system:***

1. Starting from the Windows start menu, navigate to **Control Panel** > **Administrative Tools** > **Server Manager**.
2. In the navigation bar on the left, under the **Server Manager** node, select the **Roles** node.

3. Locate the **Web Server (IIS)** section, and within that, identify the **Role Services** section.

   This section lists the status for each service. All of those in the list above should be both installed and enabled on all your central servers.