Azure AD

중요

Enterprise Manager가 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

이 가이드에서는 Azure AD SAML 애플리케이션을 생성하고 Security Cloud Sign On과(와) 통합하는 방법을 설명합니다.

참고

- Azure AD 사용자의 UPN(사용자 계정 이름)은 해당 사용자의 이메일 주소와 항상 같지는 않습니다.
- `<NameID>` 요소 및 SAML 응답의 `email` 사용자 속성은 사용자의 이메일 주소를 포함해야 합니다. 자세한 내용은 SAML 응답 요구 사항를 참조하십시오.
- 지정된 이메일 주소는 기존 제품 액세스 제어에 사용된 주소와 일치해야 합니다. 일치하지 않으면 제품 액세스 제어를 업데이트해야 합니다.

시작하기

시작하기 전에

- 관리자 권한으로 Azure 포털 에 로그인할 수 있어야 합니다.

- 엔터프라이즈 설정 마법사의 1단계: 엔터프라이즈 생성 및 2단계: 이메일 도메인 클레임 및 확인를 완료해야 합니다.

단계 **1** https://portal.azure.com에 로그인합니다.

계정에서 둘 이상의 테넌트에 액세스할 수 있는 경우 오른쪽 상단에서 계정을 선택합니다. 포털 세션을 원하는 Azure AD 테넌트로 설정합니다.

a) **Azure Active Directory**를 클릭합니다.
b) 왼쪽 사이드바에서 **Enterprise Applications(**엔터프라이즈 애플리케이션**)**을 클릭합니다.
c) **+ New Application(+** 새 애플리케이션**)**을 클릭하고 **`Azure AD SAML`** 툴킷을 검색합니다.
d) **Azure AD SAML Toolkit(Azure AD SAML** 툴킷**)**을 클릭합니다.
e) **Name(**이름**)** 필드에 **`SecureX Sign On`** 또는 다른 값을 입력하고 **Create(**생성**)**를 클릭합니다.
f) Overview(개요) 페이지의 왼쪽 사이드바에서 **Manage(**관리**)** 아래 **Single Sign On(**단일 인증**)**을 클릭합니다.
g) SSO(Single Sign-On, 단일 인증) 방법 선택 시 **SAML**을 선택합니다.
h) **Basic SAML Configuration(**기본 **SAML** 구성**)** 패널에서 **Edit(**편집**)**를 클릭합니다.

- **Identifier (Entity ID)(**식별자**(**엔터티 **ID))**에서 **Add Identifier(**식별자 추가**)**를 클릭하고 임시 값 **`https://example.com`** 또는 기타 유효한 URL을 입력합니다. 나중에 이 임시 값을 대체합니다.
- **Reply URL (Assertion Consumer Service URL)(**회신 **URL(**어설션 소비자 서비스 **URL))**에서 **Add reply URL(**회신 **URL** 추가**)**를 클릭하고 임시 값 **`https://example.com`** 또는 기타 유효한 URL을 입력합니다. 나중에 이 임시 값을 대체합니다.
- **Sign-on URL(**로그인 **URL)** 필드에 **`https://sign-on.security.cisco.com/`**을 입력합니다.
- **Save(**저장**)**를 클릭하고 **Basic SAML Configuration(**기본 **SAML** 구성**)** 패널을 닫습니다.

i) **Required claim(**필수 클레임**)**에서 고유 사용자 식별자**(**이름 **ID)** 클레임을 클릭하여 편집합니다.
j) **Source(**소스**)** 속성 필드를 `user.userprincipalname`으로 설정합니다.

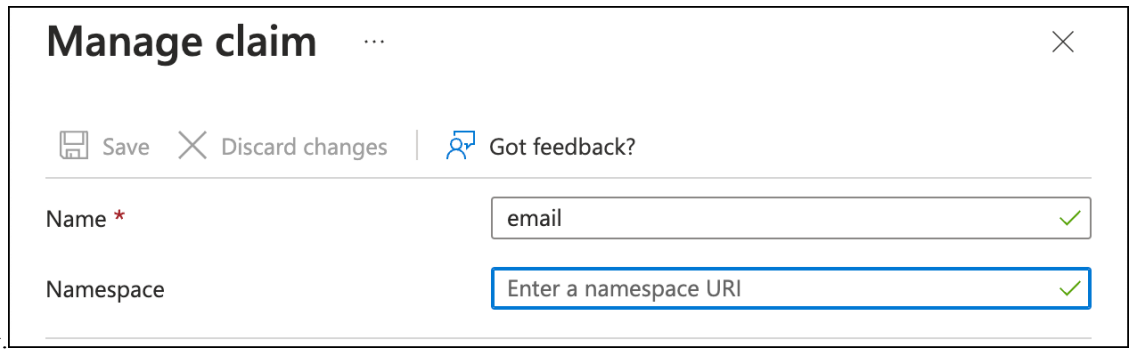
이 섹션에서는 **user.userprincipalname**의 값이 유효한 이메일 주소를 나타내는 것으로 가정합니다. 그렇지 않은 경우 **Source(**소스**)**가 **user.primaryauthoritativeemail**을 사용하도록 설정합니다.

k) **Additional Claims(**추가 클레임**)** 패널에서 **Edit(**편집**)**를 클릭하고 Azure AD 사용자 속성과 SAML 특성 간에 다음 매핑을 생성합니다.

이 섹션에서는 **user.userprincipalname**의 값이 유효한 이메일 주소를 나타내는 것으로 가정합니다. 그렇지 않은 경우 **email** 클레임의 **Source attribute(**소스 속성**)**이 **user.primaryauthoritativeemail**을 사용하도록 설정합니다.

이름	네임스페이스	소스 속성
`email`	값 없음	`user.userprincipalname`
`firstName`	값 없음	`user.givenname`
`lastName`	값 없음	`user.surname`

각 클레임에 대한 **Namespace(**네임스페이스**)** 필드의 선택을 취소해야 합니다



다.

l) **SAML Certificates(SAML** 인증서**)** 패널에서 인증서**(Base64)** 인증서에 대해 **Download(**다운로드**)**를 클릭합니다.

m) **Set up Single Sign-On with SAML(SAML**을 이용한 **SSO** 설정**)** 섹션에서 로그인 **URL** 및 **Azure AD** 식별자의 값을 복사하여 이 절차의 뒷부분에서 사용할 수 있습니다.

단계 **2** 새 브라우저 탭에서 Enterprise 설정 마법사를 엽니다. 현재 **Integrate Identity Provider(ID** 공급자 통합**) > Set Up(**설정**)** 화면(3단계: SAML 메타데이터 교환)에 있어야 합니다.

a) **Identity Provider (IdP) Name(ID** 공급자**(IdP)** 이름**)** 필드에 **`Azure SSO`** 또는 통합에 대한 다른 이름을 입력합니다.

b) Azure에서 복사한 **Login URL(**로그인 **URL)** 필드의 값을 **Single Sign-On Service URL** 필드에 입력합니다.

c) **Entity ID (Audience URI)(**엔터티 **ID(**대상 **URI))** 필드에 Azure에서 복사한 **Azure AD** 식별자 값을 입력합니다.

d) **Add File(**파일 추가**)**을 클릭하고 Azure 포털에서 다운로드한 SAML 서명 인증서를 업로드합니다.

e) 필요한 경우 사용자에 대해 무료 Duo MFA를 옵트아웃합니다.

f) **Download(**다운로드**)** 화면에서 **Next(**다음**)**를 클릭합니다.

g) 이 절차에서 나중에 사용할 수 있도록 **Single Sign-On Service URL (ACS URL)** 및 **Entity ID (Audience URI)** 필드의 값을 복사합니다.

h) **Next(**다음**)**를 클릭합니다.

단계 **3** Azure 콘솔 브라우저 탭으로 돌아갑니다.

a) **Basic SAML Configuration(**기본 **SAML** 구성**)** 섹션에서 **Edit(**편집**)**를 클릭합니다.

b) **Identifier (Entity ID)(**식별자 **(**엔터티 **ID))** 필드에서 입력한 임시 ID 공급자를 엔터프라이즈 설정 마법사에서 복사한 **Entity ID (Audience URI)(**엔터티 **ID(**대상 **URI))** 필드의 값으로 대체합니다.

c) **Reply URL (Assertion Consumer Service URL)(**회신 **URL(**어설션 소비자 서비스 **URL))** 필드에서 입력한 임시 ID 공급자를 엔터프라이즈 설정 마법사에서 복사한 **ACS URL(Single Sign-On Service URL)** 필드의 값으로 대체합니다.

d) **Save(**저장**)**를 클릭하고 **Basic SAML Configuration(**기본 **SAML** 구성**)** 패널을 닫습니다.

단계 **4** 엔터프라이즈 설정 마법사로 돌아가 통합을 테스트합니다. **Configure(**구성**)** 화면(4단계: SSO 통합 테스트)에 있어야 하며 다음을 수행해야 합니다.

a) 제공된 URL을 복사하여 개인(시크릿) 창을 엽니다.

b) SAML 애플리케이션과 연결된 Azure AD 계정으로 로그인합니다.
SecureX 애플리케이션 포털로 돌아가면 테스트가 성공한 것입니다. 오류가 발생하면 문제 해결의 내용을 참조하십시오.

c) **Next(**다음**)**를 클릭하여 활성화 화면으로 진행합니다.

d) 준비가 되면 **Activate my IdP(**내 **IdP** 활성화**)**를 클릭한 다음 대화 상자에서 선택을 확인합니다.