

TestTrack and Surround SCM Data Security Best Practices

Because of the importance of data stored in TestTrack and Surround SCM, it is essential that you take steps to ensure your data is secure. These best practices form the basis for securing data stored in the Seapine License Server, TestTrack, and Surround SCM. Implementing them can help you avoid common mistakes that could leave your data vulnerable to theft, damage, or loss.

Enable Encryption

The Seapine License Server, Surround SCM, and TestTrack are all client/server applications with data flowing between the clients and the server. Encrypting the data sent between servers and clients provides extra security.

The Seapine License Server and TestTrack each have server admin utilities that allow you to set options to encrypt communications between the Seapine License Server and other applications. In Surround SCM, all administrative tasks are accessed through the Administration menu.

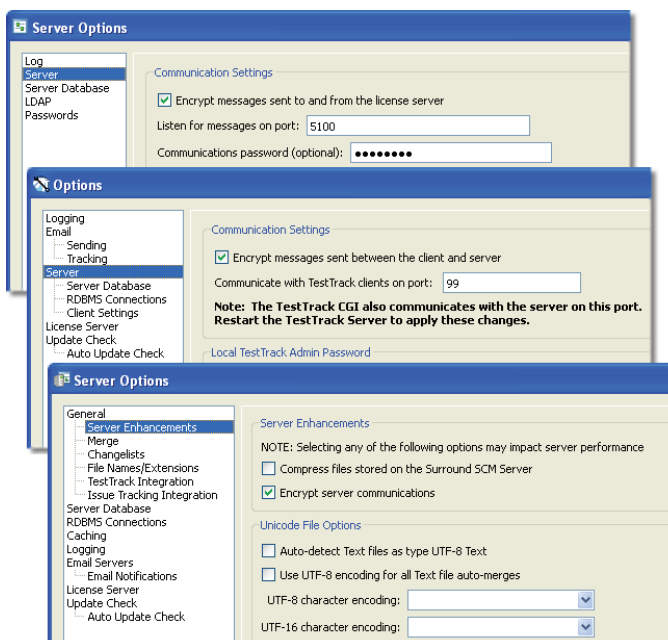


Figure 1: Encryption options

Enforce Strong Password Rules

Passwords are one of the easiest ways to protect against unauthorized access to a system. Yet most users do not choose strong passwords. Effective passwords should:

- Be a minimum of eight characters
- Use mixed case and a combination of alphanumeric characters and punctuation
- Not be real words or patterns of letters on the keyboard
- Not follow the pattern of previous passwords
- Not contain personal information or elements of the user ID

You can use LDAP or the Seapine License Server Admin Utility to enforce password requirements.

Change Administrative Default Passwords

TestTrack and Surround SCM are both installed with a default administrative user, local user, and license server passwords. Change these passwords the first time you use TestTrack or Surround SCM. Changing the passwords before adding any data to the server also guarantees your data is not exposed to the risk of theft or corruption from users who would otherwise be denied access.

Restrict Access to Database Files

The TestTrack and Surround SCM clients do not need write access to database files because they communicate through the server applications. You can use file-level security in the operating system to restrict client access to the database files.

Check Log Files Regularly

Review the server logs on a regular basis to check for suspicious activity. In TestTrack and the Seapine License Server, you can access the server log through the corresponding server admin utility. In Surround SCM, access the server log through the Administration menu.

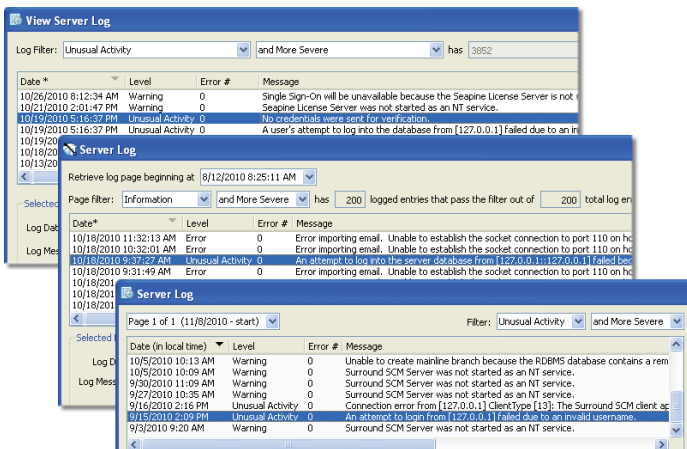


Figure 2: Server logs

You can also enable email notifications in the TestTrack and Surround SCM server logging options to stay informed about specific levels of activity as events are recorded in the server log.

Restrict Access to Unused Functionality

TestTrack and Surround SCM use security groups to control access to commands and functionality. Careful consideration of how different users will use the application can greatly reduce security issues. Well-designed security groups prevent users from accidentally changing data they should not have access to. When creating a new security group, review all security settings to ensure only the functions you want users to access are enabled. After you create one security group, you can duplicate it and make minor adjustments instead of starting from scratch every time you need to create a security group.

Back Up Database Files

Even with proactive security measures in place, you should still back up your data on a regular basis. Nightly backups ensure data loss will be minimal in the event of a virus attack, hardware failure, or malicious activity.

Make sure you back up both the server database and the TestTrack project or Surround SCM mainline databases. Because data is stored in both places, backing up all databases ensures you have a lessened likelihood of data corruption. [Seapine's knowledgebase](#) includes articles on how to back up databases. If you use an RDBMS, refer to the vendor documentation.

Keep Applications Up to Date

One of the easiest ways to avoid known security bugs is to ensure you are using the latest version of an application. In Surround SCM and TestTrack, you can set up automatic notifications to alert you of new version releases. Upgrading an application as soon as a new version is available not only provides you with the newest features but could also provide you with additional security features or options that might not be available in older versions.

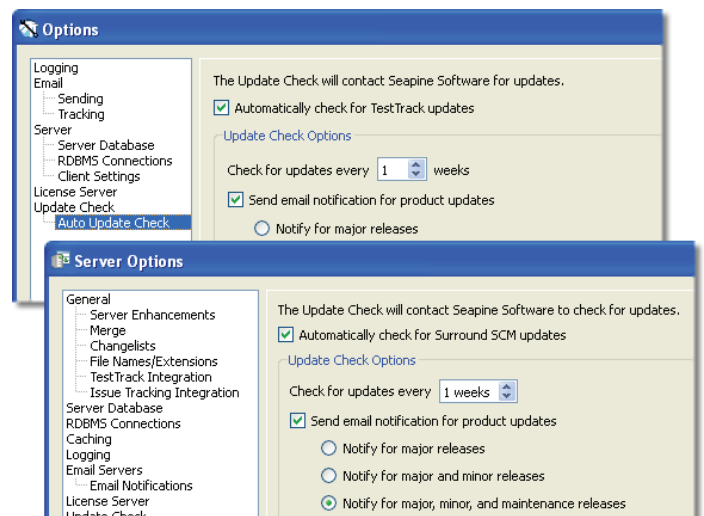


Figure 3: Automatic client update options

The same is true if you use an RDBMS. Systems automatically generate updates and security patches as soon as they are available. Installing the updates keeps your RDBMS version running with the necessary features to meet current security standards.