Quest®

Stat®

Security Guide

Legend

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

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

Stat® -Security Guide
Updated – November 25, 2019
Version - 6.x

Contents

1

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.

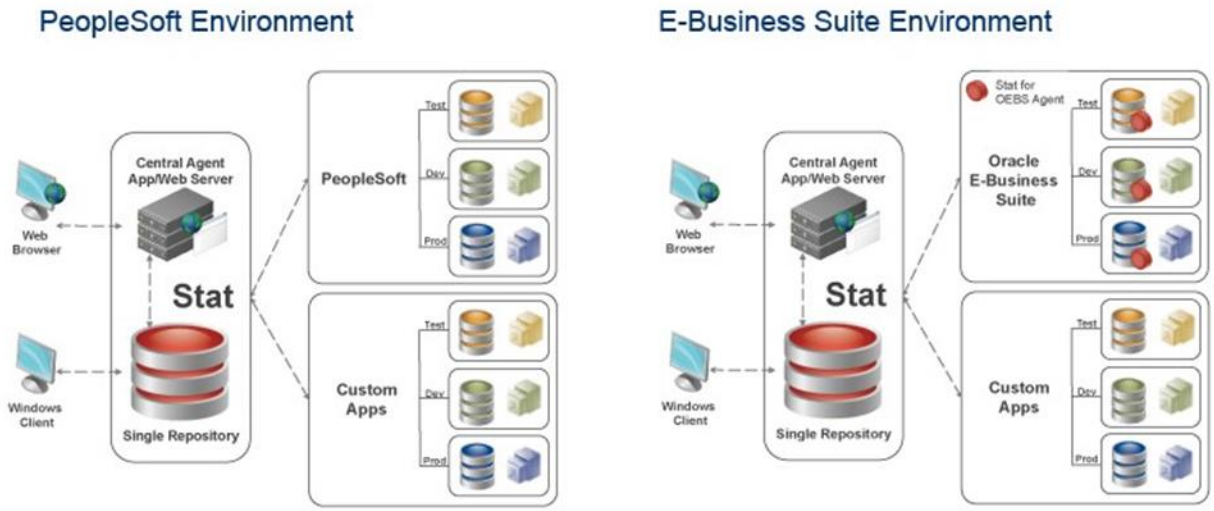
This document describes the security features of Quest's Stat. It reviews access control, customer data protection, secure network communication, and more. There is also an appendix that describes how Stat security features meet the NIST recommended federal information security standards as detailed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

2

About Stat

Stat is based on a four-tier architectural model consisting of a client tier, a web tier, a business logic tier, and a database tier. The components within each tier work together to provide a complete change management solution for PeopleSoft and Oracle Applications, as well as other application environments. Figure 1 gives an overview of the Stat architecture.

Figure 1: Stat Architecture



Client Tier

Users interact directly with Stat through the client application installed on their Windows-based workstation. They interact with Stat Web through a browser window. The Stat Windows Client can be installed either locally or on a network. It connects with the Stat Repository through various native environment interfaces.

Web Tier and Business Logic Tier

The Stat Central Agent is a web-based application that occupies the Web Tier and the Business Logic Tier. It comprises the web Container and EJB3 (Enterprise Java Bean) Container.

The Stat Central Agent interacts directly with the Stat Repository and the application environments to automate such tasks as generating and printing reports, sending e-mail messages, archiving objects, and maintaining database parameters.

Database Tier

The Stat Repository contains activity data and configuration information for the Stat Windows client and the Stat Central Agent. The database engine or Database Management System (DBMS) is not a component provided by Stat.

Application Environments

Stat provides version control and change management support for PeopleSoft, Oracle E_Business Suite, and other (generic) application environments.

The Stat Agent for Oracle E-Business is a background daemon that runs on each Oracle E-Business server. It receives requests from the Stat Central Agent, processes the requests, and sends resulting information back to the Stat Central Agent.

Security Features in Stat

The following sections describe security aspects of Stat.

Security Layers

Stat has a two-layered security system. At the first layer, login protocols control access to the Stat Repository, and at the second layer, a set of internal security measures controls access to sensitive areas within the repository data- base.

Internal security is based on service domains and user classes. User classes are logical groupings of access rights which are assigned to users according to their functional needs. These rights can include everything from working within different service domains to adding and editing activity codes. User classes effectively maintain security within Stat by limiting users' access to only the data and functions that pertain to them.

Login Security

Whenever a user attempts to login to Stat via the Windows Client , two security checks, or "passes," are made against the Stat Repository before the user's login ID and password are validated. As described below, a total of three validations are performed before a user is granted access to the system. This process is as follows:

1. In the Stat Login window, the user selects a database and enters his or her login ID (username) and password.
2. Stat connects to the selected database using the login ID specified in the Stat.ini file (by default, "STATLOGIN") and an encrypted password.
3. The STATLOGIN ID accesses the Stat_Login table. It cannot access any other table. This is the first pass.
4. From the Stat_Login table, the schema owner's login ID and password are selected. The login ID and password are stored encrypted in the table.
5. The STATLOGIN ID disconnects from the database.
6. Stat re-connects to the database using the schema owner's login ID and password obtained during the first login.

   This is the second pass.
7. Stat then checks the user table to validate that the user's login ID is in the table. This is the global application validation.

If the user’s login ID is valid, the appropriate security is put in place and Stat is loaded with all the internal security measures defined for the user in place. The user never actually logs into the Stat Repository using his or her login ID. First the STATLOGIN ID is used, then the schema owner’s ID from the Stat_Login table. Stat user IDs are used to identify the functions that users can and cannot perform once they are logged in.

A user’s ID is disabled when someone attempts to log in with the ID and incorrect password a predefined number of times. The password must be reset by a system administrator before the user can login again. All successful and unsuccessful login attempts are recorded by Stat.

Role Based Access Control

Internal Stat security is based on service domains and user classes. User classes are collections of access rights that control a user's ability to view information and perform functions within service domains. To operate within a service domain, a user must be assigned to at least one user class that is associated with that service domain. For example, the table below illustrates the security rights assigned to a user based on hypothetical service domains and user classes. The user has access to the Change Control and Information Systems service domains, but not the

Human Resources service domain.

Service Domain	Access	Default	User Class
Change Control	Yes	Yes	Developer
Change Control	Yes	No	Migrator
Information Systems	Yes	No	Staff
Information Systems	Yes	No	Projects
Human Resources	No	No	N/A

In this example, the user is assigned to the Developer and Migrator user classes in the Change Control service domain. The Developer user class lets the user edit and create Change/Service Requests (CSRs), lock objects, and create archive sets, whereas the Migrator user class lets the user migrate archive sets. However, neither user class lets the user edit maintenance tables or add new users. In the Information Systems service domain, the user also has the combined rights of two user classes: Staff and Project. The Staff user class only lets users create new CSRs and view existing CSRs, whereas the Project user class lets the user create and edit projects. Lastly, in the Human Resources service domain, the user is not assigned to a user class and has no access whatsoever.

The indication of default in the Change Control domain means that when Stat prompts the user to select a service domain - for example, when opening a new CSR - the default choice is Change Control.

Defining User Classes

One of the first tasks in a Stat implementation is to define user classes. User classes are logical groupings of security rights based on the functional roles of users. For example, Stat system administrators would typically

belong to a user class that allows them to define and edit service domains, whereas most other Stat users would not belong to that class.

Stat gives you the flexibility to define as many user classes as you need. As a general rule, it is a good idea to start off with a few user classes and add more as necessary. User classes correspond to business or functional roles within an enterprise, such as Administrators and Developers. Users that fulfill multiple roles can be granted membership in multiple user classes, each corresponding to a different function. A user's rights is the summation of the rights in all the user classes to which that user belongs.

User class security is controlled by the following user class rights:

- User Classes – Add
- User Classes – Edit

The user class table is displayed in a standard maintenance window called User Class Maintenance. To open this window, select **Maintenance | Security Settings | User Classes**. The table below describes the fields in the User

Class Maintenance window.

Values	Description
Active	If selected, activates the value in Stat
User Class Code (Key Value)	A 1-10 alpha character code uniquely identifying the user class
Description (Required Value)	A 1-35 character description of the user class
Last Update (Read Only)	The date and time that this record was last updated
Updated By (Read Only)	The user that last updated this record

Defining Stat Users

Before users can work in Stat, they must be defined in the User Maintenance table. This table contains all the information about the user that Stat requires. Users are initially defined as either Technical or Functional users. Technical users can be assigned rights to access and perform Change Management activities. Functional users cannot be granted these rights.

User account security is controlled by the following user class rights:

- Stat Users– Add
- Stat Users – Edit

You can grant users the right to reset the passwords of other Stat users by assigning the right, Stat Users – Reset Password, to one of the user classes to which they belong. It is not necessary that you also grant them adding or editing rights. In this case, users can reset passwords by selecting **User Options | Passwords | Administer Passwords**.

When user's password is reset, an email is sent to their defined email address with a temporary password. User will have to login with their temporary password and create a new password.

Stat supports the use of LDAP and secure LDAP (LDAPS) for authentication of external users. If LDAP is enabled by the customer, it is important to note that each Stat user still needs to have a user account

created in the User Maintenance table, such that the user's class rights can be specified. Stat supports mixed environments that include both users signing in via LDAP and users signing in with Stat defined passwords.

Stat comes with a default Admin user account whose username is 'SYSTEM and password is 'system'. The customer is recommended to change the account's password upon the completion of the Stat install.

Editing User Class Rights

You can edit the security rights of a selected user class by clicking Edit Rights... in the User Class Maintenance window. Stat then displays the Select User Class Rights window, as shown in Figure 2 below.

The Select User Class Rights window displays a list of all the rights that can be assigned to a user class. Rights currently assigned to the selected user class are designated by a checkmark in the box to the left of the class right name. If you want to filter the list, click in the Rights Group field and select a different group of rights; for example, Maintenance - General.

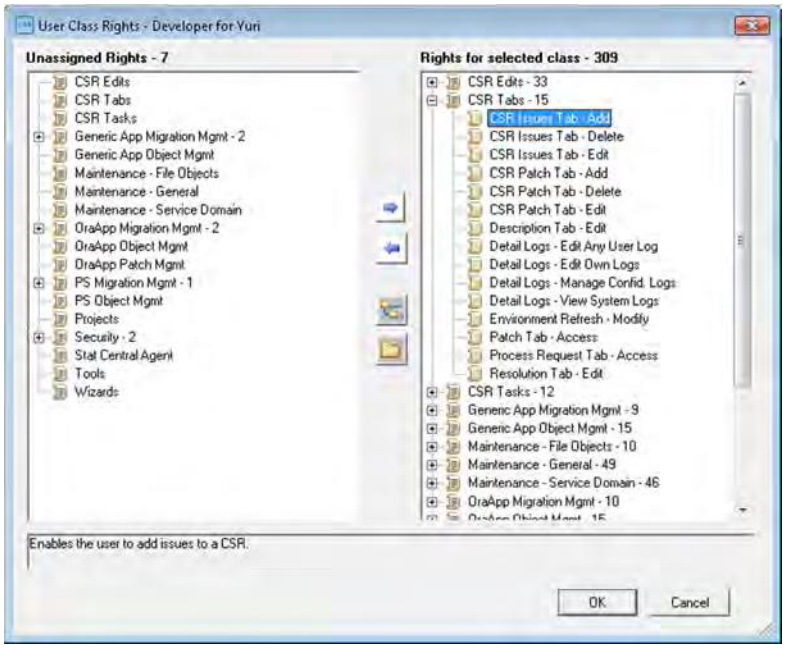
Some user class rights are specific to service domains. Users that belong to a user class with service domain-specific rights (for example, the right to migrate archive sets) can invoke these rights only within the service domains that the user class is associated with. Rights that are not service domain-specific, however, can be used in any service domain that the user is allowed to work in by belonging to an associated user class.

For example, the user class right, Undocumented Patch Wizard - Run, is not service domain-specific. This means that users that have this right in one service domain can run the wizard in all the service domains that they can access, including those in which the right is not given.

To grant the user class a right, select its corresponding checkbox. To revoke a right, deselect the checkbox. In general, if a user class has an Add right, this overrides the absence of an Edit right. For example, if a user class has the right, **Activity Codes - Add**, the user class also has the right to edit existing records, even if the class has not been granted the right, **Activity Codes - Edit**.

Note that descriptions of the particular rights can be found in the lower portion of the Edit User Class Rights window.

Figure 2: Edit User Class Rights



Permissions to View Reports

A permission control separate from User Classes is used to restrict the ability for users to view reports generated by Stat. Each report is assigned a security level from 1 to 99, where 99 is the most restrictive. The security level (number) associated with a Stat user determines whether or not the user can view a report.

User Password Security Settings

Stat allows for customization of the password policy which dictates how passwords of internal users may be constructed. Below we describe the various password policy options that can be set by an administrator.

User Password Security Settings

In the User Password Options section of the System table, you can define password parameters for all Stat users. To open the System table, select **Maintenance | General | System Table**. These password security settings do not apply to LDAP account passwords.

Figure 3: User Password Options

Below follows a description of the configurable user password options fields.

Values	Description
Password Lifetime (Required Value)	The number of days that a user's password is valid before they are required to change it. This setting has no effect if the Password Expire field is not checked. Valid values are 0 to 999.
Password History Lifetime (Required Value)	The number of days Stat retains users' password history. This value is used with the Limit Lifetime setting to prevent users from re-using the same password within the number of days indicated in this field. A setting of 0 means that no history is maintained. This setting has no effect if the Limit Lifetime field is not checked.

Expire	Indicates whether users' passwords expire after the number of days defined in the Password Lifetime field. If selected, users are prompted to change their passwords at login once they have expired. If blank, passwords never expire.
Limit Lifetime	Indicates whether users can use the same password indefinitely.
Minimum Length	The minimum number of characters required in a user account password.
Max Failed Login	The maximum number of failed login attempts before a user account is locked out of Stat.
Set Mandatory Characters	Enables the mandatory character fields for passwords. If this checkbox is selected, the settings for Upper Number, Lower, and Spec. Char. fields are active.
Upper	Indicates if users must have at least one upper -case character in their password. This setting has no effect if the Stat Mandatory Characters checkbox is not selected.
Lower	Indicates if users are required to have at least one lower-case character in their password. This setting has no effect if the Stat Mandatory Characters checkbox is not selected.
Number	Indicates if users must have at least one number in their password. This setting has no effect if the Stat Mandatory Characters checkbox is deselected.
Characters	} | { ` _ ^ }] \[ @ ? > = < ; : / . - , + * ) ( ` & % $ # ! "

Connection Manager and History

The maximum number of users who can connect to Stat equals the number of licensed seats. If the maximum number of licensed seats is reached, new connections are denied. The Connection Manager window displays a list of all the users currently connected to Stat as well as a record of denied and terminated connections. From this window you can manually disconnect users from the Stat Repository, thereby opening seats and allowing other users to connect.

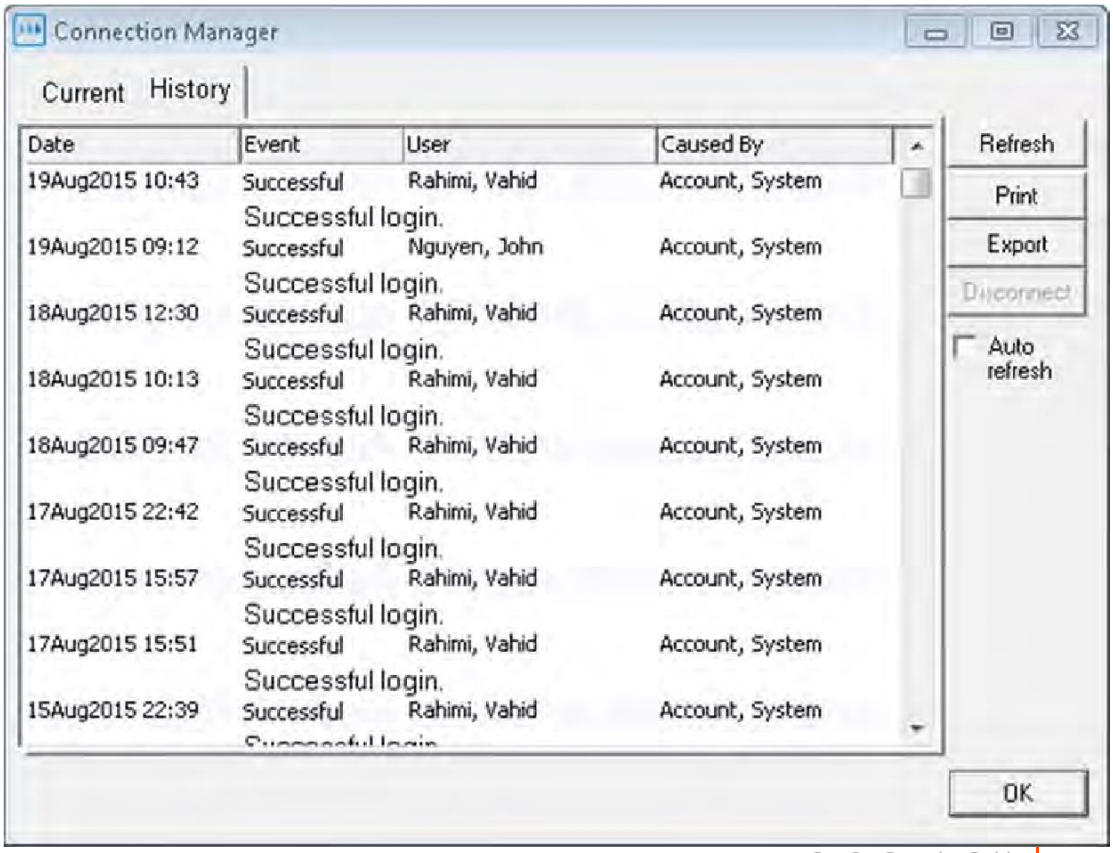
Connection History

The Connection History tab displays a record of connection denials and terminations. It includes successful and unsuccessful login attempts.

The History tab contains the following fields (columns):

Values	Description
Date	The date of the termination or denial event
Event	The type of disconnection. There are two events: "Terminated" which means that the disconnection was manually triggered and "No Licenses" which means that the System denied connection to the user(s) because the number of licensed seats has been met.
User	The name of the user for whom the connection was denied or terminated
Caused By	The event, it defaults to “Account, System.”

Figure 4: Connection Manager - History Tab



Audit Logs

In addition to the Connection History, Stat records the following log files: agent log, server log, archive log, and migration log. Sensitive information stored in the server and agent logs are only displayed in DEBUG mode. Debug can only be enabled at workstations designated as having access to the Stat-config window of the web client. The user opens Stat-config and sets either the user interface or server log to DEBUG. These logs are intended for use by administrators and database administrators. The archive and migration logs do not display sensitive information, and are intended for developers and users. Server and agent logs are stored in folders that should be secured by the customer. The log folder locations can be defined to be something other than the Stat default locations. Archive logs are stored in the database and are made visible in the Change/Service Request (CSR) view. CSR viewing is controlled by a user's privileges. Migration logs are delivered to the location specified by the user that initiated the migration.

Stat Audit Table Report

The Stat Report Library features the Stat Audit Report, which displays a list of changes that have occurred to certain Stat maintenance tables. Data is written to this table whenever values are updated, inserted, or deleted in selected maintenance tables. The report shows what values were changed, when they were changed, and by which Stat user.

Protection of Stored Data

Passwords used within Stat are encrypted and stored in the repository database. These include the passwords for Stat users, servers, and email accounts. Stat uses AES128 for password encryption. The initial encryption keys supplied by Quest can be modified on site by a privileged user. Encryption keys are therefore unique per Stat deployment (i.e. they are not hard coded).

Protection of Communicated Data

Customers connecting to Stat through the Stat client web application have the option of enabling SSL/TLS on the Stat web application server. The customer is responsible for establishing and uploading a valid SSL certificate to the application server.

Stat supports the use of Secure FTP (SFTP) for archiving of files to the Stat repository and for migrating files from the repository to other files systems. This provides Stat with a secure protocol for authenticating user accounts on the customer's SFTP file servers. The Stat Central Agent uses Java Secure Channel (JSch) by JCraft which relies upon the Java Cryptographic Extension library. The Stat fat client uses wodSFTP by WeOnlyDo Software. Both JSch and wodSFTP support the following ciphers: Blowfish, Triple DES, and AES.

Pre and Post migration steps can be configured to use SSH for communications with other servers.

SMTP and IMAP mail servers can be configured to use SSL/TLS.

POP mail servers can be configured to use SSL

Stat allows for the use of secure LDAP (LDAPS) for authentication of external users.

Network Ports

The Stat Central Agent utilizes a set of ports as defined by the value in

<stat_home>/app/standalone/configuration/standalone-full.xml.

These values are defined for a default port offset of zero which is set in a variable called `jboss.socket.binding.port-offset` in standalone.conf.bat or standalone.conf file. If there is a conflict situation or a second or third agent is necessary, you may change the `jboss.socket.binding.port-offset` in standalone.conf.bat or standalone.conf file. The value for offset is added to all the default values.

For example:

- if offset is zero, ports 8080, 8443, 9990, 9993, 4712, and 4713 are used.
- If offset is one, ports 8081, 8444, 9991, 9994, 4713, and 4714 are used.
- If offset is two, ports 8082, 8445, 9992, 9995, 4714, and 4715 are used.
- If offset is 100, ports 8180, 8543, 10090, 10093, 4812, and 4813 are used.

Table 4. Ports

Description	Ports
HTTP socket binding	8080
HTTPS socket binding (See Note)	8443
Management socket binding	9990
Management socket binding https (See Note)	9993
Transaction sockets	4712 4713

- HTTPS connector socket and Management socket — These ports are only necessary if the Stat Central Agent is configured to support HTTPS
- In addition, the Stat Central Agent uses one randomly generated port. This port can be configured to be the same port every time if a firewall is involved.
- All ports are open in both directions
- All ports are TCP
- The Stat Central agent also needs access to database ports as defined by the site. This is for both the Stat database and supported application databases.
- Ports for inbound and outbound email are configurable
- Port 21 for FTP (can be modified)
- Port 22 for SFTP (can be modified)
- The agent settings can be configured to support Natted firewalls

Changing the Stat Database Password

Stat Database password security is controlled by the user class right, **Master Database Login ID - Change**. Upon installation, the second pass Login ID and password, which correspond to the database login credentials, are set for you. The Login ID is set to “STAT” and the password is stored encrypted in the table that STAT_LOGIN has access to (see “second pass” in step 6 in section **Error! Reference source not found.**).

If you want, you can change the second pass password by selecting **Maintenance | Security Settings | Database Login Info**. Then in the Change Database User ID/Password dialog box, enter a new password. The new password must be in all upper-case alpha characters. Only the DBA should initiate a password change request, as if a user performs the change without the DBA updating the database, then no user will be able to log into Stat

Service Accounts

The Stat Central Agent requires connection parameters for the components it connects to, including the Stat repository and application environments (Oracle E-Business, PeopleSoft, other generic applications). The password credentials for the accounts it uses to connect to the application environments are encrypted and stored in the Stat repository.

Required Privileges

Stat requires administrative privileges both during installation and runtime. In Unix environments, it is possible to use a non-root user to run the Stat Central Agent, although the user requires administrative privileges to the Stat reposi- tory.

Validation and Protection of User Input

Stat verifies input provided by users prior to processing it. It checks for the correct data type (no numeric values in a text-only field) and the length of data. In addition, user passwords are masked by asterisks to prevent them from being displayed in cleartext. Stat also performs error checking to guard against buffer overflows.

IPv6

The current release is both IPv4 and IPv6 compliant.

Daylight Savings Time Extension

Stat is not be affected by the changes introduced by the Daylight Savings Time (DST) Extension (U.S. Energy Policy Act of 2005). It relies upon the Operating System for time management and does not implement any special logic around DST settings.

Customer Measures

The security features of Stat are only one part of a secure environment. The customer's operational and policy decisions have the greatest influence on the overall level of security achieved. The customer is responsible for the physical security of the server on which Stat is installed and the security of the system network.

Appendix A: Stat 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 and 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 Publica- tion 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 Stat addresses them.[3]

We would like to emphasize that the secure deployment of Stat is only one part of an information security program. If the appendix states that a particular security category is "applicable" to Stat, this means that Stat contains security features that may be relevant to some or all aspects of the category in question. It may not mean that Stat fully meets all of the requirements described in that security category, or that the use of Stat 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 Stat.

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:	Stat has a two-layered security system. At the first layer, strict login protocols control access to the Stat Repository, and at the second layer, a set of internal security measures controls access to sensitive areas within the repository database. A separate security level, which is associated with Stat users, limits which users are able to view generated reports. Internal Stat security is based on service domains and user classes. User classes are collections of access rights that control a user's ability to view information and perform functions within service domains. To operate within a service domain, a user must be assigned to at least one user class that is associated with that service domain.
Further Details:	Section(s) Security Layers, Role Based Access Control, Editing User Class Rights

Category:	Access and Training (AT)
Applicable:	No
Description:	Customers who install Stat on their systems are responsible for developing and reviewing their security awareness and training policies.
Further Details:	N/A

Category:	Audit and Accountability (AU)
Applicable:	Yes
Description:	The Connection History tab displays a record of connection denials and termina- tions. It includes successful and unsuccessful login attempts. In addition to the Connection History, Stat records the following log files: agent log, server log, archive log, and migration log. Stat also reatures the Stat Audit Table Report, which displays a list of changes that have occurred to certain Stat maintenance tables. Data is written to this table whenever values are updated, inserted, or deleted in selected maintenance tables. The report shows what values were changed, when they were changed, and by which Stat user.
Further Details:	Section(s) Connection Manager and History, Audit Logs

Category:	Certification, Accreditation and Assessments (CA)
Applicable:	No
Description:	Customers who install Stat on their systems are responsible for developing and reviewing their security assessment, accreditation and certification policies.
Further Details:	N/A

Category:	Configuration Management (CM)
Applicable:	Yes
Description:	Stat's role based access control system controls what actions users are able to perform. The password security settings allows for customization of the password policy which dictates how passwords for internal users may be created.
Further Details:	Section(s) User Password Security Settings, Connection Manager and History

Category:	Contingency Planning (CP)
Applicable:	No
Description:	Customers who install Stat on their systems are responsible for designing and implementing 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
Further Details:	N/A .

Category:	Identification And Authentication (IA)
Applicable:	Yes
Description:	All Stat users are authenticated upon login against the Stat repository. Both internal and external users (LDAP) can be supported simultaneously.
Further Details:	Section(s) Login Security, Defining User Classes, Defining Stat Users, User Password Security Settings

Category:	Incident Response (IR)
Applicable:	No
Description:	Customers who install Stat on their systems are responsible for developing and reviewing their incident response policies and procedures.
Further Details:	N/A

Category:	Maintenance (MA)
Applicable:	Yes

Description:	Quest Software provides product and security patches to its customers when necessary.
Further Details:	N/A

Category:	**Media Protection (MP)**
Applicable:	No
Description:	Customers who install Stat on their systems are responsible for developing and reviewing their own media protection policies.
Further Details:	N/A

Category:	**Physical and Environmental Protection (PE)**
Applicable:	No
Description:	Customers who install Stat on their systems are responsible for developing and reviewing their own physical and environmental policies.
Further Details:	N/A

Category:	**Planning (PL)**
Applicable:	No
Description:	Customers who install Stat on their systems are responsible for developing and reviewing their security planning policies
Further Details:	N/A

Category:	**Personal Security (PS)**
Applicable:	No
Description:	Customers who install Stat on their systems are responsible for enforcing personnel security policies, including personnel screening and termination.
Further Details:	N/A

Category:	**Risk Assessment (RA)**
Applicable:	No
Description:	Customers who install Stat on their systems are responsible for developing and reviewing their own risk assessment policies.
Further Details:	N/A

Category:	**System and Services Acquisition (SA)**
Applicable:	No
Description:	Customers who install Stat on their systems are responsible for developing and reviewing their own system and services acquisition policies.
Further Details:	N/A

Category:	**System and Communications Protection (SC)**
Applicable:	Yes
Description:	Stat supports the use of SSL to protect user communication. The customer is responsible for providing an SSL certificate. Customers can choose to use SFTP for authenticated file transfers. The network ports over which Stat components and protocols communicate are configurable.
Further Details:	Section(s) Protection of Communicated Data, Network Ports

Category:	**System and Information Integrity (SI)**
Applicable:	Yes
Description:	Stat encrypts passwords for its internal users and service accounts and stores the ciphertexts in its repository. It uses the AES-128 algorithm. Stat validates input data provided by users by restricting the type of data that can be entered, depending on the input fields..
Further Details:	Section(s) Protection of Stored Data, Validation and Protection of User Input

About us

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

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