

Foglight® 5.9.x

## **Installation and Setup Guide**

### **Installing on a UNIX System with an External MySQL Database**



© 2018 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 Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit <https://www.quest.com/legal/trademark-information.aspx>. "Apache HTTP Server", Apache, "Apache Tomcat" and "Tomcat" are trademarks of the Apache Software Foundation. Google is a registered trademark of Google Inc. Android, Chrome, Google Play, and Nexus are trademarks of Google Inc. Red Hat, JBoss, the JBoss logo, and Red Hat Enterprise Linux are registered trademarks of Red Hat, Inc. in the U.S. and other countries. CentOS is a trademark of Red Hat, Inc. in the U.S. and other countries. Fedora and the Infinity design logo are trademarks of Red Hat, Inc. Microsoft, .NET, Active Directory, Internet Explorer, Hyper-V, Office 365, SharePoint, Silverlight, SQL Server, Visual Basic, Windows, Windows Vista and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. AIX, IBM, PowerPC, PowerVM, and WebSphere are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Java, Oracle, Oracle Solaris, PeopleSoft, Siebel, Sun, WebLogic, and ZFS are trademarks or registered trademarks of Oracle and/or its affiliates in the United States and other countries. SPARC is a registered trademark of SPARC International, Inc. in the United States and other countries. Products bearing the SPARC trademarks are based on an architecture developed by Oracle Corporation. OpenLDAP is a registered trademark of the OpenLDAP Foundation. HP is a registered trademark that belongs to Hewlett-Packard Development Company, L.P. Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. MySQL is a registered trademark of MySQL AB in the United States, the European Union and other countries. Novell and eDirectory are registered trademarks of Novell, Inc., in the United States and other countries. VMware, ESX, ESXi, vSphere, vCenter, vMotion, and vCloud Director are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. Sybase is a registered trademark of Sybase, Inc. The X Window System and UNIX are registered trademarks of The Open Group. Mozilla and Firefox are registered trademarks of the Mozilla Foundation. "Eclipse", "Eclipse Foundation Member", "EclipseCon", "Eclipse Summit", "Built on Eclipse", "Eclipse Ready" "Eclipse Incubation", and "Eclipse Proposals" are trademarks of Eclipse Foundation, Inc. IOS is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Apple, iPad, iPhone, Mac OS, Safari, Swift, and Xcode are trademarks of Apple Inc., registered in the U.S. and other countries. Ubuntu is a registered trademark of Canonical Ltd. Symantec and Veritas are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. OpenSUSE, SUSE, and YAST are registered trademarks of SUSE LCC in the United States and other countries. Citrix, AppFlow, NetScaler, XenApp, and XenDesktop are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. AlertSite and DéjàClick are either trademarks or registered trademarks of Boca Internet Technologies, Inc. Samsung, Galaxy S, and Galaxy Note are registered trademarks of Samsung Electronics America, Inc. and/or its related entities. MOTOROLA is a registered trademarks of Motorola Trademark Holdings, LLC. The Trademark BlackBerry Bold is owned by Research In Motion Limited and is registered in the United States and may be pending or registered in other countries. Quest is not endorsed, sponsored, affiliated with or otherwise authorized by Research In Motion Limited. Ixia and the Ixia four-petal logo are registered trademarks or trademarks of Ixia. Opera, Opera Mini, and the O logo are trademarks of Opera Software ASA. Tevron, the Tevron logo, and CitraTest are registered trademarks of Tevron, LLC. PostgreSQL is a registered trademark of the PostgreSQL Global Development Group. MariaDB is a trademark or registered trademark of MariaDB Corporation Ab in the European Union and United States of America and/or other countries. Vormetric is a registered trademark of Vormetric, Inc. Intel, Itanium, Pentium, and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries. Debian is a registered trademark of Software in the Public Interest, Inc. OpenStack is a trademark of the OpenStack Foundation. Amazon Web Services, the "Powered by Amazon Web Services" logo, and "Amazon RDS" are trademarks of Amazon.com, Inc. or its affiliates in the United States and/or other countries. Infobright, Infobright Community Edition and Infobright Enterprise Edition are trademarks of Infobright Inc. POLYCOM®, RealPresence® Collaboration Server, and RMX® are registered trademarks of Polycom, Inc. All other marks and names mentioned herein may be trademarks of their

respective companies.

## Legend

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

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

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

Foglight Installation and Setup Guide  
Updated - October 2018  
Software Version - 5.9.x

# Contents

<b>Before Installing Foglight</b> .....	<b>6</b>
What is Foglight? .....	6
Hardware requirements and guidelines .....	6
Planning your installation .....	7
High Availability mode .....	8
Using an external database .....	9
Licensing .....	9
Managing licenses .....	10
Installation modes .....	10
<b>Installing Foglight</b> .....	<b>15</b>
Preparing to install .....	15
Installing a new version of the Management Server .....	16
Foglight Server Startup page .....	20
Next steps .....	20
External MySQL database access for remote users .....	20
Embedded Agent Manager .....	21
Installed directories .....	22
Foglight settings .....	23
Editing the <i>server.config</i> file .....	24
Enabling High Availability mode after installation .....	24
Changing external database credentials .....	24
Setting up an encrypted database connection with SSL .....	25
Setting up an encrypted LDAP connection with SSL .....	25
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 the SQL Parser properties .....	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 .....	29
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
<b>Running the Management Server</b> .....	<b>34</b>
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 and tuning the database .....	36
Initializing the database .....	36
Tuning an external MySQL database for Foglight .....	36
Starting and stopping the Management Server .....	37
Starting the Management Server .....	37
Stopping the Management Server .....	38
Starting and stopping the Management Server in High Availability mode .....	39
Logging in to Foglight .....	39
Monitoring the Management Server host .....	39
Next steps .....	40
Migrating data from an existing database .....	40
Running the Management Server FAQ .....	41
<b>Installing and Upgrading Cartridges .....</b>	<b>43</b>
<b>Installing Agents .....</b>	<b>45</b>
Agent installers .....	45
Remote agent installation .....	46

# 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](#)

**i** | **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.

**i** | **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](#).

**i** | **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.

**i** | **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.

**i** | **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](#)
- [Licensing](#)
- [Managing licenses](#)
- [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 MySQL® with an InnoDB storage engine can be used if your database administrator has installed one. Please see the [System Requirements and Platform Support Guide](#) for information about the external databases supported for Foglight.

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 and tables in the user/temp tablespace is required.

- NOTE:** External MySQL databases must be configured to use a case-sensitive character set collation (for example, UTF-8). External MySQL databases have to use the InnoDB table storage engine and must be configured for mixed-mode logging.

## 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 12: 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.

**i** | **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.

## Managing licenses

**i** | **NOTE:** This section is relevant only when installing Foglight for Virtualization, Enterprise Edition or Foglight for Storage Management systems.

When you install Foglight for Storage Management, a 45-day trial license is activated.

When you install Foglight for Virtualization, Enterprise Edition, Foglight for Storage Management is also installed along with a 45-day trial license. You must activate the Foglight for Storage Management trial license.

Foglight for Virtualization, Enterprise Edition and Foglight for Storage Management are licensed separately. You can install a purchased license of Foglight for Storage Management at any time, either during the 45-day trial, or after the trial period has expired. When the trial license expires, the Foglight for Storage Management user interface is disabled. Your access to Foglight continues according to your Foglight license.

**i** | **NOTE:** Foglight for Storage Management functionality requires an active, licensed Foglight installation. It cannot be accessed independently from Foglight.

If you later purchase a license, the process for installing a Foglight for Storage Management license is the same as it for installing a Management Server license. For more information, see [Importing a license file after installation](#).

## Installation modes

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

### Console mode

For Foglight systems, the console mode is available on UNIX® only for Solaris (SPARC 64 or x86-64) and Linux®.

For Foglight for Virtualization, Enterprise Edition and Foglight for Storage Management systems, the console mode is available on UNIX only for Linux

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

To execute the console mode, type the following command:

#### Solaris - Foglight only

```
Foglight-5_9_x-install_solaris-sparc64.bin -i console
```

```
Foglight-5_9_x-install_solaris-x86_64.bin -i console
```

#### Linux® - Foglight only

```
Foglight-5_9_x-install_linux-ia32.bin -i console
```

```
Foglight-5_9_x-install_linux-x86_64.bin -i console
```

## Linux® - Foglight for Virtualization, Enterprise Edition only

```
Foglight_Virtualization-Enterprise-x_x_x-install_linux-ia32.bin -i console
```

```
Foglight_Virtualization-Enterprise-x_x_x-install_linux-x86_64.bin -i console
```

## Linux® - Foglight for Storage Management only

```
FoglightStorageManagement-x_x_x-install_linux-ia32.bin -i console
```

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

## Silent mode

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

- i** | **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:**

### Solaris - Foglight only

```
Foglight-5_9_x-install_solaris-sparc64.bin -i silent
```

```
Foglight-5_9_x-install_solaris-x86_64.bin -i silent
```

### Linux® - Foglight only

```
Foglight-5_9_x-install_linux-ia32.bin -i silent
```

```
Foglight-5_9_x-install_linux-x86_64.bin -i silent
```

### Linux® - Foglight for Virtualization, Enterprise Edition only

```
Foglight-Virtualization-Enterprise-x_x_x-install_linux-ia32.bin -i silent
```

```
Foglight-Virtualization-Enterprise-x_x_x-install_linux-x86_64.bin -i silent
```

### Linux® - Foglight for Storage Management only

```
FoglightStorageManagement-x_x_x-install_linux-ia32.bin -i silent
```

```
FoglightStorageManagement-x_x_x-install_linux-x86_64.bin -i silent
```

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

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

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

**Table 1. Properties files that the installer uses**

<b>The installer:</b>	<b>uses the properties file:</b>
<i>FoglightStorageManagement-x_x_x-install_linux-ia32.bin</i>	<i>FoglightStorageManagement-x_x_x-install_linux-ia32.properties</i>
<i>Foglight-5_9_x-install_linux-ia32.bin</i>	<i>Foglight-5_9_x-install_linux-ia32.properties</i>

**i** | **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 2. Properties available for configuring a silent installation**

<b>Property</b>	<b>Description</b>	<b>Default</b>
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 <a href="#">Configuring the cluster multicast port used in High Availability mode</a> 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 <code>external</code> if <code>FMS_HA_MODE=1</code>	embedded
FMS_DB_ADMIN_PASSWORD	Allows you to specify the password for the database administrator user account. This setting is not required if <code>FMS_DB=embedded</code> . 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 <code>FMS_DB=embedded</code> . 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 <code>FMS_DB=embedded</code> . 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 <code>FMS_DB=embedded</code> . Must be set to the same value for all Management Servers that are part of the same HA partition.	foglight
FMS_DB_PORT	User-defined port 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 2. Properties available for configuring a silent installation**

Property	Description	Default
FMS_DB_TYPE	Specifies the database type. Must be set to the database type: (mysql). 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. <b>NOTE:</b> See the <i>Administration and Configuration Guide</i> for information about license requirements, managing licenses, and the different categories of cartridges (based on their license requirements).	None (the license file you specify is validated).
FMS_QP5APP_PORT	The port for an embedded query engine.	8448
FMS_RUN_NOW	Starts the Management Server at the end of the installation.	false
FMS_UPGRADE	Only required to update an existing installation, in which case it must be set to 1.	1
INSTALLER_UI	The property is set to SILENT for silent mode. This setting is the default one and is mandatory.	SILENT
USER_INSTALL_DIR	The Foglight installation directory. If you want to upgrade an existing installation, specify the path to the existing installation directory here (and ensure that FMS_UPGRADE is set to 1).	None.
USER_SHORTCUTS	Sets the shortcut location.	None.
FMS_SERVICE_LINUX_ENABLED	For enabling Foglight as a Linux service, in which case it must be set to 1.	0
FMS_SERVICE_LINUX_VALID_PLATFORM	For enabling Foglight as a Linux service, in which case it must be set to true.	false
FMS_SERVICE_LINUX_RUN_USER	The username who is used to run the Foglight.	None.



# 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](#).

**i** | **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.
  - i** | **NOTE:** Ensure that a host name resolution and reverse lookup are confirmed prior to installing the Foglight Management Server.
  - NOTE:** Link-local IPv6 addresses are not supported for the Management Server because many web browsers do not support link-local IPv6 addresses.
- Administrator or root access to all machines requiring a Foglight agent.
- An administrator password for Foglight. The user name *foglight* and the default password for this account can initially be used to log in to the browser interface and to use command-line interface options with root privileges. It is recommended that you change the default password for this account.
- A user account on the machine where you are installing Foglight.
- The IATEMPDIR environment variable is set to a location with sufficient space for installer self-extraction to meet the requirements described in the document available at:  
[https://flexeracomcommunity.force.com/customer/articles/en\\_US/INFO/Q000054](https://flexeracomcommunity.force.com/customer/articles/en_US/INFO/Q000054)

# 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](#)
- [External MySQL database access for remote users](#)
- [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**
    - *.../Quest/Foglight*
  - Foglight for Virtualization, Enterprise Edition**
    - *.../Quest/Foglight/Program Files*
  - Foglight for Storage Management**
    - *.../Quest/StorageManagement/Program Files*
- 2 You can also click the **Browse** button to navigate to a different location.
- 3 Click **Next**.



## Step 5: Choose link location

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

## Step 6: Pre-installation summary

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

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

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

## Step 7: Installing Foglight

Foglight installs files into the specified directory.

## Step 8: Foglight administrator password

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

## Step 9: Foglight mode

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

**i** | **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.

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

**i** | **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 10: 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 **MySQL (External database)** and then click **Next**. See the following section for instructions.

- i** | **NOTE:** The embedded database option does not appear if you selected HA as the server startup mode in [Step 9: Foglight mode](#).

If you install and configure a MySQL® database instance as an external database and this instance is to run on a different machine than the one hosting the server, select the **MySQL** option to make the database accessible remotely.

## MySQL external database

- i** | **NOTE:** For information about granting remote users access to the database, see [External MySQL database access for remote users](#).

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. This typically means that you set **Host**, **Port**, and **Database Name** to the same values as those used for the other members. In some rare cases, certain settings might be different. For example, the value for **Host** might be different if there is a firewall between the database and certain members of the cluster in your environment.

- 1 In the **Host** box, type the database host name or IP address (the default is *localhost*).
- 2 In the **Port** field, type a port number or accept the default (3306). This is the TCP/IP port on which the database communicates with the Management Server. The external database needs to be configured to communicate on this port.
- 3 In the **Database Name** field, type the name of the database (the default is *foglight*).
- 4 In the Foglight Repository **User Name** box, accept the default user name or type an alternate one. The Management Server uses this account to connect to the database.
- 5 In the Foglight Repository User Account **Password** box, accept the default password or type an alternate one. The Management Server uses this password to connect to the database.
- 6 In the Foglight Repository User Account **Retype Password** box, accept the default or, if you have provided an alternate password in step 5, re-type the password for verification.
- 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](#).

- i** | **NOTE:** 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 MySQL® database.

- i** | **NOTE:** The Repository Administrator Account User Name cannot be the same as the User Account User Name you created in step 4.

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

- 10 Click **Next**.

If a database schema already exists, the Foglight Database Found screen appears. This screen allows you to keep your existing data, create a new 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 11: Foglight ports configuration

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

**i** | **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 Help](#) 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.

**i** | **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**.

**i** | **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 12: Add Foglight license file

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

**i** | **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 **License File** box blank and click **Next**.

**i** | **NOTE:** You can install Foglight for Virtualization, Enterprise Edition with the default option of a 45-day trial license, or import an existing license. To install the default option, select Install a trial license, then click Next. To import an existing license, follow the preceding procedure.

## Step : Add Foglight to system service

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

**i** | **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 14: Foglight server startup

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

- 1 To start the Management Server (the default setting), click **Next**.  
If you do not want the installer to start the Management Server, clear the **Run Now** check box, then click **Next**.
- 2 If you selected **Run Now**, the installer starts Foglight and the Foglight Server Startup page launches in a web browser (if a web browser is available). If a web browser is not available, the Foglight Server Startup page does not launch.  
See [Foglight Server Startup page](#) for more information.  
In either case, the Install Complete screen appears.

## Step 15: 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?](#).

## Next steps

If you performed a Custom Install and you did not install a license in [Step 12: 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 with SSL](#).

## External MySQL database access for remote users

Before installing Foglight with an external MySQL® database, the `GRANT ALL ON` query needs to be executed once in order to give users remote access to the database.

### To provide users with remote access to the database:

- 1 From the **MySQL Server Instance Configuration** dialog box, select the **Modify Security Settings** check box.
- 2 Type a **new root password** (this password is used when executing the `GRANT ALL ON` query executed below).
- 3 Select the **Enable root access from remote machines** check box.

## Executing the Grant All On Query script

### Option 1

For better security, employ this option when the MySQL® instance is being used for more than one database.

#### To grant remote access to the MySQL Administrator account, create the database, and grant remote access to the database:

- From the `mysql` prompt, type:

```
GRANT ALL ON mysql.* TO 'root'@'%' IDENTIFIED BY '<password>' with grant option;

CREATE DATABASE <database_name> DEFAULT CHARACTER SET utf8 COLLATE utf8_bin;

GRANT ALL ON <database_name>.* to 'root'@'%' identified by '<password>' with grant option;
```

Where `<database_name>` is the database name you will specify while installing Foglight and `<password>` is the *root* password you specified in the procedure “To provide users with remote access to the database,” above.

This gives the *root* user (with username *root* and password `<password>`) remote access with all privileges.

### Option 2

Use this option only when the MySQL® instance is dedicated entirely to Foglight.

#### To grant remote access to the entire MySQL instance:

- From the `mysql` prompt, type:

```
GRANT ALL ON *.* TO 'root'@'%' IDENTIFIED BY '<password>' with grant option;
```

Where `<password>` is the *root* password you specified in the procedure “To provide users with remote access to the database,” above.

This gives the *root* user (with username *root* and password `<password>`) remote access with all privileges.

**i** | **IMPORTANT:** In some cases, following one of these options might not give `grant_priv` to the *root* user. If `grant_priv` is missing for `root@%` after executing the `GRANT ALL ON` query, see [Installing Foglight FAQ](#) for more information.

## 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](#).

**i** **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 3. Installed directories**

Directory	Contents
<i>bin</i>	Foglight executables for running the server and utilities.
<i>cartridge</i>	Installed cartridge files in their original form.
<i>client</i>	Files that client programs (such as the command-line client) use for remote access to Foglight.
<i>compat</i>	Cartridge files: Core-HostServices-compatibility-5_9_x.car and FTR-WS-1_0_0.car
<i>config</i>	Configuration files and subdirectories. The files in the <i>config</i> 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.
<i>docs</i>	HTML and PDF versions of the product documentation.
<i>dtd</i>	Descriptors for configuration files that can be imported into Foglight (for example, by installing a cartridge).
<i>extension</i>	Directory for extension cartridges (optional cartridges that are not installed by default).
<i>fglam</i>	Directories for the embedded Agent Manager.
<i>jre</i>	Version of the JRE (1.8) that Foglight uses.
<i>lib</i>	The Foglight JAR files.
<i>license</i>	The Foglight license file you install. <b>NOTE:</b> See the <a href="#">Administration and Configuration Guide</a> for information about license requirements, managing licenses, and the different categories of cartridges (based on their license requirements).
<i>logs</i>	Default location of the log files that Foglight generates when it runs. Generated at runtime.
<i>postgresql</i>	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: <code>[run shutdown]Db.sh in &lt;install-dir&gt;/bin</code>

**Table 3. Installed directories**

Directory	Contents
<i>scripts</i>	SQL scripts and examples of the two types of Script Agents. <i>scripts/agent</i> contains sample Type 1 and Type 2 Script Agent files. See the <a href="#">Administration and Configuration Guide</a> for more information about Script Agents. <i>scripts/sql-templates</i> 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.
<i>server</i>	JAR files and data files that a particular Foglight server variant uses (such as <i>default</i> ).
<i>state</i>	Where the running state of Foglight is kept. It includes the following sub-directories: <ul style="list-style-type: none"> <li><i>cartridge.exploded</i>. 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 <b>should not modify</b> this data (even if the server is not running).</li> <li><i>postgresql-data</i>. Default location for the embedded PostgreSQL® data.</li> </ul>
<i>support</i>	Where support bundled archive information is stored.
<i>tmp/cartridge.deployed</i>	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.
<i>tools</i>	Various Foglight utilities.
<i>UninstallerData</i>	Files that the Foglight uninstaller uses.
<i>upgrade</i>	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.

**i** | **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](#)
- [Setting up an encrypted database connection with SSL](#)
- [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 the SQL Parser properties](#)
- [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.

**i** | **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.



# Setting up an encrypted database connection with SSL

The following procedure outlines how to set up a secure external MySQL® database connection and verify that the MySQL® Server supports SSL encryption.

**i | NOTE:** This procedure must be performed after installation but before you start the Management Server.

## To set up an encrypted external MySQL database connection with SSL:

- 1 Import a CA certificate into the Management Server keystore (cacerts) as outlined in [Importing a network security certificate](#).
- 2 Update the MySQL configuration file (*my.ini*) with the new security certificate and key information by adding the following properties:
  - `ssl-ca=<cacert.pem>`
  - `ssl-cert=<server-cert.pem>`
  - `ssl-key=<server-key.pem>`
- 3 Uncomment and set the `server.database.secureconn` attribute in the *server.config* file to true, as shown below.

```
server.database.secureconn = "true";
```

**i | NOTE:** Do not enable this option until the database server's CA certificate is properly imported into `<foglight_home>/jre/lib/security/cacerts`.

- 4 Start the database.
- 5 Start the Management Server.

## To verify whether the MySQL Server (mysqld) supports SSL connections:

- 1 Ensure that the MySQL Server (*mysqld* program) for your Foglight database is running.
- 2 Login to *mysql*:

```
mysql --host <hostname> -port=<mysql_db_port_number> -user=<mysql_user> --password=<mysql_user_password>
```

- 3 At the *mysql* prompt, run the following query:

```
show variables like 'have_ssl'
```

- 4 The output shows the variable `have_ssl` with a value of either `YES` or `DISABLED`.

If the value is `YES`, the MySQL® Server supports SSL connections. If the value is `DISABLED`, the MySQL Server supports SSL connections but was not started with the appropriate SSL command options (`-ssl-<option_name>=<value>`). See the MySQL documentation for more information about these options.

# 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, `<foglight_home>/jre/lib/security/cacerts` (default password: `changeit`), with the following command:

```
<foglight_home>/jre/bin/keytool -J-server import file <path_to_cert_file>  
alias ldapsvrcert keystore <path_to_cacerts> storepass <store_pwd>
```

**i** | **NOTE:** If you do not specify the password using the `-storepass` option, `keytool` prompts you to supply it.

**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.

The following are the examples of command for importing Root CA and intermediate CA certificates:

- Root CA certificate: `<foglight_home>\jre\bin\keytool -import -trustcacerts -alias ldapsvrcert -keystore <path_to_cacerts> -storepass changeit -file <path_to_cert_file>`
  - Intermediate CA certificate 1: `<foglight_home>\jre\bin\keytool -import -alias ldapsvrcert2 -keystore <path_to_cacerts> -storepass changeit -file <path_to_cert_file>`
  - Intermediate CA certificate 2: `<foglight_home>\jre\bin\keytool -import -alias ldapsvrcert3 -keystore <path_to_cacerts> -storepass changeit -file <path_to_cert_file>`
- 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
```

**i** | **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 Help](#) 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 Help](#).

**i** | **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](#).

**i** | **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 the SQL Parser properties

The following default system properties appear in the `server.config` file. The port setting can be changed during the install process, or by editing the `server.config` file.

```
# qp5app port and info
server.qp5app.max.connections = "10";
server.qp5app.port = "8448";
```

## 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.

**i** | **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

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.

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

# Importing a network security certificate

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

<foglight\_home>/jre/bin/keytool

There are two keystores that Foglight uses:

- The built-in Tomcat™ keystore located at:  
<foglight\_home>/config/tomcat.keystore (default password: nitrogen)
- The Management Server keystore located at:  
<foglight\_home>/jre/lib/security/cacerts (default password: changeit)

### To import a certificate:

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

```
cp tomcat.keystore <your_backup_key>
```

- 2 Delete the existing *tomcat* key from the *tomcat.keystore* directory using the following command:

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

- 3 Create a new key under the *tomcat* alias using the following command:

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

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

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

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

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

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

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.

- i** | **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 tomcat.keystore -deststorepass nitrogen -destalias tomcat -srckeystore <your certificate pfx file> -srcstorepass <certificate pfx password> -srcstoretype pkcs12 -srcalias <alias name in step 2>
```

- 4 On the Management Server, open the *<foglight\_home>/server/tomcat/server.xml* file for editing.
- 5 In the *server.xml* file, locate the following *Connector* element and add *keyPass* and *keyAlias* parameters at the end:

```
<Connector executor="tomcatThreadPool" maxHttpHeaderSize="8192"
URIEncoding="UTF-8" scheme="https" secure="true" SSLEnabled="true"
clientAuth="false" keystoreFile="../../config/tomcat.keystore"
keystorePass="q171ede14ed29f0c1ee9dc65f698d8e6d" sslProtocol="TLS"
sslEnabledProtocols="TLSv1.2,TLSv1.1,TLSv1,SSLv2Hello" bindOnInit="false"
maxThreads="900" keyPass="<certificate pfx password>" keyAlias="tomcat"/>
```

## Setting the length of Foglight sessions

- i** | **NOTE:** This section applies only to Foglight for Virtualization, Enterprise Edition.

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

### To uninstall Foglight:

- 1 Stop the Foglight Management Server using the appropriate method:
  - To stop a standalone Management Server, follow the instructions in [Stopping the Management Server](#).
  - 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* shell script.
  - To launch the uninstaller in GUI mode, simply run the *Uninstall\_Foglight* shell script.
  - **Linux® and Solaris only:** To launch the uninstaller in console mode, run the *UninstallFoglight* shell script using the following command:

```
./Uninstall_Foglight -i console
```
  - To launch the uninstaller in silent mode, run the *Uninstall\_Foglight* shell script using the following command:

```
./Uninstall_Foglight -i silent -f installvariables.properties
```
- 3 After uninstallation, you can safely delete the *<foglight\_home>* directory. It is recommended that you do so, since the uninstaller does not remove certain directories within *<foglight\_home>*.

**i | 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.

### **If it was not set by executing the GRANT ALL ON query, is there a way to manually set grant\_priv to give users remote access to an external MySQL® database running with Foglight?**

Yes. In some cases, executing the GRANT ALL ON query may not set `grant_priv` to `y` for the `root` user in the `user` table.

If `grant_priv` is missing for `root@%` after running the GRANT ALL query as described in “Executing the Grant All On Query Script” on page 24, follow the instructions below to manually set the required permission.

#### **To update the user table to set grant\_priv to the required value for the root user:**

- 1 Login to MySQL as `root`:

```
mysql -u root -p <password>
```

In this command, replace `<password>` with the root password you specified in the procedure “To provide users with remote access to the database:” on page 24.

- 2 From the `mysql` prompt, run the following command to give `grant_priv` to `root` for your database:

```
GRANT ALL ON <database_name> TO 'root'@'%' IDENTIFIED BY <password> with grant option;
```

In this command, replace `<database_name>` with the database name you specified while installing Foglight and `<password>` with same root password you provided above.

# 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 and tuning 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.

#### **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=mysql -Dserver.database.host=mysqldbhost01
  Dserver.database.port=3306  Dserver.database.name=foglight
  Ddb.admin.user=root  Ddb.admin.password=foglight
  Ddb.schema.username=foglight  Ddb.schema.password=foglight
  Ddb.schema.name=foglight  jar foglight-database-tool.jar createdb
```

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`

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

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

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

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

**i** | **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.

## 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. There are four SQL files for each database type (`[dbtype]`):

- `[dbtype]_drop_db.sql`
- `[dbtype]_create_db.sql`
- `[dbtype]_create_schema.sql`
- `[dbtype]_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:

- Run the `.sql` scripts by issuing the following commands in the order shown:

a `mysql -u<DBA_username> -p<DBA_password> --force < <foglight_home>/scripts/mysql_drop_db.sql`

**i** | **NOTE:** When a user does not exist in the current database, the script generates “DROP USER failed” errors messages. These errors can be safely ignored.

b `mysql -u<DBA_username> -p<DBA_password> < <foglight_home>/scripts/mysql_create_db.sql`

c `mysql -u<foglight_username> -p<foglight_password> < <foglight_home>/scripts/mysql_create_schema.sql`

This script must be run using the Foglight Database Account User ID that you set in [Step 10: Foglight repository database type](#). The default Foglight Database Account User ID is `foglight`.

d `mysql -u<foglight_username> -p<foglight_password> < <foglight_home>/scripts/mysql_populate_db.sql`

This script must be run using the Foglight Database Account User ID that you set in [Step 10: Foglight repository database type](#). The default Foglight Database Account User ID is `foglight`.

### Example (for Foglight only):

```
a mysql -uroot -ppassword --force  
<../Quest/Foglight/scripts/mysql_drop_db.sql
```

**i** | **NOTE:** When a user does not exist in the current database, the script generates “DROP USER failed” errors messages. These errors can be safely ignored.

```
b mysql -uroot -ppassword <../Quest/Foglight/scripts/mysql_create_db.sql
```

```
c mysql -uroot -ppassword  
<../Quest/Foglight/scripts/mysql_create_schema.sql
```

```
d mysql -uroot -ppassword <../Quest/Foglight/scripts/mysql_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 and tuning the database

The following sections describe how to initialize and tune your database:

- [Initializing the database](#)
- [Tuning an external MySQL database for Foglight](#)

### Initializing the database

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

**i** | **IMPORTANT:** Do not make the MySQL® database file *my.cnf* world-writable, for example by issuing the command `chmod a+w <path_to_file>/my.cnf`. Foglight and the database cannot start if there is world access to the configuration file *my.cnf*.

### Tuning an external MySQL database for Foglight

If you are running the Management Server with an external MySQL® database in a production environment, you may want to tune your database to ensure that it is not under-resourced. The table below lists the tunable settings in the `<mysql_install_path>/my.ini` file.

**i** | **NOTE:** Database tuning is an advanced-user activity. Changing settings for your MySQL database incorrectly can result in problems with your Foglight installation, such as serious performance problems with the Management Server.

**Table 4. Tuning an external database - tunable settings**

| <b>my.ini setting</b>                        | <b>Recommended Value</b> | <b>Comments</b>                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>innodb_additional_mem_pool_size</code> | 20M                      | Additional memory pool used by InnoDB to store metadata information.                                                                                                                                                                                                                                                                                                                                                                         |
| <code>innodb_buffer_pool_size</code>         | 512M                     | InnoDB uses a buffer pool to cache both indexes and row data. The larger you set this the less disk I/O is needed to access data in tables. Note that on 32-bit systems you might be limited to 2 to 3.5G of user level memory per process, so do not set it too high. Also, ensure that the host has enough real memory free for specified buffer pool size. Performance will degrade substantially if the buffer pool uses virtual memory. |
| <code>innodb_flush_log_at_trx_commit</code>  | 2                        | Value 2 means that the transaction log is only flushed to the OS cache rather than to disk at each commit. The log file is still flushed to disk approximately once per second.                                                                                                                                                                                                                                                              |
| <code>innodb_log_buffer_size</code>          | 8M                       | The size of the buffer InnoDB uses for buffering log data.                                                                                                                                                                                                                                                                                                                                                                                   |
| <code>innodb_log_file_size</code>            | 128M                     | Size of each log file in a log group. You should set the combined size of log files to about 25 to 100% of your buffer pool size to avoid unneeded buffer pool flush activity on log file overwrite. Note that a larger log file size will increase the time needed for the recovery process.                                                                                                                                                |
| <code>max_connections</code>                 | 50 or more               | The maximum amount of concurrent sessions the MySQL® server will allow.                                                                                                                                                                                                                                                                                                                                                                      |
| <code>tmp_table_size</code>                  | 32M                      | Maximum size for internal (in-memory) temporary tables.                                                                                                                                                                                                                                                                                                                                                                                      |

## Starting and stopping the Management Server

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

- [Starting the Management Server](#)
- [Stopping the Management Server](#)
- [Starting 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 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
```

**i** | **NOTE:** To start the Management Server in High Availability mode, see [Starting and stopping the Management Server in High Availability mode](#)

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

```
Forge Server startup completed.
```

## Additional commands

Table 5. Starting the Management Server - additional commands

| Commands | Represents                    | Description                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -s       | start                         | Starts the Management Server (this option is assumed if no command is specified).                                                                                                                                                                                                                                                                                                                                |
| -d       | start the process as a daemon | Starts the Management Server as a daemon (if the process is not started as a daemon, the command prompt is held captive by the running Management Server, and remains in the foreground).<br><b>NOTE:</b> The following scripts in <code>\$FGLHOME/bin</code> directory can start the Management Server as a daemon and shut it down, respectively:<br><code>fmsStartup.sh</code><br><code>fmsShutdown.sh</code> |
| -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.<br>Can be used to set more than one VM option.                                                                                                                                                                                                                                                                                                             |
| -v       | version                       | Displays the version number for this program and exits.                                                                                                                                                                                                                                                                                                                                                          |
| -h       | help                          | Shows this information, and additional options, then exits.                                                                                                                                                                                                                                                                                                                                                      |

## Initialization scripts

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

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

## Stopping the Management Server

The following section describes how to stop the Management Server.

### To stop the Management Server:

Do one of the following:

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

```
fms --stop
```

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

# 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.

**i** | **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

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

## To log in to Foglight using a web browser:

- 1 Open a web browser and type the following:

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

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

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

**i** | **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](#) on page 37.

- 1 Log in to Foglight.
- 2 On the navigation panel, under Dashboards, click **Administration > Agents > Agent Status**.
- 3 On the Agent Status dashboard, find the UnixAgentPlus called `EmbeddedHostMonitor`.

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

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

- 1 On the navigation panel, under Dashboards, click **Infrastructure**.
- 2 From the Select a Service list, select the service for the host.
- 3 On the Monitoring tab, select the host from the list.

For more information about monitoring activities and exploring the data collected for the host, see the [Foglight for Infrastructure User and Reference Guide](#).

## Next steps

To install cartridges, see [Installing and Upgrading Cartridges](#).

# Migrating data from an existing database

The contents of the MySQL® database can be copied to another MySQL instance via an export/import cycle.

The following procedure performs a full export of the database and can be run against a database currently in use by a server.

**To export and import a MySQL database:**

- 1 Run the following command from the MySQL command shell:

```
mysqldump -u <username> -p <password> -h <hostname> -P <port> --databases  
<database name> --routines --single-transaction > backup.sql
```

The `-h` parameter can be omitted if the database is on the same host.

- 2 Import the database using the following syntax:

```
mysql -u <username> -p <password> -P <port> < backup.sql
```

The import process recreates the tables in the database. Therefore, any data that was in the destination environment prior to the import is lost.

**i | NOTE: The Foglight servers must be stopped during the import process.**

When moving a database between environments, care should be taken to ensure that the Foglight schema version is lower or equal to the Management Server version in the destination environment, as an upgrade to a new schema is possible. Start the Management Server with the option:

```
-Dfoglight.database.upgrade=true
```

or run `foglight_db_upgrade.sh`.



# Running the Management Server FAQ

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

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

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

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

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

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

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

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

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

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

```
SELINUX=disabled
```

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

## I am running Foglight with a MySQL® database. When I try to start Foglight, it fails to start and an SQL exception appears in the logs. Why does this happen?

If you encounter this problem, the cause might be that the MySQL database file `my.cnf` has been made world-writable.

Do not make the MySQL database file `my.cnf` world-writable, for example by issuing the command `chmod a+w <foglight_home>/mysql/my.cnf`. Foglight and the database cannot start if there is world access to the configuration file `my.cnf`.

## 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.

- i** | **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.

# 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 Help](#) for instructions on enabling and disabling cartridges after installation.

## To install a cartridge:

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

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

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

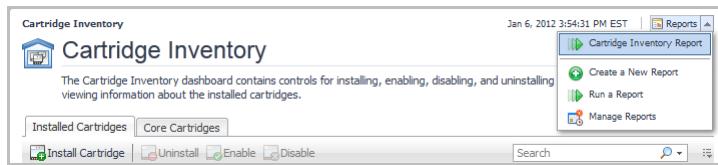
For more information about cartridge installation and configuration, see the [Administration and Configuration Guide](#).

**i** **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](#).

# 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.

**i** | **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.

**i** | **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](#).

## We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

## Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece—you—to the community, to the new Quest.

## Contacting Quest

For sales or other inquiries, visit <https://www.quest.com/company/contact-us.aspx/>.

## 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.