QSM® The Intelligence behind Successful Software Projects

SLIM-Collaborate 3.0 Application Security

SLIM-Collaborate employs multiple practices to ensure the security of data and personally identifiable information stored in the application. This document describes the key methods used in the product.

Authentication and Passwords

Editing or viewing project data in SLIM-Collaborate requires a user to log into Collaborate with a user name and password. SLIM-Collaborate provides an internal authentication method to verify login credentials. Customers may optionally use a corporate directory server or a custom authentication method to store and verify passwords.

Passwords are never saved in plain text in the SLIM-Collaborate user database, and are not displayed on the screen during user logins. If the user name and password do not match, a single error message that does not give any indication of whether the user name was found will appear.

If the customer uses the SLIM-Collaborate internal authentication, encrypted passwords are stored in the SLIM-Collaborate database. This method uses SHA-512 encryption and the "salted hash" mechanism to protect against attempts by an intruder to guess a password. Each user is responsible for choosing or changing their password via the "My Preferences" menu item on the main Collaborate site.

Site Administrators may deactivate a user's profile to prevent that user from logging in. Only site administrators can deactivate or reactivate a user.

Users who forget their password can enter their username and request a password reset from the link provided on the login page. If the username matches an existing user profile, a password reset link will be sent to the email address in the user's profile. The password reset link is valid for 48 hours and in only available once. To discourage unauthorized reset requests, users who mistype their usernames when requesting a password reset are not informed of the error. This helps prevent unauthorized users from gaining information useful for stealing user names. Passwords can also be reset by the Site Administrator directly in the Admin site.

If for some reason all Site Administrators are locked out of the system during the valid license period, QSM can supply an authorized administrator with a one-time use key to log in and correct the problem. Once used, the key becomes invalid so other users cannot attempt to use it later. Before sending this "unlock" key, QSM reserves the right to employ all reasonable methods to verify that the request is authorized. This may include contacting more than one other person from the requesting company.

QSM® The Intelligence behind Successful Software Projects

Authorization

Each SLIM-Collaborate user is assigned a role with permissions by the Site Admin. Only projects which the user has permission to access are visible to that user. (Site Administrators have permission to all projects.) Actions available on a project depend on the user's role and permissions. See the SLIM-Collaborate 3.0 online documentation for further details.

Personal Data

Personally identifiable information stored in the SLIM-Collaborate is encrypted using the Advanced Encryption Standard. Personally identifiable information includes names, email addresses, physical addresses, and telephone numbers.

If the customer uses a QSM hosted instance, all personal data transmissions between the user's computer and SLIM-Collaborate are protected over secured sockets layer version 3.0 high-grade encryption and SHA-256 with RSA encryption.

Web Vulnerabilities

SLIM-Collaborate follows industry standards to protect against web vulnerabilities such as cross-site scripting, cross-site request forgery, SQL injection, and LDAP injection.

Cross-site Scripting

All user data is encoded before it is displayed in the browser, preventing malicious users from executing scripts that are not part of the SLIM-Collaborate code. This prevents cross-site scripting attacks from any source, including data entered within SLIM-Collaborate, data imported into SLIM-Collaborate by other authorized techniques, or any other manner in which data is entered into the SLIM-Collaborate database.

Data and text entered directly in SLIM-Collaborate is also validated using Microsoft IIS page validation to check for malicious scripts before it is saved. Users who attempt to enter invalid data are redirected to an error page.

Cross-site request forgery

All requests that change data are checked to be sure the request came from within SLIM-Collaborate. SLIM-Collaborate uses two hidden, encoded tokens which must match site and session specific cookie values, and requests that do not match are rejected.

SQL Injection

To mitigate threats from SQL injection, SLIM-Collaborate uses a data layer framework that generates parameterized SQL queries.

LDAP Injection

If SLIM-Collaborate is configured to use the optional LDAP user authentication, the password authentication is checked through a bind call rather than a search for the password value, so it is not susceptible to LDAP injection.

QSM Hosted Sites

The hosted environment is secured with managed firewalls, a threat management system, and DDoS mitigation services. Environmental protections, software, and recovery infrastructure are designed, developed, implemented, operated, maintained and monitored to meet any availability commitments and requirements. In the event a website requires data restoration, full database remote backups are performed on a nightly basis through a secure and encrypted gateway.

Client (On-Premise) Hosting

Connection security will depend on the configuration of the client's chosen hosting environment. For Collaborate sites hosted by the client, the access and encryption settings needed to protect data are custom configurable.