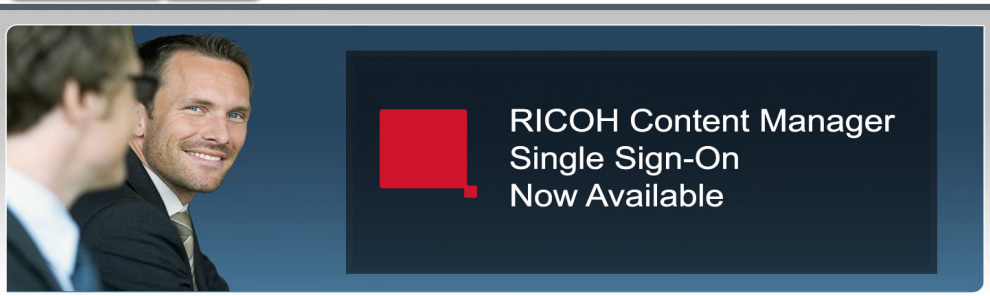

Single Sign-On (SSO)

Single Sign-On is an authentication process that allows a user to access multiple applications with a single set of login credentials. SSO for RCM leverages an organization's identity database to validate users and grant access to files in order to relieve system administrators of the burdensome task of managing multiple user databases. SSO advantages include:

- Reduces IT administration costs
- Increases user productivity
- Reduces risks associated with minimizing bad password habits
- Accelerates adoptions of company-promoted applications

Below is a high-level summary of the steps executed when an RCM user makes an SSO request:

1. The user logs on to a user portal and clicks on the icon (unique RCM SSO URL) for RCM.
2. The identity provider associated with that icon sends an SSO request to RCM, in the form of a SAML message.
3. The SAML message is received by RCM's service provider and authenticated.
4. If authentication succeeds, then the SSO server-side controller validates the information contained in the SAML message.
5. If validation succeeds, then the user session is initialized, and the RCM home screen displays the cabinets for the user in question.

If you have any questions, please send an email that includes your phone number to this address: customerservice@ricoh-contentmanager.com.

Access resources that will help you learn how to use the RICOH Content Manager UI.

RCM User Guide

Ricoh USA, Inc., 70 Valley Stream Parkway, Malvern, PA 19355