Overview

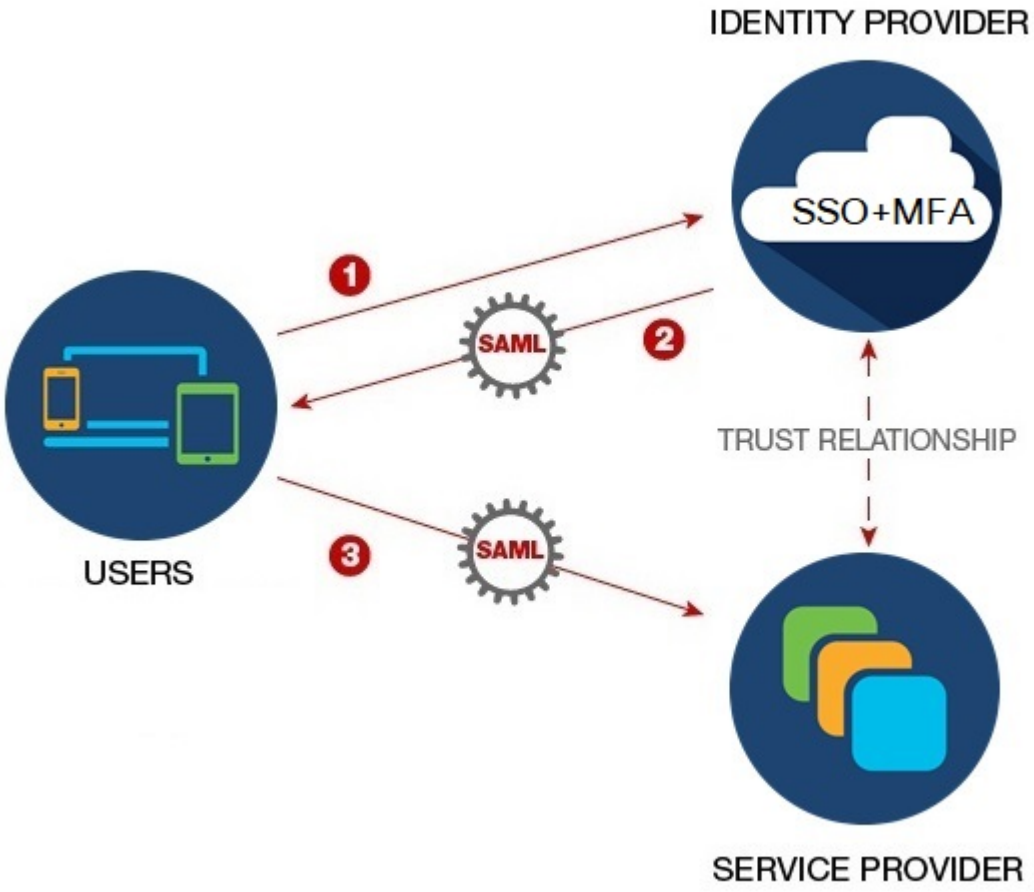
Important **Enterprise Manager has been discontinued**. You can now use Security Cloud Control to manage your identity provider integrations. See the Identity provider integration guide for more information.

All of your existing identity provider integration data is available through Security Cloud Control.

Overview

You can integrate your own or third-party identity provider (IdP) with Cisco Security Cloud Sign On using Security Assertion Markup Language (SAML). SAML is an XML-based open standard for exchanging authentication and authorization data between an identity provider (IdP) and a service provider (SP). In this case, the service provider is Security Cloud Sign On. Once integrated, users can use their single sign on

credentials to sign in to Security Cloud Sign



Multi-Factor authentication requirements

Security Cloud Sign On requires Duo Multi-Factor Authentication for all accounts. Customers who integrate their own identity provider with using SAML (Security Assertion Markup Language) may opt-out of Duo MFA.

Once enrolled in Duo MFA, users can optionally enroll with Google Authenticator. Once enrolled with Google Authenticator, subsequent sign-ons will only present a Google Authenticator challenge, not a Duo MFA challenge.

This same policy is enforced if you are using federated sign-on through Cisco Customer Identity or Microsoft (under **Other login options** on the Security Cloud Sign On page).

Customers with existing IdP integrations

If you have an IdP integration with Security Cloud Sign On that was **not** created with the self-service tool described in this guide, you cannot use the tool to update your existing configuration. You will need to open a open a case with Cisco TAC if you need to modify any of the following settings for your integration:

- SAML single sign on URL or Entity ID URI
- x.509 signing certificate
- Multi-Factor Authentication (MFA) settings