Quest™

Foglight® 8.1.0

Installation and Setup Guide

Installing on a UNIX System with an Embedded PostgreSQL Database

© 2025 Quest Software Inc.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, and Where next meets now are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. "Apache HTTP Server", Apache, "Apache Tomcat" and "Tomcat" are trademarks of the Apache Software Foundation. Google is a registered trademark of Google Inc. Android, Chrome, Google Play, and Nexus are trademarks of Google Inc. Red Hat, JBoss, the JBoss logo, and Red Hat Enterprise Linux are registered trademarks of Red Hat, Inc. in the U.S. and other countries. CentOS is a trademark of Red Hat, Inc. in the U.S. and other countries. Fedora and the Infinity design logo are trademarks of Red Hat, Inc. Microsoft, .NET, Active Directory, Internet Explorer, Hyper-V, Office 365, SharePoint, Silverlight, SQL Server, Visual Basic, Windows, Windows Vista and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. AIX, IBM, PowerPC, PowerVM, and WebSphere are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Java, Oracle, Oracle Solaris, PeopleSoft, Siebel, Sun, WebLogic, and ZFS are trademarks or registered trademarks of Oracle and/or its affiliates in the United States and other countries. SPARC is a registered trademark of SPARC International, Inc. in the United States and other countries. Products bearing the SPARC trademarks are based on an architecture developed by Oracle Corporation. OpenLDAP is a registered trademark of the OpenLDAP Foundation. HP is a registered trademark that belongs to Hewlett-Packard Development Company, L.P. Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. MySQL is a registered trademark of MySQL AB in the United States, the European Union and other countries. Novell and eDirectory are registered trademarks of Novell, Inc., in the United States and other countries. VMware, ESX, ESXi, vSphere, vCenter, vMotion, and vCloud Director are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. Sybase is a registered trademark of Sybase, Inc. The X Window System and UNIX are registered trademarks of The Open Group. Mozilla and Firefox are registered trademarks of the Mozilla Foundation. "Eclipse", "Eclipse Foundation Member", "EclipseCon", "Eclipse Summit", "Built on Eclipse", "Eclipse Ready" "Eclipse Incubation", and "Eclipse Proposals" are trademarks of Eclipse Foundation, Inc. IOS is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Apple, iPad, iPhone, Mac OS, Safari, Swift, and Xcode are trademarks of Apple Inc., registered in the U.S. and other countries. Ubuntu is a registered trademark of Canonical Ltd. Symantec and Veritas are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. OpenSUSE, SUSE, and YAST are registered trademarks of SUSE LCC in the United States and other countries. Citrix, AppFlow, NetScaler, XenApp, and XenDesktop are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. AlertSite and DéjàClick are either trademarks or registered trademarks of Boca Internet Technologies, Inc. Samsung, Galaxy S, and Galaxy Note are registered trademarks of Samsung Electronics America, Inc. and/or its related entities. MOTOROLA is a registered trademarks of Motorola Trademark Holdings, LLC. The Trademark BlackBerry Bold is owned by Research In Motion Limited and is registered in the United States and may be pending or registered in other countries. Quest is not endorsed, sponsored, affiliated with or otherwise authorized by Research In Motion Limited. Ixia and the Ixia four-petal logo are registered trademarks or trademarks of Ixia. Opera, Opera Mini, and the O logo are trademarks of Opera Software ASA. Tevron, the Tevron logo, and CitraTest are registered trademarks of Tevron, LLC. PostgreSQL is a registered trademark of the PostgreSQL Global Development Group. MariaDB is a trademark or registered trademark of MariaDB Corporation Ab in the European Union and United States of America and/or other countries. Vormetric is a registered trademark of Vormetric, Inc. Intel, Itanium, Pentium, and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries. Debian is a registered trademark of Software in the Public Interest, Inc. OpenStack is a trademark of the OpenStack Foundation. Amazon Web Services, the "Powered by Amazon Web Services" logo, and "Amazon RDS" are trademarks of Amazon.com, Inc. or its affiliates in the United States and/or other countries. Infobright, Infobright Community Edition and Infobright Enterprise Edition are trademarks of Infobright Inc. POLYCOM®, RealPresence® Collaboration Server, and RMX® are registered trademarks of Polycom, Inc. All other marks and names mentioned herein may be trademarks

of their respective companies.

Legend

CAUTION: **A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

WARNING: **A WARNING icon indicates a potential for property damage, personal injury, or death.**

IMPORTANT NOTE, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Foglight Installation and Setup Guide Foglight Version - 8.1.0

Contents

Before Installing Foglight 6
What is Foglight? 6
Hardware requirements and guidelines 6
Planning your installation 7
Using the embedded database 8
Licensing 8
Installation modes 9

Installing Foglight 12
Preparing to install 12
Installing a new version of the Management Server 13
Installing the Management Server - Standard Install option 13
Installing the Management Server - Custom Install option 14
Foglight Server Startup page 18
Next steps 18
Embedded Agent Manager 18
Installed directories 19
Foglight settings 20
Editing the *server.config* file 21
Importing self-signed certificates to Foglight TrustStore 21
Setting up an encrypted LDAP connection with SSL 22
Using encryption when sending email from Foglight 22
Setting parameters for an embedded database 22
Configuring ports 23
Setting memory parameters for the server 24
Adding command-line options 24
Binding the Management Server to an IP address 25
Configuring Foglight to use stronger encryption 25
Configuring Foglight to use the HTTPS port 26
Setting the length of Foglight sessions 28
Configuring anti-virus exclusion settings 28
Uninstalling Foglight 29
Upgrading the Management Server 29

Running the Management Server 30
Initializing the database 30
Accessing the database 30
Starting and stopping the Management Server 30
Starting the Management Server 31
Stopping the Management Server 31
Logging in to Foglight 31
Monitoring the Management Server host 32
Next steps 32

Running the Management Server FAQ 32

Installing and Upgrading Cartridges 34

Installing Agents 36
Agent installers 36
Remote agent installation 37

Appendix: Switching from an Embedded to an External Database 39

About Us 40
Technical support resources 40

1

Before Installing Foglight

This guide provides instructions for installing, configuring, and starting Foglight®.

This section provides setup information and an initial overview of installing Foglight:

- What is Foglight?
- Hardware requirements and guidelines
- Planning your installation

IMPORTANT: See the *Release Notes* for the cartridges you are installing. These documents contain important information about the latest versions of these components, such as information about late-breaking changes, updates, and known and resolved issues.

What is Foglight?

Foglight solution simplifies application performance monitoring and reduces the skills and effort required to manage applications, the user experience, and the supporting infrastructure.

Unlike other solutions, Foglight uses a single code base, and has a model-driven design that couples fast deployment and accelerated time-to-value. It offers the modular flexibility required to deliver a range of capabilities and sophistication to meet the needs of any organization, from organizations focused on technology-centric monitoring to organizations that have completed the transition to application-centric or transactional monitoring.

Foglight performs equally well in physical, virtual, and mixed infrastructure environments, providing visibility into issues affecting the application and end user experience. Intuitive workflows help you quickly move from the symptom to the root cause in the application, database, infrastructure, or network to resolve issues, reducing mean time to resolution. Predefined and drag-and-drop dashboards provide insight that is tailored to each stakeholder. By offering comprehensive visibility into your monitored environment, Foglight helps ensure that cross-functional teams collaborate on and prioritize issues that matter most to the business.

Hardware requirements and guidelines

The hardware requirements to run Foglight can vary widely, based on a number of factors, including:

- The number and type of agents that are being used
- The persistence and data roll-up policies
- Agent configuration settings

Before doing a production implementation, conduct a proper scoping and sizing exercise with a qualified Quest Software Inc. representative. Arrange for a sizing analysis by contacting your Quest Software Inc. Sales Representative.

Installation recommendations

Running Foglight requires the following components:

- Foglight Management Server
- Foglight database repository

These components can be installed on a single tier or on multiple tiers. It is critical to realize that both the Management Server and database repository require dedicated resources to support them. In order to help facilitate sizing, the resources required to support each component are addressed separately. They can either be summed to support a single-tier installation, or treated independently as the requirements for each server in a two-tier installation.

Hardware requirements

For the current single- and multi-tier hardware requirements, see the *Foglight online Help*.

Planning your installation

Before you install Foglight, review the components that you are going to install. Ensure that you have the necessary information, such as port numbers and server names, and the locations where you are going to install the components.

NOTE: This guide provides instructions for installing new instances of Foglight only, not for upgrading Foglight.
For best practices for upgrading Foglight, an overview of the upgrade process, and upgrade procedures, see the *Upgrade Guide*.

NOTE: You can choose to use an embedded database or an external database. The instructions in this guide are for embedded database installations only.

The following list summarizes the main stages involved in installing and configuring Foglight:

Stage 1: Install the Management Server and configure the Management Server and database. The Management Server is the data collection and processing server.

Stage 2: Start the Management Server and log in.

NOTE: If you are using the embedded database, the database initialization occurs when you start the Management Server.

Stage 3: Install and configure cartridges. Cartridges extend the functionality of Foglight, and are installed on the machine hosting the Management Server. A cartridge contains one or more cartridge components, such as agents for deployment, communication capabilities, modifications to the way that data is transformed or handled, rules, reports, and views.

Stage 4: Install, configure, and start the Foglight Agent Manager. The Agent Manager is a client that manages agents installed on monitored hosts.

Stage 5: Install and configure agents. Agents are deployed on machines in your monitored environment and send data to the Management Server. There are several types of agents. One or more instances of each type of agent managed by the Agent Manager can be deployed per host. For example, there is an agent that collects metrics from the operating system of the host machine. There are also agents that are embedded into systems or the software that they monitor.

IMPORTANT: Install and configure the Agent Manager before deploying agents that are installed on a monitored host.

For more information, see these topics:

- Using the embedded database
- Licensing
- Installation modes

Using the embedded database

Foglight offers the option to use PostgreSQL® as an embedded database. The lifecycle of the embedded database matches that of the Management Server. If the Management Server is stopped or started, the embedded database is automatically stopped or started.

For instructions to migrate from using an embedded PostgreSQL® database with the Management Server to using an external PostgreSQL database, see Appendix: Switching from an Embedded to an External Database.

Licensing

This section provides information about licensing for Foglight.

IMPORTANT: See *Foglight online Help* for information about license requirements, managing licenses, and the different categories of cartridges (based on their license requirements).

Providing a license file during installation

You can install a license file during installation if you perform a Custom Install. See Step 13: Add Foglight license file in Installing a new version of the Management Server.

Importing a license file after installation

You can also import a license after installing Foglight. There are three ways of providing a license file to the Management Server after installation.

Using the manual process

- Move an existing license file into the *<foglight_home>/license* folder.

Using the Foglight Administration module

- Upload a license file using the Foglight Administration module. See *Foglight online Help* for instructions.

Using the command line

1. Start the Foglight Management Server.
2. Ensure that `JAVA_HOME` is set.
3. If you have not already done so, extract the file *fglcmd.zip* in *<foglight_home>/tools*.
4. Upload a license by navigating to *<foglight_home>/tools* and entering the following command:

   ```
   fglcmd -usr <username> -pwd <password> -cmd license:import -f <license_file>
   ```

   The preceding command assumes that you are using the default port 8080 and *localhost*. If you are not running with these default values, use the following options to indicate server and port:

   ```
   -port <xx> -srv <server_name>
   ```

For example, if you want to connect to the Management Server using the default HTTPS port, include the option `-port 8443` with the `fglcmd` command.

NOTE: See the *Foglight online Help* for information about running the fglcmd utility and the options that can be used with fglcmd, including additional license-management commands.

Installation modes

The default mode for the installer is the graphical user interface mode. On UNIX® systems, in cases where a graphics display is not available, the Foglight installer can be started in command-line mode by using the console mode or silent mode.

Console mode

For Foglight systems, the console mode is available on UNIX® only for Linux®.

For Foglight Evolve, the console mode is available on UNIX only for Linux.

In console mode, the install instructions are in text format, but otherwise are the same as the graphical user interface install.

To execute the console mode, type the following command:

Linux® - Foglight only

```
Foglight-8_1_0-install_linux-x86_64.bin -i console
```

Linux® - Foglight Evolve

```
Foglight_Evolve-x_x_x-install_linux-x86_64.bin -i console
```

Silent mode

In silent mode, a properties file is used to feed in the installation parameters. The file consists of a list of key-value pairs, which are described in the following table.

To run the installer in silent mode:

Linux® - Foglight only

```
Foglight-8_1_0-install_linux-x86_64.bin -i silent
```

Linux® - Foglight Evolve only

```
Foglight-Evolve-x_x_x-install_linux-x86_64.bin -i silent
```

To use a specific properties file in silent mode, append the following option:

```
-f <fms_silent_install>.properties
```

The installer loads the specified properties file. When the file name and installer prefix are the same, the installer uses the properties automatically.

NOTE: In certain configurations the Management Server uses ports in addition to the ones that you set using the silent installer. See the *Foglight online Help* for details.

The following table lists the properties available for configuring a silent installation, and their default values.

Table 1. Properties available for configuring a silent installation

Property	Description	Default
FMS_ADMIN_PASSWORD	Administrator password for Foglight.	foglight
FMS_CLUSTER_MCAST_PORT	Cluster Multicast port.	45566
FMS_DB	Allows you to specify whether the database is embedded or external. Must be set to external if FMS_HA_MODE=1	embedded
FMS_DB_ADMIN_PASSWORD	Allows you to specify the password for the database administrator user account. This setting is not required if FMS_DB=embedded.	None.
FMS_DB_ADMIN_USER	Allows you to specify the database administrator user account. This setting is not required if FMS_DB=embedded.	foglight
FMS_DB_HOST	Allows you to specify the host name of the database machine. This setting is not required if FMS_DB=embedded.	127.0.0.1
FMS_DB_NAME	Allows you to specify the name of the Foglight database. This setting is not required if FMS_DB=embedded.	foglight
FMS_DB_PORT	User-defined port for the database.	15432
FMS_DB_SETUPNOW	0 = Set up the database after installation is complete. 1 = Set up the database as part of the installation.	1
FMS_DB_TYPE	Specifies the database type. This setting is not required if FMS_DB=embedded.	postgresql
FMS_DB_USER	Database user name.	foglight
FMS_DB_USER_PASSWORD	Database user password.	foglight
FMS_FEDERATION_PORT	Federation communication port.	1099
FMS_HA_MODE	0 = Run Foglight in standalone mode. 1 = Run Foglight in HA (High Availability) mode.	0
FMS_HA_PARTITION	High Availability (HA) partition name. Only required if FMS_HA_MODE=1.	FMS_HA
FMS_HTTP_PORT	HTTP port.	8080
FMS_HTTPS_ONLY	0 = Do not run Foglight in secure mode (HTTPS) only. 1 = Run Foglight in secure mode (HTTPS) only.	0
FMS_HTTPS_PORT	HTTPS port.	8443
FMS_LICENSE_AGREEMENT	License agreement acknowledgment.	yes
FMS_LICENSE_FILE	Allows you to add a license file by specifying the path to the license. **NOTE:** See the *Foglight online Help* for information about license requirements, managing licenses, and the different categories of cartridges (based on their license requirements).	None (the license file you specify is validated).
FMS_QP5APP_PORT	The port for an embedded query engine.	8448
FMS_RUN_NOW	Starts the Management Server at the end of the installation.	false
FMS_UPGRADE	Only required to update an existing installation, in which case it must be set to 1.	1

Table 1. Properties available for configuring a silent installation

Property	Description	Default
INSTALLER_UI	The property is set to SILENT for silent mode. This setting is the default one and is mandatory.	SILENT
USER_INSTALL_DIR	The Foglight installation directory. If you want to upgrade an existing installation, specify the path to the existing installation directory here (and ensure that FMS_UPGRADE is set to 1).	None.
USER_SHORTCUTS	Sets the shortcut location.	None.
FMS_SERVICE_LINUX_ENABLED	For enabling Foglight as a Linux service, in which case it must be set to 1.	0
FMS_SERVICE_LINUX_VALID_PLATFORM	For enabling Foglight as a Linux service, in which case it must be set to true.	false
FMS_SERVICE_LINUX_RUN_USER	The username who is used to run the Foglight.	None.
FMS_FIPS_APPROVED_ONLY_MODE	Enable FIPS Compliance mode for the Foglight server.	false

2

Installing Foglight

The Foglight installer allows you either to install a new instance of the Foglight Management Server or to upgrade an existing installation of a Foglight Management Server. This guide provides the procedures for a new installation of the Management Server. For upgrade procedures, see the *Upgrade Guide*.

NOTE: The Management Server should be installed on a dedicated machine.

For more details, see these topics:

- Preparing to install
- Installing a new version of the Management Server
- Installed directories
- Foglight settings
- Uninstalling Foglight
- Upgrading the Management Server

Preparing to install

The requirements for installing Foglight are:

- A machine to host the Management Server. The Management Server should run on a dedicated machine because it must process and store large volumes of data.

  NOTE: Ensure that a host name resolution and reverse lookup are confirmed prior to installing the Foglight Management Server.

  NOTE: Link-local IPv6 addresses are not supported for the Management Server because many web browsers do not support link-local IPv6 addresses.

- Administrator or root access to all machines requiring a Foglight agent.
- An administrator password for Foglight. The user name *foglight* and the default password for this account can initially be used to log in to the browser interface and to use command-line interface options with root privileges. It is recommended that you change the default password for this account.

  NOTE: The installer does not allow installing Foglight with embedded PostgreSQL® as *root* on Unix.

- A user account on the machine where you are installing Foglight.
- The IATEMPDIR environment variable is set to a location with sufficient space for installer self-extraction to meet the requirements.

Installing a new version of the Management Server

Once all system requirements are in place, you are ready to install the Management Server. The installer prompts you to input data, and shows progress during the installation process.

The Foglight installer offers two installation options:

- **Standard** — This option accepts all of the installer defaults, and installs an embedded PostgreSQL® database only. To use this option, follow the instructions in Installing the Management Server - Standard Install option.
- **Custom** — This option allows you to modify the installer defaults, and to choose an external database type. To use this option, follow the instructions in Installing the Management Server - Custom Install option.

The Foglight installation process consists of the same basic steps for all platforms. For specific platform customizations, see Installed directories.

For more details, see these topics:

- Installing the Management Server - Standard Install option
- Installing the Management Server - Custom Install option
- Foglight Server Startup page
- Next steps
- Embedded Agent Manager

Installing the Management Server - Standard Install option

Start the installation process by initiating the executable included on the Foglight install media. Each installation screen includes a **Previous** button, allowing you to go back and adjust the information you have specified.

Step 1: Introduction

The Introduction screen provides an overview of the mechanics of the installation interface. Review the contents of this screen, then click **Next**.

Step 2: Transaction Product Agreement

1. Read the Transaction Product Agreement statement, and accept or decline the terms of the agreement.
2. If you selected **I accept the terms of the License Agreement**, click **Next**.

Step 3: Select installation type

Accept the default **Standard Install** by clicking **Next**.

Step 4: Installing Foglight

Foglight installs files into the default directories.

Step 5: Foglight ports configuration

NOTE: For Foglight Evolve only.

1. Configure the server ports. The Foglight Ports Configuration screen displays default ports that you can assign.
2. If you want to revert to the default values, click **Defaults**.
3. Click **Next**.

   NOTE: If there are any port assignment conflicts, an error message dialog box appears. You can either click **Review Ports,** if you want to return to the Foglight Ports Configuration screen to configure the conflicting port(s), or click **Ignore and Continue** to continue with the installation without resolving the port conflicts. Select one of these options to continue.

Step 6: Foglight server startup

The Foglight Server Startup step provides you with the option of starting the Management Server from the installer.

1. To start the Management Server at this point (the default setting), click **Next**.

   If you do not want the installer to start the Management Server, clear the **Run Now** check box, and then click **Next**.
2. If you selected **Run Now**, the installer starts Foglight and the Foglight Server Startup page launches in a Web browser (if a Web browser is available). See Foglight Server Startup page for more information.

   In either case, the Install Complete screen appears.

Step 7: Install complete

Click **Done** to complete the installation process.

Proceed to Next steps.

Installing the Management Server - Custom Install option

Start the installation process by initiating the executable included on the Foglight installation media. Each installation screen includes a **Previous** button, allowing you to go back and adjust the information you have specified.

Step 1: Introduction

The Introduction screen provides an overview of the mechanics of the installation interface. Review the contents of the screen, then click **Next**.

Step 2: Transaction Product Agreement

1. Read the Transaction Product Agreement statement, and accept or decline the terms of the agreement.
2. If you selected **I accept the terms of the License Agreement**, click **Next**.

Step 3: Select installation type

Click the **Custom Install** option, then click **Next**.

NOTE: The **Standard Install** option is only available if you are installing with an embedded database.

Step 4: Choose installation folder

1. Choose the location where you want to install Foglight, depending on the product that you want to install. You can accept the default location:

   Foglight

   - *.../Quest/Foglight*

   Foglight Evolve

   - *.../Quest/Foglight/Program Files*
2. You can also click the **Browse** button to navigate to a different location.
3. Click **Next**.

Step 5: Choose link location

1. Choose the location where you want to create links (shortcuts).
2. Click **Next**.

Step 6: Pre-installation summary

Review the installation information. If you are satisfied with the parameters of your installation, click **Install**.

To change the installation parameters, click **Previous**.

NOTE: The installation type (New Install) is displayed on this screen. If you want to upgrade an existing installation of the Management Server, continue clicking Previous until you return to the Choose Install Folder screen. See the *Upgrade Guide* for detailed upgrade instructions.

Step 7: Installing Foglight

Foglight installs files into the specified directory.

Step 8: Foglight administrator password

1. In the **Foglight Administrator Password** box, accept the default password (*foglight)* or type an alternate one.
2. In the **Retype Administrator Password** box, accept the default *(foglight)* or, if you have provided an alternate password in step 1, retype the password for verification.
3. **Optional —** To run Foglight in secure mode (HTTPS) only, select the **Secure Server (HTTPS Only)** check box.
4. Click **Next**.

Step 9: Foglight mode

1. Accept the default server mode (Standalone).

NOTE: A server running in HA mode can only use an external database.

2 Click **Next**.

Step 10: FIPS Compliance mode

This step allows you to enable FIPS Compliance mode. Select the checkbox if you want to enable FIPS compliance mode.

NOTE: Once the FIPS Compliance mode is enabled during installation, you cannot disable it without a complete reinstall of Foglight.

Step 11: Foglight repository database type

This step allows you to select the Foglight database type. At the completion of this step, the installer creates the user (*foglight* is the default user ID) in the database and sets the appropriate permissions.

- Select **Use an Embedded PostgreSQL database** and then click **Next**. See the following section for instructions.

NOTE: The Embedded PostgreSQL® database is not supported on Windows Server® 2003.

Embedded PostgreSQL database

1 Accept the default port (15432) or type an alternate in the Repository **Port** field.

2 In the Repository Administrator **Password** box, accept the default password provided (*foglight*) or type an alternate one. The Management Server uses the administrator account credentials to create the PostgreSQL® database.

3 In the **Retype Password** box, accept the default *(foglight)* or, if you have provided an alternate password, re-type the password for verification.

4 In the **User Name** box, accept the default user ID (*foglight*) or type an alternate one. The Management Server uses this account to connect to the database.

5 In the User Account **Password** box, accept the default password (*foglight*) or type an alternate one. The Management Server uses this password to connect to the database.

6 In the User Account **Retype Password** box, accept the default *(foglight)* or, if you have provided an alternate password in step 5, retype the password for verification.

7 Click **Next**.

A progress box appears as the embedded database is installed.

Step 12: Foglight ports configuration

1 Configure the server ports. The Foglight Ports Configuration screen displays default ports that you can assign.

NOTE: In certain configurations, the Management Server uses other ports than the ones that you can set on this screen. See the *Foglight online Help* for details.

2 If you want to revert to the default values, click **Defaults**.

3 Click **Next**.

NOTE: If there are any port assignment conflicts, an error message dialog box appears. Click **Review Ports**, if you want to return to the Foglight Ports Configuration screen to configure the conflicting port(s), or click **Ignore and Continue** to continue with the installation without resolving the port conflicts. Select one of these options to continue.

Step 13: Add Foglight license file

1 Specify the path to the Foglight license file in the **License File** box, or browse to a license file by clicking the **Browse button**.

IMPORTANT: See the *Foglight online Help* for information about license requirements, managing licenses, and the different categories of cartridges (based on their license requirements).

2 Click **Next**.

Alternatively, you can provide a license file to the Management Server after the installation is complete. To do so, leave the **License File** box blank and click **Next**.

Step 14: Add Foglight to system service

The Foglight Server Startup step enables to add Foglight to the system service.

NOTE: To customize the Foglight Management Server starts as a system service, the current user must have sudo without password privilege; otherwise the script will be generated without being added into the system service and you can edit and execute the script later.

1 To start the Foglight Management Server without adding Foglight to the system service (the default setting), click **Next**.

2 To start the Foglight Management Server as a system service, select **Yes, add foglight to the system service**.

Step 15: Foglight server startup

The Foglight Server Startup step enables you to start the Management Server.

1 To start the Management Server (the default setting), click **Next**.

If you do not want the installer to start the Management Server, clear the **Run Now** check box, then click **Next**.

2 If you selected **Run Now**, the installer starts Foglight and the Foglight Server Startup page launches in a web browser (if a web browser is available). If a web browser is not available, the Foglight Server Startup page does not launch.

See Foglight Server Startup page for more information.

In either case, the Install Complete screen appears.

Step 16: Install complete

Click **Done** to complete the installation process.

Foglight Server Startup page

If you selected the **Run Now** check box in the Foglight Server Startup step in the installer, the installer starts Foglight and launches the Foglight startup page.

When the server startup is complete, a link to the Foglight login page appears. For more information, see Logging in to Foglight.

NOTE: The default link to the login page points to http://localhost:8080. In some instances, this link may not correspond to the URL of your Foglight server. In such cases, see Why does clicking the login link on the server startup page not work?.

Configuration about SQL Server Failover

If you want to use the SQL Server Failover function on the Foglight Management Server, perform the following configurations:

1 On the primary database instance, issue the following command:

```
select name, sid, password_hash from master.sys.sql_logins where
name='<username>';
```

Store the *username, sid*, and *password_hash* for later use.

2 On the secondary database instance(s), issue the following command:

NOTE: Variables contained within angle brackets should be changed to the values that you obtained in step 1.

NOTE: The value of <*databasename*> is the db instance that you create during the installation of the Foglight Management Sever.

```
CREATE LOGIN [<username>]
WITH PASSWORD = <password_hash> HASHED,
   SID = <sid>,
   DEFAULT_DATABASE = [<databasename>],
   DEFAULT_LANGUAGE = [us_english],
   CHECK_EXPIRATION = OFF,
   CHECK_POLICY = OFF;
```

Next steps

If you performed a Standard Install, follow the instructions in Importing a license file after installation to provide a license file to the Management Server after installation.

If you performed a Custom Install and you did not install a license in Step 13: Add Foglight license file, follow the instructions in Importing a license file after installation to provide a license file to the Management Server after installation.

IMPORTANT: See the *Foglight online Help* for information about license requirements, managing licenses, and the different categories of cartridges (based on their license requirements).

If you did not select the **Run Now** option in the Foglight Server Startup step of the installer, start the Management Server by following the instructions in Starting and stopping the Management Server.

To log in to Foglight, see Logging in to Foglight.

Embedded Agent Manager

An instance of the Agent Manager is automatically installed with new installations of the Management Server. This embedded Agent Manager instance runs on the Management Server machine. You can deploy agents to the embedded Agent Manager if you want to monitor the machine on which the Management Server runs.

In certain environments, Foglight starts and stops the embedded Agent Manager along with the Management Server by default. For more information about running the embedded Agent Manager, see the *Foglight online Help*.

You can run the embedded Agent Manager in tandem with the server or not.

NOTE: Although the Foglight Agent Manager Adapter cartridge is installed by default with the embedded Agent Manager, you must install an Agent Manager cartridge that contains installers for your supported platforms, in order to deploy the Agent Manager to remote hosts.
See the *Foglight online Help* for information about selecting an Agent Manager cartridge, downloading installers, and installing, configuring, and running the Agent Manager.

Installed directories

The following table describes the directories that are created under your target installation folder. They may vary, depending on the product features that you selected and the components installed for your platform.

Table 1. Installed directories

Directory	Contents
bin	Foglight executables for running the server and utilities.
cartridge	Installed cartridge files in their original form.
client	Files that client programs (such as the command-line client) use for remote access to Foglight.
compat	Cartridge files: Core-HostServices-compatibility-8_1_0.car and FTR-WS-1_0_0.car
config	Configuration files and subdirectories. The files in the *config* directory contain settings that are most likely to require editing. Files at the next level are less likely to need changing. Files at the lowest level contain settings that are unlikely to need changing except in special circumstances.
docs	HTML and PDF versions of the product documentation.
dtd	Descriptors for configuration files that can be imported into Foglight (for example, by installing a cartridge).
extension	Directory for extension cartridges (optional cartridges that are not installed by default).
fglam	Directories for the embedded Agent Manager.
jre	Version of the JRE (1.8) that Foglight uses.
lib	The Foglight JAR files.
license	The Foglight license file you install. **NOTE:** See the Foglight online Help for information about license requirements, managing licenses, and the different categories of cartridges (based on their license requirements).
logs	Default location of the log files that Foglight generates when it runs. Generated at runtime.
postgresql	Default location for the embedded PostgreSQL® library. If the embedded database is selected during installation, then the database is created, populated, and used for Foglight runtime. To start the embedded database separately, without running Foglight, use these parameters: `[run|shutdown]Db.sh` in *<install-dir>/bin*

Table 1. Installed directories

Directory	Contents
scripts	SQL scripts and examples of the two types of Script Agents. *scripts/agent* contains sample Type 1 and Type 2 Script Agent files. *scripts/sql-templates* contains SQL scripts to drop/create schema, or create/populate the database. The scripts included in this directory are specific to the type of database that you selected when installing Foglight.
server	JAR files and data files that a particular Foglight server variant uses (such as *default*).
state	Where the running state of Foglight is kept. It includes the following sub-directories: • *cartridge.exploded*. A working directory for deploying cartridges. It contains files extracted from installed cartridges. This is the same data as in the corresponding CAR files, just unzipped. The contents change on cartridge redeployment, but should not change on server restart. Users **should not modify** this data (even if the server is not running). • *postgresql-data*. Default location for the embedded PostgreSQL® data.
support	Where support bundled archive information is stored.
tmp/cartridge.deployed	A working directory for deploying cartridges. This directory contains files extracted from cartridges for the current Management Server run. Contents may change on restart or cartridge redeployment. This data can be deleted if the server is not running. The server re-creates what is necessary on restart.
tools	Various Foglight utilities.
UninstallerData	Files that the Foglight uninstaller uses.
upgrade	Directory that the installer uses.

Foglight settings

Foglight can run with its default settings. Edit these settings if you need to change run-time parameters such as settings for running the Management Server in High Availability (HA) mode or the ports that the Management Server uses. Many Foglight settings can be changed by editing the file *<foglight_home>/config/server.config*, which contains settings.

NOTE: In certain configurations the Management Server may use ports in addition to the ones that you set using server.config. See the *Foglight online Help* for details.

For more details, see these topics:

- Editing the server.config file
- Importing self-signed certificates to Foglight TrustStore
- Setting up an encrypted LDAP connection with SSL
- Using encryption when sending email from Foglight
- Setting parameters for an embedded database
- Configuring ports
- Setting memory parameters for the server
- Adding command-line options

- Binding the Management Server to an IP address
- Configuring Foglight to use stronger encryption
- Configuring Foglight to use the HTTPS port
- Setting the length of Foglight sessions

Editing the *server.config* file

The *<foglight_home>/config/server.config* file contains parameters for port settings, virtual memory, command-line options, and server federation. You can edit the file using a text editor. Values within quotation marks can be edited.

Importing self-signed certificates to Foglight TrustStore

Foglight needs to verify self-signed certificates. It is necessary to configure the TrustStore properly for encrypted database/LDAP connection.

Non-FIPS mode

In non-FIPS mode, to be compatible with former Foglight versions, Foglight uses JRE TrustStore as the default TrustStore. The default TrustStore will NOT be preserved during Foglight upgrade. Foglight also support a separate TrustStore, which will be preserved during upgrade. Choose the one that best suits your needs:

Option 1: Import the certificate into the embedded JRE TrustStore, *<foglight_home>/jre/lib/security/cacerts* (default password: `changeit`), with the following command:

```
<foglight_home>/jre/bin/keytool -import -file <path_to_cert_file> -alias
<alias_of_cert> -keystore <foglight_home>/jre/lib/security/cacerts -storepass
<store_pwd>
```

Option 2: Prepare and import the certificate into Foglight TrustStore with the following steps:

1 Prepare TrustStore: copy *<foglight_home>/config/security/trust.keystore.sample* to *<foglight_home>/config/security/trust.keystore*

2 Import the certificate into the Foglight TrustStore, *<foglight_home>/config/security/trust.keystore* (default password: `nitrogen`), with the following command:

```
<foglight_home>/jre/bin/keytool -import -file <path_to_cert_file> -alias
<alias_of_cert> -keystore <foglight_home>/config/security/trust.keystore -
storepass <store_pwd>
```

FIPS-compliant mode

In FIPS-compliant mode, it is required to use FIPS-validated KeyStore type BCFKS.

Import the certificate into the Foglight default TrustStore in FIPS-compliant mode, *<foglight_home>/config/security/trust.fips.keystore* (default password: `nitrogen`) with the following command:

```
<foglight_home>/jre/bin/keytool -import -trustcacerts -alias <alias_of_cert> -
file <path_to_cert_file> -keystore
<foglight_home>/config/security/trust.fips.keystore -deststoretype BCFKS -
provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
<foglight_home>/server/core/bc-fips.jar -storepass <store_pwd>
```

Setting up an encrypted LDAP connection with SSL

Use the following instructions if you need to encrypt communication between the Management Server and the LDAP server.

To encrypt communication between Management Server and LDAP:

1. Acquire the LDAP server certificate in *.pem* format from the administrator.
2. Import the certificate into the Management Server keystore, see Importing self-signed certificates to Foglight TrustStore.

   NOTE: In addition to the Root CA certificate, there may be one or more intermediate CA certificates. If so, make sure to import the Root CA certificate and all intermediate CA certificates in sequence.

3. On the navigation panel, under **Dashboards**, click **Administration > Users & Security > Directory Services Settings**.
4. Under LDAP Locations, click **Edit**.
5. Specify the LDAP server URL in the following format:

   ```
   ldaps://ldap_server_host_name:636
   ```

   NOTE: The port number for LDAP over SSL is usually 636. Confirm the exact port number with your LDAP server administrator.

6. Restart the Management Server.

Using encryption when sending email from Foglight

You can use encryption when sending email from Foglight. To do so, you must enable Foglight to use the SSL protocol and configure the mail server used by Foglight to use an SSL certificate that is not self-signed.

You can configure Foglight to use the SSL protocol either on the Email Configuration Dashboard or by editing the related `mail.use.ssl` registry variable. See the *Foglight online Help* for more information.

See the documentation for your mail server for information about configuring it to use an SSL certificate.

Setting parameters for an embedded database

The file *<foglight_home>/config/server.config* contains a number of settings related to the embedded database. In most cases, you do not need to change these settings. If you need to edit these parameters, you must restart the Management Server after doing so.

Specifying whether an embedded database is used

When you run Foglight with an embedded database, the parameter `server.database.embedded` is set to `true`. If you are switching from an embedded to an external database, you must set this parameter to `false`.

For more information, see Appendix: Switching from an Embedded to an External Database.

If you have been running Foglight with an external database, then set `server.database.embedded` to `true` and restart the Management Server, Foglight starts with the embedded database. The data displayed in Foglight after you perform these steps depends on whether you had previously run Foglight with the embedded database:

- **If you have previously run Foglight with the embedded database**: The Management Server reflects the state of the previously run embedded database.
- **If you did not previously run Foglight with the embedded database**: The state of the Management Server is like new, since no data exists in the database.

Configuring the database start up and shut down grace periods

There are also optional settings for configuring the startup and shutdown grace periods for the embedded database: `server.database.embedded.startup.grace` and `server.database.embedded.shutdown.grace`.

Foglight starts and stops the embedded database. These settings control the length of time that Foglight waits before considering an attempt to start or stop the database to have failed.

The values for these optional settings are specified in seconds, as in the default values shown in the following example.

```
server.database.embedded.startup.grace = "300";
server.database.embedded.shutdown.grace = "300";
```

Understanding the Password and Socket settings

The file *server.config* also contains parameters that set the password and socket that the embedded database uses.

Embedded database Password parameter

The password that the `server.database.embedded.password` parameter specifies is the root password used for the embedded database. The default value is `foglight`.

If you selected the embedded database option while installing Foglight and now want to switch to using an embedded database, you do not need to change the root password.

If you did not select the embedded database option during installation, you need to specify the correct root password as the value of `server.database.embedded.password`. This password can be specified in either an encrypted or plain-text format. If necessary, you can encrypt the password using the *<foglight_home>/bin/keyman.sh* tool.

During installation, the Foglight installer overwrites the default value of `server.database.embedded.password` when you select the embedded database.

IMPORTANT: Do not use “<“ and “>” in your password, for example jo<anne>123. These characters corrupt the XML in the server.config file, causing Foglight to fail to start successfully.

Embedded database Socket parameter

The `server.database.embedded.socket` parameter specifies a UNIX® domain socket. This parameter is used on Linux® and Solaris platforms only. The installer generates a unique socket name for each installation.

IMPORTANT: Do not change this setting.

Configuring ports

You can set a number of different ports using the file *<foglight_home>/config/server.config*, including mandatory ports required for Foglight to run.

For a list of these ports, their default values, and the configuration parameters you can use to set them in *server.config*, see the *Foglight online Help*.

NOTE: In certain configurations the Management Server may use ports in addition to the ones that you set using server.config. See the Foglight online Help for details.

Setting memory parameters for the server

If you are running the Management Server by running *bin/fms*, you can configure the Java® Virtual Machine's (JVM) minimum and maximum memory parameters for the server in the *<foglight_home>/config/server.config* file.

If you are starting Foglight using the `run.[bat|sh]` command, the JVM heap memory parameters set in the *<foglight_home>/config/server.config* file do not take effect. Use `-X` options to pass the memory parameters straight to the VM.

If your installation supports a large number (hundreds) of agents, you can set the Java® heap memory minimum (`-Xms`) and maximum (`-Xmx`) options to the same size. For example, assigning 1GB of memory can be set in the *server.config* file as follows:

```
server.vm.option0 = "-Xms1280M";
server.vm.option1 = "-Xmx1280M";
```

Ensure that you uncomment these lines in the file.

You can set up to 100 VM options in total.

NOTE: The `-Xms` and `-Xmx` options are different for 32-bit and 64-bit JVMs and available physical memory. The values of the `-Xms` and `-Xmx` options do not necessarily have to be the same size. However, the value of the `-Xmx` option should not exceed certain limits that the System Administrator specifies.

Process heap use

When a thread is created and run, a run-time stack is dynamically allocated from the native process heap (not the Java® heap). This native heap requires a large contiguous memory block. If the system you are running does not have enough RAM, or if the operating system cannot find a large enough contiguous memory block, new native threads cannot be created and a `java.lang.OutOfMemoryError` occurs.

If the VM generates errors relating to a failure to allocate native resources, or relating to exhaustion of process address space, you must increase the native process heap size. Errors appear as a Java VM internal error message or a detail message associated with an out-of-memory error. Messages with the relevant errors indicate that the problem is process heap exhaustion.

You cannot directly set the size of the process heap. The process heap uses memory within the 32-bit address space not used by the garbage-collected heap. To increase the size of the process heap, decrease the maximum Java heap size using the `-Xmx` option in the *server.config* file.

Default stack size

The default stack size can be adjusted with the `-Xss` option.

Adding command-line options

The *server.config* file allows you to add up to 10 command-line options for the `fms` command.

Each command-line argument corresponds to a space-delimited argument passed to the Foglight process.

For example, the following lines in the *<foglight_home>/config/server.config* file:

```
server.cmdline.option0 = "--name";
server.cmdline.option1 = "process_name";
```

Correspond to this direct argument on the command line:

```
fms --name process_name
```

Certain arguments can be specified in a single line that uses the long name for an option. For example:

```
server.cmdline.option0 = "--host=hostname";
```

Which corresponds to the following command-line argument:

```
fms --host=hostname
```

Binding the Management Server to an IP address

To cause the Foglight Management Server to bind to a specific IP address, use the dedicated properties in the *<foglight_home>/config/server.config* file. For example:

```
server.bind.address = "192.0.2.2";
```

```
server.remote.address = "host1.example.com";
```

Where `host1.example.com` is the host name assigned to the bind address in DNS. If no DNS name is available, a raw IP address can be used in this property.

Binding Foglight to a specific IP address can be used where, for example, the same IP address is to be used by multiple Management Server instances on a single host, each IP address delineating a virtual boundary between instances. In such situations, the Management Server will only listen for incoming TCP traffic on that specific IP address. By default, the Management Server listens to all IPv4 and IPv6 addresses.

Configuring Foglight to use stronger encryption

NOTE: This only works in non-FIPS mode. Stronger encryption with fixed key size is used in FIPS-compliant mode.

Foglight Management Server 5.6.3 and later includes unlimited strength security policies. In some cases, such as Credential Management, this encryption level may be insufficient. If 256-bit (or higher) AES keys are necessary, use the following procedure to configure the Management Server to use stronger encryption.

To configure Foglight to use stronger encryption:

1. Stop the Management Server.
2. Open the file *<foglight_home>/config/server.config* on the Management Server machine.
3. Set the java system property `foglight.credentials.enc.key.size` to 256 (or higher):

   ```
   server.vm.option0 = "-Dfoglight.credentials.enc.key.size=256";
   ```
4. Save the *server.config* file.
5. Restart the Management Server.

Configuring Foglight to use the HTTPS port

If you do not choose to install Foglight in Secure Server mode, you can edit *server.config* after installation and manually configure Foglight to restrict the Management Server to use the HTTPS port when accessing the browser interface.

You must have a signed, valid certificate to use this HTTPS configuration. It is recommended that you obtain a valid certificate from a third party as outlined in Importing a network security certificate.

To configure the Management Server to use the HTTPS port:

1. Stop the Management Server.
2. Open the file *<foglight_home>/config/server.config* on the Management Server machine.
3. Set the parameter `server.console.httpsonly` to `true`:

   `server`.console.httpsonly = "true";
4. Save the *server.config* file.
5. Import the signed certificate into the Foglight keystore. See Importing a network security certificate for instructions.
6. Restart the Management Server.
7. Launch the Foglight browser interface using the appropriate HTTPS URL (*https://<hostname>:<https_port>*) to ensure that the Management Server can be accessed using HTTPS.

NOTE: The Foglight Management Server uses the HTTP port for local access even if you are accessing the browser interface through an HTTPS connection. If that is the case, both ports are open: the HTTPS port for external requests coming from the browser interface and the HTTP port for local requests. For example, the reporting service accesses the Foglight Management Server through the HTTP port while external requests use HTTPS.
You must configure your firewall or network security applications to allow both ports to remain open.

Importing a network security certificate

In order to set up the Foglight Management Server to use HTTPS, you must generate a key pair (security certificate) into the Foglight keystore. This security certificate allows the server to communicate through the HTTPS protocol. Delete the existing certificate shipped with Foglight before generating a new key pair. Use the keytool utility shipped with Foglight to create, import, and export certificates. This utility can be found at:

<foglight_home>/jre/bin/keytool

There are two keystores that Foglight uses:

- The built-in Tomcat™ keystore located at:
  <foglight_home>/config/tomcat.keystore (default password: `nitrogen`)

  <foglight_home>/config/tomcat_fips.keystore(For FIPS compliance mode, default password: `nitrogen`)
- The Management Server keystore located at:
  <foglight_home>/jre/lib/security/cacerts (default password: `changeit`)

To import a certificate:

1. Back up the existing *tomcat* key using the following command:

   ```
   cp tomcat.keystore <your_backup_key>
   ```
2. Delete the existing *tomcat* key from the *tomcat.keystore* directory using the following command:

   ```
   <foglight_home>/jre/bin/keytool<foglight_home>/config/tomcat.keystore -
   keystore tomcat.keystore -storepass nitrogen -alias tomcat -delete
   ```
3. Create a new key under the *tomcat* alias using the following command:

```
<foglight_home>/jre/bin/keytool<foglight_home>/config/tomcat.keystore-keystore
tomcat.keystore -storepass nitrogen -genkeypair -alias tomcat -validity <number
of days> -keyalg RSA -keysize 2048 -dname "CN=<your_fmsserver_dns_name>,
OU=<your_organizational unit_name>, O=<your_organization_name>,
L=<your_city_name>, ST=<your_state_name>, C=<your_two-letter_country_code>" -
ext SAN=dns:<your_fmsserver_dns_name>,ip:<your_fmsserver_ip>
```

4 Generate a Certificate Signing Request (CSR) using the following command:

```
<foglight_home>/jre/bin/keytool<foglight_home>/config/tomcat.keystore-keystore
tomcat.keystore -storepass nitrogen -alias tomcat -validity <number of days> -
certreq -ext san=dns:<your_fmsserver_dns_name>,ip:<your_fmsserver_ip> -file
<your_request_file.csr>
```

This file must be signed by Certification Authority (CA).

5 Once you have the certificate signed, import it back to the *tomcat.keystore* using the following command:

```
<foglight_home>/jre/bin/keytool<foglight_home>/config/tomcat.keystore-keystore
tomcat.keystore -storepass nitrogen -alias tomcat -validity <number of days> -
trustcacerts -import -file <your_converted_cerificate>
```

When importing a certificate for Foglight in FIPS-compliant mode, continue with the following steps:

6 Backup the default tomcat FIPS keystore using the following command:

```
cp tomcat_fips.keystore <your_backup_key>
```

7 Covert *tomcat.keystore* from JKS format to FIPS-verified BCFKS format using the following command:

```
<foglight_home>/jre/bin/keytool -importkeystore -srckeystore tomcat.keystore -
destkeystore tomcat_fips.keystore -deststoretype BCFKS -provider
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
<foglight_home>/server/core/bc-fips.jar
```

You will get a prompted message similar to the following: *... is not trusted. Install reply anyway? [no]:*

Type `yes` to install the new certificate.

The following is an example of commands for importing a certificate.

```
cd <foglight_home>/config
cp tomcat.keystore tomcat.keystore.backup
<foglight_home>/jre/bin/keytool -keystore tomcat.keystore -storepass nitrogen -
alias tomcat -delete
<foglight_home>/jre/bin/keytool -keystore tomcat.keystore -storepass nitrogen -
genkeypair -alias tomcat -validity 730 -keyalg RSA -keysize 2048 -dname
"CN=fms.quest.com, OU=Foglight, O=Quest, L=Aliso Viejo, ST=CA, C=US" -ext
SAN=dns:fms.quest.com,ip:192.168.1.1
<foglight_home>/jre/bin/keytool -keystore tomcat.keystore -storepass nitrogen -
alias tomcat -validity 730 -certreq -ext san=dns:fms.quest.com,ip:192.168.1.1 -
file san.p7b
<foglight_home>/jre/bin/keytool -keystore tomcat.keystore -storepass nitrogen -
alias tomcat -validity 730 -trustcacerts -import -file san.p7b
```

Importing a PKCS #12 (pfx) format certificate

If you have an existing SSL certificate and you want to use this certificate in Tomcat, follow the steps below to import this SSL certificate.

NOTE: This certificate must be provided in the PKCS #12 (pfx) format. If the certificate and private key are saved in separate files, run the following command to merge them to the PKCS12 format:
openssl pkcs12 -export -in <certfile> -inkey <keyfile> -out <keystorefile> -name tomcat -CAfile <cacertfile> -caname root

To import a certificate in Tomcat:

1 Delete the existing *tomcat* certificate from the *tomcat.keystore* directory using the following command:

```
<foglight_home>/jre/bin/keytool -keystore tomcat.keystore -storepass nitrogen
-alias tomcat -delete
```

2 Obtain the certificate's alias name from the certificate PFX file using the following command:

```
<foglight_home>/jre/bin/keytool -keystore <your certificate pfx file> -
storepass <certificate pfx password> -list -v
```

The following is an example of command output. The value of Alias name is required in step 3.

```
Your keystore contains 1 entry

Alias name: tq-294043e3-fd9d-42ee-a596-0217c7d6d5f8

Creation date: May 8, 2020

Entry type: PrivateKeyEntry
```

3 Merge the Tomcat keystore and the PKCS12 keystore using the following command:

```
<foglight_home>/jre/bin/keytool -importkeystore -destkeystore
<foglight_home>/config/tomcat.keystore -deststorepass nitrogen -destalias
tomcat -destkeypass nitrogen -srckeystore <your certificate pfx file> -
srcstorepass <certificate pfx password> -srcstoretype pkcs12 -srcalias <alias
name in step 2>
```

Setting the length of Foglight sessions

NOTE: This section applies only to Foglight Evolve.

You can configure the length of inactive Foglight browser interface sessions by changing the value of the parameter `server.console.session.timeout`. This parameter controls the length of time that Foglight waits before automatically logging you out of an idle browser interface session.

To change the Foglight session time-out setting:

1 Stop the Management Server. Open the file *<foglight_home>/config/server.config* on the Management Server machine. Set the parameter `server.console.session.timeout` to the desired value in minutes.

The default value is 60 minutes. If you set the value to less than or equal to `0`, or greater than `30000000`, Foglight never logs you out of the browser interface, regardless of how long the session has been inactive.

For example, to increase the time-out to 2 hours (120 minutes), you would set this parameter as follows:

```
server.console.session.timeout = "120";
```

2 Save the *server.config* file.

3 Restart the Management Server.

Configuring anti-virus exclusion settings

Anti-virus software may negatively impact the CPU and system performance of machines running Foglight. To reduce resource consumption, it is highly recommended to exclude the relevant directory, processes, and executables from being scanned by the anti-virus software.

- The common installation directory is as follows:

  <foglight_home>

- Foglight related processes to exclude from virus scanning are as follows:
  - *<Foglight Base Folder>/bin/fms*
  - *<Foglight Base Folder>/bin/fmsha*
  - *<Foglight Base Folder>/bin/qcn_runner*
  - *<Foglight Base Folder>/bin/qp5app*
  - *<Foglight Base Folder>/bin/remotemonitor*
- Embedded FglAM processes to exclude from virus scanning:

  Base Folder: *<Foglight Base Folder>/fglam*
- Foglight Embedded Database Repository processes to exclude from virus scanning are as follows:
  - *<Foglight Base Folder>/postgresql/bin/postgres*
  - *<Foglight Base Folder>/postgresql/bin/pg_ctl*
  - *<Foglight Base Folder>/postgresql/bin/initdb*
  - *<Foglight Base Folder>/postgresql/bin/createdb*

Uninstalling Foglight

You can uninstall Foglight using the uninstaller utility for your platform. The uninstaller can be found in *<foglight_home>/UninstallerData*.

The default mode for the uninstaller is the graphical user interface (GUI) mode. In cases where a graphics display is not available on UNIX® systems, the Foglight uninstaller can be run from the command line by using console mode or silent mode. Console mode is available only for Linux® and Solaris.

To uninstall Foglight:

1. Stop the Foglight Management Server. See Stopping the Management Server for instructions.
2. Navigate to the *UninstallerData* directory of your Foglight installation and run the *Uninstall_Foglight* shell script.
   - To launch the uninstaller in GUI mode, simply run the *Uninstall_Foglight* shell script.
   - **Linux® and Solaris only:** To launch the uninstaller in console mode, run the *UninstallFoglight* shell script using the following command:
     `./Uninstall_Foglight -i console`
   - To launch the uninstaller in silent mode, run the *Uninstall_Foglight* shell script using the following command:
     `./Uninstall_Foglight -i silent -f installvariables.properties`
3. After uninstallation, you can safely delete the *<foglight_home>* directory. It is recommended that you do so, since the uninstaller does not remove certain directories within *<foglight_home>*.

NOTE: After uninstallation, you can also safely delete any Foglight shortcuts, regardless of their location.

Upgrading the Management Server

See the *Upgrade Guide* for detailed upgrade instructions.

3

Running the Management Server

The instructions in this section assume that you have already installed Foglight. If you have not, see Installing Foglight for installation instructions.

For more details, see these topics:

- Initializing the database
- Starting and stopping the Management Server
- Logging in to Foglight
- Running the Management Server FAQ

Initializing the database

If you are using the embedded database, the PostgreSQL® database is installed and initialed during the installation.

Starting and stopping the Management Server

The following sections describe how to start and stop the Management Server:

- Starting the Management Server
- Stopping the Management Server

Starting the Management Server

The following sections describe how to start the Management Server from the command line and lists additional commands for use when starting or running the Management Server.

To start the Management Server from the command line:

- Navigate to the directory *<foglight_home>/bin* and run the following command:

  ```
  fms
  ```

When the Management Server starts successfully, the following message appears in the command window:

```
Forge Server startup completed.
```

Additional commands

Table 1. Starting the Management Server - additional commands

Commands	Represents	Description
`-s`	start	Starts the Management Server (this option is assumed if no command is specified).

`-d`	start the process as a daemon	Starts the Management Server as a daemon (if the process is not started as a daemon, the command prompt is held captive by the running Management Server, and remains in the foreground).
		NOTE: The following scripts in *$FGLHOME/bin* directory can start the Management Server as a daemon and shut it down, respectively:
		`fmsStartup.sh`
		`fmsShutdown.sh`

`-n`	name	Provides a unique name for this instance of the Management Server.
`-j`	jvm-argument	Sets an option to be passed directly to the Java® VM. Can be used to set more than one VM option.
`-v`	version	Displays the version number for this program and exits.
`-h`	help	Shows this information, and additional options, then exits.

Initialization scripts

Another option is to start the Management Server using initialization scripts. This option is particularly useful when you want to automatically start the Management Server after it has been rebooted.

The initialization scripts can be found in the directory <*foglight_home*>*/scripts/init.d.* A *readme.txt* file is available in the same location. Review this file before running the script as it contains valuable information on how to use the script for your specific platform.

Stopping the Management Server

The following section describes how to stop the Management Server.

To stop the Management Server:

Do one of the following:

- Type **Ctrl-C** on the command window in which the Management Server started.
- Navigate to the *bin* directory and run the following command:
  `fms --stop`

When the server has stopped successfully, the **Start** command window closes.

Logging in to Foglight

NOTE: The Management Server must be running before you can log in to Foglight.

To log in to Foglight using a web browser:

1 Open a web browser and type the following:

`http://<hostname>:<port>`

Where `<hostname>` is the name of the machine where the Management Server is installed and `<port>` is the HTTP port specified during installation (the default is `8080`).

2 Enter a valid user name and password and click **Login**.

> **NOTE:** The Foglight browser interface requires JavaScript. Ensure that you have enabled JavaScript in your web browser before you attempt to log in.

Monitoring the Management Server host

During the installation, or upgrade, a HostAgent is automatically created to monitor the host where the Management Server, the embedded Foglight Agent Manager, and embedded database run. The health of this host directly affects the health and performance of Foglight.

To view the HostAgent:

1 Start the Management Server.

For detailed information, see Starting the Management Server.

1 Log in to Foglight.

2 On the navigation panel, under Dashboards, click **Administration > Agents > Agent Status**.

3 On the Agent Status dashboard, find the UnixAgentPlus called `EmbeddedHostMonitor`.

Information about the status and data collection of the agent are available on this dashboard.

To view the data that the HostAgent collects for the Management Server host:

1 On the navigation panel, under Dashboards, click **Infrastructure**.

2 From the Select a Service list, select the service for the host.

3 On the Monitoring tab, select the host from the list.

For more information about monitoring activities and exploring the data collected for the host, see the Foglight online Help.

Next steps

To install cartridges, see Installing and Upgrading Cartridges.

Running the Management Server FAQ

Why do I see an extra process named Quest Process Runner when I run Foglight?

On UNIX®, Foglight uses the Quest Common Process Runner to run processes such as the embedded database, the embedded Agent Manager, and command actions.

Why does the error message “cannot restore segment prot after reloc: Permission denied” appear when I start the Management Server?

Newer Linux® distributions have enabled new kernel security extensions from the SELinux project at the NSA (National Security Agency). SELinux is an NSA project to improve the security of Linux through Mandatory Access Control (MAC). These extensions allow finer-grained control over system security. However, SELinux also changes some default system behaviors, such as shared library loading, which can be problematic to third-party programs.

If you see the error message “cannot restore segment prot after reloc: Permission denied” when you start the Management Server, your SELinux configuration is preventing IDL (the Interface Definition Language) from launching.

To rectify this issue, you can perform one of the following workarounds:

- Change the default security context for the Management Server by issuing the command:

  `chcon -t texrel_shlib_t` <foglight_home>/jre/lib/i386/*.so

  `chcon -t texrel_shlib_t` <foglight_home>/jre/lib/i386/server/*.so

- Disable SELinux altogether by setting it to `disabled` in your */etc/sysconfig/selinux* file:

  `SELINUX=disabled`

For more information about SELinux, consult your Linux® distribution vendor.

If I stop the Management Server by closing the Command Prompt window, an error appears when I start up the server again. How do I restart the server?

It is recommended that you do not use this method to stop the Management Server. However, if you do use this method, follow the following workaround.

1. If you are running the embedded database, stop the database manually before restarting the Management Server.
2. Remove the stale *.pid* file that is located in the *state* directory. The logs or the console output inform you which *.pid* file to remove when you restart the server.

Why does the “JavaScript Disabled” error message appear when I try to log in to Foglight?

The Foglight browser interface requires JavaScript. You may need to modify the security settings in your web browser to enable this functionality. Depending on your browser, this setting may be labeled either “Enable JavaScript” (for example, in Firefox®), or “Enable Active Scripting” (for example, in Internet Explorer®).

Why does clicking the login link on the server startup page not work?

The default link to the login page points to `http://localhost:8080`. In some instances, this link may not correspond to the URL of your Foglight server, resulting in the link not working. This issue can also occur when Foglight is not able to identify your local host. Add your host/IP information to the `etc/hosts` files to correct this issue.

Why does a link-local IPv6 address not work with the Foglight web user interface?

Configuring the Management Server with a link-local IPv6 address is not supported because many web browsers do not support link-local IPv6 addresses. To correct this issue, update your host/IP information in the `etc/hosts` file.

4

Installing and Upgrading Cartridges

Using the Foglight Administration Module, you can install cartridges on the machine hosting the Management Server, enable and manage cartridges, and download agent installers.

The Cartridge Inventory dashboard contains controls for installing, enabling, disabling, and uninstalling cartridges, and for viewing information about the installed cartridges.

Installation is the first step in adding a cartridge to the Management Server. A cartridge file has the extension *.car*. Installing the *.car* file causes the Management Server to be aware of all cartridges in the *.car* file.

A cartridge must also be enabled before it is added to the Management Server. You can choose to enable a cartridge during installation, or afterward. See the *Foglight online Help* for instructions on enabling and disabling cartridges after installation.

To install a cartridge:

1. Navigate to the *Cartridge Inventory* dashboard (**Dashboards** > **Administration > Cartridges > Cartridge Inventory**).
2. Click **Install Cartridge**.
3. In the Install Cartridge dialog box, click **Browse** to navigate to a *.car* file on your local machine using a file chooser. Click **OK** in the file chooser when you have selected the *.car* file that you want to install.
4. The check box **Enable on install** is selected by default.
   - To enable the cartridge when it is installed, leave this check box selected.
   - To enable the cartridge after installation, clear this check box.
5. Click **Install Cartridge**.

If the installation is successful, the message "*Cartridge has been installed successfully"* appears in the Install Cartridge area and the cartridge is listed in the Cartridge Inventory.

If **Enable on install** was not selected (see Step 4), a disabled symbol ( ) appears in the row for that cartridge in the Installed Cartridges table on the Cartridge Inventory dashboard.

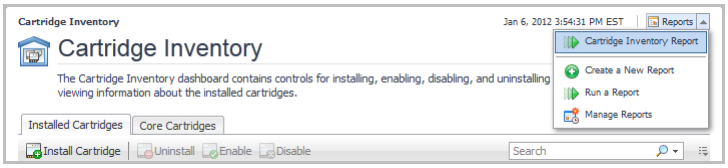
For more information about cartridge installation and configuration, see the *Foglight online Help*.

NOTE: Warning messages similar to the following appear in the Management Server log when you install a cartridge:
`WARN — Module system:<name> was converted to the newest version during loading`
These warnings are expected and do not affect functionality.

Cartridge Inventory Report

To obtain a full list of the cartridges installed on the Management Server, open the Cartridge Inventory dashboard (**Administration > Cartridges > Cartridge Inventory**), and select **Cartridge Inventory Report** from the Reports menu.

Figure 1. Cartridge Inventory Report



Upgrading cartridges

For complete cartridge upgrade instructions, see the *Upgrade Guide*.

Next steps:

- To install a separate (non-embedded) instance of the Foglight Agent Manager, see the *Foglight online Help*.

5

Installing Agents

A cartridge may include one or more executable Foglight agent installers. The agent installers included in a cartridge are listed on the Components for Download dashboard (on the navigation panel, select **Administration > Cartridges > Components for Download**).

Agents must be installed on all the machines you want to monitor. For agents that are installed on the monitored host, you must install and configure the Agent Manager.

NOTE: Foglight 4-converted agents create two processes for themselves when activated by the Agent Manager.

For more details, see these topics:

- Agent installers
- Remote agent installation

Agent installers

Agents that depend on the Agent Manager are installed using the remote installation procedure. See Remote agent installation.

Some cartridges Foglight include one or more executable agent installers. The agent installers that are available for download are listed on the Components for Download dashboard. You can use the controls on this dashboard to download agent installers from the Management Server to a remote machine.

To download an agent installer:

1. On the navigation panel, under **Dashboards**, click **Administration > Cartridges > Components for Download**.

   The Components for Download dashboard appears.

2. Click the name of the installer that you want to download.
3. Follow the on-screen instructions for each step of the installation process and specify the appropriate installation options.

NOTE: For agents that are installed individually, run the agent installer executable and set up the agent on each machine you want to monitor with that type of agent.
The Agent Manager defines agents with their Agent Package name. When displayed in the Create Agent dialog, the agent names are prepended with the cartridge name.

Depending on the type of agent that you installed, you may need to edit its properties to configure it for the part of your environment that you want to monitor. For information about agent properties, see the Foglight online Help for the cartridge with which the agent was included.

Remote agent installation

You can install Foglight agents on any remote host on which the Agent Manager is installed.

For more information about remote agent installation, see the *Foglight online Help*.

A

Appendix: Switching from an Embedded to an External Database

You may find a performance improvement in Foglight if you use an external database.

This section describes how to migrate from using an embedded PostgreSQL® database with the Management Server to using an external PostgreSQL database.

1 Stop the Management Server.

2 Start the embedded database manually:

```
<foglight_home>/bin/runDb.sh
```

3 Export the database content:

```
<foglight_home>/postgresql/bin/pg_dump -U root -h localhost -p 15432 foglight >
<foglight_home>/foglight_dump.sql
```

4 Shut down the database:

```
<foglight_home>/bin/shutdownDb.sh
```

5 Connect to the external PostgreSQL instance:

```
<foglight_home>/postgresql/bin/psql -h [postgresql host] -p [postgresql port] -
U [superuser] [dbname]
```

6 Create the “foglight” user by running:

```
postgres=# CREATE USER "foglight" WITH PASSWORD 'foglight';
```

7 Re-import the data dump:

```
postgres=# \i <foglight_home>/foglight_dump.sql
```

> **NOTE:** You have to use slash in the path when executing this command on a Windows® platform. You may see some errors like in the following example:
>
> ```
> psql:dump_db.sql:51991: ERROR:  role "root" does not exist
> psql:dump_db.sql:51992: ERROR:  role "root" does not exist
> ```
>
> It is safe to ignore these errors because the embedded database includes the super user `root` but the external may not.
>
> Also, the *foglight_dump.sql* includes these two statements at the end of the file:
>
> ```
> REVOKE ALL ON SCHEMA public FROM root;
> GRANT ALL ON SCHEMA public TO root;
> ```

8 Configure the Management Server to use this new database by opening the following file:

```
<foglight_home>/config/server.config
```

9 Update the following values in the `server.config` file:

```
server.database.host = "[postgresql host]";
server.database.port = "[postgresql port]";
```

```
server.database.name = "[postgresql dbname]";
server.database.embedded = "false";
```

> **NOTE:** The `server.database.password` must also be updated if in Step 6 you set a different password than the embedded “foglight” user password.

10 Restart the Management Server.

11 Verify that the Management Server starts successfully:

   a Open the most recent Management Server log file in *<foglight_home>/logs*.

   b Look for the message `Forge Server startup completed` and ensure that there are no errors listed after it.

12 Verify that the Management Server connects to the migrated external PostgreSQL database. There are two ways to do so:

- Open the most recent Management Server log file in *<foglight_home>/logs*. Verify that the parameter `server.database.host` lists your external PostgreSQL database host as its value and that `server.database.embedded` is set to `false`.
- Log in to the browser interface and navigate to **Dashboards > Administration > Setup & Support > Management Server Configuration**. Verify that your external PostgreSQL database host is listed in the **Database Host** box and that **Embedded** is set to *false*.

About Us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit https://www.quest.com/.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.