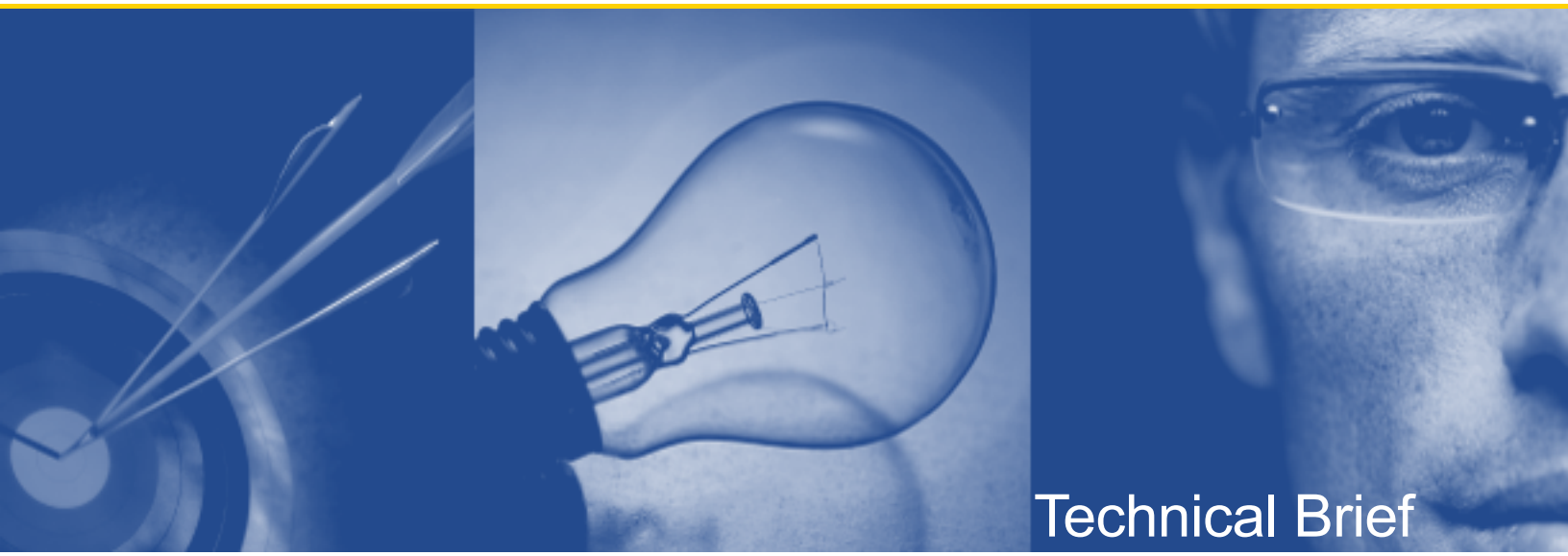
QUEST SOFTWARE
Smart Systems Management

Security and Compliance in Foglight 5.2.4

Written by
Einar Mykletun Ph.D.
Quest Software, Inc.



WARRANTY

The information contained in this document is subject to change without notice. Quest Software makes no warranty of any kind with respect to this information. QUEST SOFTWARE SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTY OF THE MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Quest Software shall not be liable for any direct, indirect, incidental, consequential, or other damage alleged in connection with the furnishing or use of this information.

TRADEMARKS

All trademarks and registered trademarks used in this guide are property of their respective owners.

World Headquarters:
5 Polaris Way
Aliso Viejo, CA 92656
e-mail: info@quest.com

Please refer to our Web site (www.quest.com) for regional and international office information.

Updated—October 2009

CONTENTS

INTRODUCTION

Managing information systems security is a priority for every organization. In fact, the level of security provided by software vendors has become a differentiating factor for IT purchase decisions. Quest Software strives to meet standards designed to provide its customers with their desired level of security, whether it relates to privacy, authenticity and integrity of data, availability, or protection against malicious users and attacks.

This document describes the security features of Quest Foglight. It reviews access control, customer data protection, secure network communication, and more. There is also an appendix that describes how Foglight's security features meet the NIST recommended federal information security standards as detailed in the Federal Information Security Management Act (FISMA).

ABOUT FOGLIGHT

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's 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 a HTTP or HTTPS connection. Individual cartridges can be installed on FMS 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, known as Foglight Clients. Some cartridges may contain agents that are deployed locally on the FMS server. These agents collect monitoring data and report it back to FMS. Users can then access this data in various forms. Figure 1 provides an overview of the interaction between Foglight components.

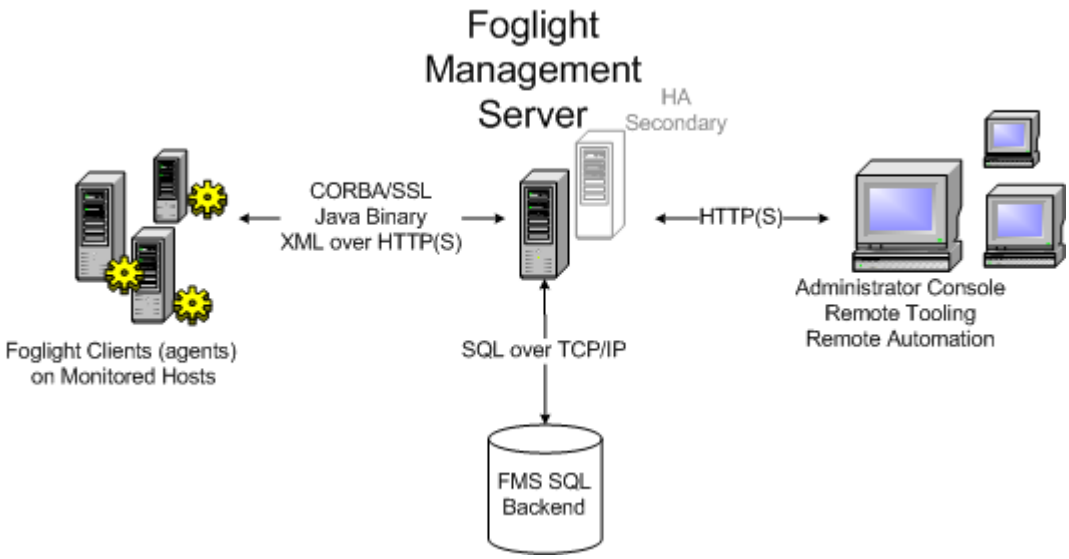


Figure 1. Overview of interaction between Foglight components

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, Sun Java Systems Directory Server, 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).

FMS database repository

Foglight supports using specific versions of both MySQL and Oracle databases for its backend 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. The database will require manual configuration.

Agent credentials

When installing Foglight cartridge agents.it typically is 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 Administrator console and give an agent access to applications or operating systems on the monitored host(s).

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

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.

There are two types of groups in Foglight: internal and external groups. Internal groups are created using the Foglight administration console. External groups are mapped from an LDAP-compatible directory service supported by Foglight.

Foglight comes with one default internal user (foglight) with administrative access and 4 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:

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 to 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 user name and a password and can belong to one or more groups.	A user logging in to Foglight as is authorized to perform a certain set of actions based on the roles that have been assigned to the user's group(s).
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 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 depicts the interrelationship of users, groups, roles, permissions, and configuration items.

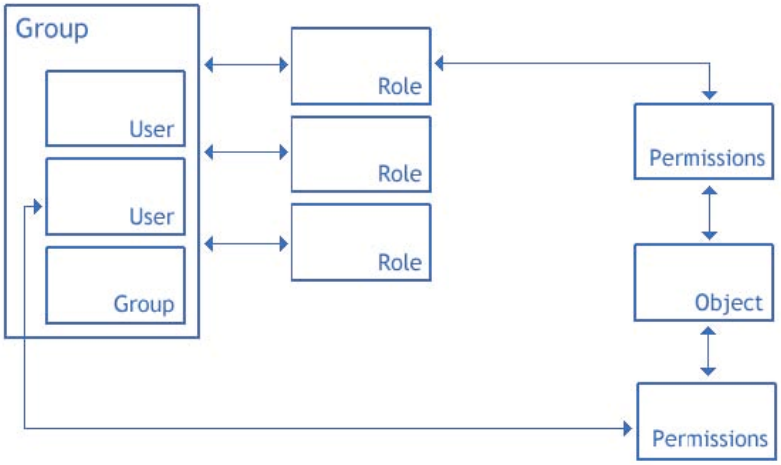


Figure 2. Interrelationship of users, groups, roles, permissions, and configuration items

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

The Manage Groups page contains a table that lists all of the groups that have been created in the administration console or imported from an LDAP-compatible directory service supported by Foglight, 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 Administration role) and for internal users.

- An internal user's password will expire after ninety (90) days.
- An administrator's password will expire after forty-five (45) days. The one exception is the password for the default user foglight, which does not expire.

- A user will be locked out of the system for fifteen (15) minutes after he or she enters an incorrect password for five (5) consecutive login attempts.
- Foglight will remind a user fifteen (15) days before his or her password expires.
- The password must:
    - Be at least seven (7) characters long.
    - Contain both alphabetic and numeric characters.
- The password cannot:
    - Be the same as the user name.
    - Be a dictionary word.
    - Be just the repetition of a single character.
    - Be longer than twenty (20) characters.
    - Be the same as any of the user's last twelve (12) passwords.

Users with the Foglight Security Administration role can view and edit the configurable password policies on the Configure Password Settings page 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.
- A user's password cannot be a dictionary word.
- A user's password cannot be just the repetition of a single character.
- A user's password cannot be 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 internal users and users with the Foglight Security Administration role. The numbers listed in the drop-down menus on the Configure Password Settings page correspond to 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 complexity level 1.

Required Privileges

Installing Foglight Management Server

To install Foglight, administrative privileges on the target operating system is 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 below (Manual Database Configuration).

Running Foglight Management Server

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

Installing Agent components

Certain cartridges (for example, the Foglight Cartridge for Java EE) include one or more executable agent installers. The Agent Installers page within the FMS 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. In this case, the database will need to be manually configured prior to starting FMS. This configuration requires executing the scripts in the `<foglight_home>\scripts\sql` directory as described in the Installation Guide. Some scripts must be run using an account with administrative privileges.

Protection of Data Collection Infrastructure

Installation of data collection middleware

There are many types of Foglight agents; most communicate with FMS through a provided middleware component. Presently, Foglight supports two implementations of this middleware—Foglight Agent Manager (FglAM) and the Service Provider Interface Daemon (SPID). FglAM will replace all existing SPID installations at a future date.

It is only necessary to install one of the middleware architecture options (SPID or FglAM); for this reason the two architectures are separated in the sections below.

Both middleware components 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).

Administrator privileges:	
SPID	Installation of SPID requires administrator access to the monitored host
FglAM	FglAM can be installed without administrator access, but such access is required to enable startup scripts/windows services to allow automatic launching of FglAM upon machine reboot

Once installed, each middleware component manages the lifecycle of a number of hosted agents and provides a central communications link between those agents and FMS. Hosted agents and the middleware can be upgraded from FMS using this central communications link.

SPID installations can be migrated to FglAM in two ways: (1) as a remote upgrade from FMS via the central communications link, or (2) as part of a local installation on the monitored host. The former allows the administrator hands-off management of the Foglight infrastructure, while the latter allows for manual customization of the resulting system with greater control.

Agents requiring privilege escalation

Some data collection agents hosted by SPID or FglAM require administrator privileges to perform their assigned tasks. In order to avoid running the entire middleware host with the required privileges, we use a privilege escalation mechanism to create the required access for the agents that need it.

Privilege escalation	
SPID	SPID implements this functionality using a small launcher application which must be installed with “setuid root” permissions by the administrator. This launcher in turn is responsible for running the hosted agent with the required privileges. This launcher uses a number of different heuristics to validate that it is only launched in the context of a running SPID instance, and that it can only be configured to launch agents which have been installed by SPID. It is recommended that the administrator take proper measures to secure write access to the contents of their SPID installation on disk, so that a malicious user cannot replace components of the SPID installation with hostile executables.
FglAM	FglAM, by default, uses the well known “sudo” facility (a very fine-grained configurable system) to implement privilege escalation. Sudo can be configured to only allow 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 FglAM. FglAM also provides an alternative setuid root-based launcher, similar to the implementation provided in SPID. 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 get in the way of a timely demonstration. We do not recommend that this setuid root-based launcher be configured as part of our standard installation instructions.

Protection of Stored Data

Foglight Server and Foglight Clients use the Java Cryptographic Extension library for its cryptographic operations. The Triple DES (Data Encryption Standard) algorithm in Chain Block Cipher mode with a 112-bit key is used for encrypting FMS service account's passwords (e.g. 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. We recommend customers to change the default Java KeyStore password upon the installation of FMS. Note that 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 FMS can no longer decrypt existing ciphertexts under the old key).

FMS repository DBA 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.

Credentials for Foglight agents

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 via access control. Any agent property that is marked as sensitive is masked during display in user interface consoles.

Agent Properties	
SPID	When an SPID-based agent starts running on a monitored host, it requests its configuration properties from FMS. Any properties marked as sensitive in the agent properties schema are Triple DES encrypted by the agent upon receipt and stored in a cache file on the local file system. The Triple DES encryption key is not stored on the monitored host. Instead it is dynamically generated when needed (during encryption and decryption) based on certain metadata specific to the agent and monitored host.
FglAM	All agent properties are stored in cleartext 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 Foglight 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 FMS.

Basic HTTP access (non-SSL) can be disabled by disabling the HTTP port in the server. This will disable both HTTP access to the FMS web user interface as well as HTTP communication for agents that use the XML over HTTP protocol (see below).This forces the use of HTTPS connections.

Communication between FMS and agents

Most Foglight agents communicate with FMS through one of the included middleware applications, SPID or FglAM. The exceptions are the Java cartridge agents that communicate with FMS across a separate binary protocol and ones 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 FMS and Middleware

SPID	The SPID communication layer implements a protocol based on CORBA. This protocol opens a number of continuous network connections between the monitored host and FMS (four plus one per hosted agent). These connections are predominantly unidirectional (SPID to FMS), but FMS may attempt to open a reverse connection to the monitored host. SPID supports optional mutual SSL communication but it is not enabled by default. To enable SPID SSL communication one needs to configure the `Orb.xml` and `ORBInitRefs.xml` files within the `<SPIDHOME>/cache/SPINetwork/SPINetwork/0` directory on the monitored host. Both the SPID agent and FMS contain a self-signed Foglight SSL certificate for use with the SPID protocol in their respective Java KeyStores. These certificates cannot be replaced with certificates of a customer's choice.
FglAM	FglAM implements a communication layer with XML messages sent to FMS over HTTP(S). These messages are sent to the same ports which FMS uses for all HTTP-based traffic, including the web applications. FglAM allows the user to configure HTTP or HTTPS URLs for FMS, or a combination of both. When HTTPS is used, FglAM by default will reject an invalid certificate - either self-signed, signed by an unrecognized certificate authority, or a certificate which declares a Common Name which does not match the FMS host name (providing protection against man-in-the-middle attacks). Certificates can be added to the FglAM keystore. Like a web browser, FglAM supports configuration options to relax these certificate verification controls, but these options will reduce the security provided by the SSL mechanism. If FMS is configured to only allow HTTPS access, FglAM must be configured with an HTTPS URL to connect to FMS. By default. FMS uses the SSL_RSA_WITH_RC4_128_MD5 cipher suite (RSA, RC4, and MD5) for its communication with FglAM. FglAM supports concentrators; these are intermediate instances of FglAM that relay communication between leaf FglAM instances and FMS. These concentrators support HTTP or HTTPS communication with the upstream FMS. HTTPS communication with downstream FglAM instances will be supported in future versions. Current versions of FglAM only support HTTP communication between leaf nodes and concentrators.

Communication between FMS and Java agents

No encryption is used to protect the communication channel between Java agents (non SPID-based agents) and FMS. Data sent is in proprietary binary form.

Communication between FMS and XML over HTTP(S)

The XML over HTTP(S) protocol is another low-level method for submitting data to FMS. 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 FMS and the Repository Database

The Foglight repository database may be installed either on the same or separate server as the FMS server. Data is transmitted using the database communication protocol (of MySQL or Oracle) between FMS 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. Here are the steps for configuring FMS to only permit the use of specific TLS cipher suites for communications with its web server (all traffic over HTTPS). Note that by enabling this configuration, FMS will only accept the cipher suites explicitly listed below.

1. On the Foglight Management server, edit the following files:

```
FMSHOME\server\default\deploy\server_https.xml
FMSHOME\server\default\deploy\server_full.xml
```

2. Add this explicit cipher suite order to the "Connector" configuration:

```
<Connector port="${foglight.https.port}" address="${jboss.bind.address}"
maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
emptySessionPath="true" URIEncoding="UTF-8" SSLEnabled="true"
scheme="https" secure="true" clientAuth="false"
keystoreFile="${jboss.server.home.dir}/conf/tomcat.keystore"
keystorePass="nitrogen" sslProtocol = "TLS"
compression="on" 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"
/>
```

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 table shows the Foglight default port assignments for FMS:

Port Name	Port Number	Outgoing / Incoming
Embedded MySQL Port	13306	Outgoing/Incoming
Cluster Multi-cast Port	45566	Incoming/Outgoing
Web UI HTTP Port	8080	Incoming
Web UI HTTPS Port	8443	Incoming
AJP13 Port	8009	Incoming
JNDI RMI Port	1098	Incoming/Outgoing
JNDI JNP Port	1099	Incoming/Outgoing
JRMP Invoker Port	4444	Incoming/Outgoing
HA JNDI RMI Port	1101	Incoming/Outgoing
HA JNDI JNP Port	1100	Incoming/Outgoing
HA JRMP Invoker Port	4447	Incoming/Outgoing
HA Pooled Invoker Port	4446	Incoming/Outgoing
HA JNDI UDP Group Port	1102	Incoming/Outgoing

High Availability (HA) refers to running a secondary instance of Foglight as a hot backup server (redundant mode).

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

Port Name	Port Number	Outgoing / Incoming
External MySQL Port	3306	Outgoing
Database Port (Oracle)	1521	Outgoing

Agent Adapter Ports

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

Port Name	Port Number	Outgoing / Incoming
SPID	3528	Incoming
SPID over SSL	3529	Incoming
FglAM	8080	Incoming
FglAM over SSL	8443	Incoming
JavaEE Agent	41705	Incoming

Middleware Communication

SPID	Which port is used to connect SPID to FMS t depends on whether or not SSL has been enabled on the SPID client. Port 3528 is used for non-SSL connections and port 3529 for SSL connections. FMS is configured to listen on both of these ports; it can handle simultaneous connections from either SSL or non-SSL enabled SPID clients. SPID accepts connections from its agents and manages communication to FMS on their behalf. Agents are installed locally on the same host as SPID and connect to SPID over TCP Port 5150. This is a local host connection, although SPID doesn't enforce that the connection originates from the local host. All communication between agents and FMS is initiated by agents, and agents do not listen (accept connections) to any ports.
FglAM	FglAM connects to FMS using the same HTTP(S) ports as the Web UI. FglAM uses standard URL format to configure the address of the upstream FMS, so if the port number is changed in the FMS configuration, then it is a simple matter to configure FglAM to use the updated port number. FglAM instances that are configured to communicate through a concentrator FglAM can use any desired port for their communication to that concentrator host. This needs to be configured on both the upstream as well as downstream FglAM instance. Some agents hosted by FglAM are run out-of-process, and use local TCP connections to communicate with the master FglAM process. Two protocols are used for this local communication: legacy RAPSD for agents which are supported by both FglAM and SPID (this is the same protocol implemented by SPID for local agent communication), and FglAM's XML-over-HTTP for new agents implemented with the FglAM API (this is the same protocol used by FglAM to connect to the upstream FMS or concentrators). In both cases, the master FglAM 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 local host; 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 Foglight Management Server's file system. When Foglight is opened, the parameters are read and cached internally; the configuration files on disk are not re-read until FMS restarts. This allows modification of the configuration files while Foglight is running without affecting real-time processing.

Audit Log

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

The View Audit Information page enables you to review these logs and to filter them to show information for a specific span of time. It also lists users who have logged in to the administration console, any changes with to user, group or role settings, as well as changes made to configuration items, including rules, schedules or registry variables.

The following information is listed 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 and can be viewed within the Admin Console. A subset of the Foglight methods that are audited include: 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 FMS: troubleshooting data (including warnings and errors), debug information, lifecycle information, and 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 wiped on uninstall. If required, the customer will have to delete the Foglight files from the file system.

IPv6

FglAM supports IPv6 communication with the FMS, and also with upstream FglAM concentrators. SPID does not support IPv6.

Monitoring Patches for Embedded Database

Quest Software monitors and will provide patches and/or upgrades to address any relevant vulnerabilities that may affect the embedded MySQL database that is provided with Foglight. To receive product updates or security patches, a customer may be required to upgrade to the latest release of Foglight.

Customers who use an external database (MySQL or Oracle) are responsible for applying the latest security patches to their databases 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.

CUSTOMER MEASURES

Foglight's security features are only one part of a secure environment. The customer's operational and policy decisions will have a great influence on the overall level of security. Customers will need to be responsible for the physical security of Foglight and its network. Administrators should change default passwords and replace them with strong passwords.

DISCLAIMER

Quest 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's products.

APPENDIX A: FOGLIGHT AND FISMA COMPLIANCE

The Federal Information Security Management Act[1] (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 an assets of the agency, including those provided or managed by another agency, contractor, or other source."

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[2]. 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.[3]

We would like to emphasize that the secure deployment of Foglight is only one part of an information security program. If the appendix states that a particular security category is "applicable" to Foglight, this means that Foglight contains security features that may be relevant to some or all aspects of the category in question. It may not mean that Foglight fully meets all of the requirements described in that security category, or that the use of Foglight by itself will guarantee compliance with any information security standards or control programs. The specification, selection and implementation of a successful security program depends on how the customer deploys, operates, and maintains its entire network and physical infrastructure, including Foglight.

1 http://csrc.nist.gov/sec-cert/

2 http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf

3 Note that under 800-53, these seventeen listed categories define general security control "families" (e.g., "AC"), and that each family in turn contains several subcategories (e.g., "AC-1", "AC-2", "AC-3", etc.) that further detail related aspects of information security and assurance. Consult Appendix F of 800-53 for further information.

NIST 800-53 Categories

Category:	Access Control (AC)
Applicable:	Yes
Description:	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. This means that the storage and management of the user accounts, as well as their roles and passwords, can be centrally managed through those directories.
Further Details:	Section(s) 3.2, 3.3

Category:	Awareness and Training (AT)
Applicable:	No
Description:	This category does not apply to Foglight; the customer is responsible for developing and reviewing all security awareness and training policies.
Further Details:	N/A

Category:	Audit and Accountability (AU)
Applicable:	Yes
Description:	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.
Further Details:	Section(s) 3.11, 3.12

Category:	Certification, Accreditation and Assessments (CA)
Applicable:	No
Description:	This category does not apply to Foglight; the customer is responsible for developing and reviewing all security assessment, accreditation and certification policies.
Further Details:	N/A

Category:	Configuration Management (CM)
Applicable:	Yes
Description:	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.
Further Details:	Section(s) 3.9, 3.10, 3.11, 3.12

Category:	Contingency Planning (CP)
Applicable:	No
Description:	This category does not apply to Foglight; customers are responsible for designing and implementing 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.
Further Details:	N/A

Category:	Identification and Authentication (IA)
Applicable:	Yes
Description:	Foglight enforces identification and authentication through password protected user accounts. Well-defined password policies can be used to restrict the types of passwords that can be created. Only authorized users are able to log on to the Foglight and the web server. The customer can also choose to authenticate users against an LDAP supported directory.
Further Details:	Section(s) 3.2, 3.3, 3.4

Category:	Incident Response (IR)
Applicable:	No
Description:	This category does not apply to Foglight; the customer is responsible for developing and reviewing incident response policies and procedures.
Further Details:	N/A

Category:	Maintenance (MA)
Applicable:	Yes
Description:	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.
Further Details:	Section(s) 3.16

Category:	Media Protection (MP)
Applicable:	No
Description:	This category does not apply to Foglight; the customer is responsible for developing and reviewing media protection policies.
Further Details:	N/A

Category:	Physical and Environmental Protection (PE)
Applicable:	No
Description:	This category does not apply to Foglight; the customer is responsible for developing and reviewing physical and environmental policies.
Further Details:	N/A

Category:	Planning (PL)
Applicable:	No
Description:	This category does not apply to Foglight; the customer is responsible for developing and reviewing security planning policies.
Further Details:	N/A

Category:	Personnel Security (PS)
Applicable:	No
Description:	This category does not apply to Foglight; the customer is responsible for enforcing personnel security policies, including personnel screening and termination.
Further Details:	N/A

Category:	Risk Assessment (RA)
Applicable:	No
Description:	This category does not apply to Foglight; the customer is responsible for developing and reviewing risk assessment policies.
Further Details:	N/A

Category:	System and Services Acquisition (SA)
Applicable:	Yes
Description:	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, as well as some recommended security features that will be implemented in future product releases.
Further Details:	N/A

Category:	System and Communications Protection (SC)
Applicable:	Yes
Description:	The Foglight 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. SPI and FglAM communication between agents and FMS can also be protected with SSL. Communication between Java agents (non SPI-based) and FMS is unencrypted. No security is enforced to protect communication between FMS and an external database. The network ports over which Foglight components and protocols communicate are configurable.
Further Details:	Section(s) 3.6, 8, 3.9

Category:	System and Information Integrity (SI)
Applicable:	Yes
Description:	Foglight server and clients use the Java Cryptographic Extension library for its cryptographic operations. The Triple DES (Data Encryption Standard) algorithm in chain block cipher mode is used for encrypting FMS service account's passwords (e.g. 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.
Further Details:	Section(s) 3.7

ABOUT QUEST SOFTWARE, INC.

Now more than ever, organizations need to work smart and improve efficiency. Quest Software creates and supports smart systems management products—helping our customers solve everyday IT challenges faster and easier. Visit www.quest.com for more information.

Contacting Quest Software

Phone:	949.754.8000 (United States and Canada)
Email:	info@quest.com
Mail:	Quest Software, Inc. World Headquarters 5 Polaris Way Aliso Viejo, CA 92656 USA
Web site	www.quest.com

Please 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 commercial version and have a valid maintenance contract. Quest Support provides around the clock coverage with SupportLink, our web self-service. Visit SupportLink at http://support.quest.com

From SupportLink, you can do the following:

- Quickly find thousands of solutions (Knowledgebase articles/documents).
- Download patches and upgrades.
- Seek help from a Support engineer.
- Log and update your case, and check its status.

View the ***Global Support Guide*** for a detailed explanation of support programs, online services, contact information, and policy and procedures. The guide is available at: http://support.quest.com/pdfs/Global Support Guide.pdf