SAML requirements for identity providers

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

The SAML response from your IdP to Security Cloud Sign On must adhere to a few rules as described in SAML response requirements, on page 1.

You will also need to obtain the SAML metadata requirements from your IdP.

SAML response requirements

SAML response signed with SHA-256

The SAML response returned by the identity provider must be signed with the SHA-256 signature algorithm. Security Cloud Sign On will reject responses that are unsigned or signed with another algorithm.

SAML response attributes

The assertion in the SAML response sent by your IdP must contain the following attribute names and must be mapped to the IdP's corresponding attributes.

SAML assertion attribute name	IdP user attribute
firstName	User's first or given name.
lastName	User's lastname or surname.

SAML assertion attribute name	IdP user attribute
email	User's email. This must match the value of the **<NameID>** element in the SAML response.

For example, the following XML snippet is an example of an **<AttributeStatement>** element included in a SAML response to the Security Cloud Sign On ACL 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>
```

NameID element

The **<NameID>** element in the SAML response from your IdP must have a valid email address as its value, and the email must match the value of the **email** attribute in the SAML response attributes, on page 1.

The **Format** attribute of the **<NameID>** 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**.

Below is an example `<NameID>` element.

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

SAML metadata requirements

The following metadata from your IdP's SAML application is required to integrate with Security Cloud Sign On.

- **Single sign-on service initial URL** – This is sometimes referred to as "SSO URL" or "Login URL". This URL can be used to start an IdP-initiated authentication to Security Cloud Sign On.
- **Entity ID URI** – The global, unique name for your IdP. This is sometimes referred to as "Issuer".

- **X.509 signing certificate** – The public key of the public/private key pair your IdP uses to sign SAML assertions.