

Surround SCM Security Best Practices

Surround SCM security controls the activities users can perform on server, repository, and branch levels. Managing security for users can become overwhelming as the number of security groups, repositories, and branches increases. The approaches to security management discussed in this guide can help minimize the administrative effort required to provide users with access to the information they need in Surround SCM.

Security Levels

Security groups control access to the activities users can perform. Surround SCM includes server, repository, and branch security.

Server security

Server security, which restricts the activities users can perform in all branches and repositories, controls access to general activities, administrative functions, user management, security group management, file activities, and branch activities.

Repository security

Repository security restricts the file-related activities users can perform in specific repositories. If repository security is configured for a security group, users can only perform activities enabled for the specified repositories.

Branch security

Branch security restricts the file-related activities users can perform in specific branches. If branch security is configured for a security group, users can only perform activities enabled for the specified branches. Branch security is generally used to provide a security group with access to a specific branch while maintaining the repository security settings in other branches.

How Security is Applied

Before you configure security groups, it is important to understand how server, repository, and branch security are enforced. Surround SCM security is optimistic, which means the most granular security permissions are used if a conflict exists between commands enabled in different security levels. For example, if the Add Files command is enabled in server security but disabled in repository security, users cannot add files in the selected repository because repository security overrides server security. Repository security

always overrides server security, and branch security always overrides server and repository security.

Users can belong to more than one security group. If commands enabled in one security group are disabled, but commands in another group are enabled, the enabled commands override the disabled commands and users can perform the related activity. For example, if a user belongs to a group that allows checking out files and another group that does not, the user can check out files.

Repository-level Group Management

A repository-centric security model is generally the best way to manage a large number of users and projects with minimal administrative effort.

Create a security group to allow read-only access to all repositories

Before you start configuring security, create a security group that provides read-only access to all users. We will refer to this as the All Users group. This group provides a baseline of security for all users that can be built on by using other groups and configuring repository and branch security. All new users should be added to the All Users group.

First, configure server security for this group. We recommend enabling all commands in the General category and disabling all commands in the Admin, Users, Security Groups, and Files categories. In the Branch category, only enable the View Branch History, Promote Branch, and Rebase Branch commands. Enabling these commands allows users to view repositories and files, but does not allow them to perform read/write actions, such as checking files in and out.

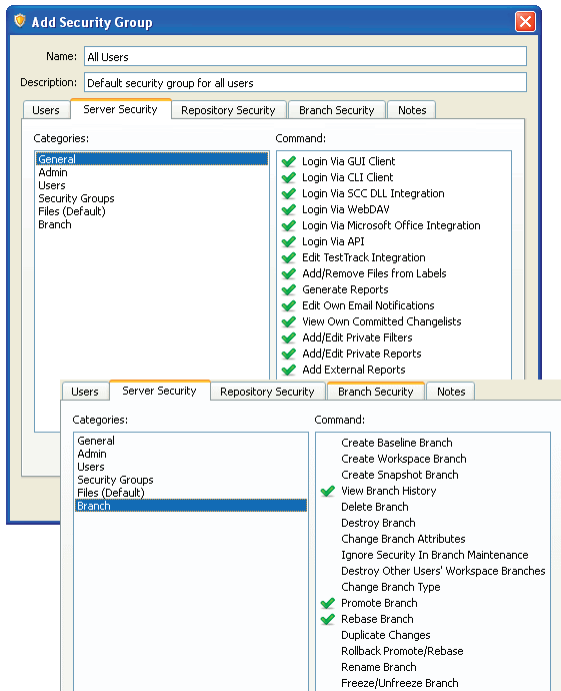


Figure 1: Server security for All Users group

Next, configure repository security for the highest level, or base, repository in the mainline branch. Add the base repository to the repository list on the Repository Security tab and only enable the View Repository List option. This allows users to view all repositories in the mainline branch.

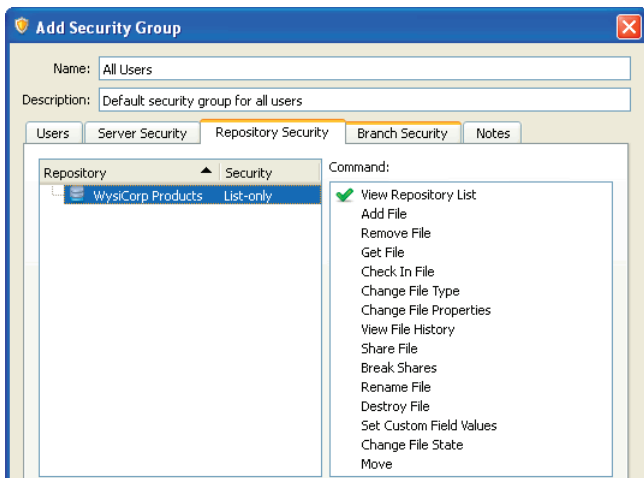


Figure 2: Repository security for All Users group

Optionally create a power users security group

You may want to provide some users, such as managers or team leads, with the ability to perform administrative activities, such as modifying security group settings or setting server options. If you do not want to give these users access to all administrative commands enabled in the default admin security group, create a power users security group and enable the appropriate commands.

Create a security group for each project repository

When a project repository is created, add a new security group for the project, and then add users working on the project to the group. Keep in mind that members of this group also belong to the All Users group.

Project-based security groups allow you to control access to new repositories. If users are not assigned to a project security group, they can only perform actions on the repository based on the permissions enabled for the All Users group. If you only enabled the recommended server security commands, the All Users group has read-only access to repositories.

Hide repositories from non-project users

You may not want users outside of the project team to view repositories or files for a project for confidentiality reasons. You can hide repositories so they are only visible to users in the project security group.

To hide a repository, right-click it and choose Properties. Click the Security tab, then select the All Users security group and click Override. Click Disable All to disable all commands and click OK to save the changes.

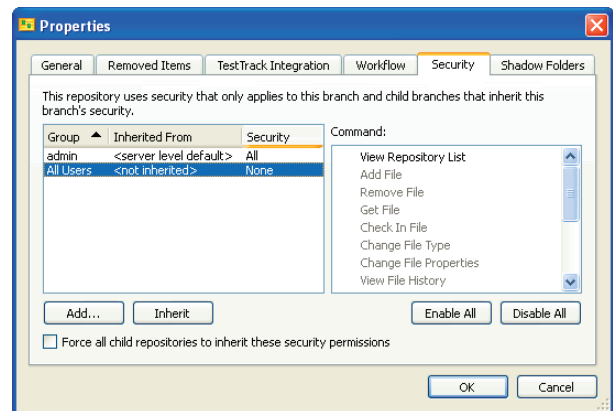


Figure 3: Hidden repository security properties

Users in the All Users group cannot view the hidden repository. When new branches are created they inherit the repository security, which means the repository in the new branch is not visible to the All Users group.

Branch-level Group Management

When a new branch is created, repository security is inherited and used by default. If you only want a specific security group to have read/write access to a branch, you must set the branch to use its own security and create a security group for the branch users.

Only use branch security when you want to provide a group with access to a specific branch while retaining repository security settings in other branches.

Set branches to start with no specific security applied

Because branches inherit security privileges from the parent branch by default, you need to remove the repository security settings before you set branch security. Users with access to the repository in the mainline branch can also access the repository in new branches. Setting branch security overrides the server and repository security to provide access to a specific branch.

To set a branch to use its own security, right-click the branch and choose Properties. Click the Security tab. Select the Use own security option and select 'Start with no specific security applied'. Click OK to save the changes.



Figure 4: Branch-level security properties

Create a security group for branch users

After a branch is set to use its own security, create a security group for users who need to access the branch.

When you create the group, click the Branch Security tab and click Add. Select the branch to provide access to and click OK. Select the file commands you want to enable access for and click OK to save the changes.

New branches are not visible to the All Users security group. To make a branch visible and provide read-only access to it, set the branch to use its own security and then set the branch security in the All Users group to read-only.

Configure Password Requirements

In addition to the settings in Surround SCM, you can improve security by configuring password creation rules. In the Seapine License Server Admin Utility, select Server Options. In the Passwords category, you can specify the minimum password length and the number of alpha, numeric, and non-alphanumeric characters required in a password.

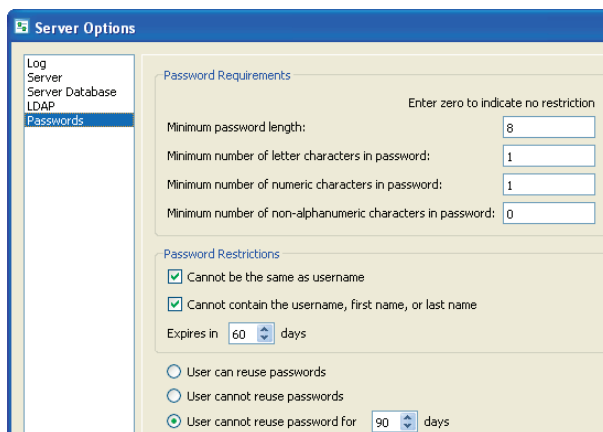


Figure 5: Seapine License Server password requirements

Strong passwords contain eight or more characters and a mix of alpha, numeric, and non-alphanumeric characters.