Migrating to FlexNet Manager Suite 2015 R2 On Premises

Contents

Legal Information

Document Name: Migrating to FlexNet Manager Suite 2015 R2 SP3 on Premises

Part Number: FMS-11.3.0-MG01

Product Release Date: 17 February 2016

Copyright Notice

Copyright © 2016 Flexera Software LLC. All Rights Reserved.

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

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

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

Intellectual Property

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

Restricted Rights Legend

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

1

Migrating to FlexNet Manager Suite 2015 R2 SP3 on Premises

Topics:

- *Process Overview*
- *Design the Final Topography*
- *Prerequisites and Preparations*

📋

Note • *This document does not cover upgrading from FlexNet Manager Suite 2014 (any revision) or 2015 to FlexNet Manager Suite 2015 R2 SP3. For that simple process, see Upgrading FlexNet Manager Suite to 2015 R2 SP3 on Premises. As well, managed service providers (MSPs) should see the separate documentation for multi-tenant environments.*

FlexNet Manager Suite is a powerful and sophisticated tool, which has been extensively rewritten since FlexNet Manager Platform 9.2, with a new user interface and some significant back-end changes. Therefore migration is a significant project. Planning your upgrade is made more challenging because there are many different configurations of the 9.2 product, each of which represents a different starting point to migrate to the 2015 R2 SP3 release. This document covers the major starting points, and includes consideration of functionality required going forward.

This document is intended for use by:

- System engineers responsible for implementing and maintaining the system
- Network and security personnel with responsibility for infrastructure that the system relies on
- Flexera Software consultants implementing your system.

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

Process Overview

When upgrading to FlexNet Manager Suite 2015 R2 SP3, there are several possible starting points, each causing variations in the process. You may also desire a variety of possible outcomes. Having so many choices can make a guide like this seem complicated. The following flowchart and description illustrates your choices. To simplify further, you may wish to highlight the path through the possibilities that applies to your enterprise. The discussion that follows references each step in the flow chart by the numbers shown. The process outlined here has been proven successful, and you need to follow carefully.

Important • *Not shown in the flowchart is an initial backup of your database(s) and also of your existing server(s), using your normal backup procedures. In the unlikely event that you are dissatisfied with the result of this migration, the only 'roll back' option is to restore these backups.*

1 Upgrading to FlexNet Manager Suite 2015

2 Is Inventory Manager co-installed? — N →

↓ Y

3 Is IM version 9.2.3? — N → **4** Migrate Inventory Manager to 9.2.3

↓ Y

2a Is IM separately installed? — Y →

↓ N

5 Shared (single) DB? — N →

↓ Y

6 Run process to split DB (separate IM and FNMP)

↓

7 Upgrade FNMP to FNMS 2015 (incl local inventory beacon)

↓

8 Roll out operational inventory beacons

↓

9 Using *solely* IM 9.2 inventory? — Y ↓ — N → **10** Migration granularity at subnet level? — N → **11** Use IM 9.2 to upgrade MDs to 2015 with IB fail-over

↓ Y (from 10)

12 Switch each required DS to IB

13 Target MDs for staged migration

↓

14 Are all required MDs switched over? — N ↑ (back to 13)

↓ Y

15 Decommission unused IM servers (incl DS)

16 FlexNet Manager Suite 2015 is operational

1. Upgrading — The starting point

FlexNet Manager Suite 2015 R2 SP3 is a single, integrated solution for license optimization. However, you may be coming to this solution from a variety of starting points, such as:

1. FlexNet Manager Suite 2014. This is a simple upgrade path, for which a simplified document is available (see *Upgrading FlexNet Manager Suite 2014 Rx to 2015 R2 SP3 on Premises*).

2. FlexNet Manager Platform 9.2 or earlier; or its fore-runner Compliance Manager across many different releases. Provided that any one of these products is installed *on its own* (specifically, *without* a co-installation of Inventory Manager on the same application server), you may migrate this product directly to FlexNet Manager Suite 2015 R2 SP3 using this guide. If you also had a separate installation of Inventory Manager on another server, you may choose to upgrade it as part of this project, or to consider its upgrade separately if you wish, since earlier versions of Inventory Manager can still integrate with FlexNet Manager Suite.

3. Any of FlexNet Manager Platform 9.2 or earlier or Compliance Manager (any version) installed on the same application server as Inventory Manager. This is the most challenging case, as FlexNet Manager Suite now has integrated handling of its own inventory data, and no longer requires the separate Inventory Manager product. However, it is possible that you may prefer to preserve Inventory Manager for some of its more fine-grained targeting capabilities.

The following discussion points clarify the issues and options around case 2 (either no Inventory Manager, or implemented on a separate application server) and case 3 (co-installation on the same application server). (The question of a shared database is treated separately below.)

2. Is Inventory Manager co-installed?

"Co-installed" here means that Inventory Manager and your previous compliance product were installed on the same application server. You can usually tell whether Inventory Manager is installed with your earlier implementation by opening the product in the MMC console. If, along with the **FlexNet Manager Platform** node, you see nodes like **Managed Device Settings**, **Discovery and Adoption**, and **Remote Task Manager** in the console tree on the left, then Inventory Manager is co-installed on the same server. In this case, you will need to commission a new server (or set of servers, virtual or physical) for FlexNet Manager Suite 2015 R2 SP3 alone. Your existing combined server rolls forward as your Inventory Manager (only) server, at least for the time being, and we will uninstall your old FlexNet Manager Platform from this server in due course.

The rare exception is that you may have Inventory Manager installed, but on a *separate* server (question 2A). It will have its own MMC interface on that server with the same kind of nodes in the console tree (but not the **FlexNet Manager Platform** node). When Inventory Manager is separately installed like this, you may choose whether to:

- Defer any upgrade of the Inventory Manager product to a separate project that you will tackle later. In this case, go directly to step 5.

- Include the upgrade of Inventory Manager in this same project, as documented here. In this case take steps 3 and 4.

If you do not have *any* implementation of Inventory Manager, your decision tree is simplified, and you race ahead to step 7 (down the **N** exit from step 2a).

Details: *Identify and Update Inventory Manager Server* on page 36.

3 and 4. Ensure that Inventory Manager is up-to-date.

For the upgrade process, the scripts to assist your process with database separation and clean-up are based on the schema at 9.2.3. For that reason alone, you need to have Inventory Manager up-to-date before proceeding.

Also from a business perspective, if you plan to carry forward with Inventory Manager as an inventory source feeding your system (an option we discuss later), you are likely to use release 9.2.3 of Inventory Manager, since it has additional functionality particularly in relation to Oracle inventory gathering. So it will be convenient to complete this upgrade as part of the same project.

For these reasons, there is summary guidance for upgrading Inventory Manager included in this document (see *Identify and Update Inventory Manager Server* on page 36). If you want further information, use the Upgrade Guide installed with the 9.2 product to guide you.

Once you have done that, you are at the baseline to commence the upgrade to FlexNet Manager Suite 2015 R2 SP3.

5. Do both products share a single database?

If, in step 2, you identified that your products were co-installed on the same server, then you do have a shared database as well, so your answer here is **Y**.

If you have separate application servers, you may still have them sharing a common database. You could ask your DBA, or you can check a registry key as described later. Details: *Identify and Update Inventory Manager Server* on page 36.

The upgrade process requires that a shared database is first split into two. One database is preserved for on-going operation of Inventory Manager. The other can be upgraded to FlexNet Manager Suite 2015 R2 SP3.

💡

Tip • *The minimum supported database release is Microsoft SQL Server 2008. You'll also notice that the new product requires two or three additional databases that were not present in the 9.2 release (typically on the same database server).*

If you are sure that your previous implementation already had separate databases (and on a supported version of SQL Server), you can skip forward to step 7.

6. Split the databases

Separating the databases is required for the migration process. As well, since you may want to continue with Inventory Manager functionality for some time, splitting the databases allows for one copy to migrate up to FlexNet Manager Suite 2015 R2 SP3 while the other continues for Inventory Manager. You achieve this by:

• Doing a backup of your current joint database

• Doing a restore to make a second copy with a new name

• Running the scripts provided to clean out from each database the content belonging to the 'other' product.

Details: *Splitting a Shared Database* on page 49.

7. Upgrade your compliance product to FlexNet Manager Suite 2015 R2 SP3

If your earlier implementation had two separate servers for your compliance product and for Inventory Manager, you can apply the software upgrade to your compliance server directly.

In contrast, if you previously had a single server hosting both compliance and inventory, you now commission a new application server and install FlexNet Manager Suite 2015 R2 SP3 as a fresh installation. (Details are provided for planning your new implementation.) You can also uninstall the old compliance product from the previously combined server, which now becomes your Inventory Manager server.

In both cases, you also install an inventory beacon on your central application server. This 'home base' inventory beacon allows you to continue managing the compliance connections recorded in your database in your previous implementation. (Inventory beacons on separate servers cannot access legacy connections that were migrated from your 9.2 Inventory Manager database into your FlexNet Manager Suite 2015 R2 SP3 database. Only the local inventory beacon has database access.)

Full details for this step are included in the chapter *Upgrading FlexNet Manager Suite* on page 51.

8. Roll out your inventory beacon hierarchy

Your old Inventory Manager product possibly used a hierarchy of distribution servers to send out packages and upload inventory collected by inventory agents installed on managed devices. (Around release 9.0, the distribution servers were renamed inventory beacons; but to avoid confusion in this document, we will continue to call them distribution servers.)

Inventory beacons supplied with FlexNet Manager Suite 2015 R2 SP3 are completely re-architected, and you should roll out a new hierarchy of 2015 R2 SP3 inventory beacons on separate machines (which can be virtual machines if you so choose).

Note • Inventory beacons for 2015 R2 SP3 are not compatible with earlier distribution servers (including those for 9.2 or later that were called inventory beacons), and cannot coexist on the same computer.

Exactly how you do this depends on your strategy, decided in the following steps. For example, if you want the fastest possible automated switch-over, you simply replace the distribution server software with FlexNet Beacon software, as described in more detail in step 12.

Your alternative strategy involves parallel operation of 9.2 inventory gathering with 2015 R2 SP3 inventory beacons. Since these cannot exist simultaneously on the same server, parallel operation requires that you roll out a parallel machine hierarchy.

Keeping both the old distribution server hierarchy and the new inventory beacon hierarchy operational in parallel allows for an orderly transition. Later, if you decide to move away from Inventory Manager, you can decommission and re-purpose the former distribution servers.

Details: *Managing Device Migration by Individual Device* on page 83.

9. Using solely Inventory Manager 9.2 for FlexNet inventory collections?

Broadly, you need to decide what functionality from Inventory Manager you want to preserve, and for how long. FlexNet Manager Suite 2015 R2 SP3 deliberately simplifies management of FlexNet inventory agents on target devices. Consider this functionality comparison:

Inventory Manager 9.2	FlexNet Manager Suite 2015 R2 SP3
Choose between client-side policy merging and server-side policy merging. (Client-side policy merging was more commonly used for deployment activities. Any managed devices relying on client-side policy merging must continue to be managed under Inventory Manager 9.2.)	Only server-side policy merging is supported (as appropriate for gathering inventory), and is the required setting for all FlexNet inventory agents managed under this system.
Manually configure settings packages for inventory agents.	Settings are determined automatically, based on behavioral rules you create.
Manually deploy settings packages to managed devices.	Inventory agents (on inventoried devices) are updated automatically.
Create multiple schedules for inventory agents and data upload.	All FlexNet inventory agents share a single schedule for local inventory gathering, and there is one schedule for discovery across the network (but there are individual schedules for importing inventory data from each third party system, and for importing each kind of business data like purchases).
Ability to run custom remote execution commands.	Only the specific remote execution tasks required for inventory are available.
Manually identify target computers for adoption as managed devices.	Option to automatically install an inventory agent on any computers that are discovered (and do not already have an agent installed). This rule-based 'adoption' can be targeted to individual machines or to subnets.

By comparing product functionality with your requirements, you need to decide whether to:

- Persist with Inventory Manager 9.2.3, using it as an inventory feed into FlexNet Manager Suite 2015 R2 SP3, and not using the FlexNet inventory gathering features in FlexNet Manager Suite 2015 R2 SP3 at all. You are preserving Inventory Manager functionality, shown in the left-hand column above, across your *entire* computing estate. This means you are done, and take the **Y** exit from step 9 to leap forward to the finish line at step 16. (Otherwise you take the **N** exit and continue with step 10.)

- Switch entirely to the simplified native inventory gathering incorporated in FlexNet Manager Suite 2015 R2 SP3, using the new rule-based approach. You plan to enjoy the simplified management in the right-hand column above. You need to make the choice described for step 10 to work out how you will handle this.

- Combine the systems, using distinct features of each in those parts of your enterprise for which they are best suited. (Technically, this is like the switch-over scenario, except that you make the transition period of indeterminate length.) You might, for example, use Inventory Manager to manage a set of machine-room servers for which you demand individual scheduling and custom configurations of the inventory agent; whereas you might prefer the simplified management of FlexNet Manager Suite 2015 R2 SP3 for things like management or desktop and mobile devices. The current migration process makes it practical to isolate parts of your present infrastructure for upgrade, and protect other parts to continue with the old system. Nothing in the process sets a time limit on this kind of parallel operation. Of course, if you plan to extend this parallel operation, you should consider the impact on other corporate processes, such as acquisition of new

machines and how these should be targeted for adoption by one system or the other. In the meantime, if considering parallel operation, you should also continue with both steps 10 and 11 for the appropriate parts of your environment that are to be migrated to 2015 R2 SP3.

10. Migration can be controlled at the level of subnets

This choice is about how much individual control you want over the migration of your computing estate (or parts of it, if you are mixing the approaches) from the old system to the new system. The simple path is to have control at the level of each subnet. Particularly if you have first tested the migration in a test environment, migrating a subnet at a time may represent a good balance of control with resourcing and time. If subnet granularity is not sufficient for your needs, you can have control that extends down to the level of each individual device if necessary. The following table clarifies the differences between these two levels of control.

Functionality/tasks	Control migration by subnet	Control migration by device
Server deployment	Deploy aninventory beacon into each subnet as you target that subnet. (Because you process a subnet at a time, a server previously used as a distribution server in the old system can be re-purposed as an inventory beacon in the next subnet. The total number of servers required is the number of subnets + 1.)	Deploy inventory beacons in a parallel hierarchy so that managed devices can operate through the 9.2 distribution server hierarchy today and gradually switch over to the new 2015 R2 SP3 inventory beacons as they are updated. In general, this approach requires as many new inventory beacons as you have old deployment servers. (It is not possible to co-install the FlexNet Beacon software on a server running the deployment server code.)
Migration mode setting	Not required; but may be used as a "starter's gun" to commence migration. Must be clear (not checked) for this migration method to proceed. At any time that migration mode is set, devices connecting to 2015 R2 SP3 inventory beacons successfully report inventory results through those inventory beacons into the new FlexNet Manager Suite database; but they do so using their settings current at the moment that migration mode was disabled (in other words, if they switch over while migration mode is disabled, they use settings obtained from the 9.2 system). Only after the migration mode is turned off do they receive an updated policy which aligns them with the settings in the 2015 R2 SP3 version of FlexNet Manager Suite (the policy updates	Must be selected (checked). In migration mode, devices must be: • Already upgraded to the 2015 R2 SP3 client • Identified in a target used to control migration. Those managed devices that do not meet these requirements receive a 404 "Not found" error when they access a DL on a new inventory beacon, and fail over to an existing distribution server. Once the migration is sufficiently advanced, you may have sufficient confidence to allow "all the rest" to migrate at once, At this point, you may turn off migration mode. When this is off, all devices that access the DL on an inventory beacon receive their new

Functionality/tasks	Control migration by subnet	Control migration by device
	generally occur within about 15 minutes of migration mode being turned off).	policy and switch over (irrevocably) to the new system.
Updating managed device (agent) version	Choose whether to: • Update managed devices before they migrate (permitted, but not required) • Allow the 2015 R2 SP3 system to automatically update clients to the level you specify as part of their automated migration.	You *must* upgrade all targeted managed devices (using your 9.2 technology) *before* they can be migrated to the new system. If any of these managed devices previously used client-side policy merging, they must be switched to server-side policy management before the upgrade.
Preparing the managed devices	No preparation of the 9.2 devices required.	In addition to the update of the agent software on all migrating managed devices, you must decide how these device are encouraged to try getting policy from the DL on an inventory beacon: • If you do nothing, the final built-in step in the netselector algorithm (a randomization across the DLs available to this device, for load sharing) causes (on average) an equal share of managed devices to attempt the connection to the DL on the inventory beacon at each policy request. (For example, if you have a distribution server and an inventory beacon accessible in a subnet, on average 50% of devices access each of the two servers at each policy request.) By design, of course, this randomization is not deterministic, and is generally not adequate to ensure that every last device migrates in a reasonable time frame. • Using the 9.2 system before devices switch over, you can deploy a device settings package that adds the `MgsInventoryBeaconMatch` netselector algorithm to the updated devices. This addition ensures that all devices prioritize the new

Functionality/tasks	Control migration by subnet	Control migration by device
		inventory beacons above all old distribution servers, ensuring that *every* managed device attempts to connect to the DL on a new inventory beacon. (The response each gets is still determined by the setting of migration mode and the targeting for migration.)
Preparing the 9.2 distribution system	No preparation of the 9.2 system required.	For each distribution server in your 9.2 hierarchy: • Declare an additional download location (DL) in the MMS 9.2 interface. • This new DL must use either the HTTP or HTTPS protocol (other protocols supported by 9.2 cannot be used in this case). • Configure the URL setting for this DL (even though it is being declared on a 9.2 distribution server) so that it points to the download location on the parallel inventory beacon that managed devices are able to access after they migrate. This download location acts as a "double agent" or "mole": it is specified in 9.2 so that the clients reporting to 9.2 may find it; but when contacted for policy updates, it admits only updated and targeted devices to the 2015 R2 SP3 system (all others fail over to existing distribution servers). Once provided with a 2015 R2 SP3 policy, devices cannot switch back to the 9.2 system.
Trigger migration	Within each subnet, start migration simply by changing the DNS alias that currently points to the local distribution server to point instead to the local inventory beacon. (If you were not previously using a DNS alias to point to the distribution server, create one now. It's best practice.) All managed devices	When migration mode is on, and managed devices have been updated, declare a target in the web interface for FlexNet Manager Suite 2015 R2 SP3 that includes those devices you want to switch over. At the next policy update cycle, targeted devices get their policy update and commence reporting to the

Functionality/tasks	Control migration by subnet	Control migration by device
	that access the new DL on the inventory beacon are updated with their 2015 R2 SP3 policy (subject to migration mode being off, as described above).	new system. You can then repeat the process of declaring a new target for the next set of devices, and waiting for these devices to update their policies.
Roll back	If roll back is required for any reason in any subnet, simply switch the DNS alias back to the 9.2 distribution server. All devices revert to the old server, and receive a policy 'update' that reverts them to their previous settings.	Not available.

For those areas where you will control migration by subnet, read on in step 12. For areas where you choose to control migration down to the level of individual devices, read on at step 11.

11. Upgrade agents on managed devices to 2015 R2 SP3

Use your existing 9.2 Inventory Manager system to upgrade managed devices to the inventory agents supplied with FlexNet Manager Suite 2015 R2 SP3. A package is provided to assist with this.

- If you are eventually migrating your entire estate away from Inventory Manager 9.2, you can upgrade managed devices indiscriminately if you wish, since the new inventory agent is backward compatible with the 9.2 Inventory Manager system, and continues to operate through the 9.2 distribution server hierarchy for the time being.

- If you want parts of your estate (perhaps server rooms) to continue indefinitely under your 9.2 infrastructure, methods are provided where you can exclude target machines from this upgrade. For example, you can use an existing security group that identifies these machines (or create a `Legacy` security group) as an 'exclusion' from the upgrade process.

The upgrade package also updates the managed devices to use the `MgsInventoryBeaconMatch` netselector algorithm to recognize and prioritize the inventory beacon(s) deployed with FlexNet Manager Suite 2015 R2 SP3, alongside their existing fail-over list of the old distribution server hierarchy. In migration mode, the inventory beacons do nothing for unknown devices, and so each manage device calls the inventory beacon, gets nothing, and fails over to its preferred 9.2 distribution server and continues normal operation in your existing infrastructure — until notified otherwise!

Important • *Managed devices upgraded to the 2015 R2 SP3 inventory agent must first be switched into server-side policy merging.*

Details: see *Prepare Managed Device Self-Upgrade Package* on page 41 and *Distribute Self-Upgrade and Settings Packages* on page 45. Now, for these devices, skip to step 13.

12. Switch each required distribution server to an inventory beacon

Include this step only if, at step 10, you chose to migrate (parts of) your computing estate with control at subnet granularity.

The 'subnet switch-over' approach relies on you exchanging the distribution server within the subnet for an inventory beacon. (If the subnet contains multiple distribution servers, switch all at the same time to prevent managed device toggling back and forth as they randomly access different servers.) The server types must be switched because all your 9.2 managed devices have a local record of the distribution server(s) they can access. If your migration process 'drops' a distribution server instead of replacing it with an inventory beacon, all managed devices that can access only that distribution server are thereby orphaned. You can only recover those orphans by visiting each one and manually upgrading and redirecting them. You avoid any nasty surprises simply by doing an *in place* switch of each distribution server to an inventory beacon. There are two ways you can achieve this:

- (Strongly recommended.) Use a DNS alias to redirect all requests for the distribution server to the inventory beacon. Inventory and other uploads instantly switch to the new system. Provided that migration mode is off, the next cycle of policy updates see all agents updated with their new policies (including all rules relevant to their assigned subnets and the like). For as long as you maintain the original distribution server in place, you have an easy roll-back option available if required: simply redirect the DNS alias back to the distribution server.

- You can do an in-place replacement of the distribution server software with the FlexNet Beacon software (these two cannot be installed on the same server at the same time). As part of this exchange, you preserve the same IP address and DNS entry. However, this approach does not provide an easy roll-back option (to roll back, you would need to uninstall the new software and re-install the old).

Once the inventory beacon is in place (and migration mode is off), as each managed device calls for its latest policy, it is automatically updated to the latest approved managed device software, and given the policy needed for the new FlexNet Manager Suite 2015 R2 SP3 system. After a decent interval to ensure that all managed devices (even the notebooks carried by road warriors) have been updated, you arrive at step 16.

13. Target managed devices for staged migration to the new system

You already have [at least some of] your inventory beacons rolled out, and the [selected] managed devices are ready to connect with those inventory beacons. Now, in your web interface for FlexNet Manager Suite 2015 R2 SP3, you create a rule for a small target group of devices to manage through those inventory beacons. This group can be as small as one in the first instance, until you satisfy yourself that everything works as expected. For details about targeting from the Inventory Manager side, see *Targeting the Inventory Agent Upgrades and Migration* on page 46.

Each upgraded managed device, when it next 'phones home', tries to connect to an inventory beacon as top priority. As already noted, in migration mode the inventory beacon rejects any devices that are not specified in its target, and those rejected devices fail over to the existing hierarchy of distribution servers, and continue operations under 9.2 as always. When the pilot device(s) contact the inventory beacon, they are automatically issued a new policy that switches them out of the distribution server hierarchy, and into the inventory beacon hierarchy. From the next scheduled inventory collection, these devices start reporting their inventory directly to FlexNet Manager Suite 2015 R2 SP3. For details of targeting from the FlexNet Manager Suite side, see *Create a Roll-out Target* on page 88.

At this early stage, be very detailed in assessing the behavior of the pilot managed device(s). It is still possible to roll back to the 9.2 system, but this becomes more time-consuming as more devices migrate. As a protection against accidental regression, the system does not normally allow a device reporting through FlexNet Manager

Suite 2015 R2 SP3 to switch back to Inventory Manager, and over-riding these safeguards required direct intervention.

14. Loop until done

You can continue to target pilot devices at any level you choose so that groups of managed devices are switched progressively into the new system. If you were conservative about your rule targeting, you can continue to expand the targeting until it includes all desired managed devices. When you are satisfied with progress, you can switch to operations mode, so that *any* managed device attempting to contact the inventory beacon is now switched over. (Note that the devices in the Legacy security group never come knocking on an inventory beacon, but continue operating as part of your Inventory Manager infrastructure, unaffected by the changes.) There is a single check box that switches from migration mode into operations mode, which automatically welcomes all remaining visiting devices into management by FlexNet Manager Suite 2015 R2 SP3.

15. Decommission or re-purpose redundant Inventory Manager servers

When you are satisfied that all the managed devices previously reporting to a given distribution server have begun reporting into FlexNet Manager Suite 2015 R2 SP3, you can decommission that distribution server (by uninstalling the DS software). If desirable, you might re-purpose this server hardware to become your next inventory beacon, rolling it into the migration process back at step 8. Eventually, if you are not preserving any Inventory Manager 9.2 functionality, even your central inventory server may be re-purposed.

16. Done!

Your new FlexNet Manager Suite 2015 R2 SP3 system is fully operational, with (optionally) some parallel use of Inventory Manager 9.2.3 for specialized management of inventory agents with specialized schedules or custom configurations. A final topic highlights a few manual clean-up actions (see *Finishing Off* on page 94).

Design the Final Topography

Whereas in release 9.2 or earlier, Inventory Manager and FlexNet Manager Platform (or earlier compliance product) might be installed on a single server (and so thought of as 'combined'), it is important now that you approach migration thinking of *completely separate products*. In particular, it is vital to mentally separate two ways of handling inventory:

• FlexNet Manager Suite 2015 R2 SP3 has its own direct inventory-gathering capacity (and may require a separate "inventory server" to handle this); but as outlined in *Process Overview* on page 6, this is completely independent of the 9.2 Inventory Manager product.

• You may also wish to continue operation of the 9.2 Inventory Manager solution (always referred to a Inventory Manager in this document) as a separate inventory source for import into FlexNet Manager Suite 2015 R2 SP3. If you do this, Inventory Manager is "just another inventory source" along with Microsoft SCCM and any other inventory sources you may use.

At this stage of the design, the focus is entirely on the implementation of FlexNet Manager Suite 2015 R2 SP3, independent of Inventory Manager. So proceed now to design your FlexNet Manager Suite 2015 R2 SP3 implementation.

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

Note • Both the inventory server (processing server, or application server in a single-server implementation) and the inventory beacon(s) are expected to be members of Active Directory domains. (For test environments, consultants may see article 000017145 How to run FlexNet Manager Suite processing server on a workgroup computer.) 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 • When you are migrating from 9.2 or earlier, it is mandatory to install an inventory beacon on the batch server (defined shortly). This inventory beacon (alone of all beacons) has access to the database, where migrated connections are stored.

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

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

Tip • Currently MSMQ limits the hostname of the batch server to 14 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. (This server may be shared between FlexNet Manager Suite and FlexNet Manager for Engineering Applications.)

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

Tip • If you previously had separate servers for FlexNet Manager Platform and Inventory Manager, you can start with your FlexNet Manager Platform 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.
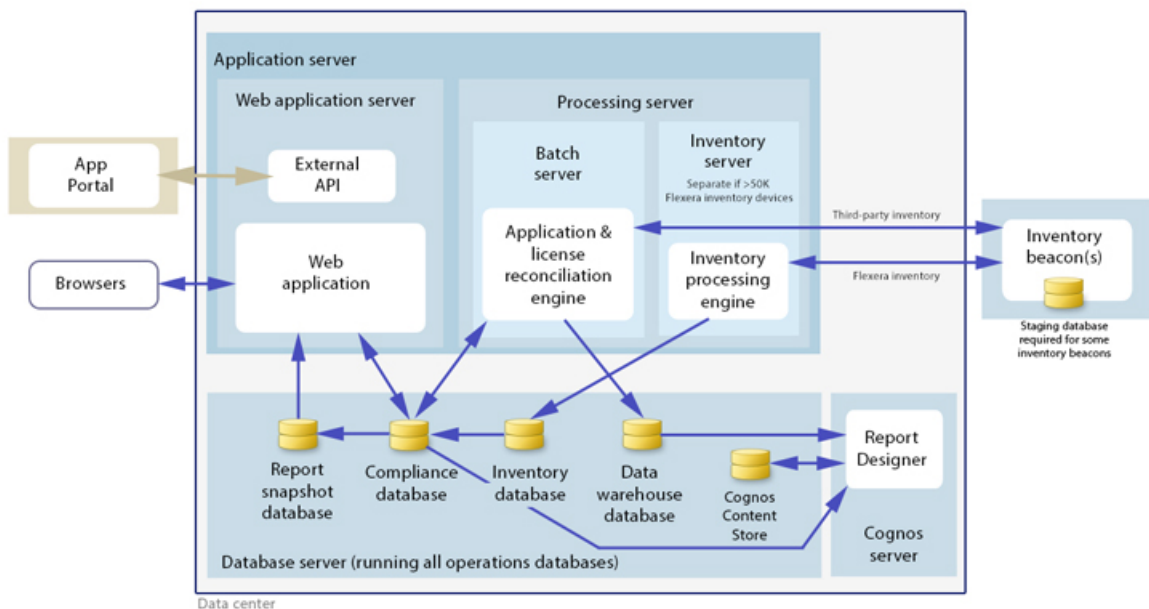
Tip •   When you implement your web application server as a separate server, you must configure one or two network shares that all servers can access to share uploaded data between them. The shared drives are identified during the installation process. For details, see Configure Network Shares for Multi-Server on page 31.

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.

Your previous combined server

If your previous implementation had FlexNet Manager Platform and Inventory Manager co-installed on the same server, you should plan for this server to roll forward as your Inventory Manager 9.2.3 implementation. This path minimizes disruption. Even when you are planning eventually to decommission Inventory Manager and rely entirely on the functionality in FlexNet Manager Suite 2015 R2 SP3, plan for this server to continue operations through the transition period.

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 Page > Configuring Direct Inventory Gathering.

Output

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

Don't forget the inventory beacons you intend to deploy. You should include an inventory beacon on your batch server (or processing server, or application server, depending on your scaling decisions), as this is a requirement to carry forward management of connection strings that were set up previously on your old Inventory Manager system. Thereafter you may choose to deploy a hierarchy of inventory beacons (perhaps mirroring your hierarchy of distribution servers used in your old system), ensuring that every targeted device will have access (preferably high-speed LAN access) to an inventory beacon. One or more of these inventory beacons may be used for 'bootstrapping' your managed devices that attempt to switch over to the new system.

Label each block in your diagram with:

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

- The actual server name and IP address

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

- For inventory beacons, whether they will be used for bootstrapping.

Tip • The DNS name and IP address of the inventory beacons used for bootstrapping must be known in advance of the inventory beacons themselves being deployed in the processes that follow.

Add to this diagram the additional server(s) being rolled forward for Inventory Manager 9.2.3 (either in the transition period, or longer term).

Additional details will be added later.

Prerequisites and Preparations

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

Locate License Details

A license file for your existing product(s) was sent to you with your original order confirmation. (While you are under a maintenance agreement, this same license entitles you to this system upgrade.) You will require your license file when you start from a single server combining Inventory Manager with FlexNet Manager Platform (or its predecessor Compliance Manager), and migrating to a multi-server implementation.

Important • *If you are updating from Inventory Manager 9.0 or earlier to Inventory Manager 9.2.3 as part of this overall upgrade process, you must obtain a new license file, as the format of the licence file changed between these releases. You will also require a new license file if you are purchasing additional options, such as FlexNet Manager for VMware.*

In all other cases, locate your license file(s), originally despatched with your order confirmation.

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

Microsoft Message Queuing (MSMQ)

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 14-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 enabled, the PowerShell configuration script (described later) will attempt to enable the Windows feature. This requires that the installing user (see section on accounts, below) has sufficient permissions to allow this if required. It also requires that the Windows CAB files are still available to the server.

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

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

💡

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

Privileges	Required on	Purpose
Database administration privileges — suggested AD account: `db-admin` (Typically this is an existing database administrator within your enterprise.)		
Database administrator, with db_owner rights on all databases related to FlexNet Manager Suite.	Database servers	Provides the following accounts with database access rights as described.

Privileges	Required on	Purpose
Member of the **public** database role in the `model` database on the database server.	Database servers	Required so that the account can run scripts that check the database compatibility level.
SELECT rights to the `dbo.sysjobs` and `dbo.sysjobsteps` tables in the **msdb** database.	Database servers	Only required if an existing installation of FlexNet Manager Suite 2015 or earlier is being migrated to a later release.
Installing administrator privileges — suggested AD account: `fnms-admin` (Account details must be made available to `db-admin`.)		
Local administrator	• Central application server(s) (including, where separated, web application server, batch server, any separate batch servers, and inventory server); • All inventory beacons.	Installs and configures software on all servers. On inventory beacons, interactive login to the inventory beacon interface also requires local administrator privileges (that is, on inventory beacons this is an operational account as well as being required for setup).
Set the execution policy for, and execute, PowerShell scripts	Central application server(s) (including, where separated, web application server, batch server, any separate batch servers, 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, any separate batch servers, and inventory server); • All inventory beacons.	Runs PowerShell scripts during installation that create scheduled tasks.
Internet connection to `https://flexerasoftware.flexnetoperations.com`	A central server (with network access to all other central application servers in a multi-server implementation).	Retrieve product downloads and licenses for implementation.
Internet connection to `http://www.managesoft.com` (Typically granted through membership in the `FNMS Administrators` security group in Active Directory.)	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.

Privileges	Required on	Purpose
Service account privileges — suggested AD account: `svc-flexnet` (Account details must be made available to `db-admin`.)		
Logon as a Service, and run all FlexNet services 💡 *Tip • Admin access for this account is convenient, and typically granted through membership in the `FNMS Administrators` security group in Active Directory; otherwise read, write, and execute permissions are required on all folders containing FlexNet installations, FlexNet data, and FlexNet log files.*	• Central application server(s) (including, where separated, web application server, batch server, any separate batch servers, and inventory server); • All inventory beacons.	Runs all system operations, including batch services and web services. 🔲 *Important • In a multi-server implementation, the same service account must be used on all central servers, and it must be a Windows domain account. This is required for proper functioning of Microsoft Message Queueing between the servers. (A distinct service account may be used for inventory beacons.)*
Logon as a Batch Job	• Central application server(s) (including, where separated, web application server, batch server, any separate batch servers, and inventory server); • All inventory beacons.	When the service account runs a batch job, this setting means the login is not an interactive user. 💡 *Tip • This is particularly important on the batch server (for authorization details, see Authorize the Service Account on page 61).*
Run scheduled tasks as a service account.	• Central application server(s) (including, where separated, web application server, batch server, any separate batch servers, and inventory server); • All inventory beacons.	Runs scheduled tasks within normal operations.
Run IIS application pools as a service account	• Central application server(s) (including, where separated, web application server, batch server, any separate batch servers, and inventory server);	Normal operations

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

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

Note • At implementation time, all services are configured with the correct password using the PowerShell scripts provided. If at any time the password on the service account is forced to change, the services will cease to operate. To ensure service continuity, you may either (a) allow the service account password to never expire (as normal for Windows service accounts), where permitted by your corporate policies; or (b) review the accounts listed in Password Maintenance on page 98.

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

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

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

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

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

- *Any operational account needing to log in to a central inventory beacon installed on your batch 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 previous implementation receives inputs from operators and through scheduled tasks, all these should be blocked before you migrate.

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.

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

3. 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. Shut down all related Windows Scheduled Tasks. For example:

   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 **ManageSoft** 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.

Check Database Collation Sequence

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

This means that they should be installed on one or more database instances that have this as the default collation sequence. If you are carrying forward the database instance that previously supported your 9.2 implementation,

this already complies with the appropriate collations sequence. For any new DB instance, use this process to check the collation sequence.

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

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

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

Important • *If you have not already backed up your database, do so now.*

Configure .NET and IIS

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

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

* web application server

* batch server

* inventory 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. Should you wish to upgrade PowerShell to release 4.0, Microsoft also requires Microsoft .NET Framework 4.5 on the same server. Take both these matters into account at the same time (see Upgrade PowerShell on Inventory Beacons on page 30 for more details).*

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

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

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

   a) Open Windows Programs and Features.

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

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

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

a) Open Windows Programs and Features.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

For Windows Server 2012, use:

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

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

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

If you are currently working on any of:

- Your web application server

- Your batch server

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

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

9. Open the IIS settings page. For example:

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

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

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

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

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

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

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

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

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

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

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

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

Upgrade PowerShell on Inventory Beacons

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

The minimum requirement on inventory beacons is PowerShell 3.0.

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

- .NET 4.0, with the *three* patches required for inventory beacons installed (as in *Configure .NET and IIS* on page 28), and PowerShell 3.0

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

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

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

   This produces output similar to the following:

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

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

   For example:

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

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

3. If this inventory beacon is running .NET version 4, ensure that these three patches are installed (you may have completed this earlier, under *Configure .NET and IIS* on page 28):

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

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

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

Configure Network Shares for Multi-Server

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

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

- The data import directory used for handing off any content imported through the web interface of FlexNet Manager Suite (such as one-off inventory spreadsheets) to the batch server for processing (default value: `%ProgramData%\Flexera Software\FlexNet Manager Platform\DataImport\`). It may be on any of your central servers, as convenient in your implementation; and it may be on any drive and any file path. You must configure the share manually in Microsoft Windows.

- The parallel data export folder used to stage data for integration with other systems like FlexNet Manager for Engineering Applications. This is typically located as a peer of the above (default value: `%ProgramData%\Flexera Software\FlexNet Manager Platform\DataExport\`).

You may implement these shares as you see fit.

For added security, you may set up these shares so that they are available to the minimum number of accounts (rather than open to all). From *Identify (or Set Up) Accounts*, you are already acquainted with the Active Directory security group `FNMS Administrators`, which minimally contains the operational service account (suggested: `svc-flexnet`), the installing administrator account (suggested: `fnms-admin`), and any accounts with interactive logins to any of your central servers. If you wish, you can restrict these network shares so that they are open only to members of `FNMS Administrators`, with the group providing full control for both daily operations and any required maintenance/troubleshooting.

Configure Internet Explorer

Microsoft Internet Explorer needs configuration.

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

1. Open Internet Explorer, and navigate to:

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

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

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

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

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

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

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

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

- URLs to add to your trusted locations

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

- Javascript must be enabled

- Cookies must be enabled

- Windows authentication must be enabled

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

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

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

Drivers for Spreadsheet Imports

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

You need a driver update if 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)

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

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

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

Download the Materials

Collect the contents for your upgrade process.

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

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

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

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

3. Click through the link for FlexNet Manager Suite 2015 R2 SP3 to access the downloads.

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

5. Download the release notes, and review the requirements for the Windows Server computer(s) on which you will install FlexNet Manager Suite 2015 R2 SP3.

💡

Tip • Use your block diagram of the servers to note requirements, and check these off when you validate that the machines are adequately provisioned. Resolve any issues with server provisioning before proceeding with the implementation.

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

- `FlexNet Manager Suite 2015 R2 SP3 Installer.zip`

- `Database Migration to FNMS 2015 R2 SP3.zip`

- `Inventory Agent 92 Upgrades to 2015 R2 SP3.zip`

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

- Tier 1 Adapter Tools.zip.

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

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

💡

Tip • There are additional downloads required if you are also upgrading your Inventory Manager installation. These are covered in Identify and Update Inventory Manager Server on page 36.

2

Preparing Inventory Manager

Topics:

- *Identify and Update Inventory Manager Server*
- *Prepare Managed Device Self-Upgrade Package*
- *Distribute Self-Upgrade and Settings Packages*
- *Targeting the Inventory Agent Upgrades and Migration*
- *Splitting a Shared Database*

If you do not have any installation of Inventory Manager as part of your current implementation (see the first topic following for ways of checking), you may skip ahead to the following chapter, *Upgrading FlexNet Manager Suite* on page 51.

Otherwise, your Inventory Manager system (including the inventory agents installed on managed devices throughout your enterprise) can be prepared for the migration even before FlexNet Manager Suite 2015 R2 SP3 is installed. Work through the following topics.

Identify and Update Inventory Manager Server

This process corresponds to steps 2 through 5 in the overall flowchart in *Process Overview* on page 6. Complete all the following on the central server(s) of your current implementation.

1. If you have not already done so, back up your server(s) now.

2. If you have been using FlexNet Report Designer (powered by Cognos) and intend to continue using it with FlexNet Manager Suite 2015 R2 SP3:

    a) On your application server (where Inventory Manager runs), open `regedit`.

    b) Navigate to `HKLM\SOFTWARE\ManageSoft Corp\Compliance\CurrentVersion\BIDispatchUrl`.

    c) Take a note of the URL recorded there. You will use it when importing the updated reports package.

    d) Close `regedit`.

3. Open your existing compliance product in the MMC console.

4. Look for the following nodes in the left-hand console tree:

    • **Managed Device Settings**

    • **Discovery and Adoption**

    • **Remote Task Manager**.

    If any of these nodes is present, Inventory Manager is co-installed on the same server as your compliance product. This server will roll forward as your Inventory Manager (only) server, at least for the time being. Check that your server plan includes a new server (or set of servers) for FlexNet Manager Suite 2015 R2 SP3. Also make a note that you must clean your previous compliance product off this server, as described in the process below. This co-location also means that your two products were using a shared database. Make a note that you need the process for splitting this database, described in *Splitting a Shared Database* on page 49. For now, skip to step 6.

5. If you have been managing inventory from computers collected through FlexNet inventory agents, there is an installation of Inventory Manager on another server. Identify that server (if need be, asking operators how they have been accessing the inventory). To determine whether your two separately-installed products were accessing a shared database:

    a) Start the registry browser on each of these two servers (compliance and inventory).

    b) Browse to the following registry keys:

    • For 64-bit operating systems: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ManageSoft Corp\ManageSoft\Reporter\CurrentVersion\DatabaseConnectionString`

    • For 32-bit operating systems: `HKEY_LOCAL_MACHINE\SOFTWARE\ManageSoft Corp\ManageSoft \Reporter\CurrentVersion\DatabaseConnectionString`

    c) Compare the values of the `Database` and `Server` settings.
    If these two values each match across both servers, your two products were using a shared database. Make a note that you need the process for splitting this database, described in *Splitting a Shared Database* on page 49.

6. On the server with Inventory Manager installed, in the MMC interface for the product (or combined products), open the **Help** menu, and select **Help about Inventory Manager**.
If the release shown is 9.2.3, you are done with this procedure. Skip forward to *Prepare Managed Device Self-Upgrade Package* on page 41.

If the release is shown as 9.2, Flexera Software recommends that you upgrade to release 9.2.3. This upgrade delivers enhancements consistent with the FlexNet Manager Suite 2015 R2 SP3 upgrade, which will be helpful while these products co-exist (full details are available in the release notes for 9.2.3). Should you choose to do without those enhancements, technically the 9.2 release is sufficient to move forward with the upgrade of FlexNet Manager Suite.

If the release is prior to (less than) 9.2, you should upgrade the Inventory Manager 9.2.3 as the foundation for moving forward with the joint systems.

7. Using your login credentials for Flexera Software Product and Licensing Center, navigate to the product download page for FlexNet Manager Platform 9.2.3: *https://flexerasoftware.flexnetoperations.com/control/inst/download?element=5631471*.

   a) Log in to *https://flexerasoftware.flexnetoperations.com*.

   b) Click `FlexNet Manager Platform`.

   c) Click `FlexNet Manager Platform` again on the next page.

   d) In the `9.2.3` row, click `FlexNet Manager Platform` again.

8. Download at least the following:

   • Release notes (`FlexNet Manager Platform Release Notes.pdf`)

   • For database migration: Database Migration Scripts 9.2.3 (`Database Migration.zip`)

   • For updates to the Inventory Manager software: Flexera Inventory Manager 9.2.3 Installer (`im923.exe`)

9. If you have not already done so, log on to the Inventory Manager server with a privileged account that:

   • Is a member of the domain where Inventory Manager and your database server are installed

   • Has Administrator privileges on your Inventory Manager server

   • Has Database Owner privileges.

10. Ensure that there is sufficient disk space on your database server to accommodate a complete copy of your existing database.

   ⓘ

   Important • This is the space required for the database upgrade process. If you plan to use the same database server for two products rolling forward, be aware that, in addition to separating the Inventory Manager and FlexNet Manager Suite databases, the latter product also requires two or three additional databases:

   • *Its own inventory database, suggested name* `FNMSInventory`

   • `FNMSSnapshot`*, used for performance improvement particularly relating to reports*

   • `FNMSDataWarehouse` *(this may have been present in the 9.2 implementation, where it was an option; but in 2015 R2 SP3 it is a requirement).*

11. If you have not already done so, back up your database (see your SQL Server documentation for procedures).

12. Ensure that all operators are logged out of Inventory Manager and your compliance product (such as FlexNet Manager Platform).

13. Unzip the `Database Migration.zip` archive to a convenient working location on the Inventory Manager server (such as `C:\temp\IMUpdate`).

14. Open a Command Prompt window, and navigate to your working copy of the migration folder (such as `C:\Temp\IMUpdate\Database Migration\Inventory Manager`).

15. Run the `mgsDatabaseUpdate.exe` program, using the following syntax:

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

where:

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

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

```
mgsDatabaseUpdate.exe -i InventoryManager.xml -nsu -l mig.log
```

Check messages on the command line to confirm that the database migration was successful. If any error messages occur, check the log file to troubleshoot the problem. Do not proceed to the next step until the database migration is successful.

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

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

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

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

If you decide to re-index at this time:

a) Start SQL Server Management Studio.

b) Open `ReIndexAll.sql` (**File** > **Open...** and browse to `Database Migration\Inventory Manager` in the unzipped archive, and select the file).

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

> *Tip • Reindexing is especially important if you have a lot of records in the `Installation` and `InstallationHistory` tables.*

17. Still logged in on the inventory server, ensure that:

- All processes have completed—open the Windows Task Manager to check. If `ndrplag.exe` is still processing tasks, allow it to finish.

- The system is in a stable state (one that will not be modified by processing imports or the like).

- The administration console (MMC interface) is closed.

18. If this is a co-located installation of Inventory Manager and your compliance product on the same server, keep the former, and remove the latter as follows:

> *Tip • It is a requirement that you remove the co-located compliance product before updating Inventory Manager.*

a) On the application server, open **Program and Features** (**Control Panel** > **Uninstall a Program**).

b) Uninstall FlexNet Manager Platform (or your earlier compliance product, such as Compliance Manager), and then close **Program and Features**.

c) Use Windows Task Scheduler to remove the scheduled task called `Execute business importer connections`.

19. Navigate to where you downloaded the Flexera Inventory Manager 9.2.3 Installer (`im923.exe`), and double-click the executable.
A setup page for Flexera Inventory Manager appears.

20. In the menu bar, click **Install**.
The **Install** menu is displayed.

21. Under the **Inventory Server** heading, select **Install**.
The installation wizard is invoked, and checks your system for prerequisites, as well as for content that must *not* be present. Depending on the results of these tests, you may be asked to perform various functions before you can progress with the installation. When the checks are satisfactorily completed, the wizard displays its welcome page.

22. Step through the installation wizard.

Tip • *If you prefer step-by-step guidance through the wizard, open UpgradeGuide.pdf from the documentation folder of your existing Inventory Manager installation, and in chapter 3, Upgrading administration servers, find the process To upgrade an administration server. Detailed documentation of the wizard starts from step 4 of this process.*

23. When installation wizard is complete, enable the following scheduled tasks (steps described below):

- `Generate ManageSoft system status information`

- `Generate ManageSoft Wake on LAN jobs`

- `Import ManageSoft application usage logs`

- `Import ManageSoft discovery information`

- `Import ManageSoft distribution logs`

- `Import ManageSoft installation logs`

- `Import ManageSoft inventories`

- `Import ManageSoft remote task status information`

- `Import ManageSoft system status information`

- `Merge ManageSoft policies`

- `Process ManageSoft remote execution actions`.

Three other Inventory Manager schedules are created:

- `Process ManageSoft distribution jobs` —This task is always 'Running' and does not need to be enabled.

- `Reconcile ManageSoft directory tables with AD` —This task is disabled by default. If you do want to enable this task, ensure that its timing will not clash with the Merge ManageSoft policies task as it also performs reconciliation.

- `Service the ManageSoft database` —This task is disabled by default, but can be manually enabled or run if and as appropriate for your environment.

To enable the scheduled tasks in the list above:

a) Navigate to **Scheduled Tasks** (for example, **Start** > **Settings** > **Control Panel**).

b) For each of the scheduled tasks listed above, right-click the task and select **Properties**.

c) Select the **Enabled (scheduled task runs at specified time)** check box.

d) Click **OK**, and repeat for the remaining scheduled tasks in the list.

24. Decide when to upgrade some of your distribution servers, and which ones to target for removal:

- There is no urgency: the upgraded central Inventory Manager server is backward-compatible with earlier distribution servers.

- Some of your distribution servers may shortly face decommissioning, or re-purposing as inventory beacons. There is no value in upgrading these.

- For the time being, use the distribution server hierarchy recorded in Inventory Manager to identify all distribution servers and their specific purposes (such as "desktop inventory", "machine room inventory", "Oracle introspection", and the like). From the list, identify the ones that can be targeted for removal as their managed devices are switched over to FlexNet Manager Suite 2015 R2 SP3.

- When you decide to migrate any distribution servers, use the previous *UpgradeGuide.pdf*, chapter 4, *Upgrading distribution servers*, to guide you.

Prepare Managed Device Self-Upgrade Package

You have identified the managed devices in your estate that are to migrate to exclusive management using FlexNet Manager Suite 2015 R2 SP3.

Important • Managed devices migrating to 2015 R2 SP3 must be covered by server-side policy merging. Any managed devices for which client-side policy merging remains important must not be migrated, and must continue under Inventory Manager 9.2. The switch to server-side policy merging is incorporated in the self-upgrade package provided.

You have further identified how to target these devices, whether by operating system, security group, or other techniques. You also have ready your block diagram of all servers, including inventory beacons and which of these will be used for bootstrapping managed devices into the new system (see *Design the Final Topography*

on page 17). And you have completed the upgrade of your central Inventory Manager Server to 9.2 SP3 (or thereabouts).

Warning • You must NOT upgrade the managed devices until after your central server has been upgraded.

Now prepare the self-upgrade package for the target managed devices.

Tip • This procedure covers Windows-based managed devices. For non-Windows managed devices, see your previous UpgradeGuide.pdf from the documentation folder of your existing Inventory Manager installation, and refer to chapter 5.

This procedure corresponds to step 11 in the flow-chart in *Process Overview* on page 6.

1. In your 9.2 implementation of Inventory Manager:

   a) Expand **Managed Device Settings**, and choose a managed device configuration.

      You may have only the **Managed Device Default Configuration**, in which case open that. But if you have another settings package that you normally issue as standard to the majority of your managed devices, open that settings package instead.

   b) In the groups list, scroll down to (and select) the `NetSelector Agent`.

   c) In the **Settings in package** list, record the current value of the `Selector algorithm`.
      You will use the values as input to your new system, later in the process.

2. Copy `Inventory Agent 92 Upgrades to 2015 R2 SP3.zip` to this server, and unzip to a convenient location (such as `C:\Temp`).

   You downloaded this archive in the process under *Download the Materials* on page 33.

3. If your migration of Inventory Manager has not taken you all the way to 9.2 SP3, locate the files `linuxdpkg` and `linuxrpm` from the unzipped archive, and copy them to *warehouse-folder*`\Repository` `\Environments` (the default value for *warehouse-folder* is `C:\ManageSoft`).

4. Open a Command Prompt and navigate to *install-dir*`\Common`.

   Replace *install-dir* with the installation directory for Inventory Manager 9.2 SP3.

5. Execute the following command:

   ```
   mgsreceive.exe -N extracted-archive-folder\Flexera -d Flexera -o pack=FALSE
   ```

   where *extracted-archive-folder* is the folder (such as `C:\Temp`) where you unzipped the upgrade packages. This loads the upgrade and settings packages into your 9.2 software library, visible in the MMC.

6. Open your upgraded Inventory Manager.

   We must customize the settings package before distribution and targeting.

7. Under the **Flexera Software** node, expand the **Software Library** node, and continue expanding it (**Flexera** > **FNMS 2015 R2 SP3 Migration Settings** > **1.0.0** > **Rev 1.0**) until the **FNMS 2015 R2 SP3 Migration Settings** project is visible. Right-click the package and select **Edit...**.

8. In the navigation bar, expand **Registry Entries** > **All Registry Entries** > HKEY_LOCAL_MACHINE >
   SOFTWARE > ManageSoft Corp > ManageSoft > Common > DownloadSettings > InventoryBeacon
   node.

9. In the right-hand pane, double-click the **Host** entry.

   The **Host Properties** dialog appears.

10. In the **Value** field, enter the fully qualified domain name of an inventory beacon in your FlexNet Manager Suite
    2015 R2 SP3 system that will be used for bootstrapping managed devices across to the new system.

    You identified the inventory beacon(s) for bootstrapping as part of your design work in *Design the Final
    Topography* on page 17.

    *Note • If you are not using HTTP protocol on the standard port 80, you may also modify the following settings
    in your package:*

Location	Notes
Port	The default value for HTTP protocol is 80, and the default for HTTPS protocol is 443. If necessary, edit the port value to match the configuration of this inventory beacon.
Protocol	Either accept the default value of http, or you may edit it if you are using the HTTPS protocol on this inventory beacon. (The value is case insensitive.)

    If you wish, you may also identify multiple inventory beacons for bootstrapping managed devices into the
    upgraded system by defining additional DownloadSettings. For example, if your NetSelector algorithms
    include MgsSubnetMatch, you may wish to include an inventory beacon in each of your subnets for
    maximum network efficiency in inventory uploads from the managed devices. You can identify all such
    inventory beacons here: each managed device will choose the one within its own subnet (or the one that gets
    top priority according to your selected algorithms).

11. In the navigation bar, expand **Registry Entries** > **All Registry Entries** > HKEY_LOCAL_MACHINE >
    SOFTWARE > ManageSoft Corp > ManageSoft > NetSelector > CurrentVersion node.

12. In the right-hand pane, double-click the **SelectorAlgorithm** entry.

    The **Selector Algorithm Properties** dialog appears.

13. In the **Value** field, replace $(ExistingSelectorAlgorithm);MgsInventoryBeaconMatch with your
    current choices of net selector algorithms, with the new MgsInventoryBeaconMatch value appended on
    the end.

    Use the list of algorithms you noted down at the start of this process. On targeted managed devices, the
    settings package also modifies the PolicySource registry value to the value Server. Only server-side policy
    management is supported in 2015 R2 SP3.

14. Click **OK** on the properties dialog, and click **Save** on the project.

15. Optionally, customize setup.ini.

    Use this file to add transforms to the installation of the managed device, suppress installation of the
    application usage agent, or prevent users cancelling the upgrade process on their computer (managed
    device). For details, see *Configure setup.ini* on page 44.

Your self-upgrade package and settings package are now ready to distribute to your distribution servers. Even though FlexNet Manager Suite 2015 R2 SP3 is not yet in place, you may distribute the packages now, as we have a separate step to apply these packages; and even thereafter, the managed devices will update, and fail over to their current fail-over locations until they are targeted by an inventory beacon in the new system. Distributing (and optionally applying) the packages *now* gives time for the upgrade and settings to percolate through your managed devices while you are completing the next stages of the central upgrade. Or, if you prefer, distribute the packages later, if that better suits your processes. Whenever you are ready, you'll find details in *Distribute Self-Upgrade and Settings Packages* on page 45.

Configure setup.ini

This file modifies the installation of the managed device.

Use this optional procedure if you wish to:

- Control the level of end-user feedback and control for the managed device upgrade

- Add a transform to the MSI package

- Switch off the installation of the application usage agent.

Each of these options is independent.

Tip • *Be aware that there are two* `.ini` *files available. This is the one for the MSI, and is called just* `setup.ini` *(not* `mgssetup.ini`*).*

1. On your 9.2 Inventory Manager application server, in the flat text editor of your choice, open `C:\ManageSoft\Repository\Packages\Flexera\Upgrade for managed devices\10.2.0\Rev 1.0\Upgrade for managed devices\setup.ini`.

2. Within the `setup.ini` file, locate the section `[Startup]`.

3. To prevent users from manually cancelling the managed device upgrade, under that heading enter

   ```
   UserInteractionLevel=/q
   ```

   This quiet-mode setting suppressed the default user interface (which includes a **Cancel** button) during the upgrade.

4. To prevent installation of the application usage agent, in the same section of the file, locate `CmdLine` and append:

   ```
   REMOVE=aua
   ```

5. To attach your transform files to the MSI, to the same `CmdLine`, append a list of your transform files, separating multiples with semi-colons(`;`), as in the following example:

   ```
   Transforms=custom1.mst;custom2.mst
   ```

6. Save and close the file.

Your modified `setup.ini` is automatically included in the upgrade package to be distributed shortly.

Distribute Self-Upgrade and Settings Packages

You have prepared, validated and (preferably) tested your self-update and settings packages for managed devices that are to migrate out of Inventory Manager control and into management through FlexNet Manager Suite 2015 R2 SP3. You now wish to distribute these packages to distribution servers accessible to those selected devices. In fact, the first level of targeting that may be applicable in your enterprise is to restrict the packages to certain distribution servers. For example, suppose that one distribution server exclusively manages inventory from a machine room, and you wish to preserve this machine room under Inventory Manager control. You should exclude that distribution server from the list that receive the upgrade package.

Tip • *The upgrade package causes managed devices to self-update to 2015 R2 SP3 inventory clients. These clients are compatible with both the 2015 R2 SP3 system and the previous 9.2 Inventory Manager system. You may like to send this package to all your managed devices to get the latest client functionality. The switch from 9.2 to 2015 R2 SP3 is controlled exclusively by the settings package. Therefore, when targeting managed devices to migrate, include the settings package; and when deciding on managed devices that should remain in the 9.2 system, exclude the settings package from these devices.*

This procedure is part of step 11 in the flow-chart in *Process Overview* on page 6.

You can distribute the packages from the **Software Library** node of Inventory Manager. This will distribute the packages for all managed device platforms:

1. Right-click the **Software Library** node and select **Distribute...**.
   The **Package Distribution Wizard** page is displayed.

2. Click **Next**.
   The **Assign Packages** page is displayed.

3. Select (by checking the boxes) **Flexera\FNMS 2015 R2 SP3 Migration Settings** and **Flexera\Upgrade for managed device\1.0.0**, and click **Next**.
   The **Select Distribution Locations** page is displayed.

4. Select each of the servers to which you will distribute, and click **Add**.

5. If required, select the **Force distribution** option.

   It is not compulsory to force distribution. This is used to overwrite packages on distribution locations, even if they are not listed as needing the update. Use this option if you are not certain that your distribution database is an accurate reflection of the state of your distribution servers.

6. Click **Next**.
   The **Distribution Priority** page is displayed.

7. Select a priority for the package.

   `Normal` is the default setting).

8. Click **Next**.
   The **Selection Summary** window is displayed.

9. Click **Next**.

The **Completing the Package Distribution Wizard** page is displayed.

10. Click **Finish**.

The package(s) is/are now sent to the selected distribution servers.

11. After allowing adequate time for the distribution and reporting traffic, verify delivery by clicking on **Reports** > **Distribution** > **Packages** > **All**.

Targeting the Inventory Agent Upgrades and Migration

The update and settings packages are distributed. Now determine which devices should act on which of these packages.

This procedure corresponds with step 13 in *Process Overview* on page 6.

You are already familiar with targeting upgrades in your previous implementation, and with the options for policy-level filtering or package-level filtering available in Inventory Manager 9.2. If your goal is that selected managed devices will migrate to FlexNet Manager Suite 2015 R2 SP3, and that another group of managed devices do not migrate but continue (at least for the time being) under Inventory Manager 9.2, it is mandatory that you target the settings package only to those devices that should migrate. (The inventory agent upgrade package is compatible with either system for both client-side policy merging and server-side policy merging, and may be sent to all inventory clients if you so wish.)

This targeting in Inventory Manager creates a pool of managed devices primed for migration (because they are both upgraded, *and* received the settings package). Later, on the FlexNet Manager Suite side, you can at first apply additional targeting to this group to allow only a test device, or a pilot group of devices, from the pool to migrate. But in due course, as you move out of the testing phase, that filtering is removed, and then every device in the migration pool will automatically switch over to FlexNet Manager Suite 2015 R2 SP3 and its hierarchy of inventory beacons. At that time, it is critical that the managed devices intended to continue under Inventory Manager 9.2 have *not* received the settings package, or they will be 'lost' by switching over to the new system.

You may have already applied a first line of control by excluding certain distribution servers from even hosting the settings package (see *Distribute Self-Upgrade and Settings Packages* on page 45).

Whether or not that is the case, you now need to exert further control, for which your options include policy-level filtering and package-level filtering. Your enterprise has most likely fixed on one or other of these approaches to use. Both are applied through the **Add to Policy** wizard in Inventory Manager. Below is a summary of the process, and more detail is available in your 9.2 documentation (including the `SoftwareDeploymentGuide.pdf` chapter 3, *Best practice* for a discussion of options, and chapter 5, *Deployment policies* for details of the wizard).

💡

Tip • If none of your existing Active Directory security groups allow for the appropriate targeting of this upgrade, consider creating purpose-specific security groups before starting this wizard. Two sample groups are discussed in the procedure below: read ahead for details.

📋

Note • If you are not using Active Directory and instead use ManageSoft policy, adapt the principles below for your corporate practices. For example, you can first assign the upgrade package to your pilot policy, and after verification, assign the same package to your production policy. Then, if you have some managed devices that you want to switch to the new system, target those devices for the client settings package. Remember that only those devices that are both upgraded to the 2015 R2 SP3 inventory client and have the updated client settings package can switch to the new system.

You may choose to do package targeting now, or later. If you do it now, the updated managed devices check for an inventory beacon, and for as long as they do not succeed, fail over to their existing hierarchy of distribution servers. If you do it later, you introduce a further delay while you wait for the update package and settings package to be applied. Doing it now allows plenty of time for the managed devices to self-update and collect the new settings package while you work on other things. The device upgrade package and the settings package must be targeted separately.

1. In Inventory Manager 9.2.x, navigate through the Software Library to select the upgrade package you have prepared and distributed.

2. Either right-click the package in the console tree and select **Add to Policy**, or in the right-hand page click the **Add this package to policy** action button.
   The **Add to Policy Wizard** is displayed.

3. Click **Next**.
   For the path described here, the **Select Deployment Policy** page is displayed. By choosing the appropriate policy, you are using policy-level filtering. You need to be aware of where in the Active Directory hierarchy this policy is attached, as it will be applied to all managed devices in this group and all its descendents. At this stage, keep in mind that the inventory agent upgrade is applicable to all managed devices, if you so choose.

4. Expand the relevant domain and browse to the policy to which you want to assign your upgrade package. With the policy selected, click **Next**.
   The **Create or Choose Group** page is displayed.

5. Select one of the following radio buttons:

   • **Create a new, empty filter group**

     Accept the default name proposed, or type a unique name that better reflects the group's purpose (such as `ManagedDeviceUpgrade`). This is often a good option for providing highly customized targeting for your upgrade package.

     Note • After completing this wizard, you must add members to this new security group, either in the Group Policy Object Editor, or using the Package Allocation wizard. Save effort at this stage by including in this security group only those devices that you wish to upgrade to the latest inventory client, but to continue under management with Inventory Manager 9.2. (We use a different security group for devices that are migrating to the new system, next time through the wizard, as noted below.)

   • **Select an existing filter group, applying the package to all group members**

     Use the **Browse for Filter Group** page to select the relevant container or security group, and select its check box before clicking **OK**. Keep in mind that this adds your upgrade package to whatever other packages and policy the members of this group receive.

- **Apply this package without filtering to all members of the selected policy**

  This allows pure policy-level filtering (by your choice of policy in the previous page), with no package-level filtering applied.

6. Click **Next**.
   The **Package Applicability** page is displayed.

7. Ensure that the default **All users on targeted computers (computer policy)** is selected, and click **Next**.

   Note • Only computer policy is supported going forward. If you need any user policies, these policies and their users and machines must be preserved for operation in Inventory Manager 9.2.

   The **Deployment Conditions** page is displayed.

8. Accept the default (**This application must be installed. (Mandatory)**) and leave both **Removal** options unchecked. Click **Next**.
   The **Postponement Options** page is displayed.

9. Set the options to suit your corporate practices for allowing users to delay the update package, and click **Next**.

   Since this update package only changes the behavior of the inventory agent and does not involve rebooting the device, it may be quite acceptable to leave all options deselected so that the end-user may not delay your migration process.

   The **Package Lifetime Options** page is displayed.

10. Accept the default **As soon as policy becomes effective**, and click **Next**.
    The **Summary** page is displayed.

11. Review the details, and if everything is as intended, click **Next**.
    The wizard creates a policy and (if required) security group as specified. This may take a few moments. Then the **Completing the Add to Policy Wizard** page appears.

    ---

    *Tip • If you created a new security group, there is a check box **Begin allocating this software package to end-users or computers** displayed on the page. Leave this checked to start the **Package Allocation** wizard and target the individual machines you want in the group. (For details about the **Package Allocation** wizard, see the section To allocation a package to users or computers in chapter 5, Deployment policies, of the `SoftwareDeploymentGuide.pdf`.)*

12. Click **Finish** to complete this wizard.

13. Repeat from step 1 for the settings package, being careful to target this package exclusively to those managed devices which you intend to migrate to the new system. Use a separate security group as noted here:

    Note • The second time through the wizard, create a second security group such as `MigrateTo2014R3`.

- *Later, in group policy, insert as members of this group all the managed devices that you want to migrate to the new system. This means that they receive the settings package.*

- *Also in group policy, make the group* `MigrateTo2014R3` *also a member of the earlier group* `ManagedDeviceUpgrade`. *This means that the migrate targets also receive the device upgrade package.*

14. To monitor progress on self-updating of the managed devices:

   a) Select the **Reporting** node.

   b) In the right-hand details panel, locate the **Package Installation** table.

   c) Locate the **Managed Devices** group, and select the link for **All**.
   All information on distributed packages is displayed.

   d) Locate the required package in the list, and click the graph icon to its left. Use the dynamically-updated graph to track the distribution and installation of the self-update package.

Once the next policy merge is run, the updated policy is applied to the target groups. Managed devices in those groups will self-update, and wait for an inventory beacon to be available to them.

Splitting a Shared Database

The migration process requires separate databases because of schema incompatibility from Inventory Manager to FlexNet Manager Suite 2015 R2 SP3.

In *Identify and Update Inventory Manager Server* on page 36, you clarified whether you previous implementations of Inventory Manager and your compliance product shared a common database. If that was NOT the case, so that they already had separate databases, skip this topic.

The previous, shared database will roll forward as your Inventory Manager database (at least for the time being). In this process you will split off a copy to convert into the FlexNet Manager Suite 2015 R2 SP3 database, and clean up both databases following the separation.

As already noted, your new database can share the same server, subject to software version and adequate disk space (and remembering the additional databases required for the new release). In *Design the Final Topography* on page 17, you identified (and recorded) your database server for FlexNet Manager Suite 2015 R2 SP3.

This procedure corresponds to step 5 in *Process Overview* on page 6.

1. Backup the existing shared database (its default name was `ManageSoft`).

   For details about backing up, see *http://msdn.microsoft.com/en-us/library/ms187510(v=sql.100).aspx*. (This is in addition to the protective backup at the start of the entire process. This time you are backing up the updated database.)

2. Did your previous implementation include the data warehouse database (then used for reports prepared in FlexNet Report Designer)? If so:

   a) Also back up this database (its default name was `FNMPDataWarehouse`).

   b) Copy this database to the SQL Server database identified for the data warehouse database in your server plan.

   Upgrade of this relocated database follows in *Upgrade/Create Databases* on page 52.

3. Use the previously-shared (`ManageSoft`) backup file you just created, and restore it on the SQL Server database identified for FlexNet Manager Suite 2015 R2 SP3 in your server plan. The default database name (used in this document) is `FNMSCompliance`.

For details about restoring, see *http://msdn.microsoft.com/en-us/library/ms177429(v=sql.100).aspx*. You will resume working on this database in *Upgrade/Create Databases* on page 52.

4. Using SQL Management Studio:

a) Connect to the SQL database server where your current Inventory Manager database is located (the default name was `ManageSoft`), and select that database.

b) Choose **File** > **Open**, navigate in the database migration folder in your downloaded archive (such as `C:\Temp\FNMSUpdate\Database Migration\FlexNet Manager Platform\Normal`), and open `IM92SchemaCleanup.sql`.

c) Execute this SQL script on the `ManageSoft` database (or equivalent if you renamed this).
This script removes tables, views, and functions that are related only to FlexNet Manager Suite, and not needed for the continued operation of Inventory Manager.

You have now separated your previously combined databases, such that the previous one (default name ManageSoft) carries forward for Inventory Manager data only, and the new copy (default name `FNMSCompliance`) is used for FlexNet Manager Suite 2015 R2 SP3.

If, as well as the shared database, your previous implementation also had your compliance product (Compliance Manager or FlexNet Manager Platform) and Inventory Manager installed on the same server, you also need to remove the compliance product from this server, allowing it to roll forward as your Inventory Manager server.

3

Upgrading FlexNet Manager Suite

Topics:

You have completed all the prerequisites in *Prerequisites and Preparations* on page 21 (and its subsections). Depending on your starting conditions, you have also separated any previously combined databases and cleaned up any co-installation of FlexNet Manager Platform (or Compliance Manager) from what is now your Inventory Manager server. Only when all these tasks are complete should you move forward to the upgrade of FlexNet Manager Suite to 2015 R2 SP3.

Upgrade/Create Databases

Any existing compliance databases must be upgraded, and 2015 R2 SP3 uses additional mandatory databases.

Tip • Previously you have been working on Inventory Manager preparations. Now clear your mind of anything to do with Inventory Manager. Keep in mind that FlexNet Manager Suite 2015 R2 SP3 also separately manages its own inventory information in its own inventory database. In this procedure, we are concerned solely with the databases for FlexNet Manager Suite 2015 R2 SP3, including its own inventory database. (Later, we will configure Inventory Manager to be a data source feeding into the FlexNet Manager Suite inventory database.) For the moment, then, nothing to do with Inventory Manager.

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

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

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

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

- *Any operational account needing to log in to a central inventory beacon installed on your batch 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.*

Tip • Because you are migrating content from a previous 9.2 implementation (or earlier), it is mandatory that you install an inventory beacon on the batch server component of your FlexNet Manager Suite central servers. As mentioned above, the account that will access that central batch server also needs to be included in this security group. For more about inventory beacons, see Deploy Inventory Beacons on page 86.

This procedure assumes that you are updating a previous database from 9.2. This may either be one that was always separate, or one that you split in the procedure *Splitting a Shared Database* on page 49.

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

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

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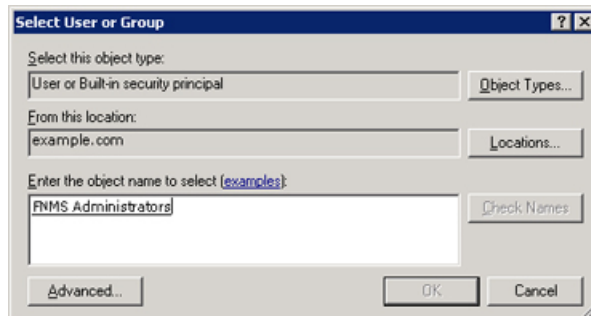
b) Use the **Object Types...** button to ensure that `User, Group, or Built-in security principal` is selected as the object type.

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

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

e) Click **OK**.
The newly added group is visible under the `Security > Logins` node. (You will use this group after the creation of each database.)
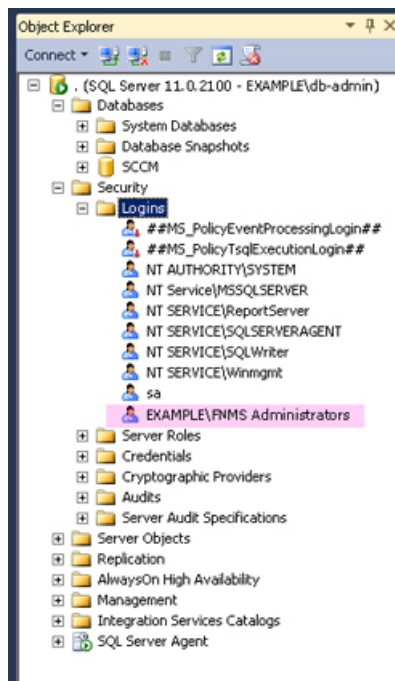
3. Back up any customized files to a temporary location, (for example, `C:\temp`).

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

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

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

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

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

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

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

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

b) Select the **Options** tab.

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

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

6. Ensure that you have sufficient disk space on the database server for a complete second copy of your database during migration.

Tip • *When considering disk space, keep in mind that FlexNet Manager Suite 2015 R2 SP3 requires the following mandatory databases, at least two of which are new since your 9.2 implementation:*

• *Its own inventory database, suggested name* `FNMSInventory`

• `FNMSSnapshot`*, used for performance improvement particularly relating to reports*

• `FNMSDataWarehouse` *(this may have been present in the 9.2 implementation, where it was an option; but in 2015 R2 SP3 it is a requirement).*

If space seems tight, before starting migration you can use Microsoft SQL Server Management Studio to allow for additional data files on a different drive (for details, see `https://msdn.microsoft.com/en-`

`us/library/ms189253.aspx`). If this is done and the primary drive runs out of space during the upgrade, Microsoft SQL Server automatically uses space on the second drive to complete the process.

7. If you have not already done so, log on to the central application server with a privileged account (suggestion: `db-admin`) that has the privileges described in *Identify (or Set Up) Accounts* on page 23.

8. If you cannot access your downloaded and unzipped archives from your current login on this application server, copy `Database Migration to FNMS 2015 R2 SP3.zip` to this server and unzip it to a convenient location, such as `C:\temp\FNMSUpgrade`.

9. Create the database for FlexNet native inventory collection.

☞

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

💡

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

🔳

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

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

💡

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

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

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

📋

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

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

Wait for completion before proceeding.

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

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

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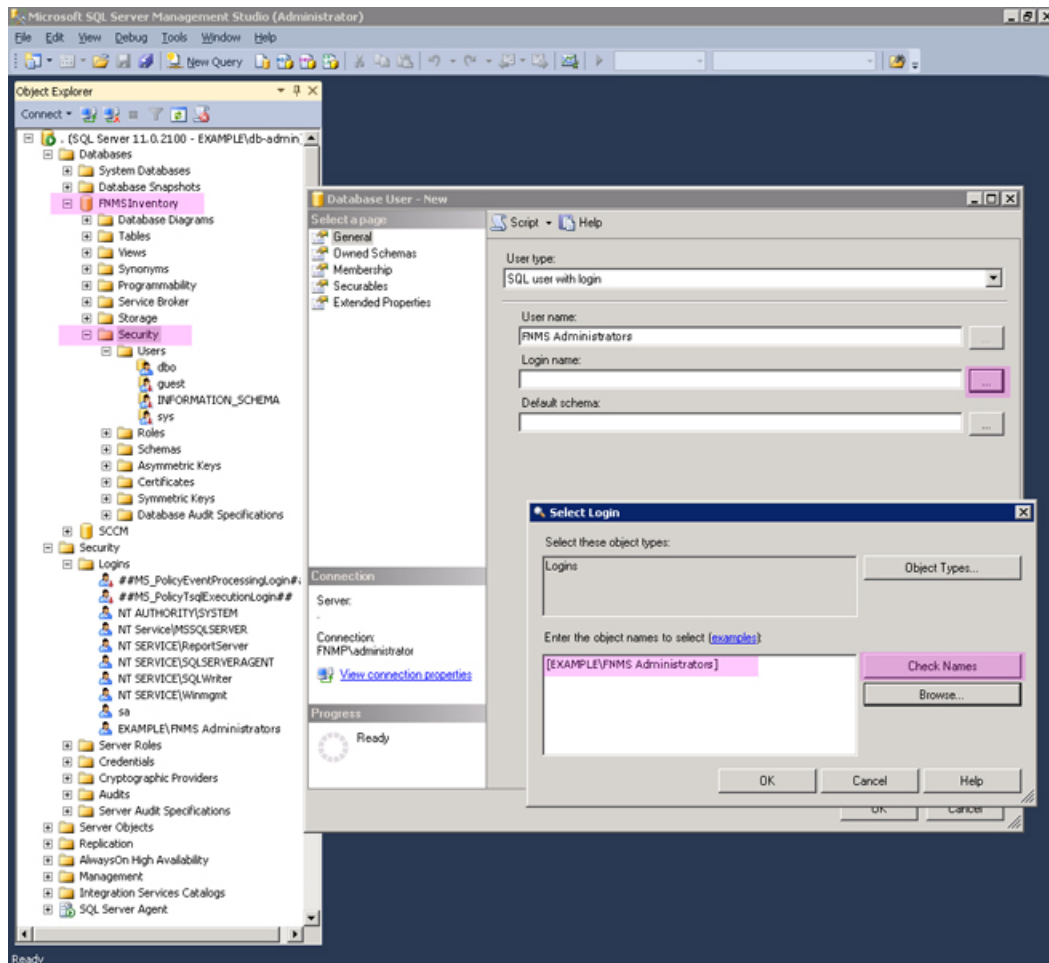
g) For your newly-added user, right-click and select the properties, and select the `Membership` page. Check the `db_owner` role, and click **OK** .

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

11. Run the `mgsDatabaseUpdate.exe` program, using the following syntax:

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

where:

`-d <databaseName>`	The name of the database to connect to. A suggested name is `FNMSCompliance`. *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 ComplianceMigration.xml`	This is the configuration file describing the migration tasks, and is of course mandatory.
`-l <logFile>`	Identifies the path and name of the file to receive a log of the migration tasks that occurred. If this option is not specified, a log file called `ComplianceMigration.log` is created in the same folder where the executable is running.
`-nsu`	Run the database update without putting the database into single user mode. (The steps to perform migration require that multiple connections are made.)
`-p <password>`	The password for the username specified with `-u`. This is only required if the database server is configured to use SQL Server authentication.

`-s <serverName>`
 or
 `-s <serverName>\<instanceName>`
	The name of the database server to connect to. If `-s` is not specified, the value at `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ManageSoft Corp\ManageSoft \Reporter\CurrentVersion\DatabaseConnectionString` is used. The registry key is present on the compliance and inventory servers. (If you have chosen to run this script on the database server itself, the registry entry is not available, and you must therefore specify the server name, or use the dot notation [.] to refer to the current server.)
	
	 If the database is in a named instance (and not in the default database on the server), the instance name must be specified as well.

`-u <userName>`	The username with which to connect to the database. This is only required if the database server is configured to use SQL Server

	authentication. If not specified, Windows Integrated Authentication is used to connect to the database server using the current user's credentials.

🔆

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

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

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

Check messages on the command line to confirm that the database migration was successful. If any error messages occur, check the log file to troubleshoot the problem. Do not proceed to the next step until the database migration is successful. For more information about database validation and remedies, see *Database Validation* on page 60.

🔆

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

12. If you are processing a copy of a previously-shared database that you split, open this database in Microsoft SQL Server Management Studio, and complete the following:

   a) Grant `db_owner` privileges to the security group (suggested: `FNMS Administrators`).

   b) Choose **File** > **Open**, navigate in the database migration folder in your downloaded archive (such as `C:\Temp\FNMSUpdate\Database Migration\FlexNet Manager Platform\Normal`), and open `FNMP92SchemaCleanup.sql`.

   c) Execute this SQL script on the `FNMSCompliance` database.
   This script removes tables, views, and functions that are related only to Inventory Manager, and not needed for the upgrade of this database to FlexNet Manager Suite 2015 R2 SP3.

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

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

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

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

   🔆

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

If you decide to re-index at this time:

a) Start SQL Server Management Studio.

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

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

14. 🗒

Note • Up until (and including) release 9.2 of FlexNet Manager Platform, it was an option to have the data warehouse database for trend-based reporting (reports built in FlexNet Report Designer, powered by Cognos). While Cognos remains optional, the data warehouse database is now mandatory, and is used by new reporting functionality within FlexNet Manager Suite 2015 R2 SP3.

Do one of the following:

• If your prior implementation included the data warehouse database (you copied it to the planned SQL Server in *Splitting a Shared Database* on page 49), migrate it now on its new SQL Server instance (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 migration was successful. If any error messages occur, check the log file to troubleshoot the problem. Do not proceed to the next step until the migration is successful. For more information about database validation and remedies, see *Database Validation* on page 60.

• If your prior implementation did *not* include the data warehouse database, it is now mandatory, whether or not you are using Cognos at this time. In the same archive folder, execute:

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

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

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

a) In the same archive folder, execute:

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

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

For more information about database validation and remedies, see *Database Validation* on page 60.

Database Validation

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

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

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

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

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

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

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

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

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

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

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

• Missing tables, indexes, columns, or foreign keys

• Extra indexes, columns or foreign keys

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

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

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

Authorize the Service Account

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

- Your batch 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).

-

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.*

Install the Web Interface

The web interface provides the user interface to manage your inventory and license position. Continue this process as administrator (`fnms-admin`) on either your

- application server (for a single server installation) or

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

Note • Are you installing on the same server that was previously a separate administration server for FlexNet Manager Platform 9.2 (or an earlier compliance product), where Inventory Manager was not co-located on the same server? 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**.*

3. *Open Windows Task Scheduler and delete the scheduled task called* `Execute business importer connections`*.*

To install the web interface for FlexNet Manager Suite 2015 R2 SP3:

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

2. Copy the downloaded archive `FlexNet Manager Suite 2015 R2 SP3 Installer.zip` from your staging location to a convenient location on this server (such as `C:\temp`), and unzip it.

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

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

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

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

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

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

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

    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* on page 31.

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* on page 61).

8. When successful, close the installation wizard.

Install the Inventory Server

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

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

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

- processing server (in a two server application installation)

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

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

2. Copy the downloaded archive `FlexNet Manager Suite 2015 R2 SP3 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* on page 61).

7. When successful, close the installation wizard.

Install the Batch Server

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

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

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

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

In these two cases, this step is already completed and you should skip ahead to *Installing a Free-Standing Studio* on page 65.

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 14 characters (excluding the domain qualifier).

1. On the batch server, open Windows Explorer.

2. Copy the downloaded archive `FlexNet Manager Suite 2015 R2 SP3 Installer.zip` from your staging location to a convenient location on this server (such as `C:\temp`), and unzip it.

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

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

   🔅

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

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

   🔅

   *Tip • Do not also select the **Batch server** option. An installed batch scheduling server also includes the batch server functionality. (A separate, child batch server independent of the batch scheduling server is not currently supported.)*

   Take note of the installation location for future reference.

6. When asked to enter the credentials to be used for running batch processes, be sure that the account you enter already has `Logon as a service` permission (see *Authorize the Service Account* on page 61).

7. 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 on page 31.

8. When successful, close the installation wizard.

Installing a Free-Standing Studio

You can install additional copies of the Business Adapter Studio.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Configure the System

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

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

1. Your web application server

2. Your batch 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 themselves, you should first ensure that these scripts have sufficient authorization to execute, as described in this process.

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

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

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

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

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

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

   a) Open IIS Manager.

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

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

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

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

      For more information (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. In the PowerShell command window, execute:

   ```
   set-executionpolicy AllSigned
   ```

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

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

6. On each server, execute:

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

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

💡

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

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

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

💡

Tip • *Helpful notes:*

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

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

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

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

- *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.)*

- *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).

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

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

c) Close the dialog.

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

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

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

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

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

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

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

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

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

(Re-)Activate the Product

You need to reimport your license for FlexNet Manager Suite.

The migration process requires that the license is reimported on the batch server, or, in smaller implementations, the server hosting that functionality:

- The application server (in a single server implementation)

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

1. On the appropriate server, save a copy of your license in a convenient folder (such as your installation folder), where it is accessible for this activation process.

2. 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 license to use FlexNet Manager Suite.

Populate the Downloadable Libraries

FlexNet Manager Suite comes with an Application Recognition Library, a SKU (stock keeping unit) Library, and several Product Use Rights Libraries (the latter depending on which options you have purchased for the product). These are updated regularly by Flexera Software and normally downloaded automatically.

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

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

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

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

If neither direct access nor access through a proxy server can be provided, you can use an alternative process to managed library updates manually (see Manual Updates of Library Data on page 72).

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

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

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

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

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

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

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

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

    • **ARL**

    • **SKU Library**

    • **PURL**.

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

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

    • `ImportPURL-*.log`

    • `PURL-*-log.txt`

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

Manual Updates of Library Data

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

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

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

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

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

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

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

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

1. When the Application Recognition Library content is updated:

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

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

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

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

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

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

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

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

2. When SKU Library content is updated:

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

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

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

d) Install the SKU Library content using this command:

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

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

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

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

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

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

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

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

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

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

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

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

Import the Sample Reporting Package

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

First, be aware that much of what used to be published in the Report Designer environment in the 9.2 product is now moved into the web interface for FlexNet Manager Suite itself. Compare the functionality of the two releases:

Release 9.2	Release 2015 R2 SP3
A product dashboard was available within the Reports Designer.	The product dashboard is now one of the main management tools in the web interface.
A number of business reports were available in Report Designer.	Business reports are now centered in the reports area of the web interface (switch to reporting mode using the large button in the header bar).
Trend analysis reporting was provided only through Report Designer.	Trend analysis reporting is available directly through the web interface.
Reports provided through Report Designer were available through a web portal, providing click-through access.	There is no longer any direct link from the web interface of FlexNet Manager Suite to reports prepared in Report Designer. Users must be given a direct link to those reports, external to the product. 💡 *Tip • Custom reports in Report Designer can still retrieve data from the FlexNet Manager Suite database.*
Reports in Report Designer were central to the operation of the system.	Many reports are still provided in Report Designer, but these are intended as examples to help you build your own reports.

If you wish to continue with custom reporting through FlexNet Report Designer, use this process to update your reports package for the new release.

1. Locate the registry key value for the Dispatch URL for FlexNet Report Designer that you noted in *Identify and Update Inventory Manager Server* on page 36.

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

   💡

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

3. Copy your Report Designer Package - Single Tenant (`FlexNetManagerPlatformReportsAndDashboard.zip`) to this folder.

   You downloaded this package as you worked through *Download the Materials* on page 33.

⬛

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

4. You may log out of the Report Designer (Cognos) server now.

Shortly you will log into your batch server, but first there are permissions to set.

5. In the web interface for FlexNet Manager Suite 2015 R2 SP3, add your current account (suggested: `fnms-admin`) as a Web Administrator for the business reporting portal as follows:

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

b) Select the **Roles** tab, and check for the existence of the `Business Reporting Portal Admin` role.

If the role does not already exist, you can create it.

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

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

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

f) Under the **Permissions** section, check whether your `Business Reporting Portal Admin` role is already listed against the **Role**. If so, you are set for permissions, and should continue with the next step *6* on page 76.

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

💡

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

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

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

💡

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

6. Using the same account, 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.

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

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

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

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

10. Copy the Dispatch URL from your earlier note (see step *1* on page 75) into the **Value** field, and click **Update**.
The value entered is written into the registry on this server, and the additional dialog disappears.

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

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

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

The Reports Designer reports are now available as baselines for your own customization and extension as required. The reports can be accessed in a web browser at http://*Cognos-webserver*:*port*/cognos10/ cgi-bin/cognos.cgi? (A typical port number is 8889, but check the value in your implementation.)

Configure Web Browsers

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

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

1. In your preferred web browser, navigate to the URL ***server-name-or-IP-address*/Suite/Help/webhelp/ index.html**.

2. Expand the table of contents on the left by clicking the book icon to the left of the title.

3. Click **Configuring Your Web Browser**, and follow the guidelines in the column for your preferred web browser.

Link to Flexera Service Gateway

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   b) Run `RegisterFlexeraServiceGateway.exe`.

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

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

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

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

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

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

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

Update Access Rights

Through your processes of database migration, all the access rights that applied in your earlier compliance product are carried forward into FlexNet Manager Suite 2015 R2 SP3.

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

If you wish to modify access rights:

1. Log in to the web interface to FlexNet Manager Suite 2015 R2 SP3.

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 option 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.

Managing Device Migration by Subnet

Controlling migration at the level of subnets makes for a greatly simplified process.

Use this process if, in the *Process Overview* on page 6, you chose the simpler path of controlling migration at subnet granularity. (If, instead, you chose to control migration down to the level of individual computers, instead see the process in *Managing Device Migration by Individual Device* on page 83).

This process has the smallest overheads beyond the deployment, installation, and configuration of the inventory beacon for each subnet (these latter three being the tasks that are common to all approaches). The only additional step is switching over the DNS alias that is referenced by managed devices as the download location to use within this subnet.

1. If you choose to update your managed devices while they are still within the 9.2 infrastructure, start with that process.

   However, there is no *requirement* to do any device updates or other preparations within the 9.2 system. Updates of the managed devices to a distinct version can be specified for FlexNet Manager Suite 2015 R2 SP3. This controls the upgrade immediately after each managed device switches over to the new system. For full details, see *Configure Updates to Inventory Agents* on page 81. You may complete this configuration before migrating over your first subnet; or you may change the authorized version at a convenient future time.

2. In the first (or next) subnet that you wish to migrate, install the server that is to act as the inventory beacon for this subnet.

3. While logged in with administrator privileges to this future inventory beacon server, install FlexNet Beacon:

   a) Start a web browser, and access the URL ***server-name-or-IP-address*/Suite/** (replacing the placeholder with the URL to access your central application server).

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

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

   d) Click **Download beacon**.

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

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

   g) 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.

   Important • If this inventory beacon will import inventory collected by ILMT, or collect data from Oracle servers, follow the links provided in the wizard to ensure that the appropriate drivers are installed on the inventory beacon.

4. Ensure that this subnet is recorded within FlexNet Manager Suite. You may:

   • Import the sites and subnets (visible to this inventory beacon) from Active Directory (for details, open the online help in the web interface and navigate to **FlexNet Manager Suite Help** > **What Is an Inventory Beacon?** > **Importing from Active Directory**)

   • Manually edit the list of sites and subnets available in the web interface for FlexNet Manager Suite 2015 R2 SP3 at **Discovery & Inventory** > **Subnets** (in the **Network** group).

   Subnets must be recorded, and assigned to inventory beacons, before inventory beacons can target any devices for migration.

5. Ensure that the subnet is assigned to your newly-installed inventory beacon:

   a) In FlexNet Manager Suite, navigate to **Discovery & Inventory** >**Unassigned Subnets**.

   b) From the list, select the subnet you are migrating now.

(You can also select multiple subnets, if you are migrating several at once.)

c) Click **Assign to a beacon**.

A new list opens above that button, showing available inventory beacons for your selection. To help with logical groupings of subnets, each inventory beacon also displays subnets already assigned to it. The status of each inventory beacon is also displayed on the right of the list, so that you do not accidentally assign any subnets to a disabled inventory beacon.

d) Select one inventory beacon from the list, and click **Save**.
The list of inventory beacons closes, and the assigned subnet is removed from the list of unassigned subnets.

The inventory beacon is now prepared to respond to all managed devices within its subnet that ask it for a policy.

6. Identify the 9.2 distribution server that has been managing devices in this subnet, and identify the alias by which that distribution server is identified in the relevant domain name server (DNS).

7. At the DNS, redirect the alias to point instead to the newly-established inventory beacon.
On their regular schedule, all managed devices request a policy update from the same download location URL that they have always used. As this URL has now been redirected to the new inventory beacon, FlexNet Beacon (subject to migration mode being off) supplies each managed device with a revised policy that switches it over to operate with FlexNet Manager Suite 2015 R2 SP3. If the current version of the FlexNet inventory agent on each managed device is not as authorized (see *Configure Updates to Inventory Agents* on page 81), the inventory beacon also supplies the appropriate upgrade (or downgrade) package, and the FlexNet inventory agent self-updates to match requirements.

8. You may decommission the previous distribution server, and optionally repurpose it as an inventory beacon in another subnet.

Because this method redirects the established URL to the new inventory beacon, it doesn't matter whether managed devices have updated their policies before or after you remove the old distribution server.

Repeat this process for each subnet in turn, until all subnets (with their managed devices) have been migrated. Thereafter, skip forward to *Migrating Citrix Inventory Collection* on page 91 (if you have been using the relevant adapter), or to *Finishing Off* on page 94.

Configure Updates to Inventory Agents

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   Replace *versionString* with the same major-minor-update numbering as is displayed by the `list-agent-versions` action. This value must be an exact match for one of the available versions listed by `list-agent-versions`. If not, no action is taken. (Notice that there is no requirement for the new version to be greater

than versions previously installed: you can specify an earlier version from the available list, which causes any later FlexNet inventory agents to downgrade to the specified earlier version.)

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

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

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

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

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

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

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

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

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

Managing Device Migration by Individual Device

Before deploying inventory beacons, choose whether to use additional targeting of inventory devices as part of your migration strategy.

In the *Process Overview* on page 6, you examined whether to control [parts of] your migration at the granularity of a subnet, or at finer levels with control potentially extending down to an individual device.

By far the simpler process is to control migration for each subnet, so that the complete set of managed devices within an individual subnet switch over together to the new system. As you validate that all is well in this subnet, you can move on to the next subnet. For more information about this approach, see *Managing Device Migration by Subnet* on page 79.

The remainder of this topic introduces concepts important to exerting control down to the level of individual devices.

Production mode accepts all who ask

When FlexNet Manager Suite 2015 R2 SP3 is *in production* (that is, when migration mode is turned off), any inventory agent (installed on a device) that contacts an inventory beacon receives a response:

- If the device fits within any target specified in the web interface on the application server, it receives the options defined for that target group (specifically, whether devices within the target group should be 'adopted' by having an inventory agent installed, and whether application usage should be tracked on devices in the group).

- If the device is not covered by any target, it receives (in production mode) default options (those options are not to install the agent, and not to track application usage). However, in receiving these default options, the device also is notified of all known inventory beacons, and the common schedule for any future actions that may be applied to it in future. From that time on, the inventory agent on these devices reports through the inventory beacons to FlexNet Manager Suite 2015 R2 SP3, and has been migrated.

This last fact is critical for migration. Your existing estate includes many inventory agents that you have updated and are now looking for a response from an inventory beacon (and, until they receive one, failing over to the old hierarchy of distribution servers). In production mode, every one of those managed devices would switch over to the inventory beacon hierarchy in 2015 R2 SP3 as soon as it contacted its first inventory beacon. This may be the desired behavior at the *end* of a migration process, when you want to sweep up the last few remaining devices; but early in the process, you may wish to target a pilot group, which requires that we prevent the sociable behavior of giving every managed device the default response.

Migration mode rejects outsiders

To allow for controlled migration of inventory agents, there is a control in the beacon settings page of the web interfacethat switches FlexNet Manager Suite from production mode to *migration mode*. In migration mode, devices already identified in target groups within FlexNet Manager Suite still receive their options as always; but the difference is that those devices *not* included in any target group receive a "not found" 404 response to their request, and therefore fail over to their old hierarchy of distribution servers, staying within the 9.2 system.

Choose your timing

Therefore, your timing decision about switching over your managed devices is this:

- Since you have opted for a staged migration using test machines and pilot groups, exercising control through different sized targets (if required, down to individual machines), ensure that the **Migration mode: Restrict inventory settings to targeted devices** check box (**Discovery & Inventory** > **Settings**, in the **Beacon settings** group) remains set when you commence your migration.

- At what point are you satisfied that the process is reliable, so that you are happy for all remaining updated devices to switch to the new system? When that time comes, clear the **Migration mode: Restrict inventory settings to targeted devices** check box.

Accepting the default option (for migration mode) gives you another safety net of staging or targeting your switch over of managed devices from 9.2 to FlexNet Manager Suite 2015 R2 SP3:

1. You may, in Inventory Manager 9.2, have used selection of your old distribution servers to control which managed devices received the update package that allowed migration (see *Distribute Self-Upgrade and Settings Packages* on page 45).

2. Still in Inventory Manager, you may have used security policy targeting of the managed devices that were to receive the same update package.

3. Now, even though large numbers of your managed devices stand ready to make the switch, only those you specifically target in FlexNet Manager Suite 2015 R2 SP3 can do so.

Once you get past the pilot stage and are confident that migrated managed devices are functioning well in the new system, you simply clear the **Migration mode: Restrict inventory settings to targeted devices** check box. This switches your entire system (and all its inventory beacons) into production mode. At that point, any managed devices that were prepared with the upgrade package but have not yet been targeted can freely and automatically switch over to the new system.

More about targets

Notice that simply defining targets in FlexNet Manager Suite is the enabling step for the switch-over. If an upgraded managed device is identified in a target, it can switch. It does not require a specific rule (actions plus targets plus schedule) to be defined.

The definitions of targets are cumulative: that is, a device identified in *any* target group is able to make the switch. For this reason, these upgrade notes suggest starting with a single target in the new system so that it is simple to maintain control.

The use of targets is also independent of the roll-out of inventory beacons. That is, if you have no targets to begin with, you may roll out as many inventory beacons as you like, and they will continue to reject managed devices as long as the **Migration mode: Restrict inventory settings to targeted devices** check box remains set.

Set Defaults and Migration Mode

Prepare your inventory settings for deployment of inventory beacons.

These settings are applied to all FlexNet inventory agents reporting to FlexNet Manager Suite through the hierarchy of inventory beacons. You can fine tune your settings at any time; but right now, you can configure some settings useful for your migration process.

1. On a convenient computer, start a web browser and access the URL *server-name-or-IP-address*/**Suite**/.

   💡

   Tip • Consider doing this from your central batch server, and once you have completed these settings, you can continue there to install the local inventory beacon on the same server.

2. Navigate to **Discovery & Inventory** > **Settings**.
   The **Inventory Settings** page is displayed.

3. In the **File inventory** section, select **Do not collect file inventory**.

   During migration, you do not want your inventory agents undertaking time-consuming work before reporting to their new inventory beacons. You may change this setting later for operational purposes as required.

4. In the **Agent inventory schedule** section, use the controls available to set the schedule for all installed inventory agents to collect inventory from their managed devices.

You can mimic the same schedule that applied to the majority of your devices under the 9.2 system. Remember that this same schedule applies to all inventory agents reporting to FlexNet Manager Suite through inventory beacons.

5. In the **Beacon settings** group, keep the default values for **Interval for beacon updates** and **Beacon version approved for use**. These control the self-updating behavior of the inventory beacons (not the inventory agents that report to them), and you can adjust these later as required.

6. Still in the **Beacon settings** group, do one of the following based on your strategy for migrating managed devices:

   • (Recommended) To require specific targeting of managed devices within FlexNet Manager Suite 2015 R2 SP3 before those devices can automatically migrate, ensure that the **Migration mode: Restrict inventory settings to targeted devices** check box remains set (checked, or ticked).

   • To allow any managed device that contacts an inventory beacon to immediately switch over to FlexNet Manager Suite 2015 R2 SP3, clear the **Migration mode: Restrict inventory settings to targeted devices** check box.

7. In the bottom right of the page, click **Save**.
   Your inventory settings are ready for delivery to any managed device that is accepted by an inventory beacon.

Deploy Inventory Beacons

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

Ensure that you have reviewed your policy for migrating inventory agents before deploying any inventory beacons (see *Managing Device Migration by Individual Device* on page 83), and set migration mode accordingly (see *Set Defaults and Migration Mode* on page 85).

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

Note • Any computer on which you will install an inventory beacon must have at least version 3.0 of PowerShell installed. For more information, see Upgrade PowerShell on Inventory Beacons *on page 30.*

Important • When you are migrating from 9.2 or earlier, it is mandatory to install an inventory beacon on your central batch server (or, for combined servers in smaller implementations, your processing server, or your application server). This inventory beacon allows you control of content migrated forward from 9.2, whereas inventory beacons installed on separate servers cannot have similar privileges. This inventory beacon must be a top-level beacon reporting directly to the neighboring inventory server, and optionally it may also be the root of your inventory beacon hierarchy (or you may have many peer top-level beacons). Notice further that the user account that will access this inventory beacon, because it is directly accessing the batch server that had the central beacon installed, must be a member of the security group (suggested as FNMS Administrators*) that has database owner privileges (see* Upgrade/Create Databases *on page 52). Finally, notice that its default settings, requiring Basic Authentication for devices to access it, mean that it cannot be used for bootstrapping new FlexNet inventory agents on managed devices to the 2015 R2 SP3 system (because until they receive their first policy, newly installed*

FlexNet inventory agents do not know any passwords for Windows authentication on any inventory beacons that require it). You may either:

- *Switch this inventory beacon on the batch server to accept anonymous authentication*

- *Use other inventory beacons for bootstrapping new managed devices.*

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

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

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

4. Click **Download beacon**.

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

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

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

8. When the configuration of this inventory beacon is complete, log in to the next server where you would like to install the FlexNet Beacon software, and repeat this process for each beacon.

9. If your sites and subnets are not already recorded in your database, you should either import them from Active Directory, or enter them manually.

   Subnets are visible in the web interface for FlexNet Manager Suite 2015 R2 SP3 at **Discovery & Inventory > Subnets** (in the **Network** group). Subnets must be recorded, and assigned to inventory beacons, before inventory beacons can target any devices for migration. For guidance about importing or entering sites and subnets, open the online help in the web interface and navigate to **FlexNet Manager Suite Help** > **What Is an Inventory Beacon?** > **Importing from Active Directory**.

10. In FlexNet Manager Suite, navigate to **Discovery & Inventory** >**Unassigned Subnets**.

11. Select one or more of the subnets in the list.

    You may select subnets for either of two reasons:

    - To disable them so that no managed devices in those subnets can be targeted. To do this, click **Ignore**, and they disappear from the list. (Find them again later in the **All Sites** list.)

    - To assign them to inventory beacons so that managed devices in those subnets can be targeted for switching to the new system, and they can collect inventory directly into FlexNet Manager Suite. In this case, continue.

12. Click **Assign to a beacon**.

    A new list opens above that button, showing available inventory beacons for your selection. To help with logical groupings of subnets, each inventory beacon also displays subnets already assigned to it. The status of each inventory beacon is also displayed on the right of the list, so that you do not accidentally assign any subnets to a disabled inventory beacon.

13. Select one inventory beacon from the list, and click **Save**.
    The list of inventory beacons closes, and the assigned subnet is removed from the list of unassigned subnets.

You are now ready to target managed devices to switch over to the new system.

Create a Roll-out Target

Create a target group for piloting the switch-over of managed devices to the new system.

Refer back to your switch-over timing decision (see *Managing Device Migration by Individual Device* on page 83 and *Set Defaults and Migration Mode* on page 85):

- If you are currently targeting a pilot roll-out group, so that the **Migration mode: Restrict inventory settings to targeted devices** check box is set (checked, ticked), continue from step 1 of this procedure to identify the target machines to switch to the new system.

- If you are ready to sweep up remaining managed devices without further targeting, you can clear the **Migration mode: Restrict inventory settings to targeted devices** check box, and skip down to step 8. Your managed devices start switching over automatically shortly after that check box is cleared, and you can start reviewing results as they obtain their updated policy.

Tip • For targeted switch-overs, remember that only targets (not complete rules) need to be defined in FlexNet Manager Suite at this time, and that any device identified in any target that contacts an inventory beacon will immediately switch to operations in the new 2015 R2 SP3 system. For a staged roll-out, then, it is convenient to define only one target at first, so that you can assess the results before approving a wider group.

1. In the web interface, navigate to **Discovery & Inventory** > **Discovery and Inventory Rules**.
2. On the left, select the **Targets** tab.
3. On the right-hand side, click **Create a target**.
   The page is replaced by the **Create an Inventory Target** page.
4. Give this target group a helpful **Name** (suggestion: `Device Migration`) and in the **Description** field, record any notes helpful to other operators, or to yourself after the purpose of this group is forgotten over time.
5. In **Define machines to target**, leave the first choice as `Include`, and from the `Select target...` option list, choose a targeting method.
   Additional controls appear allowing you to provide details appropriate to your chosen method. For example, the first time you might choose `All machines with a name like...` and then identify the machine name of your first test computer. Later, when the initial test is successful, you can change this target to define a whole subnet.

   Tip • Using the + control at the end of your first definition, you can add additional lines to your definition of this target. For example, you might have your first line target a subnet, and subsequent lines `Exclude` specific servers by name within that subnet.

   The other options on this page are not relevant to the purpose of switching over managed devices that are already deployed (in this case, through Inventory Manager 9.2).
6. Click **Create** (in the bottom right of the page).
   Your new target is updated to your inventory beacons (by default, every 15 minutes or so).
7. If you have not already targeted your update packages to managed devices through Inventory Manager 9.2 (see *Targeting the Inventory Agent Upgrades and Migration* on page 46), do so now!

Three factors are now aligned:

- Inventory beacons are in place

- Targets in FlexNet Manager Suite identify your pilot machines for switching to the new system

- Existing managed devices (from 9.2) are upgraded with instructions to look for inventory beacons.

Now, the upgraded managed devices attempt to connect to an inventory beacon. Until the inventory beacon is ready, they receive a 404 not found error, and revert to using the 9.2 hierarchy of distribution servers (operating as normal in the old system). When the inventory beacon is ready but the individual managed device is not listed in any target, that managed device also receives a 404 error and fails over. Only managed devices matching the filters you established for this target group, contacting any inventory beacon, collect your inventory settings (see *Set Defaults and Migration Mode* on page 85) and switch permanently to reporting through inventory beacons to FlexNet Manager Suite 2015 R2 SP3.

8. To prevent inventory imported through FlexNet Manager Suite 2015 R2 SP3 being hidden by old inventory still being imported from Inventory Manager 9.2, ensure that Inventory Manager is not the primary inventory source:

   a) In the System menu (gear-wheel icon in the top right corner), choose **Data Inputs**.

   b) Select the **Inventory Data** tab.
   The list of inventory connections is displayed. Most of these are imported from your previous 9.2 implementation. Only one of them is `Primary`, with all the others showing a **Make primary** button.

   c) If the connection to Inventory Manager 9.2 (default name: `ManageSoft — Flexera`) is currently the primary connection, click the **Make primary** button for the `FlexNet Manager Suite — Flexera` connection.
   New inventory imported through the inventory beacons into 2015 R2 SP3 will now be displayed in inventory results.

9. Wait.

   Time passes while

   - The inventory beacons collect your changed target specification

   - Managed devices try to access the inventory beacons, and the pilot group members are now accepted, receiving their new inventory settings

   - On the schedule you configured, inventory agents collect inventory from their local machines, and upload the results to an inventory beacon

   - The inventory beacon, within ten minutes, uploads the results to a web handler on your inventory server, which stores the results into the inventory database

   - The inventory import and reconciliation that happens by default at 2am daily collects from the inventory database and imports into the compliance database as required for license calculations.

   Some of these processes can be manually triggered; otherwise come back tomorrow, or worst case the next day.

10. In the web interface, review the inventory results collected from your test device(s) (for example, **Discovery & Inventory** > **All Inventory** [in the **Inventory** group]).

When satisfied, repeat this process to redefine the target group to include a new or wider range of devices, and continue until satisfied that everything is working as expected. As machines successfully switch over to the new system, you may also choose to move them out of the `Device Migration` target and into a production target.

Tip • Moving devices is preferable to simply removing them from a target, since removal means that when the managed device next accesses the inventory beacon to check its settings, it receives a 404 not found response (it continues to report its inventory on the previously received settings). Once a successful device is moved to a production target, you are 'finished' with the device, no longer needing to remember to come back and tidy up later.

Note • If you are not satisfied with your test cases, you may revert these devices to use the old system. In Inventory Manager 9.2, use remote execution on those devices to do a policy 'update' back to your last applicable policy for 9.2. You do not need to roll back the FlexNet inventory agent as well, as the 2015 R2 SP3 FlexNet inventory agent is backward compatible with your 9.2 system. Switching between the old and new systems is controlled by the policy applied to the managed device.

11. When you are satisfied with test results and no longer need fine-grained control, navigate to **Discovery & Inventory** > **Settings** page, and clear the **Migration mode: Restrict inventory settings to targeted devices** check box.

    Restricted targeting of managed devices in FlexNet Manager Suite is now turned off. All managed devices that received the upgrade package quickly switch over to the new inventory beacon hierarchy, and receive at least a default policy. You may remove the migration target from your list of targets. It is best practice to ensure that all devices are covered by production target groups, so that you can control the settings they receive.

    ---

    *Tip • FlexNet Manager Suite 2015 R2 SP3 records a list of inventory connections under the system menu (⚙ ▼ in the top right corner of the web interface), **Data Inputs**, on the **Inventory Data** tab. If you inspect this now, you see the inventory connection to your old Inventory Manager in the list. You cannot modify the connection details within the web interface. In the new system, connection details must be edited on the responsible inventory beacon (shown in brackets on the list). In the case of the 9.2 Inventory Manager connection, the responsible beacon is the one installed on your central batch server.*

12. Return to Inventory Manager 9.2, and monitor the declining traffic as managed devices switch over to the new system. When you think a distribution server might be finished with (because all its managed devices have switched over), visit the distribution server and disable uploads. Then in Inventory Manager, monitor the **Distribution Status** (click the **All** link), and the count of **Logs** (and **Delayed Logs**) should remain at zero. If not, it means that managed devices are still uploading content to this distribution server — you can inspect the log on the distribution server to identify the managed device that has not switched over (validate against your plan whether this managed device is intended to migrate or to stay with Inventory Manager 9.2). Once the count of logs stabilizes at 0, you can decommission the distribution server, potentially re-purposing the machine as an inventory beacon somewhere in your new system.

Migrating Citrix Inventory Collection

If your previous implementation collected inventory from XenApp or XenDesktop, it's likely that rework is required.

If your previous 9.2 implementation was collecting inventory from Citrix XenApp and XenDesktop, the inventory rules are not carried forward in your new FlexNet Manager Suite 2015 R2 SP3 implementation. Citrix has largely reimplemented these products from version 7, and your new implementation supports version 7.5 (along with versions 6.0 and 6.5). To extend this support, a redesign of the adapters to import XenApp and XenDesktop inventory has been necessary.

If you are preserving Inventory Manager 9.2 as an inventory source, any existing inventory import from XenApp or XenDesktop to that system continues to operate. If you wish, you can use your adapter connecting with Inventory Manager to import the results of those inventory collections to FlexNet Manager Suite 2015 R2 SP3.

However, if you wish to import inventory directly from XenApp or XenDesktop to FlexNet Manager Suite, please follow the appropriate procedures from the following two sections.

Update the XenApp Adapter

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

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

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

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

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

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

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

      - `XenAppAgent6`

      - `XenAppAgent65`

      - `XenAppAgent75`.

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

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

   💡

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

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

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

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

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

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

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

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

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

Update the XenDesktop Adapter

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

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

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

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

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

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

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

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

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

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

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

```
Set-ExecutionPolicy RemoteSigned
```

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

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

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

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

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

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

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

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

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

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

💡

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

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

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

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

💡

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

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

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

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

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

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

Finishing Off

Congratulations! (And there may be a few bits of housekeeping.)

You have achieved a lot.

- You separated previously co-located installations of two products, and split a shared database.

- You upgraded your Inventory Manager implementation to 9.2.3 so that it can continue operations.

- You separated your existing managed devices into two groups:

  - One group to continue on under Inventory Manager, because they needed customized settings or schedules for their installed inventory agents

  - A second group to migrate to management by FlexNet Manager Suite 2015 R2 SP3.

- You implemented FlexNet Manager Suite 2015 R2 SP3 in such a way that:

  - All intended managed devices automatically switched over to the new system, and are immediately reporting their inventory directly to the new inventory database within FlexNet Manager Suite

  - Your continuing implementation of Inventory Manager 9.2 is already set up as an inventory feed into the new system, in the same way that Microsoft SCCM or IBM's ILMT or other inventory tools can feed your compliance calculations.

- Reports have been optimized in the new system, and you may find some in new locations. As well, the system no longer uses Microsoft Reporting Services for factory-supplied reports, so that some of those reports are no longer available. If you have custom reports you developed in Reporting Services, you may need to redirect those to link to your new compliance (or if combined, operations) database.

If your plan is to continue parallel operations of FlexNet Manager Suite with Inventory Manager continuing as a data source, your work is complete.

If (on the other hand) you wish to migrate all operations Inventory Manager 9.2 across to FlexNet Manager Suite, some tasks remain to be completed manually, including these:

- Scheduled tasks you had established for Inventory Manager are not migrated into FlexNet Manager Suite 2015 R2 SP3. In the new system, you establish rules that combine actions, targets, and schedules. Navigate through **Discovery & Inventory** > **Discovery and Inventory Rules**, and click **Create a rule**.

- Of the many specialized remote execution tasks available in Inventory Manager 9.2, only three have equivalent rules available in FlexNet Manager Suite 2015 R2 SP3 (and there is other rule-based functionality not present in Inventory Manager). If you wish to transfer these three remote execution tasks from Inventory Manager to FlexNet Manager Suite, you must manually set up the appropriate rules (on the same **Discovery and Inventory Rules** page mentioned above) to suit your preferred use of these remote execution tasks:

  - `Generate Inventory`

  - `Generate VMWare Infrastructure Inventory`

  - `Generate Oracle Database Inventory`.

- If you have a regular process of network discovery to ensure that any new devices are automatically brought under management, and you want this to transfer to FlexNet Manager Suite, you need to set up matching discovery rules (once again, on the same **Discovery and Inventory Rules** page).

- When you are no longer using Inventory Manager as a data source for FlexNet Manager Suite, you can remove the connection. Do this (only) on the inventory beacon that is installed on the batch server (or server hosting that functionality), opening the **Inventory systems** page and deleting the connection, by default called `ManageSoft`. Be sure to do this ONLY when Inventory Manager is no longer required, and every inventory target has transferred and is actively managed through FlexNet Manager Suite. This is because removing this connection will also remove from the database any inventory records still coming exclusively from that source.

In addition to things that require manual effort, there are some other apparent 'gaps' that you may wonder about, but which are as expected, and do not require manual effort:

- Historical raw Computer Inventories belong in Inventory Manager and are not transferred to the new system. As managed devices switch over to 2015 R2 SP3, the **Discovery & Inventory** > **All Inventory** list (under the **Inventory** group) is now populated from their current inventory reports, as expected.

- Discovered Devices (the list of devices found by Inventory Manager in previous discovery tasks) are all migrated into FlexNet Manager Suite 2015 R2 SP3, with the exception of the following (these are consistent with the normal behavior of 2015 R2 SP3):

  - Virtual machines identified in ESX host inventory but which have not yet reported their own hardware and software inventory

  - Computers with a blank name

  - Computers with a domain name that is blank, or equal to `MANAGESOFT` or `WORKGROUP`

  - Computers that have a MAC address that is not unique across your computing estate

  - Remote devices, mobile devices or VDI templates (these are placeholders created for attaching inventory detected as use of virtualized applications and virtual desktops)

  - Computers awaiting inventory (that is, records added as assets but not linked to an inventory record).

Your implementation of FlexNet Manager Suite 2015 R2 SP3 is now production ready.

4

Notes on Issues

Topics:

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

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

Password Maintenance

When a password on the service account expires, services cease to operate. At password refresh time, ensure that the password is updated for all 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 peer-to-peer download service*

- *Flexera Inventory Manager security service.*

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

  - Upload Flexera logs and inventories

  - Upload third party inventory data

Identifying IIS Application Pool Credential Issues

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

Background

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

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

Tip • In this case, as well as IIS configuration, you may also need to update passwords on scheduled tasks and on services. For a complete list, see Password Maintenance on page 98.

Diagnosis

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

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

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

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

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

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

Repair

Update the credentials for the applications pool on each of your application servers, using the process in *Update Credentials in IIS Application Pools* on page 101.

Update Credentials in IIS Application Pools

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

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

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

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

    *   **Flexera Beacon** on the batch 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 whether these services are enabled in the Windows Server operating system:

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

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

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