Quest™

Foglight™ 5.7.5.8

Security and Compliance Guide

owners.

Legend

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

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

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

Foglight Security and Compliance Guide
Updated - March 2017
Software Version - 5.7.5.8

Contents

1

Security overview

This *Security and Compliance Guide* describes the Foglight™ security features. This document includes information about Foglight access control, data protection, and secure network communication. It also describes how Foglight 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 Foglight security features.

- Foglight security measures
- Customer security measures
- Security features in Foglight
- Disclaimer

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.

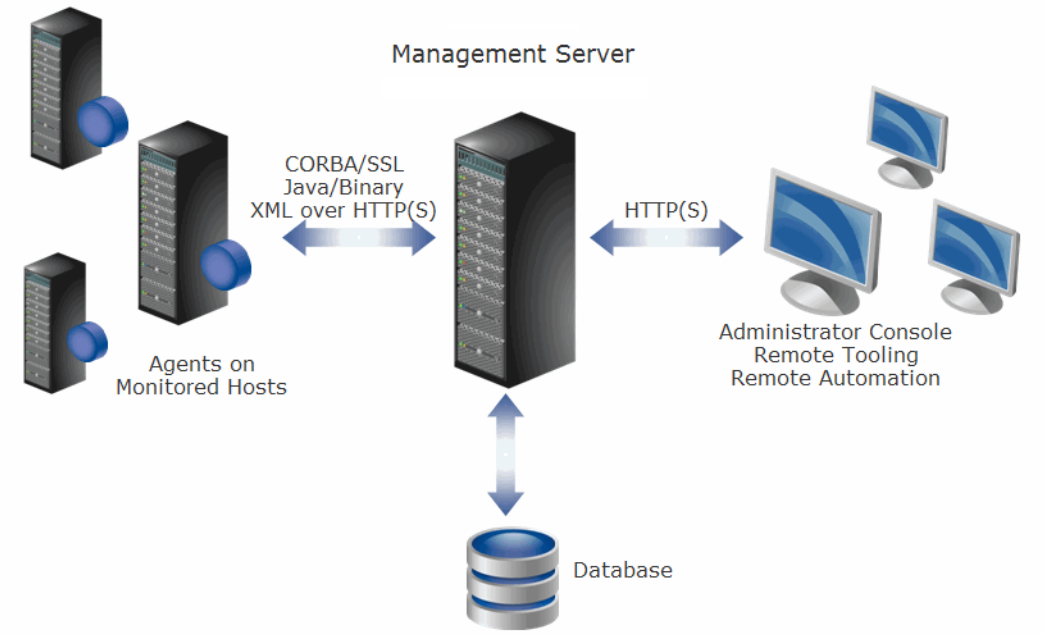
Foglight security measures

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 an Apache Tomcat® 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.

Figure 1. Overview of interaction between Foglight components



Customer security measures

Foglight™ 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.

NOTE: If your environment includes APM appliances, review Security features for APM appliances on page 20 after you finish this section.

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 hosts.

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 11.

Each Foglight cartridge may mark specific properties (for example, user names 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 user names 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™ security model is based on a role-based access control system (RBAC).

Table 1. Core RBAC objects and their use within Foglight

Term	Definition	Use in Foglight
Permission	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.	A different set of permissions can be configured for each role or user who has been granted access to a configuration item.
Role	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.	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.
User	A user has a username and a password and can belong to one or more groups.	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 groups.

Table 1. Core RBAC objects and their use within Foglight

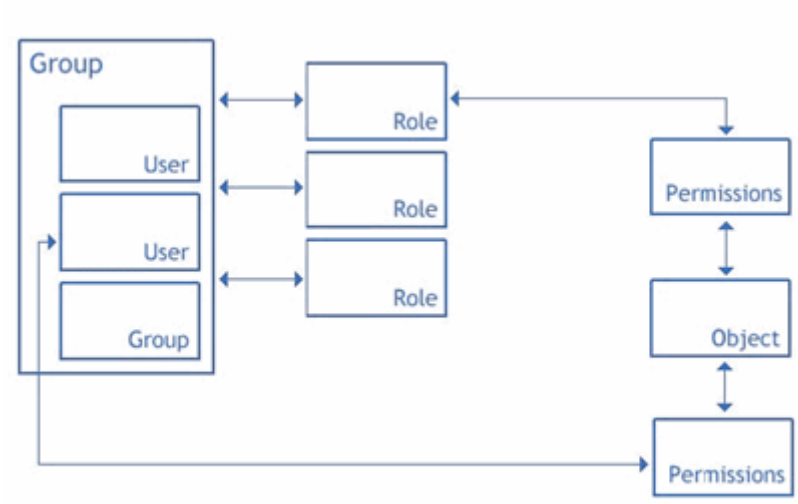
Term	Definition	Use in Foglight
Group	A group can contain one or more users or other groups. Roles are assigned to users through groups.	You can assign roles and add users to groups.
Configuration Item	A configuration item such as a rule or registry variable.	Access to configuration items can be assigned to specific users or to roles. Each configuration item is initially owned by its creator.

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.

Figure 2. Relationships between 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, Foglight™ 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 clear text 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 *<foglight_home>/server/tomcat/server.xml* directory.
3. Open the *server.xml* file for editing.
4. In the *server.xml* file, locate the following `Connector` elements:

```
<Connector executor="tomcatThreadPool" maxHttpHeaderSize="8192"
   URIEncoding="UTF-8" enableLookups="false" acceptCount="100"
   connectionTimeout="20000" disableUploadTimeout="true" bindOnInit="false"/>

<Connector executor="tomcatThreadPool" maxHttpHeaderSize="8192"
   URIEncoding="UTF-8" scheme="https" secure="true" SSLEnabled="true"
   clientAuth="false" … />
```

5. Add the `server="hidden"` attribute to each `Connector` element. For example:

```
<Connector executor="tomcatThreadPool" maxHttpHeaderSize="8192"
   URIEncoding="UTF-8" enableLookups="false" acceptCount="100"
   connectionTimeout="20000" disableUploadTimeout="true" bindOnInit="false"
   server="false"/>
```

6. Save and close the *server.xml* file 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

Foglight™ 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 Foglight™ Management Server to permit the use of specific TLS cipher suites only for communications with its Web server (all traffic over HTTPS).

NOTE: Enabling this configuration causes Foglight to accept only the cipher suites listed explicitly below.

To enable FIPS 140-2 mode for HTTPS traffic:

1. On the Management Server, open the *<foglight_home>/server/tomcat/server.xml* file for editing.
2. In the *server.xml* file, locate the following `Connector` element:

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

3. Add the following `ciphers` attribute to the `Connector` element:

```
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_ECDH_ECDSA_WITH_AES_128_CBC_SHA,
   TLS_ECDH_RSA_WITH_AES_128_CBC_SHA,
   TLS_ECDHE_ECDSA_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"
```

4. Restart the Management Server.

Network ports

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

Default port assignments

Table 2. Foglight™ Management Server default port assignments

Port Name	Port Number	Outgoing/Incoming
Embedded PostgreSQL®	15432	Incoming/Outgoing
Cluster Multicast	45566	Incoming/Outgoing
HTTP	8080	Incoming

Table 2. Foglight™ Management Server default port assignments

Port Name	Port Number	Outgoing/Incoming
HTTPS	8443	Incoming
AJP13	8009	Incoming
JNDI RMI	1098	Incoming/Outgoing
JNDI JNP	1099	Incoming/Outgoing
JRMP Invoker	4444	Incoming/Outgoing
JRMP Pooled Invoker	4445	Incoming/Outgoing
JRMP Unified Invoker	4448	Incoming/Outgoing
HA JNDI RMI	1101	Incoming/Outgoing
HA JDNI JNP	1100	Incoming/Outgoing
HA JRMP Invoker	4447	Incoming/Outgoing
HA Pooled Invoker	4446	Incoming/Outgoing
HA JNDI UDP Group	1102	Incoming/Outgoing

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.

Table 3. Ports used when Foglight is installed with an external database

Port Name	Port Number	Outgoing/Incoming
External PostgreSQL®	5432	Outgoing
Microsoft® SQL Server®	1433	Outgoing
Oracle®	1521	Outgoing

Agent adapter ports

Table 4. Agent adapter ports used when configuring the Foglight Administration Console

Port Name	Port Number	Outgoing/Incoming
Agent Manager	8080	Incoming
Agent Manager over SSL	8443	Incoming
Java EE Technology Agent	41705	Incoming

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 time span. 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 database

Quest Software Inc. monitors and provides patches and/or upgrades to address any relevant vulnerabilities that may affect the embedded PostgreSQL® 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 (PostgreSQL®, 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.

QuestClick scripts

QuestClick scripts can potentially store confidential information including IDs, passwords, account numbers, and SSNs. It is therefore important that additional security options are provided to safeguard and protect such confidential information embedded within recorded scripts.

Understanding the Foglight platform's relationship to Java

Foglight™ does not run Java™ code in the browser, and therefore is not vulnerable to Java applet security issues. The recently reported Vulnerability Note VU#625617 is one example of such an issue.

The Foglight platform uses the Java Runtime Engine (JRE) internally to run the Management Server and the Agent Manager(s). These are self-contained software systems that are fully isolated from the Foglight platform's content delivery system (the Web-based user interface) and as such they are not vulnerable to browser-based attacks. In particular, the Management Server and Agent Managers are not vulnerable to browser-based attacks that rely on the Java plug-in. Even when a Java plug-in is enabled in the browser, it cannot communicate with or influence the JRE instances that run Foglight in a separate process.

The Foglight platform's Web-based user interface is a pure HTML interface which does not use Java. As such the Web-based user interface cannot be manipulated by Java plug-in–based attacks, and it remains fully operational when the Java plug-in is fully disabled. Customers using the Foglight platform's Web-based user interface in their browsers may fully disable the Java plug-in without impacting their access to the Foglight platform.

“Clickjacking” vulnerability

Clickjacking is a vulnerability that causes an end user to unintentionally click invisible content on a web page, typically placed on top of the content they think they are clicking. This vulnerability can cause fraudulent or malicious transactions. One way to prevent clickjacking is by setting the `X-Frame-Options` response HTTP header with the page response. This prevents the page content from being rendered by another site when using `iFrame` HTML tags.

The Foglight Management Server adds the `X-Frame-Options` response HTTP header with the page response in the main URL: https://*<localhost>:<port>*/console/page. For the following two URL addresses, you can specify whether or not the page content is rendered by configuring the `Frame Option` option:

- Remote Portlet URL: https://*<localhost>:<port>*/console/remote/*<Referecen Id>*
- Network Operations Console URL: https://*<localhost>:<port>*/console/noc/*<Referecen Id>*

After specifying the value of `Frame Option`, the Foglight Management Server overwrites the value of the `X-Frame-Options` response header with the value of `Frame Option`. The value of the `Frame Option` option includes the following:

NOTE: Only the value configured in the top-level view takes effects.

- ALLOW (default value): View embedded using the <frame>/<iframe> tag can be rendered.
- SAMEORIGIN: View embedded using the <frame>/<iframe> tag can only be rendered when <frame>/<iframe> is on the same domain as its parent page.
- DENY: View embedded using the <frame>/<iframe> tag cannot be rendered.

Disclaimer

Quest Software Inc. 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 Inc. products.

2

Security features for APM appliances

A Foglight™ monitoring environment may include one or more physical appliances and/or virtual appliances used for application performance monitoring (APM). This chapter describes the security features present on the appliances.

NOTE: If you are using Foglight Experience Monitor appliances and/or Foglight Experience Viewer appliances, this section does not apply. Review the guides provided with those products. For more information, see the *Foglight Experience Monitor Security and Compliance Guide* and the *Foglight Experience Viewer Security and Compliance Guide*.

Overview of APM appliances

Appliances can host one or more of the following software components: Management Server, Sniffer, and Archiver. Appliances with a Sniffer component are attached to the customer's network where they passively monitor Web traffic. Sniffers capture, decrypt, and analyze the Web traffic, and transmit content and metrics to one or more Archivers within the same capture group as the Sniffer. Archivers receive the data from Sniffers, analyze the data, and maintain databases used for searching, reporting, and replay. Archivers send snapshots of collected data to the Management Server for display in top-level APM dashboards.

The following table describes the type of appliances that implement the security features discussed in the rest of this section. Appliances come with a predefined set of software components installed on the appliance. Appliances can be physical appliances (PowerEdge series hardware) or virtual appliances (VMware® vSphere®). Both physical and virtual appliances can exist in the same installation, with some restrictions.

Table 1. Appliance types

Appliance Type	Software Components	Available as a Physical Appliance	Available as a Virtual Appliance
All-in-One Appliance	• Management Server • Archiver • Sniffer	Yes	No
APM Appliance	• Management Server • Archiver	Yes	Yes, on separate virtual disks
Management Server Appliance	• Management Server	Yes	Yes
Archiver Appliance	• Archiver	Yes	Yes
Sniffer Appliance	• Sniffer	Yes	Yes

Trust model

The following assumptions are made about the installed environment:

- When more than one physical appliance is in use, the capture subnet ports are connected by a private cable (one Sniffer to one Archiver) or through a private network (when there is more than one Sniffer or Archiver).
- An appliance's control port is connected to the customer's network. The IP addresses assigned within this network should preferably be private, that is, not directly accessible through the public Internet.
- Only trusted, authorized personnel have physical access to the PowerEdge servers hosting physical appliances.
- Only trusted, authorized personnel have user accounts on the appliances.
- The password for the default *setup* account on each appliance is changed during the initial setup.
- The password for the default *foglight* user in Foglight™ is changed during the initial setup.

Multiple layers of defense

Appliances include multiple layers of defense to protect against intrusions and hack attempts:

- Layer 1: Firewall
- Layer 2: Port scan detection and blocking tool
- Layer 3: Customized operating system distribution
- Layer 4: Apache Tomcat server configuration

Layer 1: Firewall

Appliances are designed to be installed in network environments that have strong security measures in place, including the use of firewalls and intrusion detection systems. Appliances must be installed behind the firewall. More specifically, the appliance's control port must be accessible from behind the firewall only, while its monitoring ports may be connected to a network tap outside the firewall. The monitoring ports operate in promiscuous mode, and Web traffic that comes across these ports is copied to the Sniffer, so there is no risk of attack through these ports.

Appliances also include a built-in firewall which provides additional security beyond what is provided by the network environment. This firewall is constructed using the firewall rule-set building utility Bastille-Linux® (for details, see http://bastille-linux.sourceforge.net/). The firewall limits external access to the HTTP or HTTPS port for report viewing and additional ports used for intra-component communications.

If command-line access is needed for Quest Support to run low-level diagnostic procedures, customers may optionally open the SSH port. For more information, see Enable remote access using SSH on page 25.

The firewall also includes typical checks for illegal addresses and limits ICMP usage. Opening and closing HTTPS and SSH ports is the responsibility of APM Administrators.

Layer 2: Port scan detection and blocking tool

Many network intruders begin an attack by scanning the target network. Detection of such a scan offers one indication that an attack is about to begin. Appliance software attempts to detect such scans by monitoring access to ports that are not active on the appliance system, but are typically exploited by hackers (for example, *FTP*, *POP3*, *IMAP*). Upon detection, the appliance automatically adds the source IP address of the potential attacker to the firewall rule-set and blocks all future packets that appear to originate from that address. This functionality is implemented using the Port Sentry tool (for details, see http://sourceforge.net/projects/sentrytools).

Layer 3: Customized operating system distribution

System tools that are part of an operating system could potentially be exploited by hackers. To reduce this risk, the following measures are taken:

- Appliances have a minimal version of the 64-bit SUSE Linux® Enterprise Server (SLES) 11 operating system preinstalled.
- The latest operating system security patches and upgrades are applied with every release of the appliance software.
- Many tools and packages that represent common vulnerabilities are stripped out of the distribution. For example, server instances of *Telnet, FTP server, rlogin, NFS, Samba,* and *lpr* are not installed on the appliance.
- Access to potentially exploitable tools (such as *ping* and *traceroute*) is severely restricted.
    - *ping* — The appliance's Console Program uses the *ping* utility to verify network access during the appliance setup process. The Console Program requires a user account distinct from the browser interface user account. For more information, see User authentication on appliances on page 23.
    - *traceroute* — The *traceroute* utility is used only as an option in the alerting system; users can specify to traceroute to a particular IP address if an alert is triggered. There is no other access to the *traceroute* utility other than through the alerting system.
- Appliances implement shadow passwords to make brute force password attacks harder to execute.
- All standard Linux® user accounts available on the appliance (such as, *shutdown, halt,* and *mailnull*) have no login shell that allows an attacker to enter shell commands. For more information, see User authentication on appliances on page 23.

Layer 4: Apache Tomcat server configuration

Appliances use Apache Tomcat to facilitate communication between the software components on the appliances, primarily between the Management Server and the Archiver. Communications between software components are encrypted, with the exception of Sniffer to Archiver data transfer. Appliances require SSL and client authentication

for any request received from an external source (external to the appliance). For more information, see Secure data transfer between software components on page 27.

Restricted access to appliances

Access to appliances is restricted and secured in the following ways:

- No root access
- User authentication on appliances
- Secure remote access
- Restricted network ports for appliances
- Defense against Denial-of-Service attacks

No root access

The root account is not used to run any services. Users cannot log in as root. The appliance's *root* password is not shared with customers. The password is restricted to authorized personnel on the appliance development team. The secret *root* password is changed with every major release.

An internal foglight account is used by the appliances to run services. There is no external access to the account, that is, no one can log in to an appliance using the *foglight* account.

User authentication on appliances

Appliances control access to the Console Program using a dedicated user authentication mechanism, which is separate from the one described under Security features in Foglight on page 7. The user authentication mechanism is built on the Linux® Pluggable Authentication Modules (PAM). Account passwords are stored in encrypted form in Linux system files.

NOTE: Appliances cannot use the LDAP-compatible directory services that are supported for the browser interface.

In addition to the root and foglight accounts described under No root access, the appliances ship with a default user account called setup.

The person configuring the appliances initially uses the default *setup* account to run the setup menu facility (hereafter called the Console Program) on an appliance. This text-mode application is the *setup* user's shell, and the user is logged out when this shell is exited. The Console Program uses Yast to configure network cards and has menus to configure and start/stop Foglight™ services. The setup account does not have read access to any directory where Foglight stores sensitive customer data. The *setup* user can create additional user accounts as necessary.

NOTE: To adhere to security best practises, the setup account either needs to be updated with a new password or deleted after a new user account is created.

Secure remote access

An authorized user can access an appliance remotely using one of the following secure methods: Remote Access Controller (DRAC) or SSH.

- To use DRAC, the appliance's DRAC port needs to be connected to the public switch.

- To use SSH, the user's account on the appliance needs to be configured to enable SSH. By default, the *setup* account and all new accounts have SSH disabled. If SSH is enabled, the user account requires a strong password, which must contain at least the following elements:
  - an upper case letter
  - a lower case letter
  - a numeric character
  - one character that is not alphanumeric

For instructions, see the *Foglight APM Installation and Setup Guide*.

Restricted network ports for appliances

Table 2. Ports supporting communications among appliances and access to the Foglight™ Management Server.

Port Number	Software Component	Purpose	Direction of Communication
7611 and 7612	All appliances	Communicate with other appliances	Management Server —> Sniffer or Archiver
7621 and 7622	Archiver	Communicate with other appliances	Management Server —> Archiver
7623	Relayer	Transmit capture data from Sniffers to Archivers	Sniffer —> Relayer —> Archiver
7602	Management Server	Communicate with other appliances	Archiver or Sniffer —> Management Server
8080	Management Server	Run the Foglight browser interface	Client —> Management Server
8443	Management Server	Run the browser interface over a secure connection (HTTPS)	Client —> Management Server
22	All appliances	Enable remote access using SSH	Client —> Appliance

Other open ports

The following TCP ports are left open to detect port-scanning programs: **1**, **11**, **110**, and **143**. For more information, see Layer 2: Port scan detection and blocking tool on page 22. When time synchronization with a time server using NTP is enabled, UDP port **123** is open.

Run the browser interface over a secure connection (HTTPS)

To use port 8443 instead of 8080, set the Management Server's `httpsonly` option to `true`. When the Management Server is hosted on an appliance, the setting is located in the `appliance.config` file, which you can access from the command line.

To enable HTTPS on an appliance:

1. Log into the Console Program.
2. Select **Advanced Options**.
3. Select **Access Shell**.
4. Type: `vi /opt/quest/foglight/config.appliance/appliance.config`

5 Enable the following code by removing the leading hash symbol (#):
`server.console.httpsonly = "true";`

6 Save the change and exit vi by pressing **Esc** and then typing `:wq`

7 Type: `rcfoglight restart`

Enable remote access using SSH

To enable remote access using SSH, open port 22 for individual Console Program user accounts.

TIP: When a remote troubleshooting session is required, enable SSH for the user account that will be assigned to the troubleshooter. As soon as the troubleshooting session ends, disable SSH access for this account.

To enable SSH for an existing user:

1 Log into the Console Program.

2 Select **Console User Account**s.

3 Select **Modify Console User**.

4 Select the target user account.

5 Select **Enable/Disable SSH**.

6 If the account does not use a strong password, follow the prompts to change the password.

Defense against Denial-of-Service attacks

Any network services that are not required for the operation of APM appliances are removed. This reduces the possible avenues through which an attacker may attempt to gain access. For example, the appliance does not respond to ping requests. A firewall (Bastille) and a port scanning tool (Port Sentry) are used to restrict and monitor access to appliances. In addition, certain ports have been opened for the sole purpose of intrusion detection. If an appliance observes a computer probing any of these ports, it automatically records the computer's IP address and blocks any future access. Such an event is recorded in the logs.

Logs for appliances

In addition to the logs provided by the Management Server (see "Audit log" and Log files on page 17), appliances have the following types of logs:

- **Configuration Change Log** — All changes to the configuration through the **APM > Traffic Capture** or **APM > Traffic Analysis** dashboards are recorded in the Configuration Change Log on the appliance hosting the Management Server. For more information, see "Managing Configuration Changes" in the *Foglight™ APM Administration and Configuration Guide*.
- **Console Program Logs** — Changes to the appliance are logged in the following logs:
  - Sniffer changes: */var/log/sniffer*
  - Relayer changes: */var/log/relayer*
  - Upgrade: */var/log/install* and */var/log/rpmupgrade*
- **Support Bundle Logs** — Log files are also created when generating a support bundle from the Console Program, including:
  - */var/log/systemhealth.log*
  - */var/log/sysinfo.log*
  - */var/log/ifconfig.log*

- */var/log/ethtool.log*
- */var/log/archiver.shardtable*
- */var/log/archiver.mysql*
- */var/log/archiverproxy.threaddump*
- */var/log/appliancemon.threaddump*

Data entry validation for APM dashboards

For the APM dashboards, Foglight™ validates user input in its browser interface and on its back-end. This includes checking that the correct data type is entered (for example, no numbers are entered in a text-only box) and restricting the length of input, such as to avoid certain potential buffer overflow attacks.

Installation of upgrades and patches

When the appliance software needs to be updated, the upgrade or patch package is digitally signed with a PGP key to prevent customers from uploading unauthorized materials. Upgrades and patches are installed using the **APM > Support > Upgrade Appliances** dashboard. All registered appliances are updated. Alternatively, individual appliances can be updated using an appliance's Console Program.

Customer data protection on appliances

The following measures are implemented to protect access to customer data:

- Restricted access to sensitive captured data
- Secure data storage in the Archiver database
- Secure data transfer between software components
- Secure use of customers' private keys

Restricted access to sensitive captured data

Appliances can be configured to hide, mask, or discard (not store) sensitive data found in hit details and in the body of HTML pages.

- When sensitive data rules hide or mask data, the sensitive data is stored unaltered in the Archiver database. The sensitive data rules are applied whenever a query for data is received by the Archiver database. When returning results, sensitive data is hidden or masked in views or replay according to the user-defined rules.

  IMPORTANT: There is a special Foglight user role, called APM Sensitive Data Viewer, that allows users to view sensitive data in views and replay. Customers can restrict users with this role from viewing some types of sensitive data by selecting the Always Sensitive option when defining a sensitive data rule.

- Customers can discard sensitive data, rather than storing it in the Archiver database. In this case, the sensitive data can never be displayed in the browser interface. The sensitive data rules are applied as hits are captured.

  IMPORTANT: Applying sensitive data rules at capture time can degrade capture performance significantly.

Foglight™ implements its sensitive data rules using two types of user-defined rules: Sensitive Hit Details and Sensitive Content Expression. Sensitive hit details refer to private information, such as login names and passwords, that are contained within request fields, request headers, response headers, and cookies. Sensitive content refers to private information located in the body of HTML pages, such as credit card numbers, social security numbers (or other government identification numbers), and passwords. When defining the rules, customers identify the sensitive data, specify whether the data is hidden or masked, and specify whether the data should be considered *Always Sensitive*. For more information, see the “Managing Security Policies” topics in the *Foglight APM Administration and Configuration Guide*.

When customers want to discard sensitive data before storing a hit in the Archiver, they define the sensitive data rules *and* define a hit analyzer with a *Do not store* storage policy set. The policy determines whether the entire hit is discarded or only the details or content marked *Always Sensitive*. For each hit that matches the hit analyzer condition, Foglight evaluates the sensitive data rules and applies the storage policy. For more information, see “Defining Hit Storage Restrictions for Hit Analyzers” in the *Foglight APM Administration and Configuration Guide*.

Secure data storage in the Archiver database

Content, metrics, and other details captured from the monitored Web traffic are stored in a distributed Archiver database. The port through which the database is accessed is not open, and no tools that would allow access to this data are available to *non-root* appliance users. The only way to access the data is through controlled queries from the **APM > Search** dashboards.

By default, captured data is stored until an Archiver determines that it needs more space. The Archiver deletes the oldest data in the system to make room for new data. However, customers who require that data be stored for a limited time can configure the Archivers to remove data based on a maximum retention duration setting (for example, 48 hours or one week).

If customers need to decommission an appliance, they have the option to reset its database and verify that data is securely deleted before withdrawing the appliance from active service. For detailed instructions about purging the appliance database, see the *Foglight*™ APM Administration and Configuration Guide.

Secure data transfer between software components

Some top-level APM dashboards require that metrics and details be sent from the Archiver database to the Foglight database repository at regular intervals. This data is encrypted before being sent. For more information, see Layer 4: Apache Tomcat server configuration on page 22.

For the capture subnet, data is sent in the clear from a Sniffer component to an Archiver component through a custom-built TCP protocol over the dedicated port 7623. When these components are located on separate physical appliances, isolate the capture subnet using a crossover cable or a dedicated private switch. For virtual appliances, use a separate virtual capture network to keep this traffic from being generally available to all virtual machines in the customer’s environment.

Secure use of customers’ private keys

In addition to monitoring regular HTTP traffic, appliances can monitor Secure Socket Layer traffic (SSL/TLS). To enable monitoring of SSL traffic, customers upload their private SSL encryption keys to Foglight™ using the browser interface. These keys are naturally of high sensitivity to customers.

The SSL keys are stored centrally on the Management Server in an encrypted file. When a Sniffer needs keys, the keys are transmitted over a two-way authenticated and encrypted SSL connection from the Management Server to the Sniffer. The remote Sniffer never writes the keys to disk, using them from memory only. When a Sniffer restarts, it submits a new request for keys.

Foglight uses the AES-256 data encryption algorithm to encrypt the SSL connection. The encryption key is created upon installation and is unique to each customer. It consists of a combination of random data and certain data specific to the customer, making it difficult to guess or enter using brute force. Each Sniffer has its own client certificate that is used for client side authentication, therefore only Sniffers added by the Administrator are allowed to connect to the Management Server. This prevents external attempts to open an SSL connection to the Management Server to request keys. The Sniffers use the server's certificate for authentication to prevent any man-in-the-middle attacks.

Foglight can also use private keys stored in a SafeNet Hardware Security Modules (HSMs) server to decrypt secure traffic. Foglight accesses and uses SafeNet private keys in a secure manner consistent with the SafeNet HSM model. In particular:

- SafeNet server certificates and client certificates are used to authenticate Foglight with the HSM server.
- Foglight communicates with SafeNet HSM servers using the recommended PKCS #11 API.
- Foglight never stores SafeNet private keys on disk and never exposes them in any interface.

3

Usage feedback

The Foglight™ Management Server can collect usage data about your environment and send it to Quest Software Inc. to improve support response. This data helps Quest Software Inc. 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 may be enabled. To turn it off, click Disable on the Communication dashboard. This dashboard is accessible from the navigation panel in the Foglight browser interface, under Administration > Support > Support Notifications > Automatic Communication with Quest.

A

Appendix: 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/PubsSPs.html#800-53). 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.

- 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 1. NIST 800-53 Categories

Category	Applicable	Description	Additional Details
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. For appliances, access to an appliance is controlled through a separate user authorization mechanism. The appliance's *root* password is not distributed to customers.	• Foglight users and groups on page 8 • Role-based access control on page 8 • Restricted access to appliances on page 23
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. For appliances, changes made using the Console Program are logged. Separate logs are kept for Sniffers, Relayers, Archivers, and upgrades to appliance software.	• Audit log on page 17 • Log files on page 17 • Logs for appliances on page 25
Certification, Accreditation and Assessments (CA)	No	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.	N/A

Table 1. NIST 800-53 Categories

Category	Applicable	Description	Additional Details
Configuration Management (CM)	Yes	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. Appliances are configured to provide only the services necessary for their operation, and makes unnecessary ones unavailable. A separate configuration change log records incremental changes to traffic capture and traffic analysis settings.	• Enabling FIPS 140-2 mode for HTTPS traffic on page 15 • Network ports on page 15 • Configuration parameters on page 17 • Audit log on page 17 • Layer 3: Customized operating system distribution on page 22 • Logs for appliances on page 25
Contingency Planning (CP)	No	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.	N/A
Identification and Authentication (IA)	Yes	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. For appliances, a user authorization mechanism (built on the Linux® Pluggable Authentication Modules) controls access to an appliance.	• Foglight users and groups on page 8 • Role-based access control on page 8 • Password policies on page 9 • User authentication on appliances on page 23
Incident Response (IR)	No	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.	N/A

Table 1. NIST 800-53 Categories

Category	Applicable	Description	Additional Details
Maintenance (MA)	Yes	Quest Software Inc. monitors the embedded PostgreSQL® database included in Foglight developments for security developments and flaws and provides product updates and patches to customers when necessary. For appliances, Quest Software Inc. monitors the systems on which the appliance is based (such as SLES and Apache), and provides security patches to customers when necessary. Remote appliance maintenance using SSH is available in agreement with the customer.	• Monitoring patches for the embedded database on page 18 • Restricted access to appliances on page 23
Media Protection (MP)	No	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.	N/A
Physical and Environmental Protection (PE)	No	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.	N/A
Planning (PL)	No	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.	N/A
Personnel Security (PS)	No	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.	N/A
Risk Assessment (RA)	No	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.	N/A
System and Services Acquisition (SA)	Yes	Quest Software Inc. 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.	N/A

Table 1. NIST 800-53 Categories

Category	Applicable	Description	Additional Details
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-Agent Manager-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. For appliances, communication is encrypted between the Management Server and other components. Between Sniffers and Archivers, data is sent in the clear. Appliances are monitored for denial-of-service attacks and other potential attacks using a port scanner. To support secure communication with an appliance, SSH can be enabled.	• Protection of data collection infrastructure on page 11 • Protection of communicated data on page 13 • Enabling FIPS 140-2 mode for HTTPS traffic on page 15 • Customer data protection on appliances on page 26 • Restricted access to appliances on page 23
System and Information Integrity (SI)	Yes	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. For appliances, user access is restricted, and a firewall and port scanner are used as intrusion detection tools. Appliances are build on a customized SLES operating system on which only necessary services are installed. Ports used for network connections are restricted. Hit details and content can be marked as sensitive and access restricted to authorized users. The collected data is stored in a database that is not accessible through the network. Changes to the traffic capture and traffic analysis configuration are tracked, allowing for the system to be rolled back to a stable state in case it gets corrupted. All upgrades, patches, and hotfix packages are digitally signed.	• Protection of stored data on page 12 • Restricted access to appliances on page 23 • Layer 1: Firewall on page 21 • Layer 2: Port scan detection and blocking tool on page 22 • Layer 3: Customized operating system distribution on page 22 • Customer data protection on appliances on page 26 • Logs for appliances on page 25 • Installation of upgrades and patches on page 26

About Us

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 or call +1-949-754-8000.

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.