



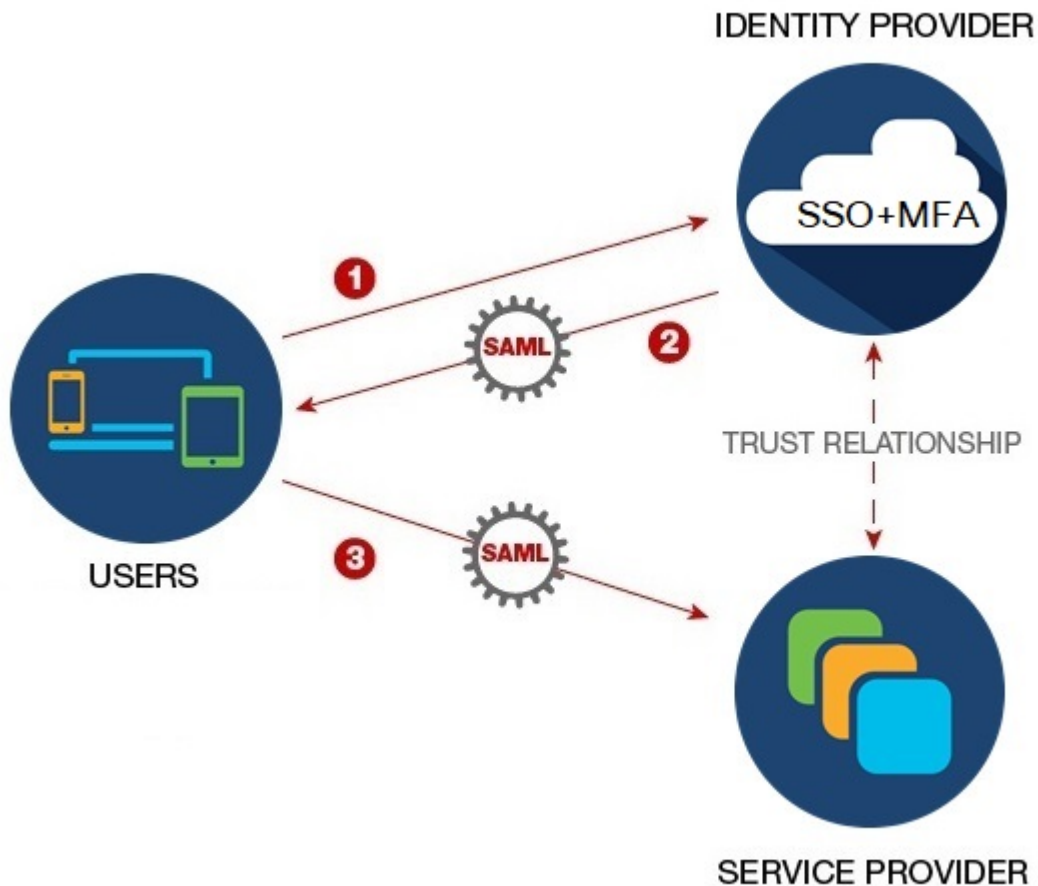
Welcome

- [Overview, on page 1](#)
- [IdP SAML requirements, on page 2](#)
- [Next Steps, on page 3](#)
- [Additional Resources, on page 3](#)

Overview

You can integrate your own or third-party identity provider with SecureX Sign On using Security Assertion Markup Language (SAML), an XML-based open standard for exchanging authentication and authorization data between an identity provider (IdP) and a service provider (SP), which in this case is SecureX Sign On.

Once integrated, users can then their usual single sign on credentials to sign in to SecureX Sign



By default, SecureX Sign-On enrolls all your IdP's users into [Duo Multi-Factor Authentication \(MFA\)](#) at no cost. If your organization already has MFA integrated with your IdP, you can optionally disable Duo-based MFA during the integration process.

IdP SAML requirements

Any identity provider that supports SAML 2.0 can be integrated with SecureX SignOn. The SAML assertion sent by your IdP the SecureX Sign On Assertion Consumer Service (ACS) URL must be configured as follows:

- The **<NameID>** element must have a valid email address as its value, and its **Format** attribute must be set to either **urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified** or **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**, for example:

```
<saml2:NameID
  Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">jdoe@example.com</saml2:NameID>
```

- The following user attributes must be asserted in the SAML assertion statement submitted to the ACS URL: `email` This attribute must have the same value as the NameID element. * `firstName` * `lastName`

- **email** – This attribute must have the same value as the NameID element.
- **firstName**
- **lastName**

For example, the following XML snippet is an example **<AttributeStatement>** element in the SAML assertion statement sent to the Assertion Consumer Service URL:

```
<saml2:AttributeStatement>
  <saml2:Attribute Name="firstName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml2:AttributeValue
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">John
  </saml2:AttributeValue>
</saml2:Attribute>
  <saml2:Attribute Name="lastName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml2:AttributeValue
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">Doe
  </saml2:AttributeValue>
</saml2:Attribute>
  <saml2:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml2:AttributeValue
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">jdoe@example.com
  </saml2:AttributeValue>
</saml2:Attribute>
</saml2:AttributeStatement>
```

Next Steps

Which type of IdP are you using?

- [Auth0](#)
- [Azure AD](#)
- [Duo SSO](#)
- [Google](#)
- [Okta SSO](#)
- [PingFederate](#)

Additional Resources

Refer to these resources for additional information:

- [Cisco SecureX sign-on quick start guide](#)
- [Cisco SecureX sign-on product page](#)
- [Cisco SecureX sign-on privacy data sheet](#)