Externe Microsoft Entra ID SSO-Authentifizierung für CRES konfigurieren

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Microsoft Entra ID Single Sign-on für die Authentifizierung beim Cisco Secure Email Encryption Service konfiguriert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Sicherer E-Mail-Verschlüsselungsdienst (registrierter Umschlag)
- Microsoft Entra-ID
- Selbstsignierte oder CA-signierte (optional) X.509 SSL-Zertifikate im PEM-Format

Verwendete Komponenten

- Administratorzugriff auf den Secure Email Encryption Service (registrierter Umschlag)
- 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.

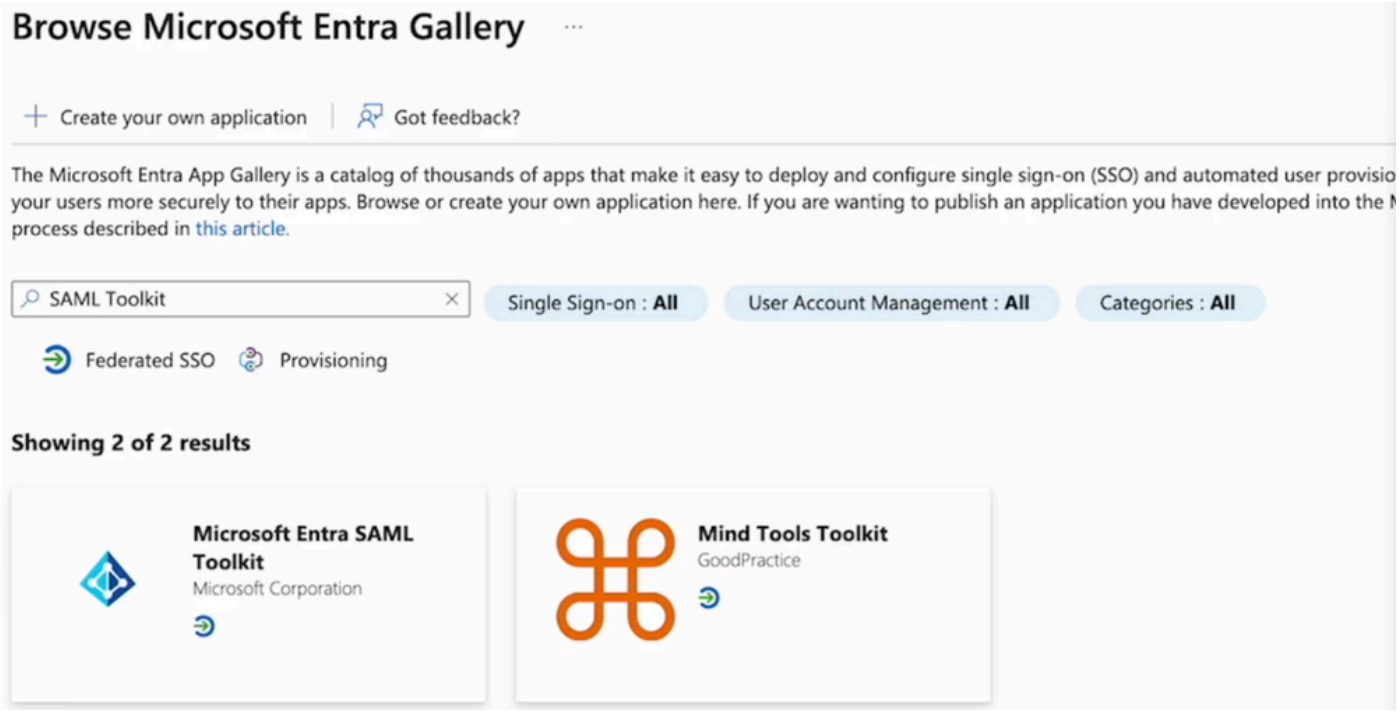
Hintergrundinformationen

- Registrierter Umschlag ermöglicht SSO-Anmeldung für Endbenutzer, die SAML verwenden.
- 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.
- Der registrierte Umschlag kann als verwaltete Identitätsanwendung festgelegt werden, die mit Microsoft Entra verbunden ist. Hierzu werden Authentifizierungsmethoden verwendet, die eine mehrstufige Authentifizierung beinhalten, da eine nur mit Kennwort durchgeführte Authentifizierung weder sicher noch empfohlen ist.
- 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

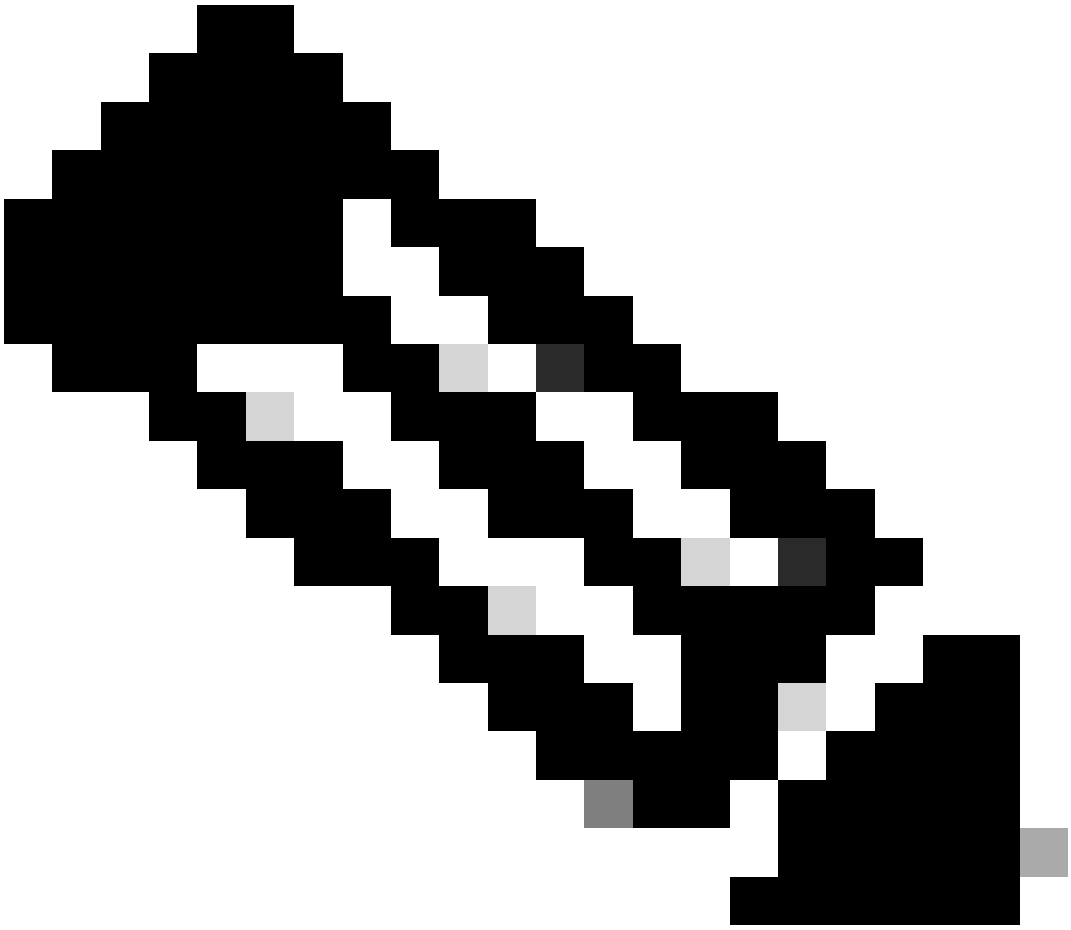
Microsoft Entra-ID

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 gezeigt:



Microsoft Entra-Katalog durchsuchen

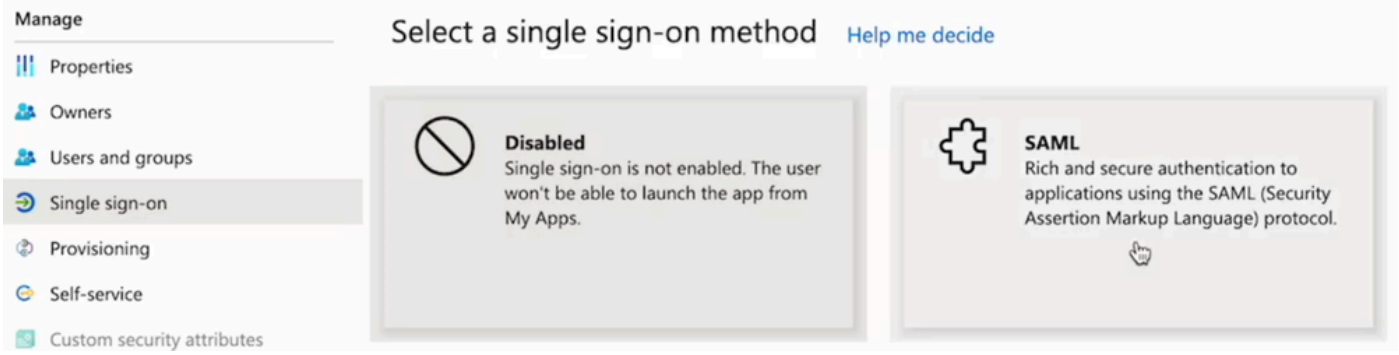
2. Geben Sie ihm einen aussagekräftigen Namen, und klicken Sie auf Erstellen. Beispiel: CRES Single Sign On.



> Anmerkung: Damit sich alle Benutzer beim CRES-Portal anmelden können, müssen Sie die erforderliche Zuweisung unter den SAML-Toolkit-Eigenschaften (CRES-Anmeldung) manuell deaktivieren und für die erforderliche Zuweisung die Option Nein auswählen.

---

3. Navigieren Sie zum linken Bereich, klicken Sie unter dem Abschnitt Verwalten auf Single Sign-on, und wählen Sie SAML aus.



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

- Kennung (Element-ID): https://res.cisco.com/
- Antwort-URL (Assertion Consumer Service-URL): https://res.cisco.com/websafe/ssourl
- Anmelde-URL: https://res.cisco.com/websafe/ssourl
- 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.

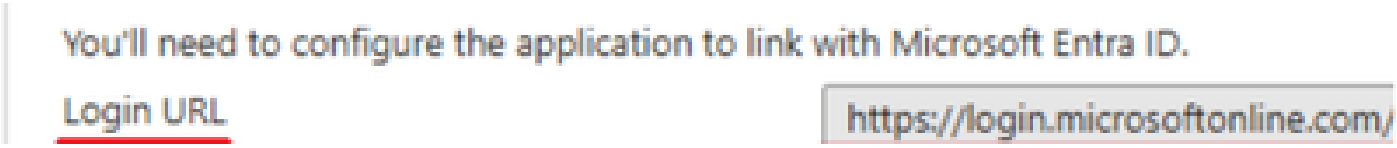
- Legen Sie das Feld Source-Attribut auf user.userprincipalname fest. Dabei wird davon ausgegangen, dass der Wert von user.userprincipalname eine gültige E-Mail-Adresse darstellt. Falls nicht, setzen Sie Source auf user.primaryautoritativeEmail.
- Klicken Sie unter Zusätzlicher Anspruchsbereich auf Bearbeiten, 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 Sie die nächsten Werte, die im CRES-Portal erforderlich sind:

- Speichern Sie die Anmelde-URL.



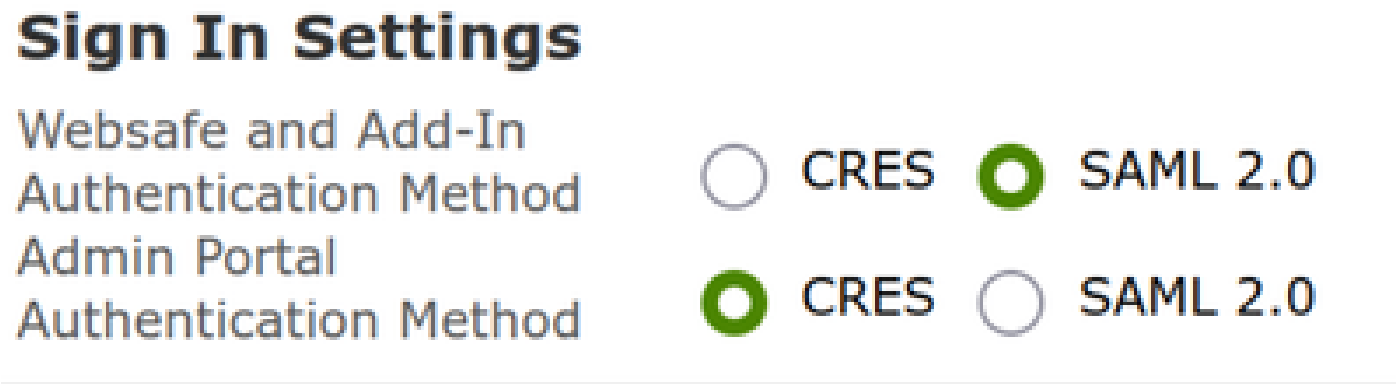
- Klicken Sie auf den Link Certificate (Base64) Download.

Cisco Email Encryption Service

1. Melden Sie sich als Administrator beim Organisationsportal des Secure Email Encryption Service an.

2. Wählen Sie auf der Registerkarte Konten die Registerkarte Konten verwalten, und klicken Sie auf Ihre Kontonummer.

3. Navigieren Sie auf der Registerkarte Details zur Authentifizierungsmethode, und wählen Sie SAML 2.0 aus.



4.- Tragen Sie die folgenden Angaben ein:

- Alternativer SSO-E-MailAttribute-Name: Email-Adresse
- Einheitenkennung des SSO-Dienstanbieters*: https://res.cisco.com/
- SSO-Kundenservice-URL*: Dieser Link wird von Entra ID bereitgestellt, unter
- SSO-Abmelde-URL: leer lassen

5.- Klicken Sie auf SAML aktivieren.

Überprüfung

Es wird ein neues Fenster angezeigt, in dem bestätigt wird, dass nach einer erfolgreichen Anmeldung die SAML-Authentifizierung aktiviert wurde. Klicken Sie auf "Weiter". Sie werden zur

Anmeldeseite Ihres Identitätsanbieters umgeleitet. Melden Sie sich mit Ihren SSO-Anmeldeinformationen an. Nach einer erfolgreichen Anmeldung können Sie das Fenster schließen. Klicken Sie auf Speichern.

Fehlerbehebung

Wenn das Fenster Sie nicht zur Anmeldeseite Ihres Identitätsanbieters umgeleitet hat, wird ein Ablaufverfolgungsbericht zurückgegeben, der Sie mit dem Fehler versorgt. Überprüfen Sie die Attribute und Ansprüche, stellen Sie sicher, dass sie mit dem gleichen Namen wie im Abschnitt CRES-Authentifizierungsmethode konfiguriert sind. Die bei der SAML-Anmeldung verwendete E-Mail-Adresse des Benutzers muss mit der E-Mail-Adresse in CRES übereinstimmen. Verwenden Sie keine Aliase.

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.