ID 제공자에 대한 SAML 요구 사항

중요 **Enterprise Manager**가 사용이 중지되었습니다. 이제 보안 클라우드 제어 를 사용하여 ID 공급자 통합을 관리할 수 있습니다. 자세한 내용은 ID 공급자 통합 가이드를 참조하십시오.

모든 기존 ID 공급자 통합 데이터는 보안 클라우드 컨트롤을 통해 사용할 수 있습니다.

개요

IdP에서 Security Cloud Sign On(으)로 보내는 SAML 응답은 SAML 응답 요구 사항, 1 페이지에 설명된 대로 몇 가지 규칙을 준수해야 합니다.

또한 IdP에서 SAML 메타데이터 요구 사항를 가져와야 합니다.

SAML 응답 요구 사항

SHA-256으로 서명된 SAML 응답

ID 공급자가 반환한 SAML 응답은 SHA-256 서명 알고리즘으로 서명되어야 합니다. Security Cloud Sign On은(는)서명되지 않았거나 다른 알고리즘으로 서명된 응답은 거부합니다.

SAML 응답 속성

IdP가 전송한 SAML 응답의 어설션에는 다음 속성 이름이 포함되어야 하며 IdP의 해당 속성에 매핑되어야 합니다.

SAML 어설션 속성 이름	IdP 사용자 속성
firstName	사용자의 이름입니다.
lastName	사용자의 성입니다.
email	사용자 이메일입니다. 이 값은 SAML 응답의 **<NameID>** 요소 값과 일치해야 합니다.

예를 들어, 다음 XML 스니펫은 Security Cloud Sign On ACL URL에 대한 SAML 응답에 포함된 **<AttributeStatement>** 요소의 예입니다.

```
<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 요소

IdP에서 보낸 SAML 응답의 **<NameID>** 요소에는 유효한 이메일 주소가 값으로 있어야 하며, 이메일은 SAML 응답 속성, 1 페이지의 **email** 속성 값과 일치해야 합니다.

<NameID>의 **Format** 속성은 **urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified** 또는 **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**로 설정해야 합니다.

아래는 `<NameID>` 요소의 예입니다.

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

SAML 메타데이터 요구 사항

Security Cloud Sign On과(와) 통합하려면 IdP의 SAML 애플리케이션에 있는 다음 메타데이터가 필요합니다.

- **SSO(Single Sign-On)** 서비스 초기 **URL** – "SSO URL" 또는 "로그인 URL"이라고도 합니다. 이 URL은 Security Cloud Sign On에 대한 IdP 시작 인증을 시작하는 데 사용할 수 있습니다.
- 엔터티 **ID URI** – IdP의 전역 고유 이름입니다. 이를 "발급자"라고도 합니다.
- **X.509** 서명 인증서 – IdP가 SAML 어설션 서명에 사용하는 공개/개인 키 쌍의 공개 키입니다.