Quest™

Foglight® Experience Monitor 5.8.1

Security and Compliance Field 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 Experience Monitor Security and Compliance Field Guide
Updated - October 2017
Foglight Experience Monitor Version - 5.8.1

Contents

1

FxM security overview

Foglight® Experience Monitor is a comprehensive appliance-based solution that empowers organizations to effectively manage, troubleshoot, and optimize all components of the service delivery chain under their control. With our turn-key, self-contained computer system, customers gain unprecedented visibility into the inner workings of their network infrastructure and the quality of the end user's experience. The appliance provides concise, accurate information in real-time about component performance, systematic failures, and a wealth of other information.

This *Security and Compliance Field Guide* describes the security features provided by the FxM appliance. The document includes information about access control, data protection, secure network communication, data encryption, and auditing. It also includes an appendix describing how to evaluate the FxM security features in connection with the federal information security standards recommended by NIST (National Institute of Standards and Technology), and promulgated under the FISMA (Federal Information Security Management Act).

This document is intended for system administrators and other users concerned with the security features of the FxM appliance.

This section provides an overview of how FxM appliances manage information security.

FxM measures

Managing information security systems is a matter of great priority for every organization. The level of security provided by software vendors has become a significant factor in IT purchase decisions. Quest Software Inc. 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.

Foglight Experience Monitor is an appliance-based solution (a rack-mounted server with pre-installed software) that plugs into the customer's network and passively monitors TCP/IP, HTTP, HTTPS, and SOAP traffic. Users access FxM reports by connecting to the appliance through a web browser. The appliance's software is built on top of the SUSE Linux® Enterprise Server (SLES) operating system, and includes an Apache™ Web Server, as well as specialized Quest software. FxM connects to a network tap or the diagnostic (mirror or span) port of a switch or router, allowing it to examine the customer's network traffic of interest. It uses a separate control port for incoming connections. If the customer provides SSL-enabled services, then it has the option of installing its private SSL keys on the FxM appliance, which allows FxM to monitor SSL traffic as well.

Foglight Experience Monitor is placed behind the customer's firewall and connects to the spanning (or diagnostic) port.

Security was a design focus for FxM from the start, because it is assumed that the data it examines may be sensitive. FxM applies data encryption to a customer's sensitive data, such as its private SSL keys. It allows the customer to configure the type of data (packets) that should be monitored for the purpose of analyzing the customer's system performance.

FxM severely limits the number of ports through which its services communicate. It allows you to enable secure communication over SSL or SSH for the following types of connections: web console, probe to portal database communication, and remote terminal access.

NOTE: Remote MySQL® connections opened by users with Remote database access enabled are not secure.

Foglight Experience Monitor also runs a firewall, a port scan protector, and a restricted instance of the Apache™ Web Server to protect against hacker attacks and exploit attempts.

For detailed information about the security features provided by FxM, see FxM security features.

Customer measures

The FxM security features are only one part of a secure environment. The customer's operational and policy decisions have a great influence upon the overall level of security achieved. In particular, the customer is responsible for the physical security of the appliance and the security of the network from which the appliance is accessible. Customers should install security patches promptly. Administrators should choose strong passwords and change them regularly.

2

FxM security features

This section describes the security features provided by FxM:

- Multiple layers of defense
- User authentication and access control
- Restricted access to the appliance
- User data protection
- Product updates

Multiple layers of defense

FxM employs multiple layers of defense to protect itself against intrusions and hack attempts. These layers include:

- A built-in firewall (see Layer 1: Firewall).
- A port scan detection and blocking tool (see Layer 2: Port scan detection and blocking tool).
- A customized installation of a Linux® operating system, in which certain unused and vulnerable services have been removed (see Layer 3: Customized operating system distribution).
- A specially-configured Apache™ Web Server (see Layer 4: Apache Server configuration).

Layer 1: Firewall

Foglight Experience Monitor appliance is designed to be installed in network environments that have strong security measures in place, including the use of firewalls and intrusion detection systems. The deployment point for the FxM appliance in a network must be behind the firewall. More specifically, the FxM control port must be accessible only behind the firewall, while the FxM monitoring ports may be connected to a network tap or switch outside the firewall. The monitoring ports operate in promiscuous mode, and all traffic that comes across them is routed into the FxM traffic analysis engine, so there is no risk of attack through these ports.

FxM itself also incorporates a built-in firewall which provides additional security beyond what is provided by the network environment. This firewall was constructed using the firewall rule-set building utility Bastille-Linux® (for details, see http://bastille-linux.sourceforge.net/). The FxM firewall limits external access to the HTTP or HTTPS port, depending on how its Apache™ Web Server is configured.

If command-line access is needed for Quest technical support to run low-level diagnostic procedures, customers may optionally open the SSH port. Normally, you should keep the SSH port closed, since it should only be opened for remote diagnostic procedures. The MySQL® port may also be opened if remote database access is configured.

The firewall also includes typical checks for illegal addresses and limits ICMP usage. Opening and closing HTTPS, SSH, and MySQL® ports is the responsibility of the FxM administrators using the FxM web console.

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. FxM attempts to detect such scans by watching for 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 FxM system 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 have been taken:

- FxM bundles the 64-bit SUSE Linux® Enterprise Server 11 SP4 operating system.
- The latest security patches and upgrades are applied to every release of the FxM software distribution.
- Many tools and packages that represent common vulnerabilities are stripped out of the distribution. For example, *Telnet, FTP server, rlogin, NFS, Samba,* and *lpr* are not installed on the appliance.
- Access to potentially exploitable tools needed by FxM to operate (such as *ping* and *traceroute*) has been severely restricted.

  Foglight Experience Monitor requires the *ping* utility to verify network access during the appliance setup process. This is only available through the console program, whose access requires a different account, other than that used to access the web console.

  The *traceroute* utility is only used 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.
- FxM employs the use of shadow passwords, in order to make brute force password attacks harder to execute.
- All standard Linux® user accounts available on the appliance (that is, *shutdown, halt, mailnull*, etc.) have no login shell that would allow an attacker to enter shell commands. Only user accounts with “Terminal access enabled” have a login shell. The shell can only be accessed through the terminal or SSH. The password for a user account is specified by the FxM user, and must be a strong password in order to enable SSH access.

Layer 4: Apache Server configuration

The Apache™ Server that is included in FxM represents the single greatest point of vulnerability, since port 80 (or 443) is the only port that is normally open on the system. Therefore, the configuration of the Apache Server included in the appliance has been “locked-down” so that it is less vulnerable than the standard Apache installation.

Many Apache exploits typically attack vulnerabilities that are exposed due to the improper configuration of the Apache Server itself. Many of the Apache capabilities that are commonly exploited are disabled in the configuration of the FxM Apache Server. For example, CGI scripts are a notorious source of vulnerabilities in Apache. FxM does not employ CGI scripts and the handler for CGI scripts is removed from the Apache configuration file, so they cannot be executed.

The Apache processes on the FxM appliance run in a user account that has limited rights. This account has no login shell and can only access a restricted set of directories. If a buffer overflow exploit were to be successful against the FxM’s Apache Server, the hacker would not easily be able to modify or read system files, since the user account in which Apache runs has no rights to access those areas of the system.

User authentication and access control

FxM 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.

This section presents the mechanisms used to authenticate FxM users (see FxM user authentication) and Foglight Experience Monitor users drilling down in to the FxM appliance (see Foglight user authentication). It also presents the privileges associated with different types of user accounts (see User authorization and privileges), and provides information about strong passwords (see Strong passwords).

FxM user authentication

At the present time, FxM does not utilize any external mechanisms for identity management. User accounts that allow access to FxM's web console are defined through the user interface (UI) by FxM administrators. Administrators may configure the system to require strong passwords for these user accounts.

For an additional level of security in this regard, the Apache™ Server on the appliance can be configured to use Secure Socket Layer (SSL). FxM utilizes the Linux® Pluggable Authentication Modules (PAM) as the underlying authentication mechanism for all types of user access to the system (web console, SSH, database, and terminal). Account passwords are stored in encrypted form, in Linux system files.

Foglight user authentication

Foglight Management Server (FMS) allows users to navigate from displays within its browser interface into the FxM web console. If the Foglight user account matches an account name in FxM, the user is automatically authenticated and does not have to login a second time in FxM.

This is accomplished by passing a unique token specific to the user account and the time of day in the URL that is used to access the FxM web console. FxM receives the token and issues a SOAP request to the Foglight Management Server to authenticate the token. If successful, that request returns the name of the user account that the Foglight user was logged into. FxM then attempts to automatically log the user into the web console, using that account name. If the user account is not found, the user is redirected to the FxM login page. If the account is found, the user will see the intended page of the FxM web console.

User authorization and privileges

FxM enforces access control by providing distinct groups of user accounts that are determined by their type (*administrative*, *power user*, *secured power user, general*, and *guest*). Each group has a different set of permissions associated with their accounts, thereby controlling what actions users can perform and what data they have access to. For detailed information about managing user accounts, see section "User accounts" in the *Foglight Experience Monitor Installation and Administration Guide*.

In addition, FxM processes run in user accounts with limited rights. For example, the Apache™ Web Server runs as a user which does not have read or write access to system files. This adds an additional layer of security in the scenario that an attacker somehow manages to execute commands through Apache.

The following table presents the role-based access control in Foglight Experience Monitor.

Table 1. FxM access control

Task	Administrative	Power User	Secured Power User	General	Guest
Enable and disable security configurations (SSH access, Apache™ SSL mode, and Remote Database access)	Yes	No	No	No	No
Configure backup scheduling and creation	Yes	No	No	No	No
Update the appliance software	Yes	No	No	No	No
Examine system logs	Yes	No	No	No	No
Create, edit, and delete user accounts	Yes	No	No	No	No
Auto-discover session identifiers, login variables, and variable rules	Yes	Yes	No	No	No
Configure parameters that affect monitoring of individual user sessions	Yes	Yes	Yes	No	No
Configure parameters that affect monitoring of servers	Yes	Yes	Yes	No	No
Upload and delete SSL keys for monitored servers	Yes	Yes	Yes	No	No
Create, distribute, and withdraw report sets	Yes	Yes	Yes	No	No
Configure alarms	Yes	Yes	Yes	Yes	No
Customize report sets	Yes	Yes	Yes	Yes	No
View metrics, resources, and alarm definitions	Yes	Yes	Yes	Yes	Yes
View report sets	Yes	Yes	Yes	Yes	Yes

Each user account also has an additional setting that determines whether that user can examine metrics in FxM, metrics that may contain personal information of end users accessing the servers that FxM is monitoring. This may include information such as IP address, login name, ISP, and geographic location.

Strong passwords

FxM requires the use of strong passwords for accounts that have SSH access enabled at all times. In addition, the administrator may configure the system so that strong passwords are required for all accounts, regardless of the type of access enabled for the account.

The FxM console program is available via a terminal that is connected to the appliance's VGA connector. Using the terminal and a keyboard that is also connected to a USB port on the appliance, administrators perform initial setup and configuration tasks with the appliance (such as supplying it with an IP address). The Linux® user account *setup* must be used to login to the appliance through the terminal to access the FxM console program. The password for the *setup* account is configurable. It is recommended that customers assign a strong password for this account.

For detailed information about strong passwords, see section "Configuring strong passwords" in the *Foglight Experience Monitor Installation and Administration Guide*.

Restricted access to the appliance

This section contains the following topics:

- FxM access ports

- Secure network communication
- Data encryption
- Configuration parameters and files
- Defense against denial-of-service attacks
- Defense against web console exploits
- Auditing
- IPv6
- 508 compliance

FxM access ports

The configuration of FxM, coupled with its firewall, severely restricts the ports through which it can be accessed. The following table summarizes the ports that are open by default, the ports that may be opened by FxM administrators through the FxM web console, and the ports that may be open when configuring FxM in a multiple-appliance cluster. These ports are accessible through FxM's control port.

NOTE: In this table, "Portal" refers to the appliance that serves as the master database for an installed cluster of FxM appliances. Portals are used to generate reports and to maintain a repository that contains all metrics collected by all monitoring appliances in the cluster. Monitoring appliances are referred to as "Probes". Probes are also equipped with a full database and reporting user interface, but the metrics displayed are only those captured by that probe.

Table 2. FxM access ports

Port	Service	Protocol	Open	Type	Direction
80	HTTP	TCP	By default	Unidirectional	Inbound
443	HTTPS	TCP	Optional: SSL support	Unidirectional	Inbound
22	SSH	TCP	Optional: SSH support is activated	Unidirectional	Inbound
25	SMTP	TCP	Optional: Simple Mail Transport	Unidirectional	Outbound
21	FTP	TCP	Optional: FxM outbound FTP for backup	Unidirectional	Outbound
123	NTP	UDP	Optional: Network Time Protocol	Unidirectional	Outbound
162	SNMPTRAP	UDP	Optional: Simple Network Management Protocol	Unidirectional	Outbound
3306	MSQL	TCP	Optional: Foglight interface and remote database access	Unidirectional	Inbound
5000	-	Custom Protocol[1]	Multi-Appliance: default data port (configurable; between Probe and Portal only)	Unidirectional	Probe to Portal
3306	MSQL	TCP	Multi-Appliance: default control port (configurable; between Probe and Portal only)	Unidirectional	Probe to Portal
8080	HTTP	TCP	Optional: for authenticating Foglight users with FMS (port is configurable in FMS and FxM)	Unidirectional	Outbound
80	HTTP	TCP	Optional: for communication with FxV (port is configurable in FxV and FxM)	Unidirectional	Outbound

1.This is a proprietary protocol used for communication between FxM appliances.

In a stand-alone appliance setup, the Apache™ Web Server on the appliance uses port 80 (the only port open by default). Customers can configure the web server for SSL mode, if necessary. In that case, port 443 is opened and port 80 is closed.

If a remote troubleshooting session is required, customers can enable SSH access to the appliance for one or more users, in which case port 22 is opened. It it recommended to disable the SSH access immediately after troubleshooting the issue.

If time synchronization with a time server via NTP is enabled, then UDP port 123 is opened.

In addition, the FxM's port scanner listens to inactive ports that are typically assigned to popular services, such as *FTP*, *Telnet*, *POP3*, etc. The following TCP ports are left open in order to detect port-scanning programs: 1, 11, 110, and 143. If the scanner detects that a machine is probing these ports, it automatically enters the machine's IP address into its firewall filter and denies future access to FxM from that IP address.

Secure network communication

The FxM web server supports the use of the SSL protocol. This allows users to connect to FxM securely via the Internet and through the customer's Intranet. In addition, FxM supports the use of SSH (Secure Shell) when command-line access is needed for Quest technical support to run low-level diagnostic procedures.

FxM supports multi-appliance use, whereby one appliance is defined to be the "portal" while the others are "probes". The appliances communicate via a custom built TCP protocol over custom ports. The default data port is 5000 and the default control port is 3306. Probe appliances periodically send their collected analysis data to the portal appliance, which in turn acts as a central repository for all monitored data. The appliances can be configured to inter-communicate via SSL, whereby data sent over port 5000 gets encrypted with AES-256. When the optional use of SSL is not chosen, data is passed in the clear between the distributed monitors and the portal appliance. There is currently no mutual authentication between the appliances.

Data encryption

FxM uses the AES-256 data encryption algorithm to encrypt the customer's private SSL keys. AES-256 is a symmetric key stream cipher that is widely used throughout industry. FxM's 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.

Configuration parameters and files

FxM stores its configuration parameters in the MySQL® database. Write access to this database is restricted to FxM administrators, who in turn need to authenticate themselves with their usernames and passwords. Read access to this database is restricted to FxM users with "Remote database access" enabled. In addition, FxM logs any changes made to its configuration, and provides an audit trail of events.

Defense against denial-of-service attacks

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

For detailed information about the FxM appliance log repositories, see section "Using the appliance support tools" in the *Foglight Experience Monitor Installation and Administration Guide*.

Defense against web console exploits

FxM validates user input in its web interfaces and on its back-end to prevent cross-site scripting and other types of attacks. Vulnerability tools are run against the appliance for every major release and corrective action is taken when necessary.

In particular, FxM implements the following strategies to guard against attacks:

- Cryptographic nonces are implemented on all forms as an authentication mechanism to prevent replay and Cross-Site Request Forgery (CSRF) attacks.
- Parameters to web console pages are strictly checked for valid characters using a whitelist approach where possible.
- Textual user input is filtered to remove possibly malicious code that could enable Cross-Site Scripting (XSS) attacks.
- All web pages have authorization checking to ensure that only users with the correct privileges are allowed access.
- File uploads are strictly validated before being used to prevent Local File Include (LFI) and Directory Traversal attacks.
- In lockdown mode, FxM prevents assignment of system access privileges through the web console. For more information about lockdown mode, see “Increasing security for user account management and access privileges” in the *Foglight Experience Monitor Installation and Administration Guide*.

Auditing

Aside from logging all information required to analyze system performance, FxM also records data in order to aid with system recovery and events related to potential attackers probing for system access. Any changes to the system’s configuration are placed in the log file, creating a trail of events that can be inspected in case FxM becomes unstable (for example, due to a mis-configuration). In addition, if FxM detects a potential attacker scanning for open communication ports, it creates a log entry and blocks future access to FxM from the attacker’s IP address.

For detailed information about the FxM appliance log repositories, see section “Using the appliance support tools” in the *Foglight Experience Monitor Installation and Administration Guide*.

IPv6

Foglight Experience Monitor does not currently support IPv6. This functionality is planned for future releases.

508 compliance

The FxM’s web interface is Section 508-compliant. For details about how to enable this feature, see section “User account management” in the *Foglight Experience Monitor Installation and Administration Guide*.

Section 508 was enacted to eliminate barriers in information technology, to make available new opportunities for people with disabilities, and to encourage development of technologies that help achieve these goals. The law applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology. Under Section 508 (29 U.S.C. ‘794d), agencies must give to disabled employees and members of the public access to information that is comparable to the access available to others. It is recommended that you review the laws and regulations listed below to further your understanding about Section 508 and how you can support implementation. You can view web-based Intranet and Internet Information and Applications under section 1194.22.

User data protection

This section contains the following topics:

Protection of customer’s data

FxM has no intrinsic knowledge of the applications that it monitors. The system analyzes network packets on the fly, and then discards them.

NOTE: Packets are not discarded if FxM is integrated with Foglight Experience Viewer. For more information, see Foglight Experience Viewer integration.

The network packets are never saved to the storage device in the system. FxM does store information about HTTP requests, including URLs, timing information, and customer defined variables. If configured to do so, FxM can retain the login names for customers’ applications, but not the passwords. This is done by identifying the “login variable” names and by recording these variables, which are usually transmitted in a query, form (or POST, GET), or cookie variable specific to the application. When enabled, this feature allows examination of metrics for individual user sessions identified by the specified login variables. All of FxM’s collected metrics are retained in a secure database that can only be accessed with an authorized login name and password. These metrics may contain sensitive data and should be handled accordingly. For more details, see section “Identifying user sessions” in the *Foglight Experience Monitor Installation and Administration Guide*.

Secure use of customer’s private keys

In addition to monitoring regular HTTP traffic, FxM also provides the option of monitoring Secure Socket Layer traffic (SSL/TLS). To enable the option of monitoring SSL traffic, customers need to upload their private SSL encryption keys to FxM via the web console. These keys are naturally of high sensitivity to customers, so FxM stores the keys in a local file with restricted access and encrypts the file using the AES-256 data encryption algorithm.

FxM can also use private keys stored in a SafeNet Hardware Security Modules (HSMs) server to decrypt secure traffic. FxM 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 the FxM appliance with the HSM server.
- FxM communicates with SafeNet HSM servers using the recommended PKCS #11 API.
- FxM never stores SafeNet private keys on disk and never exposes them in any interface.

SQL database access

All metrics in FxM are stored in databases using MySQL®. These metrics can be accessed externally using a tool like Toad® for MySQL. By default, remote database access is disabled when creating a new user, but the administrator can configure FxM to open up this access. This account cannot make any changes to the databases and has only the following privileges in MySQL:

- SELECT
- SHOW DATABASES

- SHOW TABLES

When remote access is enabled for one or more users, port 3306 is opened in the appliance's firewall.

Foglight Experience Viewer integration

FxM can be integrated with the Foglight Experience Viewer (FxV) appliance. For detailed information about FxM-FxV integration, see section "Connecting to the Foglight Experience Viewer" in the *Foglight Experience Monitor Installation and Administration Guide*.

FxV can capture, store, and play back the entire session for every user, providing monitoring, alerts on content, statistics for known problem outcomes, and robust search functionality for newly discovered problems. Sessions can be replayed as the user experienced them through the same browser software, or displayed as the original HTML code delivered by the system.

The combination of FxM and FxV results in more user data being captured and stored (on the FxV appliance) than described in section Protection of customer's data. For detailed information about the security features provided by the FxV appliance, see the *FxV Security and Compliance Field Guide*.

Product updates

This section contains the following topics:

- Installation of FxM patches
- Monitoring of embedded third party components
- Operating system security updates

Installation of FxM patches

FxM patches can be installed by uploading the patch file(s) from the FxM web console (click **Help > Upgrade**). For detailed installation instructions, see section "Updating the appliance" in the *Foglight Experience Monitor Installation and Administration Guide*.

Monitoring of embedded third party components

Quest Software Inc. monitors vulnerability reports produced by the United States Computer Emergency Readiness Team (US-CERT) to determine whether security flaws are discovered in third party components used by Foglight Experience Monitor. Depending upon the severity of such published vulnerabilities (as published by US-CERT), the FxM team takes specific actions, as specified in the following table.

Table 3. Monitoring vulnerabilities

Vulnerability Severity Level	Action Taken
High	Start investigation within five business days of the date that Quest becomes aware of the vulnerability and use all reasonable efforts to release a product update as soon as possible.

Table 3. Monitoring vulnerabilities

Vulnerability Severity Level	Action Taken
Moderate	Start investigation within three weeks of the date that Quest becomes aware of the vulnerability and use all reasonable efforts to include patches in either a minor version release or in the next major version release, depending on the impact of the vulnerability in the product.
Low	Start investigation within two months of the date that Quest becomes aware of the vulnerability and use all reasonable efforts to include patches in the next major version release.

During the investigation phase, Quest product teams determine whether the published vulnerability affects their products. Quest then releases product updates, as necessary.

Operating system security updates

As described earlier, the FxM appliance ships with the SUSE Enterprise Linux® (SLES) distribution installed. Many OS components that FxM uses are obtained directly from the SLES distribution. Others, however, are built from source and then incorporated into the FxM distribution. The following sections (SLES components and Non-SLES components) describe how security updates are handled for each type of component.

SLES components

SLES commonly ships with versions of RPMs for OS components that are older than the most currently released version. Novell® backports all relevant security fixes and patches to the older versions of these components so that they have the same level of security as the latest version. Every release of FxM applies all the latest security patches released by Novell for these components. Both Novell and RedHat follow this procedure to maintain backward compatibility and avoid introducing unforeseen problems due to changed behavior in components that their customer's applications may be relying upon. In this way, any new features implemented in newer versions do not break existing installations. Vulnerability scanning tools (for example, Nessus) report the currently installed version number of components (for example, OpenSSH) and flag them as vulnerable based upon the reporting of known vulnerabilities for those versions. These tools, however, do not have the ability to determine whether fixes for these vulnerabilities have been retrofitted into these older versions. Consequently, these alarms are typically "false positives" and do not represent true vulnerabilities.

Non-SLES components

FxM does not rely on SLES distributions for every OS component. Apache™, PHP, MySQL®, and OpenSSL are all built separately based on source obtained from sites that host these open source projects. For every major release, the FxM development team obtains the latest source, builds these projects, and incorporates the binaries into its distribution. Typically, the FxM distribution for each release contains the latest version of these components. After an FxM release is issued there are invariably vulnerabilities reported for these components. The FxM team monitors these vulnerabilities and typically issues a special one-time patch to address them, if it is determined that the issue represents a security risk for an FxM appliance. It is often the case that these vulnerabilities do not represent a security risk for FxM since many of the features in components like Apache and PHP that are commonly exploited are turned off in the FxM distribution.

A

Appendix: FxM and FISMA compliance

This section describes how to evaluate the FxM security features in connection with the federal information security standards recommended by NIST (National Institute of Standards and Technology) and promulgated under the FISMA (Federal Information Security Management Act):

- FISMA overview
- NIST 800-53 categories

FISMA overview

The *Federal Information Security Management Act (FISMA)* was passed by the U.S. Congress and signed by the U.S. President, and is 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”.

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 publication, see http://csrc.nist.gov/publications/PubsSPs.html). This document lists 17 general security categories against which an information security control program should be evaluated, so as to measure its level of compliance with an agency’s obligations under FISMA. Quest Software Inc. wishes to provide its customers with enough information regarding security aspects of Foglight Experience Monitor to enable them to perform their own evaluation of how FxM fits in with their desired FISMA compliance levels. For more information, see NIST 800-53 categories.

NIST 800-53 categories

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

The secure employment of Foglight Experience Monitor forms only one part of an information security program. A statement in this appendix that a particular security category is “applicable” to Foglight Experience Monitor means only that FxM 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 Experience Monitor fully meets all of the requirements described in that security category, or that the use of Foglight Experience Monitor 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 the Foglight Experience Monitor.

The following table presents the NIST *800-53* categories and describes how Foglight Experience Monitor addresses those that apply.

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 4. NIST 800-53 categories

Category	Applicable	Description	Additional Details
Access Control (AC)	Yes	FxM enforces a role-based access control policy, based upon types of user accounts (administrative and regular users). This enforcement restricts what data can be accessed and which actions can be performed, as well as a separation of duties.	User authorization and privileges
Awareness and Training (AT)	No	This category does not apply to FxM, as it is the responsibility of the FxM customers to develop and review their own security awareness and training policy.	N/A
Audit and Accountability (AU)	Yes	FxM records a set of events in its audit file. This includes logging all changes to its configuration and any attempt at sniffing for open ports by an attacker.	Auditing
Certification, Accreditation, and Assessments (CA)	No	This category does not apply to FxM, as it is the responsibility of the FxM customers to develop and review their own security assessment, accreditation, and certification policy.	N/A
Configuration Management (CM)	Yes	The FxM appliance is configured to only provide services necessary for its operation, and makes unavailable the services that are not necessary. The ports that FxM uses for communication are restricted and configurable only by administrators. In addition, any changes to the FxM configuration are recorded in a log file.	• Layer 2: Port scan detection and blocking tool • Layer 3: Customized operating system distribution • Layer 4: Apache Server configuration • User authorization and privileges • FxM access ports • Auditing
Contingency Planning (CP)	No	This category does not apply to FxM, since it is the responsibility of the FxM 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. They can be caused by natural disasters or terrorist actions.	N/A
Identification and Authentication (IA)	Yes	FxM 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.	User authentication and access control

Table 4. NIST 800-53 categories

Category	Applicable	Description	Additional Details
Incident Response (IR)	No	This category does not apply to FxM, since it is the responsibility of the FxM customers to develop and review their own incident response policy and procedures.	N/A
Maintenance (MA)	Yes	FxM allows for remote maintenance by Quest technical support in agreement with the customer. FxM also monitors developments and newly discovered security flaws in the systems on which it is based (such as, Fedora, SLES, Apache™), and provides security patches to its customers, when necessary.	Product updates
Media Protection (MP)	No	This category does not apply to FxM, since it is the responsibility of the FxM customers to develop and review their own media protection policy.	N/A
Physical and Environmental Protection (PE)	No	This category does not apply to FxM, since it is the responsibility of the FxM customers to develop and review their own physical and environmental policy.	N/A
Planning (PL)	No	This category does not apply to FxM, since it is the responsibility of the FxM customers to develop and review their own security planning policy.	N/A
Personnel Security (PS)	No	This category does not apply to FxM, since it is the responsibility of the FxM customers to enforce its personnel security policies, including personnel screening and employment termination.	N/A
Risk Assessment (RA)	No	This category does not apply to FxM, since it is the responsibility of the FxM customers to develop and review their own risk assessment policy.	N/A
System and Services Acquisition (SA)	No	This category does not apply to FxM, since it is the responsibility of the FxM customers to develop and review their own system and services acquisition policy.	N/A

Table 4. NIST 800-53 categories

Category	Applicable	Description	Additional Details
System and Communications Protection (SC)	Yes	FxM protects customer's sensitive data through the use of data encryption, using the AES-256 data encryption algorithm. To secure network communication with its users, the FxM web server supports the use of SSL. To support secure communication with Quest technical support, FxM allows for the establishment of SSH connections. FxM's encryption key is protected from unauthorized access. In addition, FxM provides for protection against DoS attacks through the use of a firewall and continuously monitors for potential attackers through a port scanner.	• Data encryption • Secure network communication • FxM access ports
System and Information Integrity (SI)	Yes	FxM uses a firewall and a port scanner as intrusion detection tools. FxM also verifies input given by users when they interact with the web interface, in order to protect against faulty user input. Any changes made to FxM's configuration are also recorded, in order to allow the system to roll back to a stable state, in case it gets corrupted. FxM does not currently verify the correct operation of security functions. This feature is scheduled to be included in future releases.	• Layer 1: Firewall • Layer 2: Port scan detection and blocking tool • Defense against web console exploits • Configuration parameters and files • Auditing

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 www.quest.com/contact.

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.