



FlexNet Operations 2016

Installation Guide

Legal Information

Book Name	FlexNet Operations Installation Guide
Part Number	FNO-2016-IN00
Product Release Date	February 2016
Last Modified Date	1 March 2016

Copyright Notice

Copyright © 2016 Flexera Software LLC. All Rights Reserved.

This publication contains proprietary and confidential 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.

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.

Contents

1	Introduction	1
	Documentation Conventions	2
	Contacting Us	4
2	Install Options	5
	FlexNet Operations Components	5
	Recommended Configurations	7
3	Before Installing FlexNet Operations	9
	Acquiring the FlexNet Operations Installer	10
	Planning User Accounts	10
	Configuring Database Management Systems for Use with FlexNet Operations	11
	Configuring Oracle for FlexNet Operations	11
	Configuring SQL Server for FlexNet Operations	12
	Setting Up RabbitMQ	12
	Optionally Configuring an External Wildfly Instance	13
4	Installing and Configuring FlexNet Operations	15
	Installing FlexNet Operations	16
	Setting Up the Installation with FlexNet Setup	18
	About FlexNet Setup	19
	Starting FlexNet Setup	19
	Configuring General Settings	21
	Configuring Database Settings	22
	Configuring Advanced Settings	26
	Viewing System Status	28
	Deploying FlexNet Operations Modules	28
	Starting FlexNet Operations	29

Connecting Distributed Deployments	30
Verifying Basic Functionality	33
Next Steps	34
5 Upgrading FlexNet Operations	35
Overview of the Upgrade Process	36
Preparing to Upgrade FlexNet Operations	36
Obtaining the Upgrade Files	38
Installing the Upgrade Version	39
Setting Up the Installation with FlexNet Setup	41
About FlexNet Setup	42
Starting FlexNet Setup	42
Configuring General Settings	43
Configuring Database Settings	45
Configuring Advanced Settings	49
Applying Customizations from the Prior FlexNet Operations Installation	51
Deploying FlexNet Operations Modules	51
Starting FlexNet Operations	52
Connecting Distributed Deployments	52
Verifying the Upgrade	56
More Post-upgrade Considerations	56
Additional Step for Web Service Users	57
Applying Hotfixes to FlexNet Operations Components	57
Verifying the Hotfix	58
A Configuring for Integration with Electronic Software Delivery	59
B Configuring FlexNet Operations for Secure Socket Layer	61
Configuring Server-Side Secure Socket Layer	62
Generating a Test Certificate	62
Configuring FlexNet Operations with the Test Certificate	63
Verifying the Test Certificate	64
Obtaining a Trusted Certificate	65
Configuring FlexNet Operations with a Permanent Certificate	66
Configuring Secure Socket Layer in FlexNet Operations to Disable Weak Ciphers	67
Configuring Client-Side Secure Socket Layer	68
Importing a Secure Socket Layer Server's Certificate into the Truststore	68
Configuring FlexNet Operations with a New Truststore	69
Verifying the Trusted Connection	69
C Uninstalling FlexNet Operations	71

1

Introduction

The following chapters cover the installation of FlexNet Operations.

Table 1-1 • Installation Guide chapter descriptions

Topic	Content
Install Options	Presents FlexNet Operations components and recommended deployments.
Before Installing FlexNet Operations	Covers pre-install requirements for FlexNet Operations.
Installing and Configuring FlexNet Operations	Explains how to install FlexNet Operations components with the FlexNet Operations installer and configure those components with FlexNet Setup.
Upgrading FlexNet Operations	Explains how to upgrade FlexNet Operations from a previous version as well as how to apply a hotfix to an existing installation.
Configuring for Integration with Electronic Software Delivery	Describes how to integrate FlexNet Operations with FlexNet Electronic Software Delivery.
Configuring FlexNet Operations for Secure Socket Layer	Explains how to configure FlexNet Operations for secure socket layer communication.
Uninstalling FlexNet Operations	Discusses how to uninstall an existing installation of FlexNet Operations.

Documentation Conventions

In this documentation, reader alert and style conventions are used to bring your attention to specific information or help you identify information.

Reader Alert Conventions

Reader alerts are used throughout this documentation to notify you of both supplementary and essential information. The following table explains the meaning of each alert.

Table 1-2 • Reader Alert Conventions















Image	Alert Name	Description
	Note	Notes are used to draw attention to pieces of information that should stand out.
	Important Note	Important notes are used for information that is essential for users to read.
	Caution	Cautions indicate that this information is critical to the success of the desired feature or product functionality.
	Tip	Tips are used to indicate helpful information that could assist you in better utilizing the desired function or feature.
	Best Practices	Best Practices alerts instruct you on the best way to accomplish a task.
	Edition-Specific Note	Edition-specific notes indicate that the information applies to a specific edition of a product (such as Professional or Premier edition).
	Project-Specific Note	Project-specific notes are used to highlight information that may vary depending on the project type used (such as a Basic MSI or Merge Module project).
	Version-Specific Note	Version-specific notes indicate that the information applies to a specific version of a product (such as Version 9.0 or Version 11.0).
	Windows Logo Guideline	Windows Logo Guideline alerts accompany Microsoft logo compliance requirements and recommendations.
	Security	Security alerts identify security issues.

Table 1-2 • Reader Alert Conventions (cont.)

Image	Alert Name	Description
	Task	The Task graphic indicates that procedural instructions follow.
	Advanced Note	Advanced notes are used in training manuals to identify information that is for advanced users.
	Lab	In training manuals, the Lab graphic indicates that a lab exercise follows.
	Tutorial	In training manuals, the Tutorial graphic indicates that a tutorial exercise follows.

Style Conventions

The following style conventions are used throughout this documentation.

Table 1-3 • Style Conventions

Style	Example	Description
User Interface Elements	On the File menu, click Open .	User interface elements appear in bold when referenced in tasks.
Variables	<i>FileName</i>	Variables appear in italics.
Code	<code>#define HWND_BROADCAST 0xffff</code>	Code snippets appear in a monospace typeface.
User-Inputted Text	Type <code>\$D(install)</code> at the prompt.	Text that is to be entered as a literal value is displayed in a monospace typeface, in bold, and in blue.
File Names and Directory Paths	My files are located in the following directory: <code>C:\MyDocuments\SampleCode</code>	File names and directory paths are presented in a monospace typeface.
.INI File Text	Insert the line <code>LimitdUI=Y</code> into the .INI file to display only the Welcome dialog box when the Windows Installer package is run.	Text in .INI files is presented in a monospace typeface.
Command-Line Statements	To run the installation silently, enter: <code>Setup.exe /s/v/qn</code>	Command-line statements and parameters are presented in a monospace typeface.

Table 1-3 • Style Conventions (cont.)

Style	Example	Description
Environment Variables	Set the value of the <code>windir</code> environment variable.	Environment variables are presented in a monospace typeface.
Examples	Create two groups, one called Admins and the other called General .	Examples are presented in bold.
Functions	FeatureAddItem adds a new feature to a script-created feature set.	Functions are presented in bold.
Properties	In the Name property, enter a name for this custom control that is unique among all of the controls in your project.	Properties are presented in bold.
Screen Output	If you type an incorrect parameter, the message <code>The system cannot find the path specified.</code> is displayed.	Screen output (from a log file or from the console) is displayed in a monospace typeface, and in blue.
Links	Obtain the latest modules, white papers, project samples, and more from: http://www.yourcompany.com/downloads.htm	Links appear in blue.

Contacting Us

You can connect with the FlexNet Operations customer community from anywhere in the world by visiting:

<http://www.flexeracommunity.force.com/customer>

Username and password required.

2

Install Options

This chapter discusses FlexNet Operations components and recommended configurations.

Table 2-1 • Sections in this chapter

Topic	Description
FlexNet Operations Components	A high level look at the standard and optional components of FlexNet Operations.
Recommended Configurations	Discusses common scenarios for FlexNet Operations deployments and recommends configurations for those scenarios.

FlexNet Operations Components

Decisions about FlexNet Operations components require an understanding of FlexNet Operations components and common configuration choices.

FlexNet Operations includes the following standard database and server components.

- FlexNet Operations server: The FlexNet Operations server provides access to your licensing, fulfillment and entitlement data. It has two interfaces:
 - An internal producer-facing interface, called the Producer Portal
 - A customer-facing interface, called the End-User Portal.

You can access both the producer-facing and customer-facing interfaces from a single installation of the FlexNet Operations server.

- FlexNet Operations database: The FlexNet Operations database stores your licensing, fulfillment and entitlement records.

- Reporting database: The reporting database contains the FlexNet Operations data that is used to build reports. This database is distinct from the FlexNet Operations database. Data is transmitted from the FlexNet Operations database to the reporting database in a process known as data transformation.

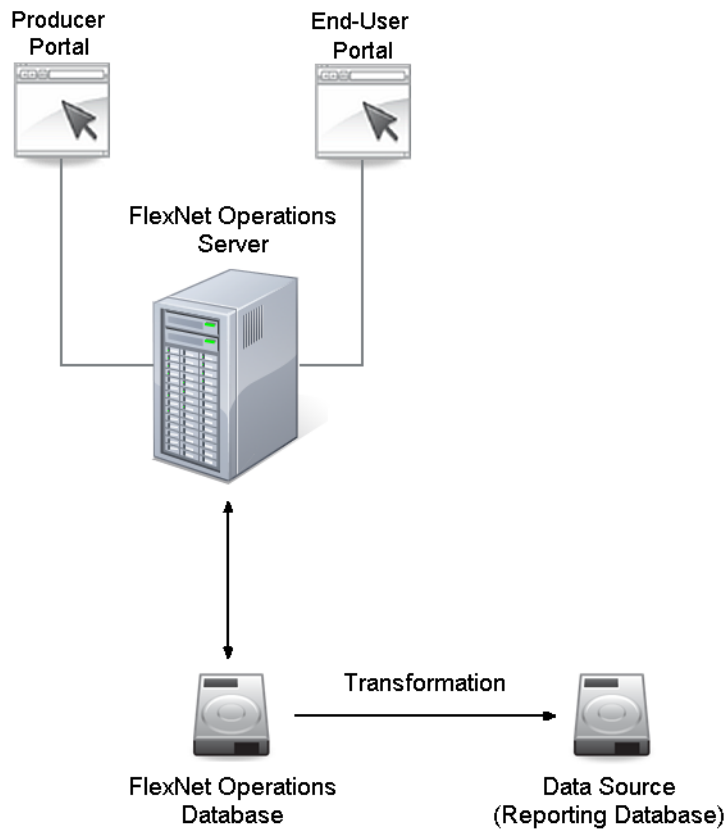


Figure 2-1: FlexNet Operations components

Additional FlexNet Operations components available when purchased:

- FlexNet Embedded: FlexNet Operations includes a database for FlexNet Embedded devices and servers for producers who purchase Advanced Lifecycle Management. Use FlexNet Setup to configure the FlexNet Embedded module.
- FlexNet Usage Management: FlexNet Operations includes a database for producers who purchase the FlexNet Usage Management module. This database contains usage records and can be deployed with FlexNet Setup after you run the installer.
- Cloud License Service: FlexNet Operations includes a database for producers who purchase the FlexNet Cloud Licensing Service module. This database supports the operation of cloud license servers.

Electronic Software Delivery functionality is a cloud-hosted service rather than a component that is locally installed. For instructions on connecting FlexNet Operations with a FlexNet Electronic Software Delivery tenant, see [Configuring for Integration with Electronic Software Delivery](#).


Recommended Configurations

The following scenarios provide guidelines for planning FlexNet Operations deployments based upon the intended use of the FlexNet Operations instance.



Note • See [Optionally Configuring an External Wildfly Instance](#) for more information about how FlexNet Operations works with Wildfly.

Table 2-2 • Recommended configurations for various deployment scenarios

Scenario	Recommended Configuration
<p>Scenario 1: Evaluating FlexNet Operations</p>	<p>One machine (physical or virtual) to host FlexNet Operations components, the database server, and RabbitMQ. This scenario uses the embedded Wildfly server.</p> <p></p> <p>Note • See Setting Up RabbitMQ for more information about how FlexNet Operations uses RabbitMQ to manage communication between FlexNet Operations components.</p>
<p>Scenario 2: Recommended configuration for deploying FlexNet Operations with FlexNet Embedded</p>	<p>Three hosts:</p> <ul style="list-style-type: none"> • Host 1 has the core FlexNet Operations module. • Host 2 has the FlexNet Embedded module. • Host 3 has RabbitMQ. <p>This scenario uses an external Wildfly server (rather than the embedded Wildfly server) on each machine that hosts a FlexNet Operations component.</p>
<p>Scenario 3: Recommended configuration for deploying FlexNet Operations with FlexNet Embedded, FlexNet Usage Management, and Cloud Licensing Service</p>	<p>Five hosts:</p> <ul style="list-style-type: none"> • Host 1 has the core FlexNet Operations module. • Host 2 has the FlexNet Embedded module. • Host 3 has the FlexNet Usage Management module. • Host 4 has the Cloud Licensing Service module. • Host 5 has RabbitMQ. <p>This scenario uses an external Wildfly server (rather than the embedded Wildfly server) on each machine that hosts a FlexNet Operations component.</p>
<p>Scenario 4: Deploying FlexNet Operations with a cloud tenant for electronic software delivery</p>	<p>See Appendix A, Configuring for Integration with Electronic Software Delivery.</p>

For information about configuring FlexNet Operations for Secure Socket Layer communication, see [Appendix B, Configuring FlexNet Operations for Secure Socket Layer](#).

3

Before Installing FlexNet Operations

Review the guidance in this chapter before installing or upgrading FlexNet Operations. The sections in this chapter outline the pre-installation steps important for successful install and upgrade procedures.

See the FlexNet Operations release notes for detailed system requirements.

Table 3-1 • Sections in this chapter

Topic	Description
Acquiring the FlexNet Operations Installer	Describes how to obtain an installer for FlexNet Operations.
Planning User Accounts	Discusses common user accounts for FlexNet Operations users and how to plan for those accounts in your organization.
Configuring Database Management Systems for Use with FlexNet Operations	Covers the steps necessary to configure Oracle and Microsoft SQL Server database management systems for use with FlexNet Operations.
Setting Up RabbitMQ	Describes how to set up RabbitMQ to handle messaging for a distributed deployment of FlexNet Operations.
Optionally Configuring an External Wildfly Instance	Discusses the option of using an external Wildfly instance instead of the FlexNet Operations embedded Wildfly instance.

Acquiring the FlexNet Operations Installer

When you purchase FlexNet Operations, Flexera Software sends a Welcome email with the links and credentials you need to log into the Flexera Software Product and Licensing Center. Following the instructions in the Welcome email, log in to the Product and Licensing Center and navigate to the FlexNet Operations download files. Click the links on the Download page to download the installer appropriate for the platform on which you plan to install FlexNet Operations.

Contact your Flexera Software representative or Flexera Software support if you have any trouble gaining access to your Flexera Software products on the Product and Licensing Center.

Planning User Accounts

Guidelines for User Accounts on Linux Systems

If you are installing FlexNet Operations on a Linux host, the user who runs the installer, and subsequently FlexNet Setup, must meet the following criteria:

- The user can be the root user or a non-root user.

When the installer is run without root privileges, follow the steps described in [Special Instructions for Linux Installers](#) to manually install FlexNet Setup as a service and start that service.
- The user must have write access to a home directory, to the selected installation directory, and to the `/var/tmp` directory.
- The user must have a valid `DISPLAY` environment variable set to a host machine that is running an X server.
Note: If you are using an X server to display to a machine other than the one on which FlexNet Operations is to run, the display machine must have the required version of Java. (See the FlexNet Operations release notes for supported platform information.)
- The current directory (`.`) must be in the path of the user running the installer.

Additional Notes about Consistent Locale Settings

The users who start the database server (who may be the users that start its Windows service), create the FlexNet Operations database, and start FlexNet Operations must all have the same locale settings.

- On Linux, the tested locale setting is `en_US.ISO8859-1`. Check the locale setting for a user by logging in as the user and typing `locale`. Set this locale by typing the following at the command line:

`setenv LC_ALL en_US.ISO8859-1`
- On Windows, the tested code page is the United States code page (437). Check the active code page for a user by opening a command window and typing `chcp`. Set this code page by typing the following at the command line:

`chcp 437`

Configuring Database Management Systems for Use with FlexNet Operations

FlexNet Operations requires a database to run. Before installing FlexNet Operations, select, install, and configure a database management system (DBMS) according to these guidelines:

- [Configuring Oracle for FlexNet Operations](#)
- [Configuring SQL Server for FlexNet Operations](#)

If you already have a DBMS installed, read one of the following sections to verify that it is installed and configured with the required settings.

Configuring Oracle for FlexNet Operations

Install the Oracle database server on a machine other than the one on which FlexNet Operations is installed. See the FlexNet Operations Release Notes for a list of supported versions of the Oracle database server.

Installing the Oracle Database Server

Follow the Oracle product documentation to install the Oracle DBMS and create a database instance. This guide states only the assumptions and requirements of the Oracle database server installation that allow it to work correctly with FlexNet Operations. FlexNet Operations has been tested with a database with the following character settings:

- Database character set: AL32UTF8
- National character set: AL16UTF16

Make note of the login name and password of an Oracle administrative user (for example, SYSTEM) because you must connect to Oracle as that user to create the FlexNet database and database user.



Note • The default SID for Oracle is ORCL.

FlexNet Operations supports Oracle Database 12c (traditional architecture only). When you install Oracle Database 12c, the check box for the **Create as Container database** option on the **Typical Install Configuration** screen is selected by default. You must ensure that the **Create as Container** database check box is not selected before you click the **Next** button on this screen.

Creating a Tablespace for the FlexNet Database

Before you run the FlexNet Operations installer, you must create a tablespace where the FlexNet Operations schema will be created. We recommend that you allocate at least 150 MB for this tablespace. You are prompted for this tablespace name when you install FlexNet Operations. The exact command or procedure varies depending on the tool you use to create the tablespace.

For example, in SQL*Plus, the command to create a 150 MB file named FN01.dbf at a path named path would be:

```
create tablespace FLEXNET datafile 'path/FN01.dbf' size 150M
autoextend on;
```

Configuring SQL Server for FlexNet Operations

Install the Microsoft SQL Server database server on a machine other than the one on which FlexNet Operations is installed. See the FlexNet Operations release notes for a list of supported versions of the Microsoft SQL database server.

Installing the SQL Server Database Server

Follow Microsoft's instructions to install SQL Server. This guide states only the assumptions and requirements of the SQL Server database server installation that allow it to work correctly with FlexNet Operations.

In the database installer, accept the default settings, except:

- Select mixed authentication (Windows and SQL Server) instead of Windows-only authentication.
- Enable the TCP/IP network protocol, if this has not already been done by default during installation.

A Note on SQL Server Express Edition

For Microsoft SQL Server Express Edition, the installation instructions are available from Microsoft at <http://msdn2.microsoft.com/en-us/library/ms143722.aspx>. There are several additional steps you must take in the installation process to correctly configure your host for FlexNet Operations:

- You must install .NET Framework 2.0 on your host, and all previous versions of .NET should be uninstalled.
- When following the installation instructions:
 - In Step 8, on the Instance Name page, select a Default instance.
 - In Step 10, select SQL Server and Windows Authentication Mode.
- After installation, you must enable TCP/IP. Launch the SQL Server Configuration Manager. In the left pane, expand SQL Server Network Configuration and click Protocols for MSSQLServer. Then, in the right pane, right-click TCP/IP and enable it.
- If the host has a firewall, you should consult the document at <http://msdn2.microsoft.com/en-us/library/ms143446.aspx> for additional considerations.

Setting Up RabbitMQ

FlexNet Operations leverages RabbitMQ to manage messaging between FlexNet Operations components. Producers must install RabbitMQ on a machine reachable from the machines that host FlexNet Setup and FlexNet Operations components prior to installing FlexNet Operations.

For simple FlexNet Operations deployments in which all FlexNet Operations components are installed on a single machine (for product evaluations, for example) it is sufficient to simply install RabbitMQ on the host machine and use the default RabbitMQ user and port values for FlexNet Operations messaging.

If RabbitMQ is installed on a machine other than a machine on which FlexNet Operations is installed—which is a common case for distributed installs—you must create a RabbitMQ account for FlexNet Operations to use for messaging. This account must exist before running the FlexNet Operations installer on each machine, and each installation must specify the same FlexNet Operations user for its RabbitMQ settings.

For information about managing and installing RabbitMQ, as well as RabbitMQ system requirements, refer to instructions on the official RabbitMQ site:

<http://www.rabbitmq.com>



Tip • If you plan to run RabbitMQ on a separate machine and using a dedicated account for FlexNet Operations, consider enabling the RabbitMQ management plugin to help monitor and troubleshoot inter-component messaging.

Optionally Configuring an External Wildfly Instance



Note • See the FlexNet Operations release notes to check which version of Wildfly FlexNet Operations supports.

The FlexNet Operations installer includes an embedded Wildfly application server. For simple deployments, such as a single-server install for evaluation purposes, the embedded Wildfly server is sufficient for most users. For more robust deployments that require stronger security—especially those that are intended to host FlexNet Operations in a production environment—producers may prefer to use external Wildfly instances that can be updated and managed independent of FlexNet Operations.

Producers planning to use external Wildfly instances with FlexNet Operations must have Wildfly already installed on each machine on which FlexNet Operations is being installed. Also, the Wildfly server must be stopped for the duration of the installation and configuration steps.



Tip • For optimal performance and reliability, limit the use of this Wildfly server to running FlexNet Operations and its components. Avoid sharing the FlexNet Operations Wildfly server with other application deployments.

Chapter 3 Before Installing FlexNet Operations

Optionally Configuring an External Wildfly Instance

4

Installing and Configuring FlexNet Operations

This chapter walks users through installing FlexNet Operations server components and setting up those components—resulting in a running FlexNet Operations instance that is ready to be configured for your organization. However, certain installation options and configuration settings, such as configuring FlexNet Operations for secure socket layer or connecting the installed instance to Flexera Software servers for electronic software delivery, are covered in other chapters or appendices.

Be sure to procure machines that comply with FlexNet Operations system requirements and complete any tasks indicated in [Before Installing FlexNet Operations](#) prior to running the FlexNet Operations installer.

Table 4-1 • Sections in this chapter

Topic	Description
Installing FlexNet Operations	Provides instructions for running the FlexNet Operations installer.
Setting Up the Installation with FlexNet Setup	<p>Explains how to use FlexNet Setup to set up a new installation of FlexNet Operations. FlexNet Setup is a web application where you specify configuration settings, database connection settings, and other options before you start FlexNet Operations for the first time. The following tasks are covered:</p> <ul style="list-style-type: none">• About FlexNet Setup• Starting FlexNet Setup• Configuring General Settings• Configuring Database Settings• Configuring Advanced Settings• Viewing System Status• Deploying FlexNet Operations Modules• Starting FlexNet Operations• Connecting Distributed Deployments

Table 4-1 • Sections in this chapter (cont.)

Topic	Description
Verifying Basic Functionality	Describes how to confirm that the installation is working and that your configuration settings have been correctly applied.
Next Steps	Discusses where to find information on supported installation and setup options as well as configuration settings to make your FlexNet Operations instance ready for regular use.



Tip • Remember to configure FlexNet Operations with your organization's license by clicking **System** > **Configure** > **Licensing** in the Producer Portal and then saving the FlexNet Embedded URL (included in the Welcome Packet email). Until you apply your purchased FlexNet Operations license in the Producer Portal, FlexNet Operations runs on the built-in, 60-day evaluators license.

Installing FlexNet Operations

The following instruction sets explain how to run the FlexNet Operations installer. In a distributed deployment, run the installer on each machine.

Follow the steps, below, to install FlexNet Operations components. Once the install process is complete, continue with the instructions in [Setting Up the Installation with FlexNet Setup](#) to perform the initial configuration steps and [Verifying Basic Functionality](#) to verify the installation.

Review the FlexNet Operations system requirements in the FlexNet Operations release notes and the prerequisites in [Before Installing FlexNet Operations](#) before you install FlexNet Operations components.



Task:


To install FlexNet Operations components

1. On the machine you want to install FlexNet Operations components, start the FlexNet Operations installer. A progress window indicates that InstallAnywhere is preparing the FlexNet Operations installer.
2. On the Welcome panel, click **Next**.
3. On the Choose Install Folder panel, specify the install directory for FlexNet Operations and click **Next**. The default install directory depends on the host operating system.
 - For Windows-based systems, it is C:\Program Files\FlexNet Operations\
 - For Unix-based systems, it is /home/<user>/FlexNet-Operations/



Important • Using spaces in the install directory can cause problems on Unix-based systems. If you specify an install directory other than the default value, avoid using spaces.

- On the Customization Options panel, choose whether to use the bundled Wildfly server or your own Wildfly server and specify a RabbitMQ URL (if different from the default). Then click **Next**.

Setting	Description
Application Server Settings	<p>Choose whether to use the bundled version of Wildfly or an external version of Wildfly.</p> <ul style="list-style-type: none"> To use the bundled version of Wildfly, leave the Use Your Own Wildfly Server checkbox unchecked. To use your own version of Wildfly, check the Use Your Own Wildfly Server checkbox and then specify the location of your Wildfly installation.  <p>Important • To use an external Wildfly version, you must have Wildfly already installed on the machine on which FlexNet Operations is being installed. Also, your Wildfly server must be stopped for the duration of the installation and configuration steps.</p>
RabbitMQ URL	<p>Specify the RabbitMQ AMQP URL or retain the default. For distributed deployments of FlexNet Operations, be sure to create a RabbitMQ account for FlexNet Operations to use.</p> <ul style="list-style-type: none"> If you set up a specific account in RabbitMQ to use for FlexNet Operations messaging, specify the username, password, hostname, port, and (optionally) virtual host using the syntax shown in the installer panel. AMQP:\\username:password@hostname:port[/vhost] If you install FlexNet Operations components all on a single machine, the default URL value is all that is needed for FlexNet Operations to connect with RabbitMQ. AMQP:\\guest:guest@localhost:5672

- On the Pre-installation Summary panel, review the installer settings and click **Install**. The installer begins installing and configuring files and shows its progress.
- On the Install Complete panel, the installer reports the result of the install process and shows the URL to use to launch the FlexNet Operations configuration tool, FlexNet Setup (typically, <http://localhost:4321/flexnetsetup>).



Note • By default, the installer attempts to start FlexNet Setup on port 4321; however, if the installer detects that port 4321 is busy, it will attempt to use a different port.

- Click **Done**. The installer attempts to launch FlexNet Setup in your system's default browser.

On Windows systems, continue by configuring installed FlexNet Operations components as shown in [Setting Up the Installation with FlexNet Setup](#).

On Linux systems, review the special instructions, below, and take any additional steps required before you configure installed components with FlexNet Setup.

Special Instructions for Linux Installers

After installing FlexNet Operations components on a Linux system, you must log out and then log in again. (This allows the installer's environment variable changes to take effect.)

Furthermore, if you ran the installer as a non-root user, you must run a script (with sudo access) to install FlexNet Setup as a service and then start the service.



Task: *To complete the FlexNet Operations install on Linux systems*

1. At the command line, type

```
sudo sh ops_install_dir/components/tomcat/bin/configure-flexnet-setup-as-service.sh
```

where *ops_install_dir* is the FlexNet Operations installation directory. For example, if you installed FlexNet Operations components to `/usr/home/FNOuser`, you would type

```
sudo sh /usr/home/FNOuser/components/tomcat/bin/configure-flexnet-setup-as-service.sh
```

This script installs FlexNet Setup as a service, but does not start it.

2. To start the service, the user needs to execute the following command.

```
service FlexNetSetup start
```

This command does not require sudo access.

These instructions install the FlexNet Setup service under root context but allow FlexNet Setup and FlexNet Operations, itself, to run as a normal user (not a root user).

Continue with the instructions in [Setting Up the Installation with FlexNet Setup](#) to perform the initial configuration tasks.

Setting Up the Installation with FlexNet Setup

After the installer completes, run FlexNet Setup to configure each FlexNet Operations component you want to deploy on the current machine.

Table 4-2 • Configuration topics

Topic	Description
About FlexNet Setup	Describes the purpose of FlexNet Setup for deploying and managing FlexNet Operations components.
Starting FlexNet Setup	Explains how to start FlexNet Setup. FlexNet Setup is where you configure FlexNet Operations, deploy configured modules, and start the FlexNet Operations server.

Table 4-2 • Configuration topics (cont.)

Topic	Description
Configuring General Settings	Describes how identify the FlexNet Operations modules to deploy and specify general settings.
Configuring Database Settings	Describes how to configure databases for each FlexNet Operations module to be deployed.
Configuring Advanced Settings	Discusses the settings available on the Advanced configuration page.
Viewing System Status	Describes how to view system status, FlexNet Setup logs, and so forth.
Deploying FlexNet Operations Modules	Shows how to deploy configured FlexNet Operations modules on the System Status page.
Starting FlexNet Operations	Explains how to deploy and undeploy FlexNet Operations modules and how to start FlexNet Operations.
Connecting Distributed Deployments	Provides steps necessary to connect FlexNet Operations components installed on different host machines. (This section is only for producers who are installing FlexNet Operations components separate machines.)

About FlexNet Setup

FlexNet Setup is a web application for post-installation setup of FlexNet Operations. The FlexNet Operations installation process installs FlexNet Setup as a service. After you install FlexNet Operations, you use FlexNet Setup to complete the initial setup tasks. Later, you can return to FlexNet Setup to check the status of FlexNet Operations server components, alter setup choices, or stop the FlexNet Operations server.



Tip • Whenever you use FlexNet Setup to alter configuration settings for FlexNet Operations components, remember to first stop the FlexNet Operations server and undeploy all FlexNet Operations components. Then, when your configuration changes are complete, redeploy all components and restart the server. Changes made to deployed components will not be applied in FlexNet Operations until the components are undeployed and redeployed.

Starting FlexNet Setup

At the completion of a successful installation, the FlexNet Operations installer attempts to launch FlexNet Setup automatically. (FlexNet Setup is started as a service on both Windows and Linux systems.) If FlexNet Setup is not already running in your web browser, you can open it manually.



Note • If you are signing in to FlexNet Setup for the first time, you must change the password for the default administrator user before you can continue to specify configuration settings.



Task: **To open FlexNet Setup manually**

- Open the following URL in a web browser:

`http://localhost:4321/flexnetsetup`

The default port for FlexNet Setup is 4321. However, if port 4321 is in use when the installer runs, the FlexNet Setup port may change. On the Install Complete panel, the FlexNet Operations installer shows the FlexNet Setup port that was assigned.



Note • If Tomcat is not running, FlexNet Setup will not open.

- To start FlexNet Setup on Windows, go to the Windows Services Console, locate the FlexNet Setup service, and start that service or, at a command prompt, type `net start FlexNetSetup`.
- To start FlexNet Setup on Linux, type `service FlexNetSetup start` at a command prompt.
- If you prefer not to run FlexNet Setup as a service, navigate to `ops_install_dir\components\tomcat\bin` and run `start-flexnet-setup`.



Task: **To sign in to FlexNet Setup**

1. On the Sign In page, provide the default administrator user credentials.
 - Username: **admin**
 - Password: **admin**
2. Click **Log In**.
3. If you are logging in to FlexNet Setup for the first time, follow the instructions, below, to change the administrator password.
 - a. Enter the current password: **admin**.
 - b. Enter a new password.
 - c. Enter the same new password a second time.
 - d. Choose a security question from the list provided.
 - e. Specify an answer to the security question you chose.
 - f. Click **Save**.

After you have successfully signed in, FlexNet Setup shows the General Settings configuration page. Continue with the setup process in [Configuring General Settings](#).

Configuring General Settings

The General Settings configuration page is where you identify FlexNet Operations modules to deploy and optionally specify other general settings.



Important • FlexNet Operations modules must be undeployed and the FlexNet Operations server must be stopped when you change configuration settings.



Tip • Your FlexNet Operations license governs the FlexNet Operations modules that operate for your organization. There is no need to configure settings for FlexNet Operations modules that are not authorized in your organization's license.



Task: *To configure general settings*

1. On the General Settings configuration page, use the Select Modules to Be Configured checkboxes to select FlexNet Operations modules you want to deploy.
2. Optionally specify Other Configurations settings.

Settings	Instructions
HTTP Port	Identify the port on which FlexNet Operations listens for HTTP communication. If you require a particular port, specify the port number; otherwise, keep the default setting for the embedded Web container: 8888 . Ensure this port is open through the firewall on the machine where FlexNet Operations is installed, if the machine hosts a firewall.
Stop Port	Identify the port on which FlexNet Operations listens for a stop message. This is the port on which FlexNet Operations listens for JNDI clients. If you require a particular port, specify the port number; otherwise, keep the default setting: 1199 .
Logging Threshold	Set the logging threshold for FlexNet Operations. Choose from <ul style="list-style-type: none">• Errors• Warnings• Information Messages (Default)• Debug Messages The logging threshold expresses the maximum level of detail for the messages written to the FlexNet application log file before FlexNet Operations starts. Only messages at or below the selected level of detail appear in the log.

Settings	Instructions
VM Heap Size	<p>Set the initial and maximum Java Virtual Machine heap size in megabytes. The default settings are</p> <ul style="list-style-type: none"> • Initial Size: 1024 • Maximum Size: 2048 <p>The maximum application memory limit is set by adjusting the heap size. The limit should be less than 80 percent of the machine's total RAM. If you have performance problems, you may want to increase these settings.</p>
User Data Directory	<p>Only used for distributed deployments, set the location of the User Data Directory. The default directory is</p> <p><code>ops_install_dir\release\flexnet-data\data.</code></p> <p>FlexNet Operations uses this directory for any files necessary for import/export operations and other temporary files.</p>

3. Click **Save**.

FlexNet Setup saves the configuration changes to FlexNet Operations. Changes are applied when FlexNet Operations modules are deployed and the FlexNet Operations server is restarted.

Continue to [Configuring Database Settings](#) to specify database settings for the FlexNet Operations modules you are deploying.

Configuring Database Settings

The Database configuration page is where you specify database settings for the FlexNet Operations modules you are deploying: FlexNet Operations, FlexNet Embedded, FlexNet Usage Management, Cloud Licensing Service, FlexNet Reporting. Here, you first configure and save the Database configuration settings and then initialize or upgrade the database schemas as necessary.



Tip • Your FlexNet Operations license governs the FlexNet Operations modules that operate for your organization. There is no need to configure settings for FlexNet Operations modules that are not authorized in your organization's license.



Task: *To configure databases*

1. In FlexNet Setup, click **Configuration** > **Database** to open the Database configuration page.
2. On the Database configuration page, provide settings for each FlexNet Operations module you are deploying on the current machine.

Settings	Instructions
Database Type	Identify the database type to be used for the current module. Choose either Microsoft SQL Server or Oracle .
Schema Name	Specify the name of the database schema for the current module. <ul style="list-style-type: none"> • New databases: For new databases, the name you provide becomes the name of the database schema FlexNet Setup creates for this module. • Existing databases: When upgrading from a prior version of FlexNet Operations, specify the schema name of the existing database.
Hostname	Specify a hostname or IP address for the database server.
Port	Specify the port on which the database server is listening. The default port value depends upon the Database Type. <ul style="list-style-type: none"> • Microsoft SQL Server: 1433 • Oracle: 1521
Database Username	Specify a username for FlexNet Setup to use when making changes to the database.
Database Password	Type the password for the database user.
Confirm Password	Re-type the password for the database user.



Tip • When configuring database settings for multiple modules, consider using the **Use Database Server Host of FlexNet Operations for this Schema** checkbox. If the database server host for one or more modules is the same as the FlexNet Operations module, you can use this checkbox to automatically populate the database configuration settings for these modules. However, each module still requires its own Schema Name.

3. Click **Save**.

FlexNet Setup stores the database configuration settings for each module you are deploying.

Continue the deployment by managing the database schemas. For each module you are deploying, you must either initialize or upgrade the schema.

- Producers who are configuring completely new FlexNet Operations instances must initialize the database schemas for the modules they are deploying.

- Producers who are upgrading FlexNet Operations from an earlier version must instead upgrade the database schemas for the modules that have existing databases and initialize database schemas for new modules.

For example, a producer who purchased FlexNet Operations plus the Advanced Lifecycle Management and Cloud Licensing Service modules and is upgrading from FlexNet Operations 12.11 Service Pack 2 would *upgrade* the schema for the core FlexNet Operations module (and for the FlexNet Reporting module) but *initialize* the schemas for FlexNet Embedded License Fulfillment Service and Cloud Licensing Service.

Initializing Database Schemas

Follow the instructions below to initialize the database schema for each FlexNet Operations module you are deploying on the current machine.



Important • *Initializing the database schema for an existing database will delete all data in the database. Never initialize the schema of an existing database in FlexNet Operations upgrade scenario. Instead, upgrade the database schema.*



Task: *To initialize a schema*

1. On the Database configuration page, click **Manage Schema**. This button opens the Manage Schema page in a popup window.
2. On the Manage Schema page, choose the module initialize and specify the database account credentials to use for that process.

Settings	Instructions
Which database do you want to initialize/upgrade?	Choose the module for which you want to initialize a schema: <ul style="list-style-type: none"> • FlexNet Operations • FlexNet Embedded • FlexNet Usage Management • Cloud Licensing Service • FlexNet Reporting
Database Username	Specify the username of an account with ownership privileges on the database server for the current module.
Database Password	Specify the password for the database username.

3. Click **Initialize**. FlexNet Setup opens a popup window that asks you to confirm your choice.
4. In the popup window, click **Initialize** to confirm and start the process. FlexNet Setup shows the initialization process.
5. When the initialization process is complete, choose whether to finish schema management activities or to manage another schema.
 - To finish schema management activities, click **Close**.

- To manage the schema of another module, click **Manage Another Database**.

For new installations, continue with [Viewing System Status](#) once all the FlexNet Operations modules you are deploying have been initialized.

Upgrading Database Schemas

Follow the instructions below to upgrade the database schema for each FlexNet Operations module you are upgrading from an earlier FlexNet Operations version.



Note • The **Upgrade** button is enabled on the Manage Schema page only when an existing database for the chosen module is present. Otherwise, only the **Initialize** button is enabled.



Task: *To upgrade a schema*

1. On the Database configuration page, click **Manage Schema**. This button opens the Manage Schema page in a popup window.
2. On the Manage Schema page, choose the module upgrade and specify the database account credentials to use for that process.

Settings	Instructions
Which database do you want to initialize/upgrade?	Choose the module for which you want to upgrade a schema: <ul style="list-style-type: none"> • FlexNet Operations • FlexNet Embedded • FlexNet Usage Management • Cloud Licensing Service • FlexNet Reporting
Database Username	Specify the username of an account with ownership privileges on the database server for the current module.
Database Password	Specify the password for the database username.

3. Click **Upgrade**. FlexNet Setup opens a popup window that asks you to confirm your choice.
4. In the popup window, click **Upgrade** to confirm and start the process. FlexNet Setup shows the upgrade process.
5. When the upgrade process is complete, choose whether to finish schema management activities or to manage another schema.
 - To finish schema management activities, click **Close**.
 - To manage the schema of another module, click **Manage Another Database**.

When database configuration settings are complete and database schemas for all the modules you are deploying have been initialized or upgraded, you can move to the System Status page, deploy modules, and start FlexNet Operations.

Continue with [Viewing System Status](#).



Note • Advanced configuration settings are discussed in the next section, but uses of these settings are covered in instruction sets dedicated to advanced tasks, such as [Configuring FlexNet Operations for Secure Socket Layer](#).

Configuring Advanced Settings

The configuration settings on the Advanced configuration page support configuring FlexNet Operations for secure socket layer communication, server performance, and for the AJP (Apache JServ Protocol) port.

This section describes the settings on the Advanced configuration page, but some of the instructions for using the Advanced configuration page are covered in dedicated sections, such as [Configuring FlexNet Operations for Secure Socket Layer](#).

- Secure Server Settings
- Secure Client Settings
- Other Ports Settings
- Performance Settings

Secure Server Settings

The following secure server settings support configuring the FlexNet Operations server for secure socket layer communication.

Setting	Description
HTTPS Port	<p>The port on which FlexNet Operations listens for HTTPS requests. Default: 8443.</p> <p>FlexNet Operations is always enabled to accept HTTPS requests, but some additional settings must be configured before using SSL. The URL to connect to FlexNet Operations with HTTPS is <code>https://host:port/flexnet</code>, where <code>port</code> is the HTTPS port number.</p> <p>For information about configuring SSL for Wildfly Web container, see Configuring FlexNet Operations for Secure Socket Layer.</p> <p>Note that HTTPS requests can be handled by a full-feature Web server instead of by FlexNet Operations itself.</p>

Setting	Description
Keystore Location	The name and location of the keystore on the current machine. Default: ops_install_dir/release/flexnet-data/site/bin/keystore . This keystore file contains the key entry for the certificate that FlexNet Operations uses to provide SSL connections to its clients (for example, browsers or activation utilities). Use the default location only if you are using the bundled keystore or another keystore for testing purposes. Otherwise, point to a keystore outside the FlexNet Operations installation.
Password	The password used to secure the keystore. The same password is used to secure the certificate key.
Confirm Password	The password for the keystore, for confirmation.

Secure Client Settings

The following secure client settings support configuring FlexNet Operations to connect as a client to an SSL server.

Setting	Description
Truststore Location	The name and location of the client-side truststore that contains the trusted certificate entry for a remote SSL server (for example, an LDAP server). Default: ops_install_dir/components/jvm/jre/lib/security/cacerts . Use the default truststore only if you are using the bundled truststore. Otherwise, point to a truststore outside the FlexNet Operations installation.
Password	The password used to secure the truststore. The same password is used to secure the certificate key.
Confirm Password	The password for the truststore, for confirmation.

Other Ports Settings

Other Port Settings includes only one setting: AJP Port.

Setting	Description
AJP Port	FlexNet Operations port for Apache JServ Protocol (AJP) connections. Default: 8009 . This is the port on which the AJP connector listens. The AJP connector integrates FlexNet Operations with a full-function proxy (such as Apache or IIS) server for security or load balancing.

Performance Settings

The following server performance settings are available on the FlexNet Setup's Advanced configuration page.

Setting	Description
Connection Pool Size	The number of connections permitted to the FlexNet Operations server. Default: 100 . Ensure that your database is capable of creating the designated number of connections.
Max Thread Count	The number of threads allocated for the scheduler. Default: 30 .
Transaction Timeout	The transaction timeout time in seconds. Default: 3600 .

Viewing System Status

The System Status page shows the status of the FlexNet Operations modules you have configured, deploys and undeploys those modules, and starts and stops the FlexNet Operations server. From this page, you can also download a log of FlexNet Setup activity.



Task: *To view system status*

- In FlexNet Setup, click **System Status**.

Initially, for new installations, the status of FlexNet Operations modules indicates that the server is not running and that the modules themselves are not yet deployed. Continue with [Deploying FlexNet Operations Modules](#).



Tip • To download a log of FlexNet Setup activity, click **Download FlexNet Setup Log**.

Deploying FlexNet Operations Modules

FlexNet Operations modules, such as the core FlexNet Operations module, the FlexNet Embedded, and FlexNet Usage Management, are initially undeployed. To be available in FlexNet Operations, a module must first be deployed.



Important • When the core FlexNet Operations module is being deployed on the current machine, it must be the first module deployed.



Task: *To deploy a module*

1. In FlexNet Setup, click **System Status**.
2. On the System Status page, click **Deploy All**. FlexNet Setup opens a popup window to show deployment progress.
3. When all modules are deployed, click **Close** in the popup window.

When all the modules are deployed, you can start the server. Continue with [Starting FlexNet Operations](#).



Tip • Deployed modules can be undeployed by clicking their **Undeploy** button or clicking **Undeploy All**. It is important to stop the FlexNet Operations server and undeploy all modules when making database changes in FlexNet Setup.

Starting FlexNet Operations

Use the Start Server and Stop Server buttons to start, stop, and restart the FlexNet Operations server.

The FlexNet Operations server must be stopped during configuration changes, and all modules undeployed. Then, before any configuration changes will appear in FlexNet Operations, modules must be re-deployed and the server restarted.



Task: *To start the server*

- On the System Status page, click **Start Server**.

FlexNet Setup updates the status messages for each module. When all modules are deployed, the System Status page shows the build number for each module and all module status messages read, [Deployed and Started](#), you can sign in to FlexNet Operations using the default administrator account.



Tip • Click **Refresh** to update the System Status information.



Tip • When the FlexNet Operations server is running, you can stop it by clicking **Stop Server**.

Producers who have FlexNet Operations modules installed on two or more separate hosts, continue with [Connecting Distributed Deployments](#).

Producers who have all FlexNet Operations modules installed on a single host, continue with [Verifying Basic Functionality](#).

Connecting Distributed Deployments

For producers who are installing FlexNet Operations in a distributed topology, some additional steps are required to connect the FlexNet Operations components on different machines.



Tip • These instructions cover connecting FlexNet Operations hosts via HTTP. To use secure socket layer communication between hosts, use HTTPS ports and configure each host for secure socket layer communication. See [Configuring FlexNet Operations for Secure Socket Layer](#).

Connecting the FlexNet Embedded Host

When the core FlexNet Operations module and the FlexNet Embedded module are installed on separate hosts, you must link the two hosts with additional configuration settings.



Task: To connect the FlexNet Embedded License Fulfillment hosts

1. On the FlexNet Operations host, open the Producer Portal and change the system configuration setting, License Fulfillment Service URL:
 - a. Sign in to the Producer portal.
 - b. In the Producer Portal, click **System > Configure > FlexNet Operations**. This opens the FlexNet Operations system configuration page.
 - c. On the FlexNet Operations system configuration page, click **External Services Configuration** to expand that group.
 - d. For **License Fulfillment Service URL**, type http://1fs_host:port/1fs/services/FulfillmentService, where *1fs_host* is the hostname of the machine that hosts the FlexNet Embedded module and *port* is the HTTP port for that host.
 - e. Click **Save Configs**.
2. On the machine that hosts the FlexNet Embedded module, open the LFS Configuration Console, edit `boc_endpoint_url` and `ems_endpoint_url`, and save the changes.
 - a. Open the following URL in a Web browser: http://1fs_host:port/1fs/jsp/config.jsp. This URL opens the LFS Configuration Console.
 - b. In the LFS Configuration Console, edit the values for `boc_endpoint_url` and `ems_endpoint_url`. (The new values are the same for both settings.)

Setting	Value
<code>boc_endpoint_url</code>	http://fno_host:port/flexnet/services/EntitlementServiceSOAP where <i>fno_host</i> is the hostname for the machine that hosts the core FlexNet Operations module and <i>port</i> is the HTTP port on the same machine.

Setting	Value
ems_endpoint_url	http://fno_host:port/flexnet/services/EntitlementServiceSOAP where <i>fno_host</i> is the hostname for the machine that hosts the core FlexNet Operations module and <i>port</i> is the HTTP port on the same machine.

- c. Click **Save**.



Important • The configuration settings in the LFS Configuration Console are not preserved if the FlexNet Embedded module is undeployed. Each time this module is re-deployed, you must repeat the steps to set the *boc_endpoint_url* and *ems_endpoint_url* values.

These steps connect the FlexNet Embedded host and the machine that hosts the core FlexNet Operations module.

Connecting the FlexNet Usage Management Host

Additional configuration steps are required when the FlexNet Usage Management module is running on a different host from those machines that host the core FlexNet Operations module and the FlexNet Embedded module. The following steps connect these host machines.



Task: *To connect the FlexNet Usage Management host*

1. On the FlexNet Operations host, open the Producer Portal and change the system configuration setting: Usage Analytics Service URL:
 - a. Sign in to the Producer portal.
 - b. In the Producer Portal, click **System > Configure > FlexNet Operations**. This opens the FlexNet Operations system configuration page.
 - c. On the FlexNet Operations system configuration page, click **External Services Configuration** to expand that group.
 - d. For **Usage Analytics Service URL**, type http://uas_host:port/uas, where *uas_host* is the hostname of the machine that hosts the FlexNet Usage Management module and *port* is the HTTP port for that host.
 - e. Click **Save Configs**.
2. On the machine that hosts the FlexNet Embedded module, open the LFS Configuration Console, edit *uas_endpoint_url*, and save the change.
 - a. Open the following URL in a Web browser: http://lfs_host:port/lfs/jsp/config.jsp. This URL opens the LFS Configuration Console.

- b. In the LFS Configuration Console, edit the value for `uas_endpoint_url`.

Setting	Value
<code>uas_endpoint_url</code>	<code>http://uas_host:port/uas/servlet/UasServlet/api/vi/usage</code> where <code>uas_host</code> is the hostname for the machine that hosts the FlexNet Usage Management module and <code>port</code> is the HTTP port on the same machine.

- c. Click **Save**.



Important • The configuration settings in the LFS Configuration Console are not preserved if the FlexNet Embedded module is undeployed. Each time this module is re-deployed, you must repeat the steps to set the `gls_endpoint_url` value.

These steps connect the FlexNet Usage Management host to the machines that host the core FlexNet Operations module and the FlexNet Embedded module.

Connecting the Cloud Licensing Service Host

When the Cloud Licensing Service module is on a different host than the machines on which the core FlexNet Operations module and the FlexNet Embedded module are running, additional configuration steps are required to connect these hosts.



Task: To connect the Cloud Licensing Service host

1. On the machine that hosts the Cloud Licensing Service module, start FlexNet Setup.
 - a. On the System Status page in FlexNet Setup, stop the server and undeploy the Cloud Licensing Service module.
 1. Click the **Undeploy** button for Cloud Licensing Service.
 2. When the FlexNet Setup completes the undeployment, click **Stop Server**.
 - b. In the file system of the Cloud Licensing Service host, open the following file in a text editor:
`ops_install_dir\services\cls\cls.properties`
 - c. In `cls.properties`, edit the value for `lfs.url` to `http://lfs_host:port/lfs/binary/request`, where `lfs_host` is the hostname for the machine that hosts the FlexNet Embedded module and `port` is the HTTP port for that machine.
 - d. Save `cls.properties`.
 - e. In FlexNet Setup, deploy the Cloud Licensing Service and start the server.
 1. Click the **Deploy** button for Cloud Licensing Service.
 2. When FlexNet Setup completes the deployment, click **Start Server**.
2. On the machine that hosts the FlexNet Embedded module, open the LFS Configuration Console, edit `gls_endpoint_url`, and save the change.

- a. Open the following URL in a Web browser: http://lfs_host:port/lfs/jsp/config.jsp. This URL opens the LFS Configuration Console.
- b. In the LFS Configuration Console, edit the value for `gls_endpoint_url`.

Setting	Value
<code>gls_endpoint_url</code>	http://c7s_host:port/gls/api/1.0 where <code>c7s_host</code> is the hostname for the machine that hosts the Cloud Licensing Service module and <code>port</code> is the HTTP port on the same machine.

- c. Click **Save**.



Important • The configuration settings in the LFS Configuration Console are not preserved if the FlexNet Embedded module is undeployed. Each time this module is re-deployed, you must repeat the steps to set the `gls_endpoint_url` value.

These steps connect the Cloud Licensing Service host to the machines that host the core FlexNet Operations module and the FlexNet Embedded module.

Continue with [Verifying Basic Functionality](#).

Verifying Basic Functionality

With FlexNet Operations modules deployed and the server started, you can sign in to FlexNet Operations for the first time.



Task: *To sign in to FlexNet Operations*

1. In a Web browser, open the Producer Portal using the hostname of a machine on which FlexNet Operations is running and the HTTP port you set on the General configuration page in FlexNet Setup.
`http://hostname:port/flexnet/operations`
1. On the Sign In page, provide the default administrator user credentials.
 - Username: `ADMNadmin`
 - Password: `admin`
2. Click **Log In**.
3. If you are logging in to FlexNet Operations for the first time, follow the instructions, below, to change the administrator password.
 - a. Enter the current password: `admin`.
 - b. Enter a new password.
 - c. Enter the same new password a second time.

- d. Choose a security question from the list provided.
- e. Specify an answer to the security question you chose.
- f. Click **Save**.

After you have successfully signed in, FlexNet Operations shows the Producer Portal home page.

A Note about the Evaluators License and Your FlexNet Operations License

Until you apply your purchased FlexNet Operations license in the Producer Portal, FlexNet Operations runs on the built-in, 60-day evaluators license, which includes licenses for all optional FlexNet Operations modules (such as FlexNet Usage Management and FlexNet Cloud Licensing Service). The evaluators license allows producers to test drive all FlexNet Operations features. However, when you apply your organization's purchased license and restart the server, FlexNet Operations refreshes to show only those features to which your organization is entitled.

FlexNet Operations servers must be connected to the Internet to acquire and renew licenses from Flexera Software servers.



Tip • To apply your organization's purchased license to FlexNet Operations, click **System > Configure > Licensing** in the Producer Portal. Then, provide the FlexNet Embedded URL included in the Welcome Packet sent to you from Flexera Software and click **Save Configs**.

Next Steps

Once FlexNet Operations is functioning, the basic installation is complete, and subsequent steps depend on the optional features, implementation details, and administrative tasks you want to employ.

- To set up FlexNet Operations for secure socket layer communication, see [Configuring FlexNet Operations for Secure Socket Layer](#).
- To configure a Electronic Software Delivery connection, see [Configuring for Integration with Electronic Software Delivery](#).
- For additional customizations to FlexNet Operations, see the FlexNet Operations Implementation Guide.
- For post-installation configuration, see the FlexNet Operations Administration Guide.
- To get started with entitlements or set up licensing for your organization, see the FlexNet Operations Getting Started Guide for Entitlement Management or the getting started guide for your licensing technology.

5

Upgrading FlexNet Operations

This chapter details the procedure for upgrading to FlexNet Operations 2016 from a previous version of FlexNet Operations. It also describes the procedure for applying a hotfix to an existing FlexNet Operations installation.

If you are installing FlexNet Operations for the first time, [Installing and Configuring FlexNet Operations](#).

Table 5-1 • Sections in this chapter

Topic	Description
Overview of the Upgrade Process	Discusses the process of upgrading an existing FlexNet Operations installation and provides additional recommendations about that process.
Preparing to Upgrade FlexNet Operations	Discusses the steps to take before upgrading, including checking the version of your existing installation and preserving customizations.
Obtaining the Upgrade Files	Explains how to acquire the upgrade files from Flexera Software.
Installing the Upgrade Version	Describes how to run the FlexNet Operations installer for an upgrade.
Setting Up the Installation with FlexNet Setup	Explains how to configure a new, upgrade installation with FlexNet Setup.
Verifying the Upgrade	Shows how to quickly verify that the upgrade has been applied.
More Post-upgrade Considerations	Discusses a number of additional considerations that producers may need to address after installing and configuring the upgrade.
Additional Step for Web Service Users	Describes an extra post-upgrade step only for producers who use Web Services with FlexNet Operations.
Applying Hotfixes to FlexNet Operations Components	Explains how to apply hotfixes to FlexNet Operations.
Verifying the Hotfix	Shows how to quickly verify that the hotfix has been applied.



Tip • Remember to configure FlexNet Operations with your organization's license by clicking **System** > **Configure** > **Licensing** in the Producer Portal and then saving the FlexNet Embedded URL (included in the Welcome Packet email). Until you apply your purchased FlexNet Operations license in the Producer Portal, FlexNet Operations runs on the built-in, 60-day evaluators license.

Overview of the Upgrade Process



Note • These upgrade instructions presume that you are upgrading to FlexNet Operations 2016 from FlexNet Operations 12.8 or newer. Upgrading to version 2016 from a version earlier than 12.8 is possible but complicated. Consider engaging Flexera Software's [Global Consulting Services](#) to help perform upgrades from pre-12.8 versions.

At a high level the steps for upgrading FlexNet Operations are

1. Prepare host machines to meet pre-install requirements.
2. Obtain the upgrade files.
3. Stop FlexNet Operations.
4. Backup your database and preserve any customizations from your existing FlexNet Operations installation.
5. Run the new FlexNet Operations installer.
6. Run FlexNet Setup to configure and deploy the new FlexNet Operations installation.
7. Copy preserved customizations from prior version into the new version.
8. For distributed deployments, perform manual configuration steps in the host machine's file system.
9. In FlexNet Setup, start the FlexNet Operations server.
10. Verify the Upgrade.



Important • If you have customized your FlexNet Operations instance, pay particular attention to the instructions in [Preparing to Upgrade FlexNet Operations](#).

Preparing to Upgrade FlexNet Operations

Observe the following guideline as you prepare to upgrade FlexNet Operations.

Verify Existing FlexNet Operations Version

Before upgrading FlexNet Operations, verify the version of your existing FlexNet Operations installation. To determine which version of FlexNet Operations you are currently running, see the Administer Operations > System Information page in the Operations user interface. The installer requires that you start with FlexNet Operations 12.8 or a later version.

Verify that Host Machines Meet Pre-installation Requirements

Compare the system requirements expressed in the FlexNet Operations release notes with your intended host machines. These machines must meet the system requirements for the version to which you plan to upgrade.

Install any pre-requisite software that does not already exist on the intended host machines.

Review the guidance in [Before Installing FlexNet Operations](#) for more information.

Preserve Modifications and Customizations

Follow the steps, below, to preserve modifications and customizations from your existing FlexNet Operations installation before you attempt to perform an upgrade:

1. Note any modifications you made to your existing FlexNet Operations configuration. These settings are not preserved during an upgrade and must be reconfigured. In particular, note whether you altered
 - Java heap size: Prior versions of FlexNet Operations assigned the Java heap size using the configurator. In FlexNet Operations 2016, the Java VM heap size is set on the **General Settings** tab in FlexNet Setup.
 - Session timeout: Prior versions of FlexNet Operations defined the session timeout on the FlexNet Platform Server configuration page (**Administer Operations > System Configuration > FlexNet Platform Server**). In FlexNet Operations 2016, the session timeout on the same page in the FlexNet Operations Producer Portal (**System > Configure > FlexNet Platform Server**).
 - In FlexNet Operations 2016, the Java VM heap size is set on the **General Settings** tab in FlexNet Setup.
2. Note any unhandled alerts that appear on the Alerts page and process them as appropriate. All existing alerts are deleted during the upgrade process.
3. Stop FlexNet Operations.
4. Back up the following components of your earlier installation:
 - Installation directory
 - Database schema
5. To ensure your customizations are preserved during the upgrade process, observe the following guidelines:
 - Copy your custom directory to a location outside your FlexNet Operations installation before running the version 2016 installer. Ensure that you include files such as JSPs and resource bundles, if any. (This is required because the custom directory in FlexNet Operations 2016 may have a different structure from the earlier version, and the earlier version cannot simply be overwritten.)
 - Review the version 2016 release notes for information about changes that may affect customizations. For example, if Java package names have changed, custom Java classes may have to be recompiled or existing class-related configurations (in System Configuration pages) may have to be changed. Custom Java classes—like ID generators—written for a release built with a previous version of Java must be recompiled. Or if changes in the new release affect the public APIs, custom Java classes may have to be updated.

- New releases often include new or changed entries in FlexNet text properties files. Customizations to those properties files may have to be recreated. However, publisher-defined text properties files are not typically affected.
 - When your FlexNet Operations instance has been upgraded to the new release, add customizations back in to FlexNet Operations incrementally.
6. On Linux systems, add write permissions to the `f1exnet` and `osinfo.sh` files in `ops_install_dir`. Without write permissions, the upgrade process does not replace these files with their new versions.
 7. To upgrade an Oracle installation, CREATE VIEW permission is required for the FlexNet DB User. Add CREATE VIEW permission to this user by using the Enterprise Manager console or SQL. This permission is automatically added by FlexNet Operations for new FlexNet Operations installations.



Note • In an Oracle upgrade, you may encounter errors when upgrading your database, if other FlexNet Operations schemas exist in the same Oracle database instance. The FlexNet Operations upgrade script detects existing tables with the same name from schemas other than the one intended. Because of this false positive, the script fails to create the needed tables in the intended schema and returns an error when it attempts to insert data into these non-existent tables.

For an Oracle upgrade, it is recommended that you select a database instance where no other FlexNet Operations schemas reside, or remove schemas that are not being used.

Testing FlexNet Operations Prior to Upgrading

If you have a previous version of FlexNet Operations installed and in production, install the latest release into a new location for testing before deployment.

When creating a test installation, point to a different database from that which your production installation uses. When you are ready to upgrade your production systems, read this section for guidelines to back up existing data and configuration settings.

Obtaining the Upgrade Files

FlexNet Operations upgrade files are delivered via the FlexNet Operations installer for the current version and configured with FlexNet Setup (installed automatically by the installer).

When you purchase FlexNet Operations, Flexera Software sends a Welcome email with the links and credentials you need to log into the Flexera Software Product and Licensing Center. Following the instructions in the Welcome email, log in to the Product and Licensing Center and navigate to the FlexNet Operations download files. Click the links on the Download page to download the new version of the FlexNet Operations installer appropriate for the platform on which you are running FlexNet Operations.

Contact your Flexera Software representative or Flexera Software support if you have any trouble gaining access to your Flexera Software products on the Product and Licensing Center.

Continue with the instructions in [Installing the Upgrade Version](#).

Installing the Upgrade Version

The following instruction sets explain how to run the FlexNet Operations installer. In a distributed deployment, run the installer on each machine. For best results, install the upgrade version to a new directory rather than overwriting your existing FlexNet Operations installation.

Follow the steps, below, to install FlexNet Operations components. Once the install process is complete, continue with the instructions in [Setting Up the Installation with FlexNet Setup](#) to perform the initial configuration steps and [Verifying the Upgrade](#) to verify the installation.



Task: *To install FlexNet Operations components*

1. On the machine you want to install FlexNet Operations components, start the FlexNet Operations installer. A progress window indicates that InstallAnywhere is preparing the FlexNet Operations installer.
2. On the Welcome panel, click **Next**.
3. On the Choose Install Folder panel, specify the install directory for FlexNet Operations and click **Next**. The default install directory depends on the host operating system.
 - For Windows-based systems, it is C:\Program Files\FlexNet Operations\
 - For Unix-based systems, it is /home/<user>/FlexNet-Operations/



Important • Using spaces in the install directory can cause problems on Unix-based systems. If you specify an install directory other than the default value, avoid using spaces.

4. On the Customization Options panel, choose whether to use the bundled Wildfly server or your own Wildfly server and specify a RabbitMQ URL (if different from the default). Then click **Next**.

Setting	Description
Application Server Settings	<p>Choose whether to use the bundled version of Wildfly or an external version of Wildfly.</p> <ul style="list-style-type: none"> • To use the bundled version of Wildfly, leave the Use Your Own Wildfly Server checkbox unchecked. • To use your own version of Wildfly, check the Use Your Own Wildfly Server checkbox and then specify the location of your Wildfly installation. <p>Important • To use an external Wildfly version, you must have Wildfly already installed on the machine on which FlexNet Operations is being installed. Also, your Wildfly server must be stopped for the duration of the installation and configuration steps.</p>

Setting	Description
RabbitMQ URL	<p>Specify the RabbitMQ AMQP URL or retain the default. For distributed deployments of FlexNet Operations, be sure to create a RabbitMQ account for FlexNet Operations to use.</p> <ul style="list-style-type: none"> If you set up a specific account in RabbitMQ to use for FlexNet Operations messaging, specify the username, password, hostname, port, and (optionally) virtual host using the syntax shown in the installer panel. AMQP://username:password@hostname:port[/vhost] If you install FlexNet Operations components all on a single machine, the default URL value is all that is needed for FlexNet Operations to connect with RabbitMQ. AMQP://guest:guest@localhost:5672

- On the Pre-installation Summary panel, review the installer settings and click **Install**. The installer begins installing and configuring files and shows its progress.
- On the Install Complete panel, the installer reports the result of the install process and shows the URL to use to launch the FlexNet Operations configuration tool, FlexNet Setup (typically, `http://localhost:4321/flexnetsetup`).



Note • By default, the installer attempts to start FlexNet Setup on port 4321; however, if the installer detects that port 4321 is busy, it will attempt to use a different port.

- Click **Done**. The installer attempts to launch FlexNet Setup in your system's default browser.

On Windows systems, continue by configuring installed FlexNet Operations components as shown in [Setting Up the Installation with FlexNet Setup](#).

On Linux systems, review the special instructions, below, and take any additional steps required before you configure installed components with FlexNet Setup.

Special Instructions for Linux Installers

After installing FlexNet Operations components on a Linux system, you must log out and then log in again. (This allows the installer's environment variable changes to take effect.)

Furthermore, if you ran the installer as a non-root user, you must run a script (with sudo access) to install FlexNet Setup as a service and then start the service.



Task: *To complete the FlexNet Operations install on Linux systems*

- At the command line, type

```
sudo sh ops_install_dir/components/tomcat/bin/configure-flexnet-setup-as-service.sh
```

where `ops_install_dir` is the FlexNet Operations installation directory. For example, if you installed FlexNet Operations components to `/usr/home/FNOuser`, you would type

```
sudo sh /usr/home/FNOuser/components/tomcat/bin/configure-flexnet-setup-as-service.sh
```

This script installs FlexNet Setup as a service, but does not start it.

2. To start the service, the user needs to execute the following command.

```
service FlexNetSetup start
```

This command does not require sudo access.

These instructions install the FlexNet Setup service under root context but allow FlexNet Setup and FlexNet Operations, itself, to run as a normal user (not a root user).

Continue with the instructions in [Setting Up the Installation with FlexNet Setup](#) to perform the initial configuration tasks when the installer finishes.

Setting Up the Installation with FlexNet Setup

After the installer completes, run FlexNet Setup to configure each FlexNet Operations component you want to deploy on the current machine.

Table 5-2 • Configuration topics

Topic	Description
About FlexNet Setup	Describes the purpose of FlexNet Setup for deploying and managing FlexNet Operations components.
Starting FlexNet Setup	Explains how to start FlexNet Setup. FlexNet Setup is where you configure FlexNet Operations, deploy configured modules, and start the FlexNet Operations server.
Configuring General Settings	Describes how identify the FlexNet Operations modules to deploy and specify general settings.
Configuring Database Settings	Describes how to configure databases for each FlexNet Operations module to be deployed.
Configuring Advanced Settings	Discusses the settings available on the Advanced configuration page.
Deploying FlexNet Operations Modules	Shows how to deploy configured FlexNet Operations modules on the System Status page.
Starting FlexNet Operations	Explains how to deploy and undeploy FlexNet Operations modules and how to start FlexNet Operations.

About FlexNet Setup

FlexNet Setup is a web application for post-installation setup of FlexNet Operations. The FlexNet Operations installation process installs FlexNet Setup as a service. After you install FlexNet Operations, you use FlexNet Setup to complete the initial setup tasks. Later, you can return to FlexNet Setup to check the status of FlexNet Operations server components, alter setup choices, or stop the FlexNet Operations server.



Tip • Whenever you use FlexNet Setup to alter configuration settings for FlexNet Operations components, remember to first stop the FlexNet Operations server and undeploy all FlexNet Operations components. Then, when your configuration changes are complete, redeploy all components and restart the server. Changes made to deployed components will not be applied in FlexNet Operations until the components are undeployed and redeployed.

Starting FlexNet Setup

At the completion of a successful installation, the FlexNet Operations installer attempts to launch FlexNet Setup automatically. (FlexNet Setup is started as a service on both Windows and Linux systems.) If FlexNet Setup is not running in your web browser, you can open it manually.



Note • If you are signing in to FlexNet Setup for the first time, you must change the password for the default administrator user before you can continue to specify configuration settings.



Task: **To open FlexNet Setup manually**

- Open the following URL in a web browser:

`http://localhost:4321/flexnetsetup`

The default port for FlexNet Setup is 4321. However, if port 4321 is in use when the installer runs, the FlexNet Setup port may change. On the Install Complete panel, the FlexNet Operations installer shows the FlexNet Setup port that was assigned.



Note • If Tomcat is not running, FlexNet Setup will not open.

- To start FlexNet Setup on Windows, go to the Windows Services Console, locate the FlexNet Setup service, and start that service or, at a command prompt, type `net start FlexNetSetup`.
- To start FlexNet Setup on Linux, type `service FlexNetSetup start` at a command prompt.
- If you prefer not to run FlexNet Setup as a service, navigate to `ops_install_dir\components\tomcat\bin` and run `start-flexnet-setup`.



Task: *To sign in to FlexNet Setup*

1. On the Sign In page, provide the default administrator user credentials.
 - Username: **admin**
 - Password: **admin**
2. Click **Log In**.
3. If you are logging in to FlexNet Setup for the first time, follow the instructions, below, to change the administrator password.
 - a. Enter the current password: **admin**.
 - b. Enter a new password.
 - c. Enter the same new password a second time.
 - d. Choose a security question from the list provided.
 - e. Specify an answer to the security question you chose.
 - f. Click **Save**.

After you have successfully signed in, FlexNet Setup shows the General Settings configuration page. Continue with the setup process in [Configuring General Settings](#).

Configuring General Settings

The General Settings configuration page is where you identify FlexNet Operations modules to deploy and optionally specify other general settings.



Important • *FlexNet Operations modules must be undeployed and the FlexNet Operations server must be stopped when you change configuration settings.*



Tip • *Your FlexNet Operations license governs the FlexNet Operations modules that operate for your organization. There is no need to configure settings for FlexNet Operations modules that are not authorized in your organization's license.*



Task: *To configure general settings*

1. On the General Settings configuration page, use the Select Modules to Be Configured checkboxes to select FlexNet Operations modules you want to deploy.
2. Optionally specify Other Configurations settings.

Settings	Instructions
HTTP Port	<p>Identify the port on which FlexNet Operations listens for HTTP communication. If you require a particular port, specify the port number; otherwise, keep the default setting for the embedded Web container: 8888.</p> <p>Ensure this port is open through the firewall on the machine where FlexNet Operations is installed, if the machine hosts a firewall.</p>
Stop Port	<p>Identify the port on which FlexNet Operations listens for a stop message. This is the port on which FlexNet Operations listens for JNDI clients.</p> <p>If you require a particular port, specify the port number; otherwise, keep the default setting: 1199.</p>
Logging Threshold	<p>Set the logging threshold for FlexNet Operations. Choose from</p> <ul style="list-style-type: none">• Errors• Warnings• Information Messages (Default)• Debug Messages <p>The logging threshold expresses the maximum level of detail for the messages written to the FlexNet application log file before FlexNet Operations starts. Only messages at or below the selected level of detail appear in the log.</p>
VM Heap Size	<p>Set the initial and maximum Java Virtual Machine heap size in megabytes. The default settings are</p> <ul style="list-style-type: none">• Initial Size: 1024• Maximum Size: 2048 <p>The maximum application memory limit is set by adjusting the heap size. The limit should be less than 80 percent of the machine's total RAM. If you have performance problems, you may want to increase these settings.</p>
User Data Directory	<p>Only used for distributed deployments, set the location of the User Data Directory. The default directory is</p> <p><i>ops_install_dir\release\flexnet-data\data.</i></p> <p>FlexNet Operations uses this directory for any files necessary for import/export operations and other temporary files.</p>

3. Click **Save**.

FlexNet Setup saves the configuration changes to FlexNet Operations. Changes are applied when FlexNet Operations modules are deployed and the FlexNet Operations server is restarted.

Continue to [Configuring Database Settings](#) to specify database settings for the FlexNet Operations modules you are deploying.

Configuring Database Settings

The Database configuration page is where you specify database settings for the FlexNet Operations modules you are deploying: FlexNet Operations, FlexNet Embedded, FlexNet Usage Management, Cloud Licensing Service, FlexNet Reporting. Here, you first configure and save the Database configuration settings and then initialize or upgrade the database schemas as necessary.



Tip • Your FlexNet Operations license governs the FlexNet Operations modules that operate for your organization. There is no need to configure settings for FlexNet Operations modules that are not authorized in your organization's license.

The database configuration is a two part process:

- [Specifying Database Settings](#)
- [Managing Database Schemas](#)

Specifying Database Settings

Follow the instructions below to set the database type, schema name, and DBMS connection options for each FlexNet Operations module to be deployed on the current machine.



Task: *To configure databases*

1. In FlexNet Setup, click **Configuration** > **Database** to open the Database configuration page.
2. On the Database configuration page, provide settings for each FlexNet Operations module you are deploying on the current machine.

Settings	Instructions
Database Type	Identify the database type to be used for the current module. Choose either Microsoft SQL Server or Oracle .
Schema Name	Specify the name of the database schema for the current module. <ul style="list-style-type: none">• New databases: For new databases, the name you provide becomes the name of the database schema FlexNet Setup creates for this module.• Existing databases: When upgrading from a prior version of FlexNet Operations, specify the schema name of the existing database.

Settings	Instructions
Hostname	Specify a hostname or IP address for the database server.
Port	Specify the port on which the database server is listening. The default port value depends upon the Database Type. <ul style="list-style-type: none">• Microsoft SQL Server: 1433• Oracle: 1521
Database Username	Specify a username for FlexNet Setup to use when making changes to the database.
Database Password	Type the password for the database user.
Confirm Password	Re-type the password for the database user.



Tip • When configuring database settings for multiple modules, consider using the **Use Database Server Host of FlexNet Operations for this Schema** checkbox. If the database server host for one or more modules is the same as the FlexNet Operations module, you can use this checkbox to automatically populate the database configuration settings for these modules. However, each module still requires its own Schema Name.

3. Click **Save**.

FlexNet Setup stores the database configuration settings for each module you are deploying. Continue the deployment by managing the database schemas.

Managing Database Schemas

For each module you are deploying, you must either initialize or upgrade the schema. Producers who are upgrading FlexNet Operations from an earlier version must initialize the database schemas for new modules and upgrade the database schemas for the modules that have existing databases.

For example, a producer who purchased FlexNet Operations plus the Advanced Lifecycle Management and Cloud Licensing Service modules and is upgrading from FlexNet Operations 12.11 Service Pack 2 would *initialize* the schemas for FlexNet Embedded and Cloud Licensing Service but then *upgrade* the schema for the core FlexNet Operations module (and for the FlexNet Reporting module).

Follow the instructions below to upgrade the database schema for each FlexNet Operations module you are upgrading from an earlier FlexNet Operations version.



Note • The **Upgrade** button is enabled on the Manage Schema page only when an existing database for the chosen module is present. Otherwise, only the **Initialize** button is enabled.



Important • When upgrading from a version of FlexNet Operations prior to version 2016, be sure to initialize the FlexNet Embedded database before upgrading the FlexNet Operations database. If the FlexNet Embedded database schema is not present, the FlexNet Operations database upgrade will fail.



Task: *To initialize a schema*

1. On the Database configuration page, click **Manage Schema**. This button opens the Manage Schema page in a popup window.
2. On the Manage Schema page, choose the module upgrade and specify the database account credentials to use for that process.

Settings	Instructions
Which database do you want to initialize/upgrade?	Choose the module for which you want to initialize a schema: <ul style="list-style-type: none"> ● FlexNet Operations ● FlexNet Embedded ● FlexNet Usage Management ● Cloud Licensing Service ● FlexNet Reporting
Database Username	Specify the username of an account with ownership privileges on the database server for the current module.
Database Password	Specify the password for the database username.

3. Click **Initialize**. FlexNet Setup opens a popup window that asks you to confirm your choice.
4. In the popup window, click **Initialize** to confirm and start the process. FlexNet Setup shows the initialization process.
5. When the initialization process is complete, choose whether to finish schema management activities or to manage another schema.
 - To finish schema management activities, click **Close**.
 - To manage the schema of another module, click **Manage Another Database**.



Task: *To upgrade a schema*

1. On the Database configuration page, click **Manage Schema**. This button opens the Manage Schema page in a popup window.
2. On the Manage Schema page, choose the module upgrade and specify the database account credentials to use for that process.

Settings	Instructions
Which database do you want to initialize/upgrade?	Choose the module for which you want to upgrade a schema: <ul style="list-style-type: none">● FlexNet Operations● FlexNet Embedded● FlexNet Usage Management● Cloud Licensing Service● FlexNet Reporting
Database Username	Specify the username of an account with ownership privileges on the database server for the current module.
Database Password	Specify the password for the database username.

3. Click **Upgrade**. FlexNet Setup opens a popup window that asks you to confirm your choice.
4. In the popup window, click **Upgrade** to confirm and start the process. FlexNet Setup shows the upgrade process.
5. When the upgrade process is complete, choose whether to finish schema management activities or to manage another schema.
 - To finish schema management activities, click **Close**.
 - To manage the schema of another module, click **Manage Another Database**.

When database configuration settings are complete and database schemas for all the modules you are deploying have been initialized or upgraded, you can move to the System Status page, apply previous customizations, deploy modules, and start FlexNet Operations.

- If you are upgrading from a prior version of FlexNet Operations that included customizations, continue with [Applying Customizations from the Prior FlexNet Operations Installation](#).
- If you are upgrading from a prior version of FlexNet Operations with no customizations, continue with [Deploying FlexNet Operations Modules](#).



Note • Advanced configuration settings are discussed, generally, in [Configuring Advanced Settings](#), but uses of these settings are covered in instruction sets dedicated to advanced tasks, such as [Configuring FlexNet Operations for Secure Socket Layer](#).

Configuring Advanced Settings

The configuration settings on the Advanced configuration page support configuring FlexNet Operations for secure socket layer communication, server performance, and for the AJP port.

This section describes the settings on the Advanced configuration page, but some of the instructions for using the Advanced configuration page are covered in dedicated sections, such as [Configuring FlexNet Operations for Secure Socket Layer](#).

- Secure Server Settings
- Secure Client Settings
- Other Ports Settings
- Performance Settings

Secure Server Settings

The following secure server settings support configuring the FlexNet Operations server for secure socket layer communication.

Setting	Description
HTTPS Port	<p>The port on which FlexNet Operations listens for HTTPS requests. Default: 8443.</p> <p>FlexNet Operations is always enabled to accept HTTPS requests, but some additional settings must be configured before using SSL. The URL to connect to FlexNet Operations with HTTPS is <code>https://host:port/flexnet</code>, where <code>port</code> is the HTTPS port number.</p> <p>For information about configuring SSL for Wildfly Web container, see Configuring FlexNet Operations for Secure Socket Layer.</p> <p>Note that HTTPS requests can be handled by a full-feature Web server instead of by FlexNet Operations itself.</p>
Keystore Location	<p>The name and location of the keystore on the current machine. Default: <code>ops_install_dir/release/flexnet-data/site/bin/keystore</code>.</p> <p>This keystore file contains the key entry for the certificate that FlexNet Operations uses to provide SSL connections to its clients (for example, browsers or activation utilities). Use the default location only if you are using the bundled keystore or another keystore for testing purposes. Otherwise, point to a keystore outside the FlexNet Operations installation.</p>
Password	<p>The password used to secure the keystore. The same password is used to secure the certificate key.</p>
Confirm Password	<p>The password for the keystore, for confirmation.</p>

Secure Client Settings

The following secure client settings support configuring FlexNet Operations to connect as a client to an SSL server.

Setting	Description
Truststore Location	The name and location of the client-side truststore that contains the trusted certificate entry for a remote SSL server (for example, an LDAP server). Default: <i>ops_install_dir/components/jvm/jre/lib/security/cacerts</i> . Use the default truststore only if you are using the bundled truststore. Otherwise, point to a truststore outside the FlexNet Operations installation.
Password	The password used to secure the truststore. The same password is used to secure the certificate key.
Confirm Password	The password for the truststore, for confirmation.

Other Ports Settings

Other Port Settings includes only one setting: AJP Port.

Setting	Description
AJP Port	FlexNet Operations port for Apache JServ Protocol (AJP) connections. Default: 8009 . This is the port on which the AJP connector listens. The AJP connector integrates FlexNet Operations with a full-function proxy (such as Apache or IIS) server for security or load balancing.

Performance Settings

The following server performance settings are available on the FlexNet Setup's Advanced configuration page.

Setting	Description
Connection Pool Size	The number of connections permitted to the FlexNet Operations server. Default: 100 . Ensure that your database is capable of creating the designated number of connections.
Max Thread Count	The number of threads allocated for the scheduler. Default: 30 .
Transaction Timeout	The transaction timeout time in seconds. Default: 3600 .

Applying Customizations from the Prior FlexNet Operations Installation

In [Preparing to Upgrade FlexNet Operations](#), producers who had modified or customized their FlexNet Operations installation were reminded to save their custom directory. With the exception of email template localizations or customizations, FlexNet Operations 2016 works with all supported customizations from FlexNet Operations 12.8 and later.

If you have not modified your prior FlexNet Operations installation, skip this step and continue with [Deploying FlexNet Operations Modules](#).

The instructions, below, explain how to apply those preserved customizations to the new FlexNet Operations installation. If



Tip • Be sure the server is stopped and FlexNet Operations modules are undeployed when you are making changes to the server.



Task: **To apply prior customizations to a new FlexNet Operations installation**

- Copy the contents of the custom directory you saved from your prior FlexNet Operations installation into the custom directory of your new FlexNet Operations installation.

Continue with [Deploying FlexNet Operations Modules](#).

For more information about customizing FlexNet Operations, see the FlexNet Operations Implementation Guide.

Deploying FlexNet Operations Modules

FlexNet Operations modules, such as the core FlexNet Operations module, the FlexNet Embedded module, and FlexNet Usage Management, are initially undeployed. To be available in FlexNet Operations, a module must first be deployed.



Important • When the core FlexNet Operations module is being deployed on the current machine, it must be the first module deployed.



Task: **To deploy a module**

1. In FlexNet Setup, click **System Status**.
2. On the System Status page, click **Deploy All**. FlexNet Setup opens a popup window to show deployment progress.
3. When all modules are deployed, click **Close** in the popup window.

When all the modules are deployed, you can start the server. Continue with [Starting FlexNet Operations](#).



Tip • Deployed modules can be undeployed by clicking their **Undeploy** button or clicking **Undeploy All**. It is important to stop the FlexNet Operations server and undeploy all modules when making database changes in FlexNet Setup.

Starting FlexNet Operations

Use the Start Server and Stop Server buttons to start, stop, and restart the FlexNet Operations server.

The FlexNet Operations server must be stopped during configuration changes, and all modules undeployed. Then, before any configuration changes will appear in FlexNet Operations, modules must be re-deployed and the server restarted.



Task:

To start the server

- On the System Status page, click **Start Server**.

FlexNet Setup updates the status messages for each module. When all modules are deployed, the System Status page shows the build number for each module and all module status messages read, **Deployed and Started**, you can sign in to FlexNet Operations using the default administrator account.



Tip • Click **Refresh** to update the System Status information.



Tip • When the FlexNet Operations server is running, you can stop it by clicking **Stop Server**.

Producers who have FlexNet Operations modules installed on two or more separate hosts, continue with [Connecting Distributed Deployments](#).

Producers who have all FlexNet Operations modules installed on a single host, continue with [Verifying the Upgrade](#).

Connecting Distributed Deployments

For producers who are upgrading FlexNet Operations in a distributed topology (in which FlexNet Embedded or other modules exist on separate machines) some additional steps are required to connect the FlexNet Operations components.



Tip • These instructions cover connecting FlexNet Operations hosts via HTTP. To use secure socket layer communication between hosts, use HTTPS ports and configure each host for secure socket layer communication. See [Configuring FlexNet Operations for Secure Socket Layer](#).

Connecting the FlexNet Embedded Host

When the core FlexNet Operations module and the FlexNet Embedded module are installed on separate hosts, you must link the two hosts with additional configuration settings.



Task: *To connect the FlexNet Embedded License Fulfillment hosts*

1. On the FlexNet Operations host, open the Producer Portal and change the system configuration setting, License Fulfillment Service URL:
 - a. Sign in to the Producer portal.
 - b. In the Producer Portal, click **System > Configure > FlexNet Operations**. This opens the FlexNet Operations system configuration page.
 - c. On the FlexNet Operations system configuration page, click **External Services Configuration** to expand that group.
 - d. For **License Fulfillment Service URL**, type http://1fs_host:port/1fs/services/FulfillmentService, where *1fs_host* is the hostname of the machine that hosts the FlexNet Embedded module and *port* is the HTTP port for that host.
 - e. Click **Save Configs**.
2. On the machine that hosts the FlexNet Embedded module, open the LFS Configuration Console, edit `boc_endpoint_url` and `ems_endpoint_url`, and save the changes.
 - a. Open the following URL in a Web browser: http://1fs_host:port/1fs/jsp/config.jsp. This URL opens the LFS Configuration Console.
 - b. In the LFS Configuration Console, edit the values for `boc_endpoint_url` and `ems_endpoint_url`. (The new values are the same for both settings.)

Setting	Value
<code>boc_endpoint_url</code>	http://fno_host:port/flexnet/services/EntitlementServiceSOAP where <i>fno_host</i> is the hostname for the machine that hosts the core FlexNet Operations module and <i>port</i> is the HTTP port on the same machine.
<code>ems_endpoint_url</code>	http://fno_host:port/flexnet/services/EntitlementServiceSOAP where <i>fno_host</i> is the hostname for the machine that hosts the core FlexNet Operations module and <i>port</i> is the HTTP port on the same machine.

- c. Click **Save**.



Important • *The configuration settings in the LFS Configuration Console are not preserved if the FlexNet Embedded module is undeployed. Each time this module is re-deployed, you must repeat the steps to set the `boc_endpoint_url` and `ems_endpoint_url` values.*

These steps connect the FlexNet Embedded host and the machine that hosts the core FlexNet Operations module.

Connecting the FlexNet Usage Management Host

Additional configuration steps are required when the FlexNet Usage Management module is running on a different host from those machines that host the core FlexNet Operations module and the FlexNet Embedded module. The following steps connect these host machines.



Task: *To connect the FlexNet Usage Management host*

1. On the FlexNet Operations host, open the Producer Portal and change the system configuration setting: Usage Analytics Service URL:
 - a. Sign in to the Producer portal.
 - b. In the Producer Portal, click **System > Configure > FlexNet Operations**. This opens the FlexNet Operations system configuration page.
 - c. On the FlexNet Operations system configuration page, click **External Services Configuration** to expand that group.
 - d. For **Usage Analytics Service URL**, type http://uas_host:port/uas, where *uas_host* is the hostname of the machine that hosts the FlexNet Usage Management module and *port* is the HTTP port for that host.
 - e. Click **Save Configs**.
2. On the machine that hosts the FlexNet Embedded module, open the LFS Configuration Console, edit `uas_endpoint_url`, and save the change.
 - a. Open the following URL in a Web browser: http://lfs_host:port/lfs/jsp/config.jsp. This URL opens the LFS Configuration Console.
 - b. In the LFS Configuration Console, edit the value for `uas_endpoint_url`.

Setting	Value
<code>uas_endpoint_url</code>	http://uas_host:port/uas/servlet/UasServlet/api/vi/usage where <i>uas_host</i> is the hostname for the machine that hosts the FlexNet Usage Management module and <i>port</i> is the HTTP port on the same machine.

- c. Click **Save**.



Important • The configuration settings in the LFS Configuration Console are not preserved if the FlexNet Embedded module is undeployed. Each time this module is re-deployed, you must repeat the steps to set the `uas_endpoint_url` value.

These steps connect the FlexNet Usage Management host to the machines that host the core FlexNet Operations module and the FlexNet Embedded module.

Connecting the Cloud Licensing Service Host

When the Cloud Licensing Service module is on a different host than the machines on which the core FlexNet Operations module and the FlexNet Embedded are running, additional configuration steps are required to connect these hosts.



Task: To connect the Cloud Licensing Service host

1. On the machine that hosts the Cloud Licensing Service module, start FlexNet Setup.
 - a. On the System Status page in FlexNet Setup, stop the server and undeploy the Cloud Licensing Service module.
 1. Click the **Undeploy** button for Cloud Licensing Service.
 2. When the FlexNet Setup completes the undeployment, click **Stop Server**.
 - b. In the file system of the Cloud Licensing Service host, open the following file in a text editor:
`ops_install_dir\services\cls\cls.properties`
 - c. In `cls.properties`, edit the value for `lfs.url` to http://lfs_host:port/lfs/binary/request, where `lfs_host` is the hostname for the machine that hosts the FlexNet Embedded module and `port` is the HTTP port for that machine.
 - d. Save `cls.properties`.
 - e. In FlexNet Setup, deploy the Cloud Licensing Service and start the server.
 1. Click the **Deploy** button for Cloud Licensing Service.
 2. When FlexNet Setup completes the deployment, click **Start Server**.
2. On the machine that hosts the FlexNet Embedded module, open the LFS Configuration Console, edit `gls_endpoint_url`, and save the change.
 - a. Open the following URL in a Web browser: http://lfs_host:port/lfs/jsp/config.jsp. This URL opens the LFS Configuration Console.
 - b. In the LFS Configuration Console, edit the value for `gls_endpoint_url`.

Setting	Value
<code>gls_endpoint_url</code>	http://cls_host:port/gls/api/1.0 where <code>cls_host</code> is the hostname for the machine that hosts the Cloud Licensing Service module and <code>port</code> is the HTTP port on the same machine.

- c. Click **Save**.



Important • The configuration settings in the LFS Configuration Console are not preserved if the FlexNet Embedded module is undeployed. Each time this module is re-deployed, you must repeat the steps to set the `gls_endpoint_url` value.

These steps connect the Cloud Licensing Service host to the machines that host the core FlexNet Operations module and the FlexNet Embedded module.

Verifying the Upgrade

With FlexNet Operations modules deployed and the server started, you can sign in to FlexNet Operations, verify the server is working, and check the FlexNet Operations version.

**Task:****To sign in to FlexNet Operations**

1. In a Web browser, open the Producer Portal using the hostname of a machine on which FlexNet Operations is running and the HTTP port set on the General configuration page in FlexNet Setup (typically 8888).

`http://hostname:port/flexnet/operations`

1. On the Sign In page, provide the your administrator user credentials.
2. Click **Log In**. FlexNet Operations shows the Producer Portal home page.
3. Click **System > About the Advanced Lifecycle Management Module**. FlexNet Operations opens the System Information page. The first table on this page shows the new version number for FlexNet Operations.

A Note about the Evaluators License and Your FlexNet Operations License

Until you apply your purchased FlexNet Operations license in the Producer Portal, FlexNet Operations runs on the built-in, 60-day evaluators license, which includes licenses for all optional FlexNet Operations modules (such as FlexNet Usage Management and FlexNet Cloud Licensing Service). The evaluators license allows producers to test drive all FlexNet Operations features. However, when you apply your organization's purchased license and restart the server, FlexNet Operations refreshes to show only those features to which your organization is entitled.

FlexNet Operations servers must be connected to the Internet to acquire and renew licenses from Flexera Software servers.



Tip • To apply your organization's purchased license to FlexNet Operations, click **System > Configure > Licensing** in the Producer Portal. Then, provide the FlexNet Embedded URL included in the Welcome Packet sent to you from Flexera Software and click **Save Configs**.

More Post-upgrade Considerations

- Note that your stop port value may be changed to a different setting from the previous version's configurations. This setting can be set in the General settings tab in FlexNet Setup during the upgrade process.
- After upgrading from a previous version, any bindings that you may have configured are returned to their default value in FlexNet Operations 2016. Track zero anchoring is not enabled when upgrading to version 2016. For a discussion of anchoring, see the FlexNet Operations Online Help.

- Receiving application updates through the Web is enabled in FlexNet Operations version 2016. The **System > Configure > Updates > Receive Updates Through Web Application** and **Daily Update Check** configuration settings are not automatically enabled in an upgraded database. It is recommended that these flags be enabled after upgrading your database.
- In addition, after upgrading from previous releases, the Allow Upgrades, Allow Renewals, and Allow Upsells flags on maintenance entities are set to false.

Additional Step for Web Service Users

If you are upgrading from a previous version of FlexNet Operations and are using web services, you must perform the following additional step after installing and configuring the new FlexNet Operations version and before starting the FlexNet Operations server.

Regenerate your Web Service client proxies using the version 2016 WSDL files and not the HTTP URLs. These files are located in the `ops_install_dir/webapp/schema` directory on the FlexNet Operations server and must be copied locally. (Refer to the FlexNet Operations Web Services Guide for more information.)

Applying Hotfixes to FlexNet Operations Components

Hotfix files are delivered in a different format from upgrade files, and the process for applying a hotfix is different from that of installing an upgrade. Follow the steps below to apply a hotfix to FlexNet Operations.



Task: *To apply a hotfix to FlexNet Operations*

1. In FlexNet Setup, click **System Status > Stop Server** to stop FlexNet Operations. When the server has stopped, the Undeploy All button becomes active.
2. On the System Status page in FlexNet Setup, click **Undeploy All**. FlexNet Setup undeploys all FlexNet Operations modules.
3. Copy hotfix archive into the following directory: `ops_install_dir\hotfix\download`.
4. Extract the contents of the archive you copied.



Tip • *If multiple hotfix archives are to be applied at the same time, be sure to extract them in the order in which they were released. Extracting them in the wrong order may overwrite a newer hotfix file with an older one.*

5. Copy the extracted hotfix files from `ops_install_dir\hotfix\download` to `ops_install_dir\hotfix\installed`.
6. On the System Status page in FlexNet Setup, click **Deploy All**. FlexNet Setup deploys all active FlexNet Operations modules.



Tip • Wait for the deploy action to complete before starting the server.

7. On the System Status page, click **Start Server**.

When FlexNet Setup deploys the FlexNet Operations modules, it applies the hotfix changes and then re-applies any preserved customizations to FlexNet Operations.

Verifying the Hotfix

With FlexNet Operations modules deployed and the server started, you can sign in to FlexNet Operations, verify the server is working, and check the FlexNet Operations version.



Task:

To sign in to FlexNet Operations

1. In a Web browser, open the Producer Portal using the hostname of a machine on which FlexNet Operations is running and the HTTP port set on the General configuration page in FlexNet Setup (typically 8888).

`http://hostname:port/flexnet/operations`

1. On the Sign In page, provide the your administrator user credentials.
2. Click **Log In**. FlexNet Operations shows the Producer Portal home page.
3. Click **System > About the Advanced Lifecycle Management Module**. FlexNet Operations opens the System Information page. The first table on this page shows the new version number for FlexNet Operations.



Configuring for Integration with Electronic Software Delivery

After installing and configuring FlexNet Operations, producers who purchase FlexNet Operations with FlexNet Electronic Software Delivery must then integrate their FlexNet Operations instance with their Electronic Software Delivery (ESD) tenant in the Flexera Software cloud. Until that integration is accomplished, ESD features of the Producer Portal and End-User Portal will not function.

Integrating FlexNet Operations with your ESD tenant has two basic requirements:

- You must specify the URL for your ESD tenant in the FlexNet Operations Producer Portal's system configuration settings.
- Your FlexNet Operations instance must be open for communication with the ESD tenant in the Flexera Software cloud.
- Working with your Flexera Software representative, you must tell Flexera Software the hostname for your FlexNet Operations instance.

Configuring External Services URLs for Electronic Software Delivery

To allow your FlexNet Operations instance to connect with your ESD tenant in the Flexera Software cloud, you must set three URLs on the FlexNet Operations system configuration page.



Task:

To configure FlexNet Operations ESD URLs

1. In the Producer Portal, click **System > Configure > FlexNet Operations**. This link opens the system configuration page for FlexNet Operations settings.
2. On the system configuration page for FlexNet Operations, expand the **External Services Configuration** group. The External Services Configuration group is where you set the ESD URLs.

- In the External Services Configuration group specify values for the following settings.

Setting	Value
FlexNet Operations Cloud URL	<p>https://tenantname-esd.flexnetoperations.com/flexnet/operations where <i>tenantname</i> is the tenant name Flexera Software provides to you in the Welcome message.</p> <p>For example, a producer with the tenant name, "rocinante," would specify a FlexNet Operations Cloud URL value of https://rocinante-esd.flexnetoperations.com/flexnet/operations</p>
Electronic Software Delivery Host Name	<p>https://tenantname-esd.flexnetoperations.com/ where <i>tenantname</i> is the tenant name Flexera Software provides to you in the Welcome message.</p> <p>For example, a producer with the tenant name, "canterbury," would specify an Electronic Software Delivery Host Name value of https://canterbury-esd.flexnetoperations.com/</p>
Electronic Software Delivery Service URL	<p>https://tenantname-esd.flexnetoperations.com/esd-service/esd where <i>tenantname</i> is the tenant name Flexera Software provides to you in the Welcome message.</p> <p>For example, a producer with the tenant name, "dulcinea," would specify a Electronic Software Delivery Service URL value of https://dulcinea-esd.flexnetoperations.com/esd-service/esd</p>

- Click **Save Configs**.

Saving these three values completes the system configuration settings the Producer Portal requires to communicate with your Electronic Software Delivery tenant.

If your FlexNet Operations instance runs behind a firewall, you must also be sure to open the FlexNet Authentication to external connections.

Enabling Inbound Communication from the Flexera Software Cloud

Most producer restrict external connections to FlexNet Operations for security reasons while selectively exposing the End-User Portal and other necessary elements to the public. To integrate your FlexNet Operations instance with cloud-hosted ESD functionality, you must also expose FlexNet Authentication to inbound communication.

FlexNet Authentication can be exposed to external connections at `http://hostname:port/flexnet/services/FlexNetAuthentication`, where *hostname* is the hostname for your FlexNet Operations instance and *port* is the HTTP port.

Remember to contact your Flexera Software representative to share your FlexNet Operations hostname. Flexera Software needs the hostname to enable communication with your FlexNet Operations instance from your ESD tenant in the Flexera Software cloud.



Configuring FlexNet Operations for Secure Socket Layer

Secure Socket Layer (SSL) allows Web servers and Web clients to communicate over a secured connection using the HTTPS protocol where both the server and the client encrypt data before sending it. If you choose not to have a full-featured Web server handle HTTPS requests for FlexNet Operations, FlexNet Operations itself can act as an SSL server to Web browsers or Web service client applications. FlexNet Operations can also act as an SSL client to a remote server, such as an LDAP (Lightweight Directory Assistance Protocol) server. HTTPS is always enabled in FlexNet Operations, but the secure server keystore and the secure client truststore may have to be configured.

Table B-1 • Sections in this appendix

Topic	Description
Configuring Server-Side Secure Socket Layer	Covers generating a test certificate, configuring FlexNet Operations with the test certificate, verifying the test certificate, obtaining a trusted certificate, configuring FlexNet Operations with a permanent certificate, and disabling weak ciphers.
Configuring Client-Side Secure Socket Layer	Covers importing an SSL server's certificate into the truststore, configuring FlexNet Operations with a new truststore, and verifying the trusted connection.

Configuring Server-Side Secure Socket Layer

When a Web browser or Web service client connects directly to FlexNet Operations using HTTPS, SSL authenticates the credentials of FlexNet Operations. Certificates to authenticate the FlexNet Operations SSL server can be self-signed. Trusted certificates are issued by a recognized certificate authority.

The following activities are briefly described in this section:

- Generating a Test Certificate
- Configuring FlexNet Operations with the Test Certificate
- Testing that the HTTPS connection to FlexNet Operations works (testing the SSL listener)
- Obtaining a Trusted Certificate
- Configuring FlexNet Operations with a Permanent Certificate (meaning the trusted certificate)
- Configuring Secure Socket Layer in FlexNet Operations to Disable Weak Ciphers

Generating a Test Certificate

A keystore containing a public key/private key pair and an expiring, self-signed certificate for testing SSL is shipped with FlexNet Operations. If the shipped keystore has expired, another test keystore can be generated using `keytool`, a command-line utility provided in the Java JDK. The following instructions enable you to generate a simple key pair and certificate keystore that is valid for three months. This keystore allows you to test that the SSL listener can run, but its certificate is also self-signed and is not trusted by the browser.



Task: *To generate a test certificate from scratch*

1. Install or locate the Java JDK. Verify that the `keytool` utility is accessible at the command line.
2. At a command line, generate a simple key pair and non-trusted certificate into a keystore file named `keystore` in the current directory by typing:

```
keytool -keystore keystore -alias tomcat -genkey -keyalg RSA
```

You are prompted to provide answers to several questions for the certificate. Press the Enter key to submit each of your answers. If you answer these questions accurately for the test certificate, the certificate that you generate can be used as the basis of your trusted certificate that you obtain from a certificate authority.

Question	Description
Enter keystore password:	Type the password for the keystore. The default SSL keystore password for FlexNet Operations is f1exnet. The password is displayed in plain text. Note the password that you enter. In the next section, Configuring FlexNet Operations with the Test Certificate, you will enter these passwords on the Advanced configuration page in FlexNet Setup.
What is your first and last name?	Type the fully qualified domain name of the machine on which FlexNet Operations is installed.
What is the name of your organizational unit?	Type the name of your division or group in your company.
What is the name of your organization?	Type the name of your company.
What is the name of your City or Locality?	Type the name of your city.
What is the name of your State or Province?	Type the name of your state or province.
What is the two-letter country code for this unit?	Type the two-letter code for your country.
Is entry correct?	Check that the entries you typed are correct, and then type yes or no . Default is no.
Enter key password for <tomcat> (RETURN if same as keystore password):	Press Enter to use the same password for the Tomcat SSL key that the keystore uses. You must use the same password.

Configuring FlexNet Operations with the Test Certificate

Follow the instructions, below, to configure FlexNet Operations with the test certificate you just generated.



Task: *To configure FlexNet Operations with the test certificate*

1. On the machine on which FlexNet Operations components are installed, copy the test keystore file that you just generated, keystore, to a location accessible from, but outside of, the FlexNet Operations installation.
2. In FlexNet Setup, navigate to the System Status page and click **Stop Server** to stop FlexNet Operations.
3. On the System Status page, click **Undeploy All**.
4. In FlexNet Setup, click **Configure** > **Advanced** to show the Advanced configuration page.
5. On the Advanced configuration page, specify Secure Server settings.

Settings	Instructions
HTTPS Port	Enter a new value for HTTPS Port or retain the default setting, 8443 .
Keystore Location	Modify the Keystore Location setting to match the location of the test keystore.
Password	Enter the keystore password for the certificate. (The default password for the bundled keystore is flexnet .)
Confirm Password	Enter the keystore password again.

6. Click **Save**. The site directory is re-created to reflect the new configuration settings.
7. Return to the System Status page and click **Deploy All**.
8. On the System Status page, click **Start Server** to restart FlexNet Operations.

FlexNet Operations is reconfigured for Secure Socket Layer communication.

Verifying the Test Certificate

The previous steps configure FlexNet Operations to accept HTTPS requests. You must now verify that you can log in to FlexNet Operations using HTTPS.



Task: *To verify the test certificate*

1. Import the trusted certificate you generated (exported from the keystore) into a browser or web service client implementation.

Because you generated the certificate yourself and you are not a known certificate authority, import the trusted certificate (exported from the keystore) into a browser or Web service client implementation.

In Internet Explorer, click **Tools** > **Internet Options** > **Content** > **Certificates**.

In Firefox, click **Edit** > **Preferences** > **Advanced** > **Security** > **View Certificates** > **Web Sites**.
2. Browse to the URL where FlexNet Operations is running.

The URL will be in the format

`https://hostname.port>/flexnet`

- *hostname* is the fully qualified domain name for the host that you specified when you generated the keystore.
- *port* is the HTTPS port number you configured for FlexNet Operations.

The login page for FlexNet Operations is displayed.



Note • If connections to FlexNet Operations come only from inside your organization, a non-expiring, self-signed certificate that is added to each internal user's Web browser certificate store may be adequate. See the options for `keytool` to generate a non-expiring, self-signed certificate.

Obtaining a Trusted Certificate

For optimal security, if users are connecting to FlexNet Operations from outside your organization, it is recommended that you obtain a trusted certificate from a certificate authority. Each certificate authority has its own instructions, but all require that you submit a certificate signing request (CSR) that you can generate from the test keystore using the `keytool` utility.



Task: *To obtain a trusted certificate*

1. Generate a CSR in a file named `tomcat.csr` for a key pair and certificate already in a keystore called `keystore` in the current directory by typing

```
keytool -certreq -keyalg RSA -alias tomcat -file tomcat.csr -keystore keystore
```

2. Submit this CSR as instructed by the certificate authority you chose.
3. After you receive a trusted certificate from the certificate authority, load the certificate authority's chain (or root) certificate (in a file named `rootcrt`) into the keystore used to generate the CSR. If the certificate is in a format parsable by the `keytool` utility, type

```
keytool -keystore keystore -import -alias root -file rootcrt -trustcacerts
```

If the certificate is not in a format parsable by the `keytool` utility, see documentation from the certificate authority for instructions on loading the root certificate.

4. After the root certificate has been loaded, load the new certificate (in a file named `newcrt`) into the keystore used to generate the CSR. If the certificate is in a format understood by the `keytool` utility, type

```
keytool -keystore keystore -import -alias tomcat -file newcrt -trustcacerts
```

If the certificate is not in a format understood by the `keytool` utility, see documentation from the certificate authority.

Configuring FlexNet Operations with a Permanent Certificate

This step is necessary to do the following:

- Point to a central repository of keystores or truststores maintained by your organization.
- Configure the location of a permanent certificate, whether trusted or self-signed.



Task: *To configure FlexNet Operations with a permanent trusted or self-signed certificate*

1. On the machine on which FlexNet Operations components are installed, copy the permanent keystore file that you just generated, keystore, to a location accessible from, but outside of, the FlexNet Operations installation, or point to a keystore maintained by your organization.
2. In FlexNet Setup, navigate to the System Status page and click **Stop Server** to stop FlexNet Operations.
3. On the System Status page, click **Undeploy All**.
4. In FlexNet Setup, click **Configure > Advanced** to show the Advanced configuration page.
5. On the Advanced configuration page, specify Secure Server settings.

Settings	Instructions
HTTPS Port	Enter a new value for HTTPS Port or retain the default setting, 8443 .
Keystore Location	Modify the Keystore Location setting to match the location of the permanent keystore.
Password	Enter the keystore password for the certificate.
Confirm Password	Enter the keystore password again.

6. Click **Save**. The site directory is re-created to reflect the new configuration settings.
7. Return to the System Status page and click **Deploy All**.
8. On the System Status page, click **Start Server** to restart FlexNet Operations.
9. For producers configuring FlexNet Operations with a self-signed certificate, import the certificate into browsers as described in [Verifying the Test Certificate](#). (For producers configuring FlexNet Operations with a trusted certificate from a known certificate authority, it is unnecessary to import the certificate.)

FlexNet Operations is reconfigured for Secure Socket Layer communication using the permanent certificate.

Configuring Secure Socket Layer in FlexNet Operations to Disable Weak Ciphers

Insufficient transport layer protection allows SSL/TLS communication to be exposed to untrusted third parties, providing the opportunity to steal sensitive information. SSL/TLS support in FlexNet Operations can be configured to disable weak cipher suites like RC4-MD5, RC4-SHA, and ECDHE-RSA-RC4-SHA to prevent vulnerability.

These changes must be made to FlexNet Operations while the FlexNet Operations modules are deployed but while the FlexNet Operations server is stopped.



Task: *To disable weak ciphers*

1. In FlexNet Setup, click **System Status** > **Stop Server** to stop the Wildfly application server on which FlexNet Operations is running.
2. With the server stopped, open `standalone-full.xml` in a text editor. This file is at `wildfly_dir\standalone\configuration\standalone-full.xml`, where `wildfly_dir` is the root directory for Wildfly. For example, if you chose to use the embedded Wildfly server when you installed FlexNet Operations, `standalone-full.xml` would be in `ops_install_dir\components\wildfly\standalone\configuration`.
3. In `standalone-full.xml`, modify the undertow subsystem to enable only TLSv1.2 protocol and add a strong cipher list in the `enabled-cipher-suites` attribute.

```
<subsystem xmlns="urn:jboss:domain:undertow:1.2">
  <server name="default-server">
    <https-listener name="default-https" socket-binding="https" security-realm="UndertowRealm"
      enabled-protocols="TLSv1.2"
      enabled-cipher-suites="TLS_RSA_WITH_AES_128_GCM_SHA256,
        TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256"/>
    ...
  </server>
  ...
</subsystem>
```

The above setting enables 128-bit AES-based ciphers, which are stronger, to be used with SSL/TLS. Most recent browser versions support these ciphers, ensuring protection for SSL communication between browsers and FlexNet Operations.

4. In FlexNet Setup, click **System Status** > **Start Server** to restart FlexNet Operations.



Important • If the FlexNet Operations core module is undeployed and redeployed after this change, these changes will be lost. To re-enable strong ciphers, you must repeat this procedure manually.

Configuring Client-Side Secure Socket Layer

FlexNet Operations can also be a client on an SSL connection to a remote server, such as an LDAP server. When FlexNet Operations connects to an SSL server as a client, FlexNet Operations receives a certificate of authentication from the SSL server. FlexNet Operations then checks the certificate against the set of certificates in its truststore (client keystore) to see if it is trusted. The default truststore is located in the JRE bundled with FlexNet Operations at `ops_install_dir\components\jvm\lib\security\cacerts`.

If the SSL server's certificate cannot be validated with the certificates in the default truststore, the SSL server's certificate must be added to the FlexNet Operations truststore before the connection can be established.

Importing a Secure Socket Layer Server's Certificate into the Truststore

This step is needed only if the SSL server's certificate cannot be validated with certificates already in the default truststore.



Task: *To import an SSL server's certificate into the FlexNet Operations truststore*

1. Obtain a certificate, called `servcrt` in these instructions, from the SSL server administrator.
2. Copy the default truststore, called `<truststore>` in these instructions, from `ops_install_dir\components\jvm\lib\security\cacerts` to a location accessible from, but outside of, the FlexNet Operations installation.
3. Install or locate the Java JDK. Verify that the `keytool` utility is accessible at the command line in the new truststore location.
4. Load the SSL server certificate into the new truststore location.

If the certificate is in a format parsable by the `keytool` utility, type

```
keytool -keystore <truststore> -import -alias mykey -file servcrt -trustcacerts
```

If it is not in a format parsable by the `keytool` utility, consult the documentation from the SSL server administrator.

Configuring FlexNet Operations with a New Truststore

Follow the instructions, below, to configure FlexNet Operations with a certificate for the SSL server to which you want FlexNet Operations to connect

This step is necessary if

- You want to point to a central repository of keystores or truststores maintained by your organization.
- You load a new certificate into the default truststore and have to configure its new location.



Task: *To configure FlexNet Operations with a certificate for a different SSL server*

1. In FlexNet Setup, navigate to the System Status page and click **Stop Server** to stop FlexNet Operations.
2. On the System Status page, click **Undeploy All**.
3. In FlexNet Setup, click **Configure** > **Advanced** to show the Advanced configuration page.
4. On the Advanced configuration page, specify Secure Client settings.

Settings	Instructions
Truststore Location	Modify the Truststore Location setting to match the location of the truststore containing the SSL server's certificate.
Password	Enter the password for the truststore. (By default, the password from the FlexNet Operations JRE is changeit .)
Confirm Password	Enter the truststore password again.

5. Click **Save**. The site directory is re-created to reflect the new configuration settings.
6. Return to the System Status page and click **Deploy All**.
7. On the System Status page, click **Start Server** to restart FlexNet Operations.

Verifying the Trusted Connection

Now that you have reconfigured FlexNet Operations to connect to the SSL server, verify that you can connect to the SSL server using FlexNet Operations.

Appendix B Configuring FlexNet Operations for Secure Socket Layer

Configuring Client-Side Secure Socket Layer



Uninstalling FlexNet Operations

Follow the instructions, below, to uninstall FlexNet Operations.



Tip • Before you run the uninstaller, consider exporting the configuration settings and saving any customizations. For producers who plan to re-install a clean version of FlexNet Operations, retaining the configuration settings from the current installation and then importing them into the new instance may save time. Likewise, producers who save the contents of the `custom` directory can quickly re-apply their customizations in the new installation.



Task:

To uninstall FlexNet Operations

1. In FlexNet Setup, navigate to the System Status page and click **Stop Server** to stop FlexNet Operations.
2. Close all files and directories in the `ops_install_dir` tree.
3. Run the FlexNet Operations uninstaller in the `ops_install_dir/_uninstaller` directory.

The uninstaller removes all files in the `ops_install_dir/` tree except those in the `config`, `custom`, `data`, `db`, `extension`, and `logs` directories. If you do not want to save any of the files in these directories, completely uninstall FlexNet Operations by deleting the `ops_install_dir` directory after the uninstaller completes.

- If FlexNet Operations was installed to run as a Windows service, the uninstaller also stops and uninstalls the Windows service.
- If you set up FlexNet Operations to start on boot in UNIX, delete the service script from where you installed it.

