Foglight® 8.0.0

Installation and Setup Guide

Installing on Windows with an External Microsoft SQL Server 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 Foglight Version - 8.0.0

Contents

Before Installing Foglight 6
What is Foglight? 6
Hardware requirements and guidelines 6
Planning your installation 7
High Availability mode 8
Using an external database 9
Creating the database manually 9
Planning for authentication with gMSA 9
Licensing 10
Installation modes 11

Installing Foglight 15
Preparing to install 15
Installing a new version of the Management Server 16
Foglight Server Startup page 21
Configuration about SQL Server Failover 21
Next steps 21
Embedded Agent Manager 22
Installed directories 22
Foglight settings 23
Editing the *server.config* file 24
Enabling High Availability mode after installation 24
Changing external database credentials 24
Importing self-signed certificates to Foglight TrustStore 25
Setting up an encrypted database connection 25
Setting up an encrypted LDAP connection with SSL 26
Using encryption when sending email from Foglight 26
Configuring ports 26
Configuring the cluster multicast port used in High Availability mode 27
Setting up Foglight server federation 27
Setting memory parameters for the server 27
Adding command-line options 28
Binding the Management Server to an IP address 28
Configuring Foglight to use stronger encryption 28
Configuring Foglight to use the HTTPS port 29
Setting the length of Foglight sessions 31
HP patch checking tool 32
Uninstalling Foglight 32
Upgrading the Management Server 33
Installing Foglight FAQ 33

Running the Management Server 34
Manual database configuration 34
Option 1 - Run the Foglight database tool to configure the database 34

Option 2 - Run SQL scripts to configure the database 35
Initializing the database 37
Starting and stopping the Management Server 37
Starting the Management Server 37
Running the Management Server as a Windows service 38
Stopping the Management Server 39
Starting and stopping the Management Server in High Availability mode 39
Logging in to Foglight 39
Monitoring the Management Server host 40
Next steps 40
Running the Management Server FAQ 40

Installing and Upgrading Cartridges 42

Installing Agents 44
Agent installers 44
Remote agent installation 45

1

Before Installing Foglight

This guide provides instructions for installing, configuring, and starting Foglight®. Before you begin, see the *System Requirements and Platform Support Guide*.

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 Foglight, the Foglight Agent Manager, and any 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.

Foglight includes several different components, which are described in the *Getting Started Guide*.

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 *System Requirements and Platform Support Guide*.

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 external 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: Install, configure, and initialize the database, then start the Foglight Management Server and log in.

NOTE: If you are using an external database, the database must be initialized successfully before you can run Foglight.

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. See the *Foglight Agent Manager Guide* for details.

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:

- High Availability mode
- Using an external database
- Creating the database manually
- Licensing
- Installation modes

High Availability mode

Before you install Foglight, determine if you are going to set up and run the Management Server in High Availability (HA) mode or as a standalone server. High Availability mode enables you to install multiple Management Servers where one server is the primary server and the others are standby servers. If the primary server stops responding, then one of the standby servers in the HA cluster takes over the responsibility.

Configuring multiple servers using HA mode offers the following benefits:

- **Automatic restart:** The restart process (FoglightHA Daemon) runs on the same host as the Management Server it is monitoring and monitors the state of the server. If the server stops responding or has a fatal error, then the restart process stops and restarts the server automatically. The process can also send out email notifications about various conditions of the server.

  NOTE: The default value for the restart process is 10 minutes (600 seconds). Machines with a slower processing speed take longer to reboot. You can modify the default time by editing the startup.grace variable in the restart_monitor.config file (located in the config directory).

- **Standby Server:** To reduce outage times, a standby server instance is created (for a particular Foglight Management Server), and forms a partition. One server becomes the primary server and communicates with the agents, receives and processes data, and processes rules. All other servers are standby servers. If a primary server stops responding, one of the standby servers resumes service and becomes the primary server.

Considerations for running the Management Server in HA mode

If you plan to run the Management Server in HA mode, there are certain considerations:

- Specific ports are required for the HA setup to work:
  - Cluster Mcast Port
  - HA JNDI RMI Port
  - HA JNDI JNP Port
  - HA JRMP Invoker Port
  - HA Pooled Invoker Port
  - HA JNDI UDP Group Port

  All of these ports must be set to the same values for all Management Servers in the HA cluster. See the *Administration and Configuration Guide* for port descriptions and default port assignments.
- By default, HA mode works only within the local subnet and uses UDP (User Datagram Protocol) for communication. You can reconfigure your HA cluster to use TCP (Transmission Control Protocol), which can work outside of the local subnet. This alternative is the recommended option if your HA cluster consists of a few designated HA Management Servers. See the *High Availability Field Guide* for more information.

- In both High Availability Mode and Single Server Mode, the database must be running for Foglight to operate. You may have to implement a combined database-backup and High Availability solution to achieve true failover of all components. Failover ensures that monitoring operations are not interrupted.
- A server running in HA mode can only use an external database.

For more information about installing and configuring HA mode, see the *High Availability Field Guide*.

Using an external database

An external instance of the Microsoft® SQL Server® database can be used if your database administrator has installed one. For information about the external databases supported for Foglight, see the *System Requirements and Platform Support Guide*.

NOTE: The Management Server supports connecting to the Microsoft SQL Server database by using the SQL Server Authentication or Windows® Authentication.

A setup with an external database has the advantage of using existing infrastructure. For setup, a remote administrator user/password (with rights to create users, tables, and databases) is required. Remote administrator access must be granted.

NOTE: SQL Server databases must be configured to use a case-sensitive character set collation (for example, UTF-8).

IMPORTANT: If you are using a SQL Server default or named instance, the SQL Server Browser Service must be running in order for Foglight to start up and connect correctly.

Creating the database manually

If your database administrator intends to manually create the external database instance instead of using the `create_db` script, ensure that all of the following requirements are met:

- SQL Server® Authentication or Windows® Authentication is used
- Collation is set to SQL_Latin1_General_CP1_CS_AS
- The Foglight database user has database owner permissions on the Foglight database
- The database account used cannot be more than 16 characters long

In addition, if you are using an SQL Server cluster, Foglight requires the SQL Host name (that is, the actual server name), the SQL instance name, and the database name.

To reduce the size of the transaction logs, set the database to Simple Recovery mode. This step is optional, but recommended.

Planning for authentication with gMSA

When authenticating to the external Foglight database using gMSA (Group Managed Service Accounts), take note of the following requirements.

- The gMSA account must have the following accounts mapped on the external SQL repository.
  - foglight
  - master
  - model
  - msdb
  - tempdb

- When authenticating with gMSA, the Foglight Managements Server and Foglight Agent Manager (FglAM) must be installed as a service. Once installed, the **Log on as** account must be updated to the gMSA account.
- The gMSA account requires the **-PrincipalsAllowedRetrieveManagedPassword** permission.This permission is also required on each service host.

  For an account *gMSA01* and host *ServiceHost*, you can grant this permission with the command: `Set-ADServiceAccount gMSA01 -PrincipalsAllowedToRetrieveManagedPassword gMSA01$,ServiceHost$` t
- The gMSA account must have read and write permissions on the FMS and FglAM installation directories.
- On the machine of the FglAM/Foglight, run the following command `Install-ADServiceAccount -Identity gMSA01`
- The gMSA account(s) must be configured with appropriate access, as stated below:
  - The FMS gMSA account needs access to:
    - SQL Server used for FMS repository if using Windows authentication
    - PI SQL Server instances
  - The FglAM gMSA account needs access to:
    - any SQL Server instances that it monitors
    - WMI/WinRM access to any hosts that need to be monitored.

Licensing

This section provides information about licensing for Foglight.

IMPORTANT: See the *Administration and Configuration Guide* 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 14: 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 the *Administration and Configuration Guide* 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 *Command-Line Reference Guide* 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. However, 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

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:

Windows® - Foglight only

```
Foglight-8_0_0-install_windows-x86_64.exe -i console
```

Windows® - Foglight Evolve

```
Foglight_Evolve-x_x_x-install_windows-x86_64.exe -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.

IMPORTANT: Silent mode does not work if you set parameters in the properties file for Foglight to connect to an external database, and an existing Foglight schema is present in that database. There is no Foglight silent installer parameter for using an existing database schema in order to prevent the contents of an existing database from being lost.
If you attempt to run the silent installer using a properties file that specifies an external database where an existing Foglight schema is present, a fatal error appears in the installation logs. See Installing Foglight FAQ for more information about the error message and workarounds.

To run the installer in silent mode:

Foglight only

```
Foglight-8_0_0-install_windows-x86_64.exe -i silent
```

Foglight for Evolve only

```
Foglight-Evolve-x_x_x-install_windows-x86_64.exe -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; for example, when Foglight is running in High Availability (HA) mode. See the *Administration and Configuration Guide* 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. Must be set to the same value for all Management Servers that are part of the same HA partition. See Configuring the cluster multicast port used in High Availability mode for more information about setting this port when running Foglight in HA mode.	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. Must be set to the same value for all Management Servers that are part of the same HA partition.	None.
FMS_DB_ADMIN_USER	Allows you to specify the database administrator user account. This setting is not required if FMS_DB=embedded. Must be set to the same value for all Management Servers that are part of the same HA partition.	foglight
FMS_DB_HOST	Allows you to specify the host name of the database machine. This setting is not required if FMS_DB=embedded. Must be set to the same value for all Management Servers that are part of the same HA partition.	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. Must be set to the same value for all Management Servers that are part of the same HA partition.	foglight
FMS_DB_PORT	Required. User-defined port or instance name for the database. Must be set to the same value for all Management Servers that are part of the same HA partition.	15432
FMS_DB_SETUPNOW	0 = Set up the database after installation is complete. 1 = Set up the database as part of the installation.	1

Table 1. Properties available for configuring a silent installation

Property	Description	Default
FMS_DB_TYPE	Specifies the database type. Must be set to the database type: (sqlsvr). This setting is not required if FMS_DB=embedded. Must be set to the same value for all Management Servers that are part of the same HA partition.	postgresql
FMS_DB_USER	Database user name. Must be set to the same value for all Management Servers that are part of the same HA partition.	foglight
FMS_DB_USER_PASSWORD	Database user password. Must be set to the same value for all Management Servers that are part of the same HA partition.	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. Must be set to the same value for all Management Servers that are part of the same HA partition.	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 *Administration and Configuration Guide* 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_SERVICE	For enabling Foglight as a Windows® service.	false
FMS_UPGRADE	Only required to update an existing installation, in which case it must be set to 1.	1
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

Table 1. Properties available for configuring a silent installation

Property	Description	Default
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
- HP patch checking tool
- Uninstalling Foglight
- Upgrading the Management Server
- Installing Foglight FAQ

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 administrator privileges. It is recommended that you change the default password for this account.
- The TEMP environment variable is set to a location with sufficient space for installer self-extraction to meet the requirements.
- If you intend to use gMSA (Group Managed Service Accounts) for authentication, the gMSA infrastructure should be configured prior to Foglight installation. Refer to the Microsoft document Group Managed Service Accounts Overview for information.

  Refer to Planning for authentication with gMSA for more information on gMSA requirements.

The following are recommendations for installing Foglight:

- InstallAnywhere recommends that you install as Administrator or use an account that is part of the Administrator group.

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

For more details, see these topics:

- Foglight Server Startup page
- Next steps
- Embedded Agent Manager

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

   - *C:/Quest/Foglight*

   Foglight Evolve

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

Step 5: Choose shortcut location

1 Choose the location where you want to create product icons. There are several options:

- **In a new Program Group**: Accept the default or type the name of the group in the field.
- **In an existing Program Group**: Use the menu to select an existing program group.
- **In the Start Menu**
- **On the Desktop**
- **In the Quick Launch Bar**
- **Other** (default): Browse your system for a shortcut location. Click the **Choose** button to enable the browser.
- **Don't create icons**

Select the **Create Icons for all Users** check box to create shortcuts for all Foglight users.

2 Click **Next**.

Step 6: Foglight service

1 The default option is Do not enable Foglight as a Windows® service. If you want Foglight to run as a Windows service, select **Enable Foglight as a Service**.

2 Click **Next**.

Step 7: 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 8: Installing Foglight

Foglight installs files into the specified directory.

Step 9: 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 10: Foglight mode

1 Select the server mode. The options are **Standalone** (the default) or **HA (High Availability**).

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

2 If you choose **HA (High Availability)**: In the **HA Partition** field, type the partition name. All servers set up in **HA (High Availability)** mode that you want to act as either primary or secondary servers for failover must be configured with the same partition name.

IMPORTANT: Servers with different partition names do not participate in the high availability setup.

NOTE: If you do not choose HA (High Availability) while installing Foglight but want to use HA mode later, you can enable HA mode after installation. For more information, see the *Foglight High Availability Field Guide*.

3 Click **Next**.

Step 11: 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.

NOTE: In Foglight FIPS-compliant mode, it is required to set TrustStore for SQL Server JDBC driver if the SQL Server uses self-signed certificate. For more information, see Setting up an encrypted database connection.

Step 12: Foglight repository database type

This step allows you to select the Foglight database type. The server on which the database is located must be running before you complete this step.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 **SQL Server (External database)** and then click **Next**. See the following section for instructions.

NOTE: The embedded database option does not appear if you selected HA as the server startup mode in Step 10: Foglight mode.

SQL Server external database

If the Management Server you are installing is configured to be part of an HA cluster, you must also configure it to connect to the same database instance as all other members of the cluster. In this case, you set **Server name** and **Database Name** to the same values as the values used for the other members. In some rare cases, certain settings might be different. For example, the value for **Server name** might be different if there is a firewall between the database and certain members of the cluster in your environment.

When using gMSA for authentication, you must install Foglight using **SQL Server Authentication**. Once Foglight is installed, you can configure the appropriate gMSA account for repository authentication. Refer to Planning for authentication with gMSA for more information.

1 In the **Server name** box, type the database host name or IP address (the default is *localhost*).

IMPORTANT: If the port number of the database is not 1433 (standard), specify the host and port (host,port) or host and instance (host\instance). For example: `10.30.125.92,14341` or `10.30.125.92\SHREK`.

2 From the Repository User Account **Authentication** drop-down list, select a method of authentication (Windows® or SQL Server®).

If you select **Windows Authentication**, your Windows user name is populated in the **User Name** box.

NOTE: For Windows authentication, using the LAN Manager Authentication security policy **Send NTLMv2 response only. Refuse LM & NTLM** is not supported. If the authentication level on the host is set for this policy, change the policy before continuing the installation.

3 In the Repository **User Name** box, type the user name if it is not already pre-filled. The Management Server uses this account to connect to the database.

4 In the Repository 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.

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

> **NOTE:** This box is applicable only if you selected SQL Server authentication in step 2.

6 In the **Database Name** box, type the name of the database (the default is *foglight*). This name is the name of the Microsoft® SQL Server instance to which you want the Management Server to connect.

> **IMPORTANT:** If you are using a SQL Server default or named instance, the SQL Server Browser Service must be running for Foglight to start up and connect correctly.

7 Select one of the following **Repository Creation** options:

- **Automatically create the repository database**
- **Manually create the repository database**

8 If you select **Manually create the repository database**, there are two methods you can use to create the database. For more information, see Manual database configuration.

> **IMPORTANT:** You must manually create the database before proceeding.

9 If you select **Automatically create the repository database**, select the Repository Administrator Account **Authentication Method**, and then type the Repository Administrator Account **User Name** and **Password**. The Management Server uses the administrator account credentials to create the SQL Server database.

> **NOTE:** The Repository Administrator Account User Name cannot be the same as the User Account User Name you created in step 3.

> **IMPORTANT:** If the Management Server you are installing is configured to be part of an HA cluster, set the Repository Administrator Account User Name and Password to the same values as the values used for the other Management Servers that share the same HA partition name.

10 Click **Next**.

If a database schema exists, the Foglight Database Found screen appears. This screen allows you to keep your existing data, create a database, or select a different database. If you are running in HA mode, select **Keep existing data**.

If you chose **Manually create the repository database** in step 7, and did not create the database at that time, an error message appears. For more information, see Manual database configuration.

Step 13: 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; for example, when Foglight is running in High Availability (HA) mode. See the *Administration and Configuration Guide* for details.

2 If you are installing Foglight in High Availability (HA) mode and are planning to have multiple HA partitions on the same sub-network, configure a different Cluster Multi-cast Port for each HA partition. The primary server and secondary servers within each HA partition must be configured to use the same Cluster Multi-cast Port.

You can set this port from the Foglight Ports Configuration screen, or change it after installation in the *server.config* file. See Configuring the cluster multicast port used in High Availability mode for information about changing this port after installing Foglight.

IMPORTANT: Errors can occur if servers that are not part of the same HA partition are configured to multicast on the same port on the same sub-network as the HA partition. See Running the Management Server FAQ for more information about these errors.

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

4 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 14: Add Foglight license file

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

IMPORTANT: See the *Administration and Configuration Guide* 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 **Install a license from the following file** box blank and click **Next**.

If you selected **Enable Foglight as a Service** in Step 6: Foglight Service, the Management Server service is enabled and started at this point.

Step 15: 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 16: Foglight server startup

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

NOTE: This screen does not appear if you enabled Foglight to run as a Windows® service.

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 17: Change service credentials [Optional]

When using gMSA authentication, the Log On user for the Foglight service must be changed after installation..

1. Open Services (services.msc)
2. Find the Foglight Service
3. Right-click on the service and choose Properties
4. Update the **Log On User** with the gMSA account. Leave the password field empty.

Step 18: 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;
```

3 Locate `<FMS_HOME>\config\server.config`, update `server.database.host` value to the *FMS DB's Availability Group Listener IP*.

NOTE: For HA environment, both HA peers' `server.database.host` value should be updated.

Next steps

If you performed a Custom Install and you did not install a license in Step 14: 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 *Administration and Configuration Guide* 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.

To set up an encrypted database connection, see Setting up an encrypted database connection.

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 *Agent Manager Guide*.

You can run the embedded Agent Manager in tandem with the server or not. For more information, see the *Agent Manager Guide*.

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 *Agent Manager Guide* 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 2. 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_0_0.car and FTR-WS-1_0_0.car

Table 2. Installed directories

Directory	Contents
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 *Administration and Configuration Guide* 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.bat` in *<install-dir>/bin*
scripts	SQL scripts and examples of the two types of Script Agents. *scripts\agent* contains sample Type 1 and Type 2 Script Agent files. See the *Administration and Configuration Guide* for more information about Script Agents. *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.

Table 2. Installed directories

Directory	Contents
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; for example, when Foglight is running in High Availability (HA) mode. See the *Administration and Configuration Guide* for details.

For more details, see these topics:

- Editing the *server.config file*
- Enabling High Availability mode after installation
- Changing external database credentials
- Importing self-signed certificates to Foglight TrustStore
- Setting up an encrypted database connection
- Setting up an encrypted LDAP connection with SSL
- Using encryption when sending email from Foglight
- Configuring ports
- Configuring the cluster multicast port used in High Availability mode
- Setting up Foglight server federation
- 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.

Enabling High Availability mode after installation

If you want to run Foglight in High Availability (HA) mode but did not select this option during installation, you can enable HA mode after installation by editing the file *server.config*. For more information, see the *Foglight High Availability Field Guide*.

Changing external database credentials

Use the following method to reconfigure Foglight to start up with a new database password. The password can be updated in the *server.config* file.

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.

To encrypt your database password using the keyman command:

1. Specify the following from the command line:

   ```
   > bin\keyman -d [FGLHOME\config] encpwd "<new password>" foglight.defaultkey
   ```

   The encrypted password appears.
2. Open the *server.config* file.
3. Replace the existing database password with the new encrypted database password on the following line:

   ```
   server.database.password = "q4056753111e8a24c9a722048fc6df1f0"
   ```
4. Restart the Management Server.

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 database connection

The *server.config* file contains the optional parameter `foglight.database.secureconn`, which is used as part of the process of setting up an encrypted database connection for a MySQL® or Oracle® database. For Microsoft® SQL Server® database, ssl is enabled by default.

In Foglight FIPS-compliant mode, it is required to import the self-signed SQL Server certificates to Foglight TrustStore. For more information, refer to Importing self-signed certificates to Foglight TrustStore.

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 *Administration and Configuration Guide* for more information.

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

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 *Administration and Configuration Guide*.

NOTE: In certain configurations the Management Server may use ports in addition to the ones that you set using server.config; for example, when Foglight is running in High Availability (HA) mode. See the *Administration and Configuration Guide* for details.

Configuring the cluster multicast port used in High Availability mode

You can change the cluster multicast port that is used when Foglight is running in High Availability (HA) mode. Members of an HA cluster use this port to communicate with each other. For more information, see the *High Availability Field Guide*.

Setting up Foglight server federation

Federation is a Foglight feature that addresses the needs of customers who monitor large-scale environments that are naturally partitioned into logical units. Each of these partitions is traditionally served by one Management Server instance and its distributed clients and agents.

Federation enables you to use one Management Server to operate, while using other Management Server as the data source. For detailed information about Foglight federation and how to create a federated environment, see the *Federation Field Guide*.

IMPORTANT: Federation is an advanced feature, which requires a dedicated Management Server separate from the Management Servers that are acting as data collectors. Contact Quest Professional Services to design and implement a federation strategy.

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.exe

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:

```
cd <foglight_home>\config
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 -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 -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 -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 -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.

HP patch checking tool

If your external database is installed on an HP-UX server, HP provides a tool for ensuring that all the patches required to run Java® on HP-UX are installed.

The tool is available from:

http://www.hp.com/go/java

To use the tool, issue the following command:

```
java -jar ./HPjconfig.jar -nogui -patches -listmis -javavers 6.0
```

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. However, in cases where a graphics display is not available, the Foglight installer can be run from the command line by using the silent uninstaller.

To uninstall Foglight:

1. Stop the Foglight Management Server using the appropriate method:
   - To stop a standalone Management Server that is not running as a Windows® service, follow the instructions in Stopping the Management Server.
   - To stop a standalone Management Server that is running as a Windows service, follow the instructions in Running the Management Server as a Windows service.
   - To stop a Management Server that is running in High Availability (HA) mode, follow the instructions in Starting and stopping the Management Server in High Availability mode.
2. Navigate to the *UninstallerData* directory of your Foglight installation and run the *Uninstall Foglight* executable.
   - To launch the uninstaller in GUI mode, simply run the *Uninstall Foglight* executable.
   - To launch the uninstaller in silent mode, run the *Uninstall Foglight* executable using the following command:
     ```
     "Uninstall Foglight.exe" -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.

Installing Foglight FAQ

When I try to install Foglight with an external database using silent mode, Foglight generates a fatal error that states "Foglight Database Found: Installation canceled". Why does this error occur?

Silent mode does not work if you set parameters in the properties file for Foglight to connect to an external database and an existing Foglight schema is present in that database. There is no Foglight silent installer parameter for using an existing database schema in order to prevent the contents of an existing database from being lost.

If you attempt to run the silent installer using a properties file that specifies an external database where an existing Foglight schema is present, a fatal error like the following appears in the installation logs and the installation fails:

```
An existing Foglight database schema was found.

Cannot continue install. Run the installer in a GUI mode.

Database Install Failed

Foglight Database Found: Installation canceled.


Status: FATAL ERROR
```

If you encounter this error, either run the installer in GUI mode or drop the database manually. When you run the installer in GUI mode, a screen appears if an existing Foglight database schema is found. This screen allows you to keep your existing data, create a database, or select a different database. See Installing a new version of the Management Server for more information.

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:

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

Manual database configuration

If you chose **Manually create the repository database** while installing the Management Server for use with an external database, there are two ways in which you can **configure the database before** starting the Management Server. Choose the one that best suits your needs:

- Option 1 - Run the Foglight database tool to configure the database
- Option 2 - Run SQL scripts to configure the database

Option 1 - Run the Foglight database tool to configure the database

Run Foglight's database tool from the command line after exiting the installer. The database tool is located in the *<foglight_home>\client* directory.

NOTE: Option 1 does not currently support the creation of a SQL Server® database with Windows® integration.

To perform manual database configuration:

- Create the database. Run the following command, including the `-D` parameters and values as required:

  ```
  java [-D...] -jar foglight-database-tool.jar createdb
  ```

  For example:

  ```
  java -Dserver.database.type=sqlsvr -Dserver.database.host=sqldbhost01
  -Dserver.database.port=1433 -Dserver.database.name=foglight -Ddb.admin.user=sa
  -Ddb.admin.password=foglight -Ddb.schema.username=foglight
  -Ddb.schema.password=foglight -Ddb.schema.name=foglight -jar foglight-
  database-tool.jar createdb
  ```

NOTE: The following SQL warnings may appear when creating the database on SQL Server®:
2012-07-03 14:52:21.231 INFO Create database "foglight"...
2012-07-03 14:52:21.809 WARN SQL Warning: Changed database context to 'master'.
2012-07-03 14:52:46.981 WARN SQL Warning: Changed database context to 'foglight'.
2012-07-03 14:52:47.044 INFO Create Schema for database "foglight"...
2012-07-03 14:52:47.512 WARN SQL Warning: Warning! The maximum key length is 900 bytes. The index 'idx_cfgbinder_agent' has maximum length of 1530 bytes. For some combination of large values, the insert/update operation will fail.
2012-07-03 14:52:47.715 WARN SQL Warning: Warning! The maximum key length is 900 bytes. The index 'incident_ticket_index' has maximum length of 1020 bytes. For some combination of large values, the insert/update operation will fail.
2012-07-03 14:52:47.715 WARN SQL Warning: Warning! The maximum key length is 900 bytes. The index 'idx_pcm_name_type' has maximum length of 1786 bytes. For some combination of large values, the insert/update operation will fail.
2012-07-03 14:52:47.934 INFO Populate for database "foglight"...

The database tool requires the following parameters:

- `-Dserver.database.type=<mysql|sqlsrv|oracle|postgresql>`
- `-Dserver.database.host`
- `-Dserver.database.port`
- `-Dserver.database.name`
- `-Ddb.admin.user`

NOTE: The -Ddb.admin.user must exist, and must have database administrator privileges.

- `-Ddb.admin.password`
- `-Ddb.schema.username`

NOTE: The tool creates the `-Ddb.schema.username` user when you run the command.

- `-Ddb.schema.password`
- `-Ddb.schema.name`

NOTE: To delete the database and start over, run the database tool with the dropdb option instead of the createdb option shown in the preceding example. The dropdb option does not remove an existing or new Repository User account.

Option 2 - Run SQL scripts to configure the database

If you clicked **Create** during the database installation step, the SQL scripts in the *<foglight_home>\scripts\sql* directory are prepared with the provided configuration options. SQL Server® generates four SQL scripts for each Authentication type:

- SQL Server Authentication:
  - `sqlsvr_drop_db.sql`
  - `sqlsvr_create_db.sql`
  - `sqlsvr_create_schema.sql`
  - `sqlsvr_populate_db.sql`
- Windows Authentication:

- `sqlsvr_integratedauth_drop_db.sql`
- `sqlsvr_integratedauth_create_db.sql`
- `sqlsvr_create_schema.sql`
- `sqlsvr_populate_db.sql`

You can review these scripts before running them.

You must run the configured scripts against the database using a third-party tool.

To perform manual database configuration with SQL Server Authentication:

1 Launch a command window.

2 Run the *.sql* scripts by issuing the following commands from the prompt in the order shown:

> **NOTE:** In the following commands, replace `<admin_username>` and `<admin_password>` with the user name and password for the user account of the Microsoft SQL Server administrator.

a
```
sqlcmd -U <admin_username> -P <admin_password> -i
<foglight_home>\scripts\sql\sqlsvr_drop_db.sql
```
This script must be run under an account with administrator privileges (for example, *sa*), because you require system access to run it.

b
```
sqlcmd -U <admin_username> -P <admin_password> -i
<foglight_home>\scripts\sql\sqlsvr_create_db.sql
```
This script must be run under an account with administrator privileges (for example, *sa*), because you require system access to run it.

> **NOTE:** The script *sqlsvr_create_db.sql* does not drop the existing schema.

c
```
sqlcmd -U <foglight_username> -P <foglight_password> -i
<foglight_home>\scripts\sql\sqlsvr_create_schema.sql
```
This script must be run using the Foglight Database Account User ID that you set in Step 12: Foglight repository database type. The default Foglight Database Account User ID is *foglight*.

> **NOTE:** Warnings related to the maximum length of index keys appear. These warnings are safe to ignore.

d
```
sqlcmd -U <foglight_username> -P <foglight_password> -i
<foglight_home>\scripts\sql\sqlsvr_populate_db.sql
```
This script must be run using the Foglight Database Account User ID that you set in Step 12: Foglight repository database type. The default Foglight Database Account User ID is *foglight*.

To perform manual database configuration with Windows authentication:

1 Launch a command window.

a
```
sqlcmd -U <admin_username> -P <admin_password> -i
<foglight_home>\scripts\sql\sqlsvr_integratedauth_drop_db.sql
```
This script must be run under an account with administrator privileges (for example, *sa*), because you require system access to run it.

b
```
sqlcmd -U <admin_username> -P <admin_password> -i
<foglight_home>\scripts\sql\sqlsvr_integratedauth_create_db.sql
```
This script must be run under an account with administrator privileges (for example, *sa*), because you require system access to run it.

> **NOTE:** The script *sqlsvr_integratedauth_create_db.sql* does not drop the existing schema.

2 Launch another command window with “Run as windows integration” domain user.

a
```
sqlcmd -i
<foglight_home>\scripts\sql\sqlsvr_create_schema.sql
```

b
```
sqlcmd -i
<foglight_home>\scripts\sql\sqlsvr_populate_db.sql
```

After you have run all four scripts, you can start the Management Server. Proceed to Starting and stopping the Management Server.

Initializing the database

For external databases, once the database has been successfully initialized, you can run Foglight.

Starting and stopping the Management Server

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

- Starting the Management Server
- Running the Management Server as a Windows service
- Stopping the Management Server
- Starting and stopping the Management Server in High Availability mode

Starting the Management Server

The following sections describe how to start the Management Server from the command line or from a Windows® shortcut 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
```

NOTE: To start the Management Server in High Availability mode, see Starting and stopping the Management Server in High Availability mode.

To start the Management Server from a Windows® shortcut:

- Depending on where you installed the startup icon, choose **Start > Programs > Quest > Foglight > Start Foglight** or double-click the **Start Foglight** icon on the desktop.

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

```
Forge Server startup completed.
```

Additional commands

Table 3. Starting the Management Server - additional commands

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

Running the Management Server as a Windows service

After the installation is completed, you can install the Management Server as a Windows® service either from the **Start** menu or the command line.

NOTE: The following procedures assume that you have installed the program shortcuts in the default location.

Using the Start Menu options

To install or remove the Management Server service from the Start menu:

- Choose **Start > Programs > Quest > Foglight 8.0.0 > Windows Service > Install Service for Foglight** (or **Remove Service for Foglight**).

To start or stop the Management Server service from the Start menu:

- Choose **Start > Programs > Quest > Foglight 8.0.0 > Windows Service > Install Service for Foglight** (or **Remove Service for Foglight**).

Using the command line

From the command line, type the following to install the Management Server as a Windows® service:

```
fms.exe --install-service
```

Additional Commands

In addition to the commands listed under Additional commands in Starting and stopping the Management Server, the following commands are available for the Foglight Management Server Windows service.

Table 4. Running the Management Server as a Windows service - additional commands

Command	Represents	Description
`-b`	start-service	Start the Management Server Windows service
`-r`	remove-service	Stop and remove the Management Server Windows service

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`
- Depending on where you installed the startup icon, choose **Start > Programs > Quest > Foglight 8.0.0 > Stop Foglight** or double-click the **Stop Foglight** icon on the desktop.

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

Starting and stopping the Management Server in High Availability mode

Configuring your server in High Availability (HA) mode allows you to run multiple servers in a partition offering HA.

NOTE: To run the HA server, you must use an external database. The database has to be running before you start the Foglight HA server.

To start the High Availability Server:

- Enter the following from the command line:
  `fmsha`

When the server has started successfully, the following message appears in the command window:

```
High Availability Server startup completed.
```

To stop the High Availability Server:

Do one of the following:

- Type **Ctrl-C** in the command window in which the Foglight HA server started.
- Open a second command window, navigate to the *bin* directory, and run the following command:
  `fmsha --stop`
  When the server has stopped successfully, the command window closes.

For more information about configuring and managing High Availability mode, see the *High Availability Field Guide*.

Logging in to Foglight

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

To log in to Foglight:

1. Depending on where you installed the program icons, navigate to **Start > Programs > Quest > Foglight > Foglight Console**
2. Enter a valid user name and password and click **Login**.

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 WindowsAgentPlus 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 for Infrastructure User and Reference Guide*.

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 Windows®, Foglight starts the Quest Common Process Runner (*qcn_runner.exe*) but does not use it to launch new processes.

I am running Foglight in High Availability (HA) mode. When I start my Management Servers, “UDP mcast receiver” errors appear in the logs for the primary and secondary Management Servers. How can I resolve these errors?

If Management Servers that are not part of a particular HA partition are configured to multicast using the same port on the same subnet as the Management Servers within the HA partition, errors like the following appear in the logs for the Management Servers that are configured in this way:

```
ERROR [UDP mcast receiver] org.jgroups.protocols.UDP - message does not have a UDP header
```

or

```
ERROR [UDP mcast receiver] org.jgroups.protocols.UDP - discarded message from different group
```

If you see this type of message, change the cluster multi-cast port of the servers that are reporting the error. In addition, if you plan to have multiple High Availability (HA) partitions on the same sub-net, configure a different cluster multicast port for each HA partition. See Configuring the cluster multicast port used in High Availability mode for instructions.

IMPORTANT: In both cases described here (resolving errors and planning to have multiple HA partitions on the same subnet), the primary server and secondary servers within each HA partition must be configured to use the same cluster multicast port.

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.

- 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 *Administration and Configuration Guide* 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 *Administration and Configuration Guide*.

NOTE: Warning messages similar to the following appear in the Management Server log when you install a cartridge:

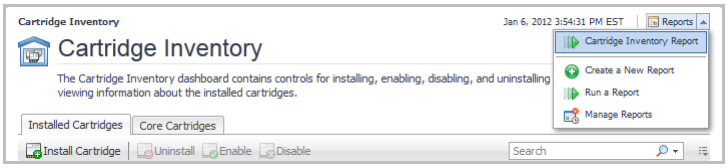
```
WARN — Module system:<name> was converted to the newest version during loading
```

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 Agent Manager Guide*.

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 and the *Administration and Configuration Guide*.

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 *Administration and Configuration Guide* and the *User Guide* 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. See the *Agent Manager Guide*.

For more information about remote agent installation, see the *Administration and Configuration Guide*.

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.