Overview

Overview / Product overview / Features / No-charge product enhancement features / Security feature / Advanced security functions

Advanced security functions

The Security feature provides advanced functions that increase the security of user accounts.

If you have an existing Lightweight Directory Access Protocol (LDAP) or Active Directory server, you can use LDAP user IDs and passwords to authenticate into RICOH ProcessDirector. Password rules and change intervals set by the LDAP server apply to the RICOH ProcessDirector user IDs.

If you use RICOH ProcessDirector user IDs and passwords to authenticate into RICOH ProcessDirector, you can specify requirements for passwords:

- Minimum length
- Maximum age before expiration
- Enforcement of password complexity rules

For both methods of authenticating into RICOH ProcessDirector, you can specify:

- Whether an account can log in multiple times concurrently
- The number of unsuccessful login or password change attempts that are allowed before the user is locked out
- The lockout duration
- How long accounts can be inactive before they are suspended

The Security feature records unsuccessful login attempts in the system log. If the Reports feature is installed, the Security feature also records unsuccessful login attempts in reports generated from the **UserActivity** report template.

The Users table and user properties notebook include user account status: **Active**, **Locked-Inactive**, or **Locked-Password Failure**.

To access these functions, click the **Administration** tab. In the left pane, click **Settings ⇒ Security**.

Parent topic: Security feature