Understand FAQs about Umbrella SSO Integrations

Contents

Introduction

This document describes frequently asked questions (FAQs) about Cisco Umbrella single sign-on (SSO) integrations.

Frequently Asked Questions about Integrations

Do you use encryption for the SAML request or response?

No, SAML requests are sent unencrypted, and SAML responses to Umbrella must also be sent unencrypted.

Is the SAML request signed?

As of December 2018, all new SAML setups on the Umbrella dashboard now have signing turned on by default. However, existing users have signing disabled until they setup SAML again. The certificate used to sign the SAML request is available in the metadata.

Can the SAML response be signed?

Yes, either the entire response must be signed, or the relevant Assertion must be signed.

What type of binding can be used?

The SAML request uses HTTP Redirect Binding. The SAML Response uses HTTP POST Binding.

Are any attributes required on the assertions in the metadata?

No, no attributes are required.

What ID or account name must be used for sign on?

Email address is required. If there is an option to specify a name ID format, select email address. Email attached as a response attribute cannot be expected to work.

When importing XML from the Umbrella dashboard, is this a local or remote metadata? Can it expire?

The XML is currently designed as local metadata. If your SAML provider considers the loaded metadata as remote or respects the expiration data, remove the expiration date from the Umbrella XML before importing.