Foglight® 5.6.3
Security and Compliance Guide
# Table of Contents

Introduction to this Guide ................................................................................................................................. 4
  About Quest Software, Inc. ................................................................................................................................. 5
  Contacting Quest Software .............................................................................................................................. 5
  Contacting Quest Support ................................................................................................................................. 5

Foglight Security Overview ........................................................................................................................................ 6
  Foglight Security Measures ................................................................................................................................. 6
  Customer Security Measures .......................................................................................................................... 7
  Security Features in Foglight ............................................................................................................................. 8
    Service Accounts ........................................................................................................................................ 8
    Foglight Users and Groups ......................................................................................................................... 8
    Role-Based Access Control ......................................................................................................................... 9
    Password Policies .................................................................................................................................... 10
    Required Privileges .................................................................................................................................. 11
  Controlling Remote System Access with Credentials ...................................................................................... 12
  Protection of Data Collection Infrastructure ................................................................................................. 12
  Protection of Stored Data ............................................................................................................................... 13
  Protection of Communicated Data .................................................................................................................. 14
  Enabling FIPS 140-2 Mode for HTTPS Traffic .............................................................................................. 16
  Network Ports ............................................................................................................................................... 17
  Configuration Parameters ............................................................................................................................... 19
  Audit Log ..................................................................................................................................................... 19
  Log Files ..................................................................................................................................................... 19
  Masking Sensitive Input Data .......................................................................................................................... 20
  Uninstalling Foglight .................................................................................................................................. 20
  IPv6 ............................................................................................................................................................. 20
  Monitoring Patches for the Embedded MySQL Database ............................................................................... 20
  Daylight Savings Time Extension .................................................................................................................. 20
  Disclaimer .................................................................................................................................................. 20

Usage Feedback ................................................................................................................................................. 21

Appendix: Foglight and FISMA Compliance ........................................................................................................ 22
  NIST 800-53 Categories ................................................................................................................................. 22

Index ............................................................................................................................................................... 27
Introduction to this Guide

Quest Software’s 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 those still focused on technology-centric monitoring to those 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.

This Security and Compliance Guide describes the security features of Foglight. This document includes information about Foglight access control, data protection, and secure network communication. The appendix describes how Foglight's security features meet the National Institute of Standards and Technology (NIST) recommended federal information security standards as detailed in the Federal Information Security Management Act (FISMA).

This document is intended for system administrators and other users concerned with the security features of Foglight.
About Quest Software, Inc.

Quest Software (Nasdaq: QSFT) simplifies and reduces the cost of managing IT for more than 100,000 customers worldwide. Our innovative solutions make solving the toughest IT management problems easier, enabling customers to save time and money across physical, virtual and cloud environments. For more information about Quest solutions for administration and automation, data protection, development and optimization, identity and access management, migration and consolidation, and performance monitoring, go to www.quest.com.

Contacting Quest Software

<table>
<thead>
<tr>
<th>Email</th>
<th><a href="mailto:info@quest.com">info@quest.com</a></th>
</tr>
</thead>
</table>
| Mail  | Quest Software, Inc.  
World Headquarters  
5 Polaris Way  
Aliso Viejo, CA  92656  
USA |
| Web site | www.quest.com |

Refer to our Web site for regional and international office information.

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a Quest product and have a valid maintenance contract. Quest Support provides unlimited 24x7 access to our support portal. Visit our support portal at http://www.quest.com/support.

From our support portal, you can do the following:

- Retrieve thousands of solutions from our Knowledge Base
- Download the latest releases and service packs
- Create, update, and review Support cases

View the Global Support Guide for a detailed explanation of support programs, online services, contact information, policies, and procedures. The guide is available at: http://www.quest.com/support.
Foglight Security Overview

This section provides an overview of how Foglight manages information security. It presents the Foglight Security Measures and Customer Security Measures at a high level, and then describes the Security Features in Foglight.

Foglight Security Measures

Foglight provides detailed insight into the service relationships of end users, business and IT services, as well as applications and databases. Intuitive and flexible dashboards can be customized to provide multiple models and views of the managed environment.

Foglight consists of the Foglight Management Server (FMS), a database repository, and a set of cartridges. Foglight relies on a browser-based user interface and is controlled via role assignments in the Foglight security model. The Foglight Web application runs in a JBoss Web application server. Users interact with the FMS Web application via an HTTP or HTTPS connection.

Individual cartridges can be installed on the Management Server to provide monitoring capabilities for a variety of different end systems, including database and Web application servers. Cartridges contain agents that are typically deployed on the monitored systems. Some cartridges may contain agents that are deployed locally on the Management Server. These agents collect monitoring data and report it back to the Management Server. Users can then access this data in various forms. The image below provides an overview of the interaction between Foglight components.
Customer Security Measures

Foglight's security features are only one part of a secure environment. The customer's operational and policy decisions have a great influence on the overall level of security. In particular, the customer is responsible for the physical security of Foglight and its network. Administrators should change default passwords and replace them with strong passwords of their choice.
Security Features in Foglight

The following sections describe the features provided by Foglight. This document does not address security features for individual Foglight cartridges. Please refer to a specific cartridge's security and compliance document for this information.

Service Accounts

Foglight manages login credentials for the following service and user accounts:

- **Foglight Users**—Foglight supports both internal and external users. Internal users are defined within Foglight while external users are mapped from one of the LDAP-compatible directory services supported by Foglight (Active Directory, Oracle Directory Server Enterprise Edition, and OpenLDAP).

- **LDAP Directory**—For Foglight to access an LDAP directory, the customer needs to provide LDAP service-account credentials (user name and password for an account with read access to the directory).

- **Foglight Management Server Database Repository**—Foglight supports using specific versions of MySQL, Oracle, and Microsoft SQL Server databases for its storage repository. The login credentials for a database administrator account are specified during Foglight installation. For customers who do not provide a database administrator account, the creation of the external database may be delayed, as the database will require manual configuration.

Agent Credentials

When installing Foglight cartridge agents it is typically necessary to enter credentials for the user accounts that are on the monitored resources, including the host and database. These credentials are entered through the agent configuration properties via the Foglight Administration Console and give an agent access to applications or operating systems on the monitored host(s).

The Management Server includes a central credential service that manages cartridge agent credentials. A lockbox contains a set of credentials and keys for their encryption and decryption. Releasing a lockbox to a credential client enables the client to release the credentials to the agent instances managed by that client, thereby granting the agent instances access to the monitored system. For more information, see “Controlling Remote System Access with Credentials” on page 12.

Each Foglight cartridge may mark specific properties (for example, usernames and passwords) of its agents as being sensitive. Such properties are given additional protection as described later in this document.

Foglight Users and Groups

There are two types of users in Foglight: internal and external users. Internal users are created using the Foglight Administration Console. External users are mapped from one of the LDAP-compatible directory services supported by Foglight. All Foglight users are authenticated upon login, based on their usernames and passwords.
Foglight includes one default internal user (foglight) with administrative access, and four default internal groups (Cartridge Developers, Foglight Administrators, Foglight Operators, and Foglight Security Administrators), none of which cannot be deleted.

**Role-Based Access Control**

Foglight’s security model is based on a role-based access control system (RBAC). The following are the core RBAC objects and their use within Foglight:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
<th>Use in Foglight</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Permission</strong></td>
<td>Permissions grant users a certain level of access to a configuration item, enabling them to perform specific actions using Foglight. These permissions do not apply to monitored information.</td>
<td>A different set of permissions can be configured for each role or user who has been granted access to a configuration item.</td>
</tr>
<tr>
<td><strong>Role</strong></td>
<td>The default roles included with Foglight dictate the actions that users can perform with Foglight features or components. Foglight System Administrators can also create custom roles.</td>
<td>Roles are assigned to groups. Users in a group have the roles that are assigned to that group. Roles can also be associated with specific configuration items.</td>
</tr>
<tr>
<td><strong>User</strong></td>
<td>A user has a username and a password and can belong to one or more groups.</td>
<td>A user logging in to Foglight is authorized to perform a certain set of actions based on the roles that have been assigned to the user’s group(s).</td>
</tr>
<tr>
<td><strong>Group</strong></td>
<td>A group can contain one or more users or other groups. Roles are assigned to users through groups.</td>
<td>You can assign roles and add users to groups.</td>
</tr>
<tr>
<td><strong>Configuration Item</strong></td>
<td>A configuration item such as a rule or registry variable.</td>
<td>Access to configuration items can be assigned to specific users or to roles. Each configuration item is initially owned by its creator.</td>
</tr>
</tbody>
</table>

Roles dictate the actions that a user can perform. There are two types of roles in Foglight: default roles (called *built-in roles*), and custom roles (called *internal roles*).

Foglight defines a configuration item as an item that is created and/or managed in the Administration Console, such as a rule, registry variable, derived metric, or schedule. Access to individual configuration items can be restricted to specific users or roles. In addition, the level of access that each user or role has to that configuration item can be controlled through permissions.
A permission represents a set of actions that can be performed with regard to that configuration item. The image below depicts the interrelationship of users, groups, roles, permissions, and configuration items.

Users who have the Foglight Security Administrator role can use the Foglight Administration dashboard to manage users, groups, roles, permissions, and configuration items.

The Groups view of the User Management dashboard contains a table that lists all of the groups that have been created in Foglight or imported from an LDAP-compatible directory service, as well as the users and the roles that have been assigned to them.

**Password Policies**

Listed below are the default restrictions that apply to passwords for administrators (Foglight users with the Foglight Security Administrator role), for internal users, and for credential lockboxes.

- An internal user's password expires after ninety (90) days.
- An administrator's password expires after forty-five (45) days. The one exception is the password for the default user `foglight`, which does not expire.
- Users are locked out of the system for fifteen (15) minutes after they enter an incorrect password for five (5) consecutive login attempts.
- Foglight reminds users fifteen (15) days before their password expires.
- The password must be at least seven (7) characters long, and must contain both alphabetic and numeric characters.
- The password cannot be:
  - the same as the user name.
  - the repetition of a single character.
  - longer than twenty (20) characters.
  - the same as any of the user's last twelve (12) passwords.
Users with the Foglight Security Administrator role can view and edit the configurable password policies on the Configure Password Settings dashboard in the Administration Console. Certain password policies cannot be viewed on this page or edited. They are as follows:

A user's password cannot be:

- the same as his or her user name.
- the repetition of a single character.
- longer than twenty (20) characters.

External users are subject to the password policies that are enforced on the operating systems that generated the user accounts.

**Setting Password Complexity Levels**

The customer sets the enforcement complexity level passwords of credential lockboxes, internal users, and users with the Foglight Security Administrator role. The Lockbox password complexity level, the User password complexity level, and the Administrator password complexity level list are available from the Configure Password Settings dashboard and define the following levels of increasing complexity:

- **Level 1**: Passwords are not checked for complexity.
- **Level 2**: Passwords must contain both alphabetic and numeric characters.
- **Level 3**: Passwords must contain at least one upper case letter, lower case letter, and numeric character, as well as at least one character that is not alphanumeric.

By default, the complexity level for both internal users' and administrators' passwords is set to level 2. Administrators' passwords cannot be set to level 1.

**Required Privileges**

**Installing Foglight Management Server**

To install Foglight, administrative privileges on the target operating system are required. In addition, the customer is prompted to provide credentials for a database administrator account during installation. The need to enter such credentials can be bypassed as described in Manual Database Configuration.

**Running Foglight Management Server**

Foglight requires administrative privileges to configure the server to run as a service (a Windows service or a Unix/Linux init.d script). Once it is configured, the service can be launched with a regular user account.

**Installing Agent Components**

Certain cartridges (for example, the Foglight Cartridge for Java EE Technologies) include one or more executable agent installers. The Components for Download dashboard, accessible from the Administration Console, can be used to download agent installers from the Management Server to a remote machine.
Manual Database Configuration

When installing the Foglight Management Server for use with an external database, the database can be set up later (that is, after the Management Server installation is complete). In this case, the database must be manually configured prior to starting the Management Server. This configuration requires executing the scripts in the `<foglight_home>/scripts/sql` directory as described in the *Installation and Setup Guide* applicable to the system and database. Some scripts must be run using an account with administrative privileges.

Controlling Remote System Access with Credentials

Foglight can control access to specific elements of a monitored system through a built-in credential management system. If an organization has specific policies in place regarding system access, such policies can be implemented using credentials managed by the Management Server.

Foglight supports a set of commonly used credentials such as:

- Challenge Response
- Domain, User Name, and Password (Windows)
- Use Client’s Login at Connection Time
- User Name
- User Name and Password

Each credential can have one or more authentication policies associated with it, based on the desired usage count, failure rate, the time range during which the credential can be used, and the amount of time during which the credential information is cached locally. Credentials can apply to specific parts of the monitored environment, such as hosts and ports.

Foglight agents need access to this information when monitoring systems that require credential verification. Credentials are stored encrypted in lockboxes. Lockboxes are released to credential clients, such as agent managers.

Protection of Data Collection Infrastructure

Installation of Data Collection Clients

There are many types of Foglight agents; most communicate with the Management Server through a provided client component—the Foglight Agent Manager (FglAM).

The Agent Manager can be installed without administrator access, but such access is required to enable startup scripts or Windows services to allow automatic launching of the Agent Manager upon machine reboot. The Agent Manager can be initially installed on a monitored host through an installer GUI, a text-based console installer, or a command-line silent mode (suitable for mass deployment using customer-provided tools).

Once installed, the Agent Manager component manages the life cycle of a number of hosted agents and provides a central communications link between those agents and the Management Server. Hosted agents and the Agent Manager can be upgraded from the Management Server using this central communications link.
Agents Requiring Privilege Escalation

Some data collection agents hosted by the Agent Manager require administrator privileges to perform their assigned tasks. In order to avoid running the entire client host with the required privileges, Foglight uses a privilege escalation mechanism to create the required access for the agents that need it.

The Agent Manager, by default, uses the well known `sudo` facility (a very fine-grained configurable system) to implement privilege escalation. `sudo` can be configured to allow only specific applications to be launched with escalated privileges, and the privileges provided to each launched application can be independently controlled. In addition, `sudo` allows the administrator to limit the parameters passed to each application; this facility is central to configuring a secure system with the Agent Manager.

The Agent Manager also provides an alternative `setuid` root-based launcher. This launcher is only intended for use in demonstration installations with minimal security needs, where the burden of properly configuring `sudo` for fine-grained access control would hinder a timely demonstration. Quest does not recommend that this `setuid` root-based launcher be configured as part of Foglight’s standard installation instructions.

Protection of Stored Data

The Foglight Management Server and Foglight cartridges use the Java Cryptographic Extension library for cryptographic operations. The Triple DES (Data Encryption Standard) algorithm in Chain Block Cipher mode with a 112-bit key is used for encrypting the Management Server service account's passwords (that is, LDAP account) and certain agent properties marked as sensitive. Triple DES is on the U.S. Government's Federal Information Processing Standards (FIPS) 140-2 list of approved encryption algorithms.

Credentials for Foglight Users

When an internal Foglight user account is created, the user's password is hashed with the MD5 algorithm and the resulting digest is stored in the Foglight database. User passwords are therefore not stored anywhere, in encrypted or in cleartext form.

LDAP Credentials

LDAP server passwords are encrypted with Triple DES. A default 112-bit Triple DES encryption key is used in all cases of installations of Foglight. This encryption key is stored in a Java keystore protected by a Foglight master password. Customers have the ability to change the Triple DES encryption key after installation by using Foglight to generate a new key. Quest recommends customers change the default Java keystore password upon the installation of the Management Server.

**Note**

Changing the default key requires the LDAP password to be re-entered so it can be encrypted under the new key (after a password change, the Management Server can no longer decrypt existing cipher texts under the old key).
Management Server Repository Database Credentials

The login credentials for the database administrator account on the Foglight repository are encrypted in identical fashion as the LDAP credentials, using the same encryption key.

Foglight Agent Credentials

Foglight cartridges include agents that require access to service account login credentials on the systems or applications that they monitor. Foglight stores these credentials in the repository database which is protected by access control. Any agent property that is marked as sensitive is masked during display in user interface consoles.

All agent properties are stored encrypted (with Triple DES) in an XML configuration file on the monitored host.

Database Repository

Collected data from Foglight agents is stored in the repository database, which is protected through user access control. This data contains collected metrics and statistics about the systems on the monitored hosts, as well as agent configuration parameters.

Protection of Communicated Data

Web Application Security

The Management Server's Web application server supports the use of SSL, in order to protect Foglight users' login credentials. Foglight provides its own self-signed SSL certificate on the Web application server, and enables customers to provide a replacement SSL certificate of their choice. SSL certificates are managed through the Java keystore on the Management Server.

Basic HTTP (non-SSL) access can be disabled by disabling the HTTP port on the server. This disables both HTTP access to the Management Server browser interface and HTTP communication for agents that use the XML-over-HTTP protocol, forcing the use of HTTPS connections.

Preventing the ApacheServerTokenNotSet Vulnerability

When running a security scan on the Management Server, customers may discover that ServerTokens for the Apache HTTP Server has not been set.

**Synopsis:** The Apache HTTP Server could allow a remote attacker to obtain sensitive information. The Apache HTTP Server uses a configuration directive called ServerTokens to control what information the server discloses about itself in the HTTP header lines of the banner in a response to a query. The information disclosed includes the operating system and the software versions running on the server. When ServerTokens has not been set, an attacker could launch attacks.

**Resolution:**

1. Stop the Management Server.
2. Navigate to the $FGLHOME\server\default\deploy\jboss-web.deployer\ directory.
3. Open the following files in an editor: server_full.xml and server_https.xml.
4 Locate the following comment: <!-- A HTTP/1.1 Connector on port 8080 -->

5 Add the server="hidden" parameter before the end /> of the section. For example:

```xml
<Connector port="${foglight.http.port}" address="${jboss.bind.address}"
  maxThreads="250" strategy="ms" maxHttpHeaderSize="8192"
  emptySessionPath="true" URIEncoding="UTF-8"
  enableLookups="false" redirectPort="${foglight.https.port}"
  acceptCount="100"
  connectionTimeout="200000" disableUploadTimeout="true"
  compression="on" server="hidden" />
```

6 Locate the following comment: <!-- SSL_* ciphers are included for completeness but are not FIPS compliant and can be excluded for sites that care -->

7 Repeat step 5.

8 Save and close both files and restart the Management Server.

**Communication between Management Server and Agents**

Most Foglight agents communicate with the Management Server through the included client application, the Agent Manager. The exceptions are the Java EE Technology agents that communicate with the Management Server across a separate binary protocol, and agents that use the low level XML over HTTP(S) data submission option. When activating an agent it is necessary to communicate its properties, which may include login credentials for accounts on the monitored host.

**Communication between Management Server and Clients**

The Agent Manager (FglAM) implements a communication layer with XML messages sent to the Management Server over HTTP(S). These messages are sent to the same ports that the Management Server uses for all HTTP-based traffic, including the Web applications.

The Agent Manager allows the user to configure HTTP or HTTPS URLs for the Management Server, or a combination of both. When HTTPS is used, the Agent Manager rejects invalid certificates by default -- either self-signed, signed by an unrecognized certificate authority, or a certificate that declares a Common Name that does not match the Management Server host name (thus providing protection against man-in-the-middle attacks). Certificates can be added to the Agent Manager keystore. Like a Web browser, Agent Manager supports configuration options to relax these certificate verification controls, but these options will reduce the security provided by the SSL mechanism. If the Management Server is configured to only allow HTTPS access, the Agent Manager must be configured with an HTTPS URL to connect to the Management Server. By default, the Management Server uses the SSL_RSA_WITH_RC4_128_MD5 cipher suite (RSA, RC4, and MD5) for its communication with the Agent Manager.

The Agent Manager supports concentrators. A concentrator is an Agent Manager instance that works similarly to an HTTP proxy. It is configured to accept connections from other Agent Manager instances (called downstream instances) and forward these connections to an upstream target, either the Management Server or another Agent Manager concentrator. These concentrators support HTTP or HTTPS communication with the upstream Management Server.
A concentrator’s upstream connection is independent of the downstream connections. For example, several Agent Manager instances on a local subnet can communicate to a concentrator using HTTP while the concentrator forwards requests over a non-secure network to the Management Server using HTTPS (or vice-versa).

**Communication between Management Server and Java EE Technology Agents**

No encryption is used to protect the communication channel between Java EE Technology agents (which are not based on the Agent Manager) and the Management Server. Data is sent in proprietary binary form.

**Communication between Management Server and XML over HTTP(S) Agents**

The XML over HTTP(S) protocol is another low-level method for submitting data to the Management Server. SSL is supported for the XML over HTTP protocol in the default server configuration. An agent using this protocol simply needs to use the HTTPS server port (8443) to open secure connections.

**Communication between Management Server and Repository Database**

The Foglight repository database may be installed either on the same or separate server as the Management Server. Data is transmitted using the database communication protocol (of MySQL, Oracle, or SQL Server) between the Management Server and the repository database. No security is enforced to protect this channel of communication.

**Enabling FIPS 140-2 Mode for HTTPS Traffic**

Some customers require that all network traffic be protected with FIPS 140-2 compliant ciphers. The following procedure can be used to configure the Management Server to permit the use of specific TLS cipher suites only for communications with its Web server (all traffic over HTTPS).

**Note**

By enabling this configuration, Foglight will accept only the cipher suites listed explicitly below.

1. On the Foglight Management Server, edit the following files:
   
   `<foglight_home>\server\default\deploy\server_https.xml`
   `<foglight_home>\server\default\deploy\server_full.xml`

2. Modify the `ciphers` attribute within the `Connector` element to read:

   ```
   ciphers="TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
   TLS_DHE_DSS_WITH_AES_128_CBC_SHA,
   TLS_RSA_WITH_AES_256_CBC_SHA,
   TLS_DHE_RSA_WITH_AES_256_CBC_SHA,
   TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
   TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA,
   TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA,
   TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA,
   TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,
   TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,
   TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
   TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,
   TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,```

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA,
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
TLS_RSA_WITH_3DES_EDE_CBC_SHA,
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA,
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA"

3 Restart the Foglight Management Server.

Network Ports
The Foglight installation process allows you to configure port assignments. The default ports are displayed during installation.

Default Port Assignments
The following Port Assignments show the Foglight default port assignments for FMS:

<table>
<thead>
<tr>
<th>Port Name</th>
<th>Port Number</th>
<th>Outgoing/Incoming</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded MySQL</td>
<td>13306</td>
<td>Incoming/Outgoing</td>
</tr>
<tr>
<td>Cluster Multicast</td>
<td>45566</td>
<td>Incoming/Outgoing</td>
</tr>
<tr>
<td>HTTP</td>
<td>8080</td>
<td>Incoming</td>
</tr>
<tr>
<td>HTTPS</td>
<td>8443</td>
<td>Incoming</td>
</tr>
<tr>
<td>AJP13</td>
<td>8009</td>
<td>Incoming</td>
</tr>
<tr>
<td>JNDI RMI</td>
<td>1098</td>
<td>Incoming/Outgoing</td>
</tr>
<tr>
<td>JNDI JNP</td>
<td>1099</td>
<td>Incoming/Outgoing</td>
</tr>
<tr>
<td>JRMP Invoker</td>
<td>4444</td>
<td>Incoming/Outgoing</td>
</tr>
<tr>
<td>JRMP Pooled Invoker</td>
<td>4445</td>
<td>Incoming/Outgoing</td>
</tr>
<tr>
<td>JRMP Unified Invoker</td>
<td>4448</td>
<td>Incoming/Outgoing</td>
</tr>
<tr>
<td>HA JNDI RMI</td>
<td>1101</td>
<td>Incoming/Outgoing</td>
</tr>
<tr>
<td>HA JNDI JNP</td>
<td>1100</td>
<td>Incoming/Outgoing</td>
</tr>
<tr>
<td>HA JRMP Invoker</td>
<td>4447</td>
<td>Incoming/Outgoing</td>
</tr>
<tr>
<td>HA Pooled Invoker</td>
<td>4446</td>
<td>Incoming/Outgoing</td>
</tr>
<tr>
<td>HA JNDI UDP Group</td>
<td>1102</td>
<td>Incoming/Outgoing</td>
</tr>
</tbody>
</table>
High Availability (HA) refers to running a secondary instance of Foglight as a failover backup server (redundant mode). Foglight listens to the multicast port (45566) only when configured for HA mode.

The following ports are used when Foglight is installed with an external database:

<table>
<thead>
<tr>
<th>Port Name</th>
<th>Port Number</th>
<th>Outgoing/Incoming</th>
</tr>
</thead>
<tbody>
<tr>
<td>External MySQL</td>
<td>3306</td>
<td>Outgoing</td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td>1433</td>
<td>Outgoing</td>
</tr>
<tr>
<td>Oracle</td>
<td>1521</td>
<td>Outgoing</td>
</tr>
</tbody>
</table>

**Agent Adapter Ports**

The following agent adapter ports should be used when configuring the Foglight Administration Console.

<table>
<thead>
<tr>
<th>Port Name</th>
<th>Port Number</th>
<th>Outgoing/Incoming</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Manager</td>
<td>8080</td>
<td>Incoming</td>
</tr>
<tr>
<td>Agent Manager over SSL</td>
<td>8443</td>
<td>Incoming</td>
</tr>
<tr>
<td>Java EE Technology Agent</td>
<td>41705</td>
<td>Incoming</td>
</tr>
</tbody>
</table>

**Client Communication**

The Agent Manager connects to the Management Server using the same HTTP(S) ports as the browser interface. The Agent Manager uses the standard URL format to configure the address of the upstream Management Server; therefore if the port number is changed in the Management Server configuration, it is a simple matter to configure the Agent Manager to use the updated port.

Agent Manager instances that are configured to communicate through a concentrator can use any customer-designated port for their communication with that concentrator host. This needs to be configured on both the upstream and downstream Agent Manager instance.

Some agents hosted by the Agent Manager are run out-of-process, and use local TCP connections to communicate with the master Agent Manager process. Two protocols are used for this local communication: legacy RAPSD for agents which are supported by the Agent Manager, and the Agent Manager’s XML-over-HTTP for new agents implemented with the Agent Manager API (this is the same protocol used by the Agent Manager to connect to the upstream Management Server or concentrators). In both cases, the master Agent Manager process listens for local connections on an available port assigned randomly by the OS from the ephemeral port range. In both cases, these ports will only accept connections from localhost; neither case supports encryption for this local-only traffic.
Configuration Parameters

The Foglight Management Server stores its configuration parameters in configuration files within the Foglight directory on the Management Server's file system. When Foglight is launched, the parameters are read and cached internally; the configuration files on disk are not re-read until the Management Server restarts. This allows modification of the configuration files while Foglight is running without affecting real-time processing.

Audit Log

From the Foglight Administration Console, users can select security and change audit logs for a specific time period and display those logs in the Audit Viewer.

The View Audit Information dashboard allows you to review these logs and to filter them to show information for a specific timespan. It also lists users who have logged in to Foglight, changes to user, group or role settings, and changes made to configuration items, including rules, schedules, or registry variables.

The following information appears in each log entry in the table:

- Timestamp: displays the date, time, and time zone at which the specified action occurred.
- User Name: displays the user name for the user who caused the action to be performed.
- Service Name: displays the name of the Foglight service that performed the action.
- Operation Name: displays the operation that was performed by Foglight. If applicable, the name of the item that was changed is also displayed in this column.

Audit log entries are stored in the Foglight database.

A subset of the Foglight methods that are audited includes:

- start/stop data collection
- install/uninstall cartridge
- activate/deactivate cartridge
- delete rules

Log Files

The following information is recorded in the Foglight log files on the Management Server:

- troubleshooting data (including warnings and errors)
- debug information
- life-cycle information
- agent information.

No user names or passwords are stored in the log file. These files are stored unencrypted on the file system within the Foglight directory structure. Any system user with read privileges to these files can access the logs.
Masking Sensitive Input Data
Foglight masks password entries with asterisks to prevent them from being displayed. Foglight also masks agent properties that are marked as sensitive.

Uninstalling Foglight
Uninstalling Foglight leaves certain files in the Foglight folder, and database content (schema) is not deleted. Only the internally embedded database is erased on uninstall. If required, the customer must delete the Foglight files from the file system manually.

IPv6
The Agent Manager supports IPv6 communication with the Management Server, and also with upstream Agent Manager concentrators.

Monitoring Patches for the Embedded MySQL Database
Quest Software monitors and provides patches and/or upgrades to address any relevant vulnerabilities that may affect the embedded MySQL database provided with Foglight. To receive product updates or security patches, a customer may be required to upgrade to the latest version of Foglight.

Customers who use an external database (MySQL, Oracle, or Microsoft SQL Server) are responsible for applying the latest security patches to their database as well as ensuring that it is securely configured.

Daylight Savings Time Extension
Foglight is not affected by the changes introduced by the Daylight Savings Time (DST) Extension (U.S. Energy Policy Act of 2005). It relies on the operating system for time management and does not implement any special logic regarding DST settings.

Disclaimer
Quest Software has made every effort to ensure that the information provided in this document is accurate. However, Quest makes no representation about the content and suitability of this information for any purpose. This information may be modified by Quest at any time. Nothing contained herein shall be construed as a warranty, express or implied, regarding the operation of Quest Software products.
Usage Feedback

The Foglight Management Server can collect usage data about your environment and send it to Quest to improve support response. This data helps Quest identify potential bottlenecks, and improve the overall Management Server performance and server versions going forward.

The collected usage data contains information about the visited dashboards. It also includes the unique ID of the Management Server and its version information. It does not identify any users or provide additional information about their actions in the user interface.

By default, this feature is turned off (disabled). To turn it on, click Enable on the Usage Feedback dashboard. This dashboard is accessible from the navigation panel in the Foglight browser interface, under Administration > Setup & Support > Usage Feedback.
Appendix: Foglight and FISMA Compliance

The Federal Information Security Management Act (FISMA) was passed by the U.S. Congress and signed by the president as part of the Electronic Government Act of 2002. It requires “each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information system that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source”.

Note For additional details about FISMA, see http://csrc.nist.gov/sec-cert.

A major component of FISMA implementation is the publication by the National Institute of Standards and Technology (NIST), entitled “Recommended Security Controls for Federal Information Systems”, listed as NIST Special Publication 800-53 (for additional information about this document, see http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf). This document presents 17 general security categories that can be used to evaluate an information security to measure its level of compliance with FISMA. For this reason, this appendix offers the 17 categories listed in 800-53 and describes how Foglight addresses them. For more information, see NIST 800-53 Categories.

NIST 800-53 Categories

This section presents the 17 categories listed in the NIST Special Publication 800-53 and describes how Foglight addresses those that apply.

The secure employment of Foglight forms only one part of an information security program. A statement in this appendix that a particular security category is “applicable” to Foglight means only that Foglight contains security features that are or may be relevant to some or all aspects of the security category in question. It does not necessarily mean that Foglight fully meets all of the requirements described in that security category, or that the use of Foglight by itself guarantees compliance with any particular information security standards or control programs. The selection, specification, and implementation of security controls in accordance with a customer-specific security program is ultimately dependent upon the manner in which the customer deploys, operates, and maintains all of its network and physical infrastructure, including Foglight.
### Note
Under the NIST Special Publication 800-53, the 17 categories listed in this table define general security control “families” (for example, AC), and each family in turn contains several subcategories (for example, AC-1, AC-2, AC-3, etc.) that further detail related aspects of information security and assurance. For additional information, see Appendix F of NIST Special Publication 800-53.

<table>
<thead>
<tr>
<th>Category</th>
<th>Applicable</th>
<th>Description</th>
<th>Additional Details</th>
</tr>
</thead>
</table>
| Access Control (AC)             | Yes        | Foglight 5 has an internal security service through which all requests must pass regardless of whether they originate from the user interface, the command-line or external APIs. The security service is user and role based and can be linked to LDAP or Active Directory, enabling the storage and management of the user accounts, roles, and passwords, through those directories. | • “Foglight Users and Groups” on page 8  
• “Role-Based Access Control” on page 9 |
| Awareness and Training (AT)     | No         | This category does not apply to Foglight, since it is the responsibility of the Foglight customers to develop and review their own security awareness and training policy.                                                                                                           | N/A                                                  |
| Audit and Accountability (AU)   | Yes        | Foglight can display security and change audit logs for select time periods, including information about login history as well as any administrative and configuration changes made. Audit log entries contain identifying information such as a timestamp, user name, service name, and operation name. A separate log file records troubleshooting data, debut information, lifecycle information, and agent information. No user names or passwords are included in the log file. | • “Audit Log” on page 19  
• “Log Files” on page 19 |
<table>
<thead>
<tr>
<th>Category</th>
<th>Applicable</th>
<th>Description</th>
<th>Additional Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification, Accreditation and Assessments</td>
<td>No</td>
<td>This category does not apply to Foglight, since it is the responsibility of the Foglight customers to develop and review their own security assessment, accreditation, and certification policy.</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>Yes</td>
<td>The audit and log files contain information about any configuration changes made to Foglight. Role-based access control is enforced to limit users' ability to make changes. Foglight's configuration parameters are stored in local files and are read and cached internally upon startup. The Foglight communication ports are restricted and configurable by administrators only.</td>
<td>• “Enabling FIPS 140-2 Mode for HTTPS Traffic” on page 16&lt;br&gt;• “Network Ports” on page 17&lt;br&gt;• “Configuration Parameters” on page 19&lt;br&gt;• “Audit Log” on page 19</td>
</tr>
<tr>
<td>Contingency Planning</td>
<td>No</td>
<td>This category does not apply to Foglight, since it is the responsibility of the Foglight customers to design and implement their own contingency plans. As defined by NIST (publication 800-34), disruptive events to IT systems include power-outages, fire and equipment damage, and can be caused by natural disasters or terrorist actions.</td>
<td>N/A</td>
</tr>
<tr>
<td>Identification and Authentication</td>
<td>Yes</td>
<td>Foglight enforces identification, authentication, and password policies, providing well-defined rules for controlling how user names and passwords are created, as well as ensuring that only authorized users are able to log into the system. The customer can also choose to authenticate users against an LDAP or AD supported directory.</td>
<td>• “Foglight Users and Groups” on page 8&lt;br&gt;• “Role-Based Access Control” on page 9&lt;br&gt;• “Password Policies” on page 10</td>
</tr>
<tr>
<td>Category</td>
<td>Applicable</td>
<td>Description</td>
<td>Additional Details</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td>Incident Response (IR)</td>
<td>No</td>
<td>This category does not apply to Foglight, since it is the responsibility of the Foglight customers to develop and review their own incident response policy and procedures.</td>
<td>N/A</td>
</tr>
<tr>
<td>Maintenance (MA)</td>
<td>Yes</td>
<td>Quest Software monitors the embedded MySQL database included in Foglight developments for security developments and flaws and provides product updates and patches to customers when necessary.</td>
<td>“Monitoring Patches for the Embedded MySQL Database” on page 20</td>
</tr>
<tr>
<td>Media Protection (MP)</td>
<td>No</td>
<td>This category does not apply to Foglight, since it is the responsibility of the Foglight customers to develop and review their own media protection policies.</td>
<td>N/A</td>
</tr>
<tr>
<td>Physical and Environmental Protection (PE)</td>
<td>No</td>
<td>This category does not apply to Foglight, since it is the responsibility of the Foglight customers to develop and review their own physical and environmental policies.</td>
<td>N/A</td>
</tr>
<tr>
<td>Planning (PL)</td>
<td>No</td>
<td>This category does not apply to Foglight, since it is the responsibility of the Foglight customers to develop and review their own security planning policies.</td>
<td>N/A</td>
</tr>
<tr>
<td>Personnel Security (PS)</td>
<td>No</td>
<td>This category does not apply to Foglight, since it is the responsibility of the Foglight customers to enforce their own personnel security policies, including personnel screening and employment termination.</td>
<td>N/A</td>
</tr>
<tr>
<td>Risk Assessment (RA)</td>
<td>No</td>
<td>This category does not apply to Foglight, since it is the responsibility of the Foglight customers to develop and review their own risk assessment policies.</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### System and Services Acquisition (SA)

<table>
<thead>
<tr>
<th>Category</th>
<th>Applicable</th>
<th>Description</th>
<th>Additional Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>System and Services Acquisition (SA)</td>
<td>Yes</td>
<td>Quest Software has performed an internal security and compliance assessment of Foglight, including a risk analysis. A security checklist was completed with the help of the development team. This document is the result of the assessment.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### System and Communications Protection (SC)

<table>
<thead>
<tr>
<th>Category</th>
<th>Applicable</th>
<th>Description</th>
<th>Additional Details</th>
</tr>
</thead>
</table>
| System and Communications Protection (SC) | Yes | The Management Server's Web application server supports the use of SSL to protect user communication. A self-signed SSL certificate is used by default, and the customers have the ability to upload their own SSL certificate. Agent Manager communication between agents and the Management Server can also be protected with SSL. Communication between Java agents (non-FglAM-based) and the Management Server is unencrypted. No security is enforced to protect communication between the Management Server and an external database. The network ports over which Foglight components and protocols communicate are configurable. | • “Protection of Data Collection Infrastructure” on page 12  
• “Protection of Communicated Data” on page 14  
• “Enabling FIPS 140-2 Mode for HTTPS Traffic” on page 16 |

### System and Information Integrity (SI)

<table>
<thead>
<tr>
<th>Category</th>
<th>Applicable</th>
<th>Description</th>
<th>Additional Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>System and Information Integrity (SI)</td>
<td>Yes</td>
<td>The Management Server and Cartridges/Agents use the Java Cryptographic Extension library for cryptographic operations. The Triple DES (Data Encryption Standard) algorithm in chain block cipher mode is used for encrypting the service account's passwords (for example, the LDAP account). User passwords are hashed with the MD5 algorithm and stored in the Foglight database. Agent properties marked as sensitive are masked during display and encrypted during storage.</td>
<td>“Protection of Stored Data” on page 13</td>
</tr>
</tbody>
</table>
Index

A
about Foglight 4
AC 23
Access Control 23
access control, role-based 9
agent adapter ports 18
agent credentials 8, 14
agents 13
  communicating with FMS 15
AT 23
AU 23
Audit and Accountability 23
audit log 19
Awareness and Training 23

B
browser interface 14

C
CA 24
Certification, Accreditation and Assessments 24
client 12
  communicating with FMS 15
  communication 18
  FglAM 15
CM 24
communicated data 14
communication
  between agents and FMS 15
  between client and FMS 15
  between FMS and XML over HTTP(S) agents 16
  between Java agents and FMS 16
  between repository database and FMS 16
configuration
  database 12
  item 9
  parameters 19
Configuration Management 24
Contingency Planning 24

CP 24
credentials 13
  agents 14
  database 14
  LDAP 13

D
data collection infrastructure 12
database
  credentials 14
  embedded MySQL 20
  manual configuration 12
  repository 8, 14
Daylight Savings Time 20
default port assignments 17
disclaimer 20
DST 20

E
embedded MySQL database 20
enabling FIPS 140-2 16
escalation of privileges 13
external
  database ports 18
  groups 8
  users 8

F
Federal Information Security Management Act 22
FglAM 12
  communication 18
FIPS 140-2 16
FISMA 22
Foglight
  Agent Manager 12
  uninstalling 20
  user credentials 13
  users 8
**Index**

**G**
groups 8, 9

**H**
HTTP 14
HTTPS 14
traffic 16

**I**
IA 24
Identification and Authentication 24
Incident Response 25
infrastructure 12
input data, masking 20
installing
agent components 11
client 12
Foglight Management Server 11
internal
groups 8
users 8
IPv6 20
IR 25

**J**
Java agents communicating with FMS 16

**L**
LDAP 8
credentials 13
log files 19

**M**
MA 25
Maintenance 25
manual database configuration 12
masking input data 20
Media Protection 25
MP 25

**N**
National Institute of Standards and Technology 22
network ports 17
NIST category 800-53 22
AC 23
AT 23
AU 23
CA 24
CM 24
CP 24
IA 24
IR 25
MA 25
MP 25
PE 25
PL 25
PS 25
RA 25
SA 26
SC 26
SI 26

**NIST, Special Publication 800-53** 22

**P**
password
complexity levels 11
policies 10
security 11
PE 25
permission 9
Personnel Security 25
Physical and Environmental Protection 25
PL 25
Planning 25
ports 17
agent adapters 18
external database 18
privilege escalation
agents requiring 13
privileges, required by
agents 11
Foglight Management Server 11
protecting communicated data 14
protecting stored data 13
PS 25

**R**
RA 25
registry variable 9
Index

repository database 14
communicating with FMS 16
required privileges 11
Risk Assessment 25
role 9
role-based access control 9
rule 9
running, Foglight Management Server 11

S
SA 26
SC 26
security categories 22
   Access Control 23
   Audit and Accountability 23
   Awareness and Training 23
   Certification, Accreditation and Assessments 24
   Configuration Management 24
   Contingency Planning 24
   Identification and Authentication 24
   Incident Response 25
   Maintenance 25
   Media Protection 25
   Personnel Security 25
   Physical and Environmental Protection 25
   Planning 25
   Risk Assessment 25
   System and Communications Protection 26
   System and Information Integrity 26
   System and Services Acquisition 26
service accounts 8
SI 26
Special Publication 800-53 22
statistics 21
stored data, protection of 13
support 5
System and Communications Protection 26
System and Information Integrity 26
System and Services Acquisition 26

T
technical support 5

U
uninstalling Foglight 20
usage

W
Web application security 14

X
XML over HTTP(S) agents communicating with FMS 16