Troubleshooting

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.

Single sign-on/SAML errors

HTTP 400 errors when testing your integration

If you get an HTTP 400 error when testing your IdP integration in the Enterprise settings wizard, try the following troubleshooting steps.

Check the user's sign-on email domain matches the claimed domain

Make sure the email domain of the user account you're using to test with matches your claimed domain. For instance, if you claimed a top-level domain, such as `example.com`, then users must sign in with `<username>@example.com` and not `<username>@signon.example.com`.

Check that the <NameID> element in the SAML response is an email address

The value of the `<NameId>` element in the SAML response must be an email address. The email address must match the **email** specified in the user's SAML attributes. See SAML response attributes for details.

Check that the SAML response contains the correct attribute claims

The SAML response from your IdP to Security Cloud Sign On includes the required user attributes, namely, **firstName**, **lastName**, and **email**. See SAML response requirements for details.

Check that the SAML response from your IdP is signed with SHA-256

SAML response from your identity provider must be signed with the SHA-256 signature algorithm. Security Cloud Sign On rejects assertions that are unsigned or signed with another algorithm.

Enterprise wizard errors

Error when verifying your domain

If you encounter an error when verifying your email domain, try the following troubleshooting steps.

Wait a while and try again

Wait a while and try clicking **Verify** again. The time it takes DNS record updates to propagate to DNS servers varies by service provider.

Verify TXT DNS record name and value

Verify that the name and value of the TXT DNS record you created on your domain registrar matches the displayed by the enterprise settings wizard.

Error testing single sign-on

If you encounter an error when testing your integration it's likely a SAML configuration issue or an issue with the user account. See Single sign-on/SAML errors, on page 1 for troubleshooting steps.

Integration with Cisco security products

Sign-on errors with Cisco security products

If you are able to sign on to Security Cloud Sign On but aren't able to sign on to one or more Cisco security products, check the following.

Check if the product requires you to opt-in to Security Cloud Sign On

While some Cisco security products such as Cisco Umbrella support Security Cloud Sign On by default, others require you to opt-in. The list of supported security products identifies those Cisco security products that require opt-in.

Check that your Security Cloud Sign On identity matches your product identity

Each user's Security Cloud Sign On identity (email) must match their product identity. For instance, suppose you have a Security Cloud Sign On account with the username **`user@example.com`**. To authenticate successfully with Umbrella using your Security Cloud Sign On account there must be an existing Umbrella account with the same email.