Externe Microsoft Entra ID SSO-Authentifizierung für DMP konfigurieren

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie die einmalige Anmeldung mit Microsoft Entra ID konfiguriert wird, um sich beim Cisco Domain Protection-Portal zu authentifizieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse zu folgenden Themen verfügen:

- Cisco Domänenschutz
- Microsoft Entra-ID
- Selbstsignierte oder CA-signierte (optional) X.509 SSL-Zertifikate im PEM-Format

Verwendete Komponenten

- Administratorzugriff auf Cisco Domain Protection
- Administratorzugriff auf das Microsoft Entra ID Admin Center

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

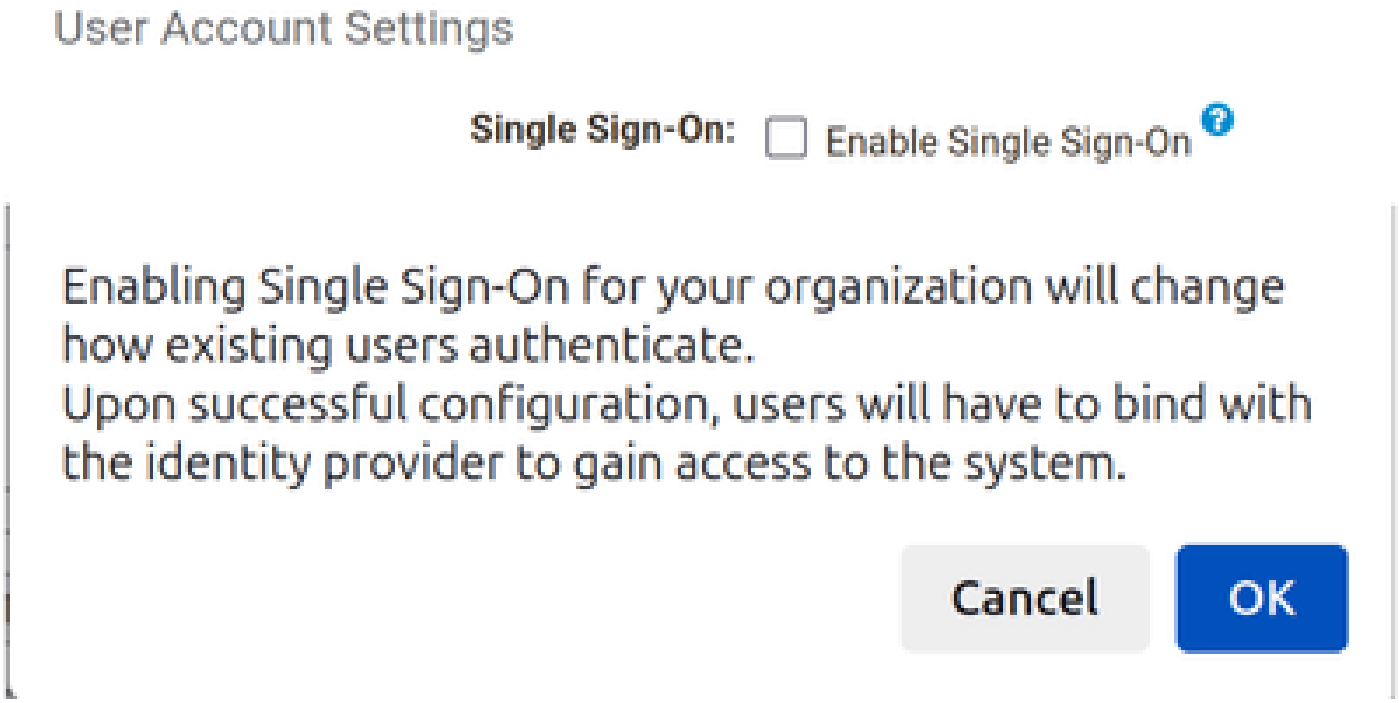
- Cisco Domain Protection aktiviert die SSO-Anmeldung für Endbenutzer über das SAML 2.0-Protokoll.
- Microsoft Entra SSO ermöglicht und steuert den Zugriff auf Ihre SaaS-Anwendungen (Software-as-a-Service), Cloud-Anwendungen oder Anwendungen vor Ort von einem beliebigen Standort aus durch einmalige Anmeldung.
- Cisco Domain Protection kann als verwaltete Identitätsanwendung festgelegt werden, die mit Microsoft Entra verbunden ist. Hierzu stehen Authentifizierungsmethoden zur Verfügung, die eine mehrstufige Authentifizierung beinhalten, da eine Authentifizierung nur über ein Kennwort nicht sicher ist und nicht empfohlen wird.
- SAML ist ein XML-basiertes, offenes Standarddatenformat, das es Administratoren ermöglicht, nach der Anmeldung bei einer dieser Anwendungen nahtlos auf einen definierten Satz von Anwendungen zuzugreifen.
- Weitere Informationen zu SAML finden Sie unter: Was ist SAML?

Konfigurieren

Cisco Domain Protection (Teil 1)

1. Melden Sie sich beim Cisco Domain Protection-Admin-Portal an, und navigieren Sie zu Admin > Organization. Klicken Sie auf die Schaltfläche Edit Organization Details (Organisationsdetails bearbeiten), wie in der Abbildung dargestellt:

2. Navigieren Sie zum Abschnitt Benutzerkonteneinstellungen, und klicken Sie auf das Kontrollkästchen Single Sign-On aktivieren. Eine Meldung wird angezeigt, wie in der Abbildung dargestellt:

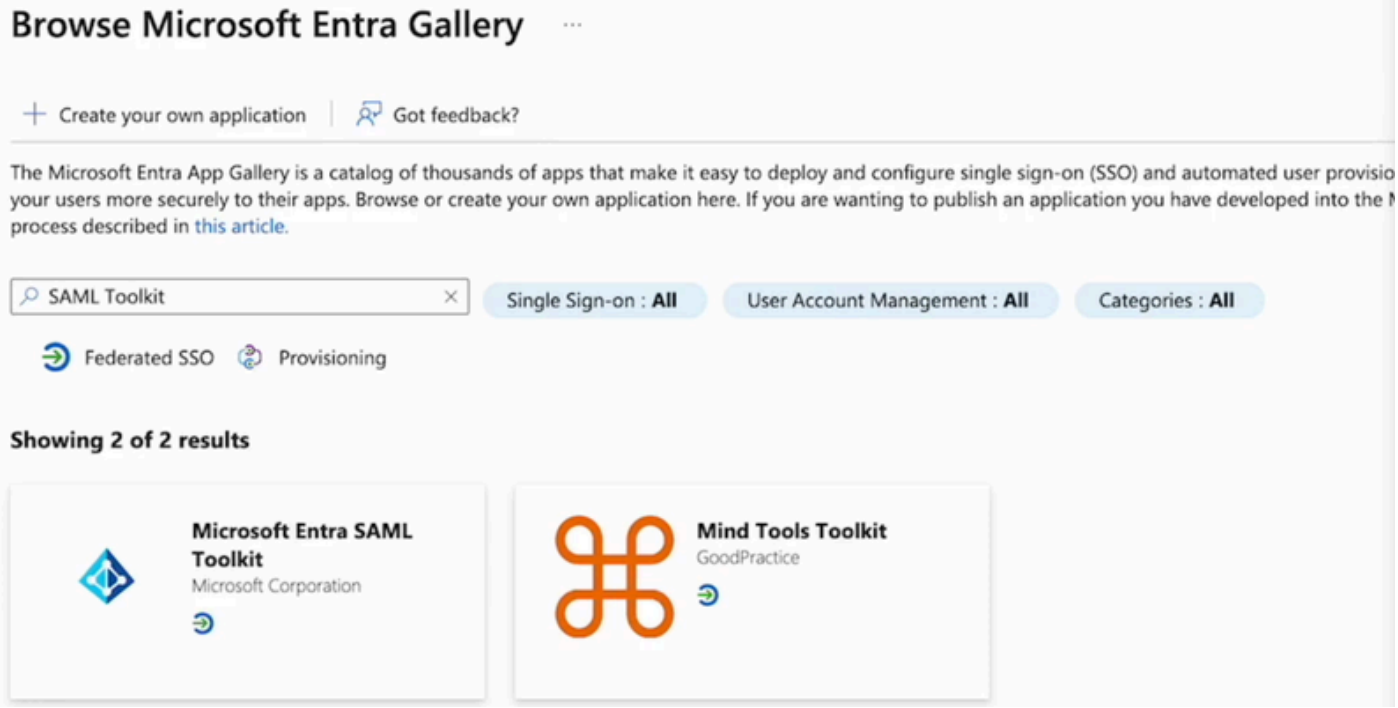


3. Klicken Sie auf die Schaltfläche OK, und kopieren Sie die URL-Parameter für die Objektkennung und den Assertion Consumer Service (ACS). Diese Parameter müssen bei der Microsoft Entra ID Basic SAML-Authentifizierung verwendet werden. Später zurückgeben, um das Name Identifier Format, SAML 2.0 Endpoint und öffentliche Zertifikatparameter einzurichten.

- Element-ID: dmp.cisco.com
- Assertion Consumer Service-URL:https://<dmp_id>.dmp.cisco.com/auth/saml/callback

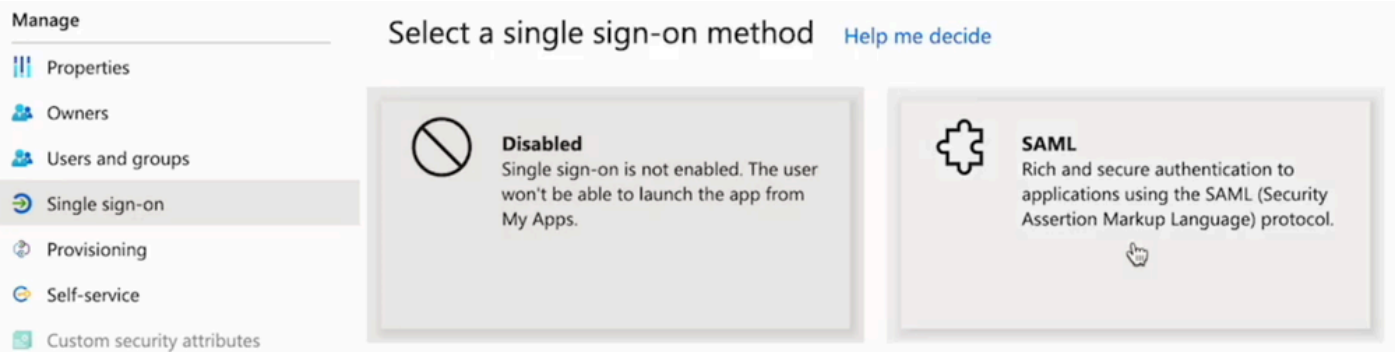
Microsoft Entra-ID

1. Navigieren Sie zum Microsoft Entra ID-Admin-Center, und klicken Sie auf die Schaltfläche Hinzufügen. Wählen Sie Enterprise Application aus, und suchen Sie nach Microsoft Entra SAML Toolkit, wie im Bild dargestellt:



2. Geben Sie ihm einen aussagekräftigen Namen, und klicken Sie auf Erstellen. Beispiel: Domain Protection Sign On.

3. Navigieren Sie zur linken Seite, unter dem Abschnitt Verwalten. Klicken Sie auf Single Sign-on, und wählen Sie SAML aus.



4. Klicken Sie im Bedienfeld "SAML-Basiskonfiguration" auf Bearbeiten, und geben Sie die folgenden Parameter ein:

- Kennung (Element-ID): dmp.cisco.com
- Antwort-URL (Assertion Consumer Service-URL): https://<dmp_id>.dmp.cisco.com/auth/saml/callback
- Anmelde-URL: https://<dmp_id>.dmp.cisco.com/auth/saml/callback
- Klicken Sie auf Speichern.

5. Klicken Sie im Bereich Attribute & Ansprüche auf Bearbeiten.

Klicken Sie unter Erforderlicher Anspruch auf den Anspruch Eindeutige Benutzerkennung (Name-ID), um ihn zu bearbeiten.

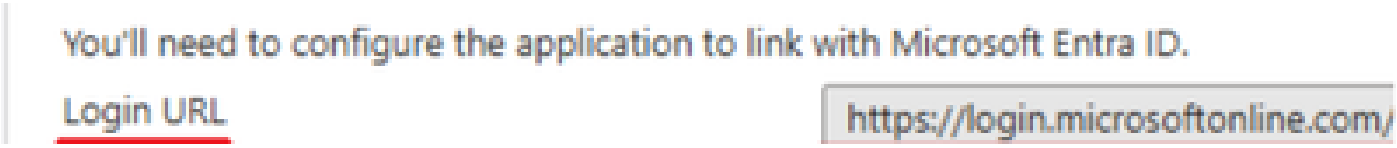
- Legen Sie das Feld Source-Attribut auf user.userprincipalname fest. Dabei wird davon ausgegangen, dass der Wert von user.userprincipalname eine gültige E-Mail-Adresse darstellt. Falls nicht, setzen Sie Source auf user.primaryautoritativeEmail.
- Klicken Sie unter Zusätzlicher Anspruchsbereich auf Bearbeiten, und erstellen Sie die Zuordnungen zwischen Microsoft Entra ID-Benutzereigenschaften und SAML-Attributen.

Name	Namespace	Quellattribut
Email-Adresse	Kein Wert	user.userprincipalname
Vorname	Kein Wert	user.givenname
Nachname	Kein Wert	Benutzer.Nachname

Vergewissern Sie sich, dass Sie das Feld Namespace für jeden Anspruch löschen, wie unten gezeigt:

6. Nach dem Ausfüllen der Abschnitte Attribute und Ansprüche wird der letzte Abschnitt des SAML-Signaturzertifikats ausgefüllt.

- Speichern der Anmelde-URL

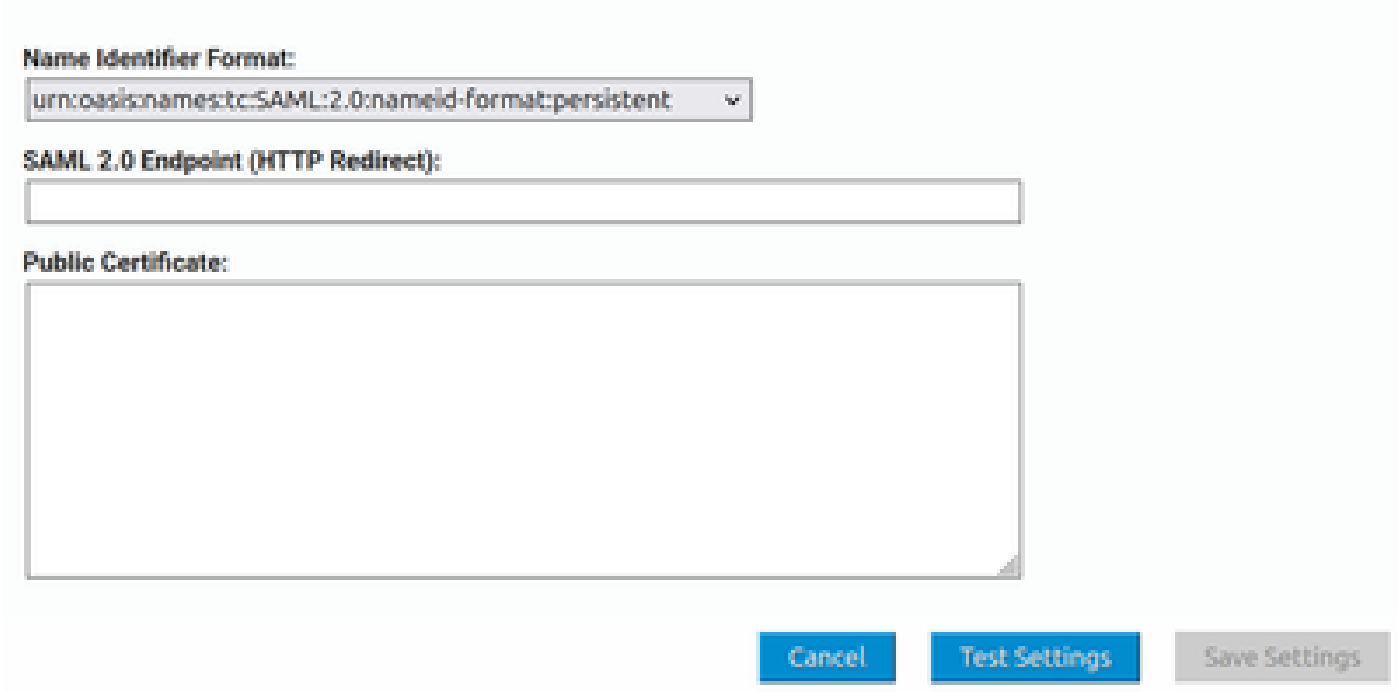


- Speichern Sie das Zertifikat (Base64).

Cisco Domain Protection (Teil 2)

Kehren Sie zum Abschnitt Cisco Domain Protection > Single Sign-On aktivieren zurück.

- Name Identifier Format: urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
- SAML 2.0-Endpunkt (HTTP Redirect): Von Microsoft Entra ID bereitgestellte Anmelde-URL
- Öffentliches Zertifikat: Zertifikat (Base64) bereitgestellt durch Microsoft Entra ID



Überprüfung

Klicken Sie auf Testeinstellungen. Es leitet Sie zur Anmeldeseite Ihres Identitätsanbieters um. Melden Sie sich mit Ihren SSO-Anmeldeinformationen an.

Nach erfolgreicher Anmeldung können Sie das Fenster schließen. Klicken Sie auf Einstellungen speichern.

Fehlerbehebung

```
Error - Error parsing X509 certificate
```

- Stellen Sie sicher, dass das Zertifikat Base64 enthält.

```
Error - Please enter a valid URL
```

- Stellen Sie sicher, dass die von der Microsoft Entra-ID bereitgestellte Anmelde-URL richtig ist.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.