

Microsoft Entra ID SSO External Authentication configureren voor CRES

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Microsoft Entra ID](#)

[Cisco Email Encryption Service](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

In dit document wordt beschreven hoe u Microsoft Entra ID Single Sign-on configureert voor verificatie naar de Cisco Secure Email Encryption Service.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Beveiligde e-mailcoderingsservice (geregistreerde envelop)
- Microsoft Entra ID
- Zelf ondertekende of CA ondertekende (optioneel) X.509 SSL-certificaten in PEM-formaat

Gebruikte componenten

- Beheerderstoegang voor de Secure Email Encryption Service (Registered Envelope)
- Beheerderstoegang Microsoft Entra ID

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

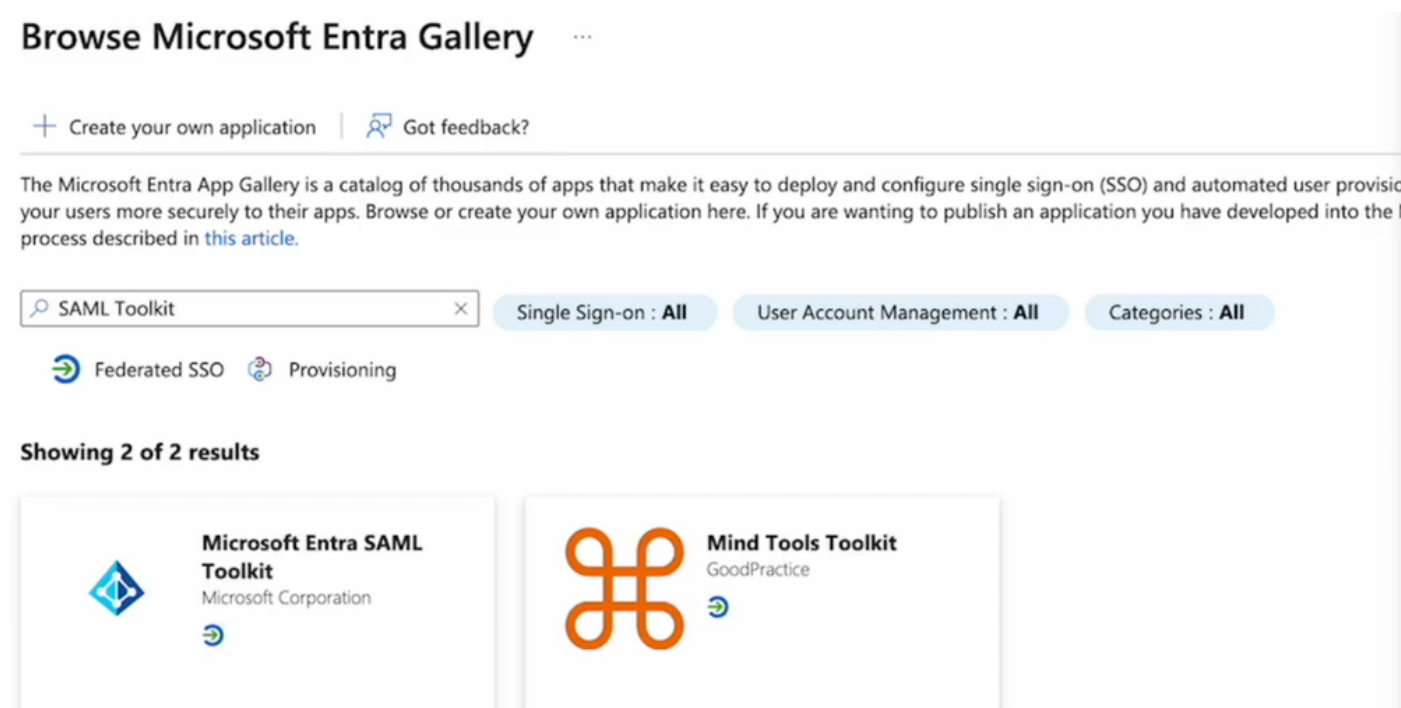
Achtergrondinformatie

- Geregistreerde envelop maakt SSO-aanmelding mogelijk voor eindgebruikers die SAML gebruiken.
- Microsoft Entra SSO biedt toegang tot uw software-as-a-service (SaaS)-apps, cloud-apps of on-premises apps vanaf elke locatie met eenmalige aanmelding.
- Geregistreerde envelop kan worden ingesteld als een beheerde identiteitstoepassing die is verbonden met Microsoft Entra met verificatiemethoden die multi-factor-verificatie bevatten, omdat alleen-wachtwoordverificatie niet veilig is en niet wordt aanbevolen.
- SAML is een op XML gebaseerde open standaard data-indeling die beheerders in staat stelt om naadloos toegang te krijgen tot een gedefinieerde set applicaties na het aanmelden bij een van die applicaties.
- Voor meer informatie over SAML, zie: [Wat is SAML?](#)

Configureren

Microsoft Entra ID

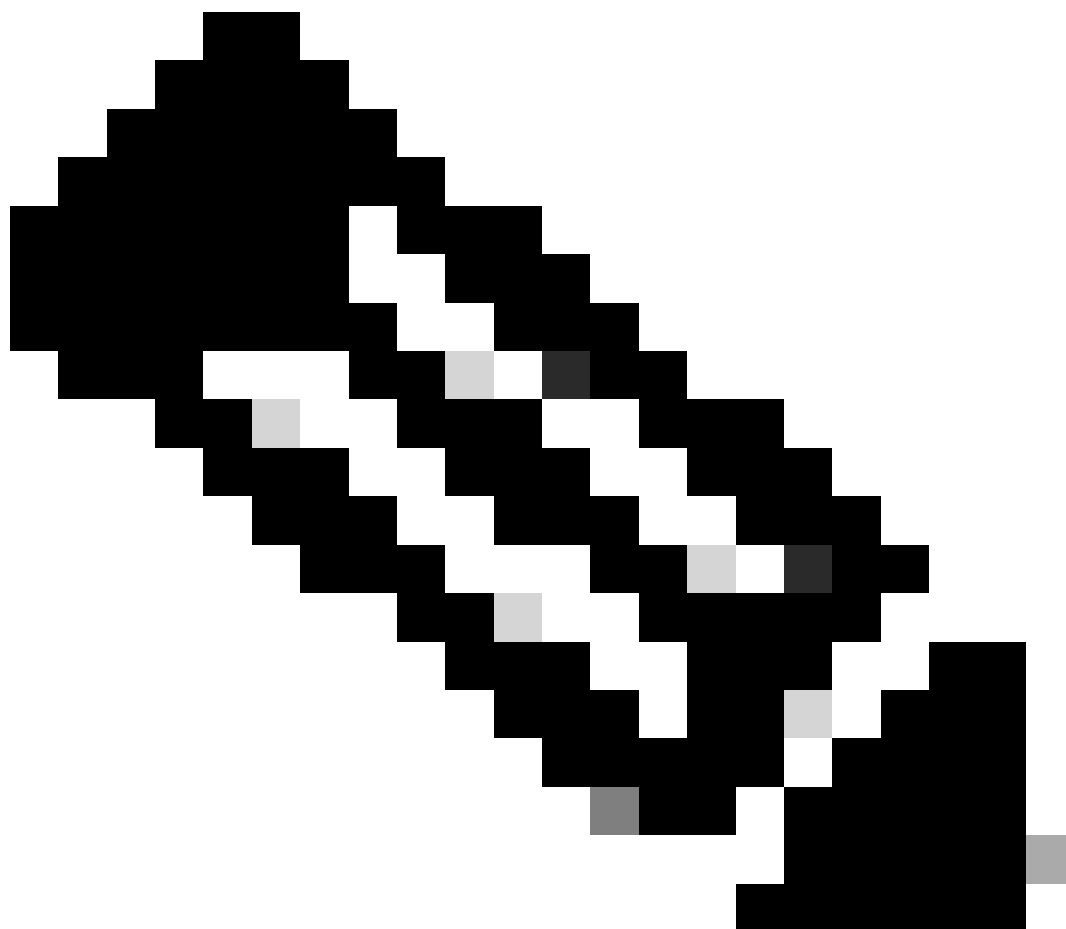
1. Navigeer naar het Microsoft Entra ID-beheercentrum en klik op de knop Toevoegen. Selecteer Enterprise Application en zoek naar Microsoft Entra SAML Toolkit, zoals weergegeven in de afbeelding:



Bladeren door Microsoft Entra Gallery

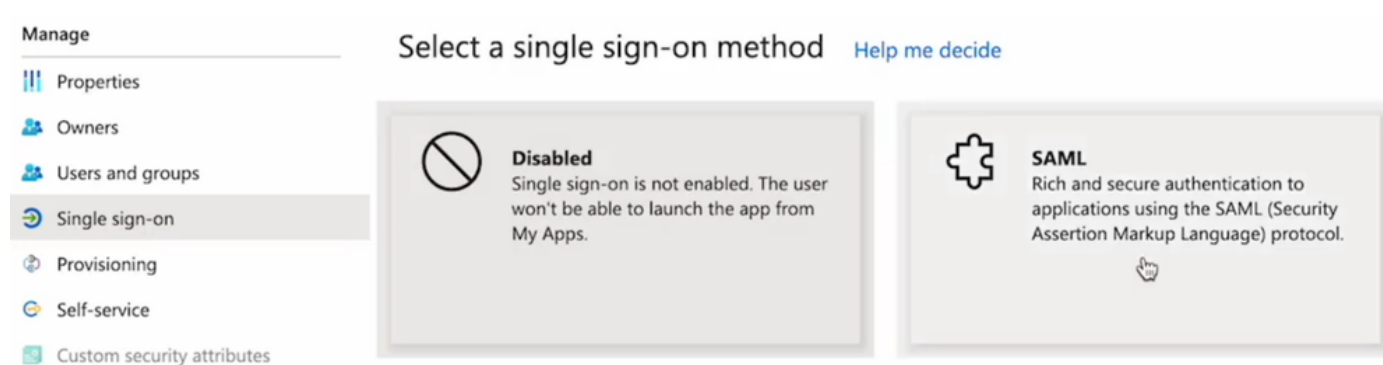
2. Noem het met een betekenisvolle waarde en klik op Maken. Bijvoorbeeld CRES Single Sign

On.



Opmerking: Als u wilt dat alle gebruikers zich kunnen aanmelden bij het CRES-portaal, moet u handmatig Vereiste toewijzing uitschakelen onder de eigenschappen CRES Sign On (SAML-toolkit) en voor Toewijzing Vereist selecteer Nee.

3. Navigeer naar het linkerzijpaneel, klik onder de sectie Beheren op Eenmalige aanmelding en selecteer SAML.



4. Klik in het deelvenster Basisconfiguratie van SAML op Bewerken en vul de kenmerken als volgt in:

- Identificatiecode (Entiteit-ID): <https://res.cisco.com/>
- Beantwoord-URL (Bewering Consumer Service-URL): <https://res.cisco.com/websafe/ssourl>
- Inloggen op URL: <https://res.cisco.com/websafe/ssourl>
- Klik op Save (Opslaan).

5. Klik in het deelvenster Kenmerken en claims op Bewerken.

Klik onder Vereiste claim op de unieke gebruikersidentificatiecode (naam-ID) om deze te bewerken.

- Stel het attribuutveld Bron in op user.userprincipalname. Hierbij wordt ervan uitgegaan dat de waarde van user.userprincipalname een geldig e-mailadres vertegenwoordigt. Als dit niet het geval is, stelt u Bron in op user.primary authoritative email.
- Klik onder het paneel Extra claims op Bewerken en maak de toewijzingen tussen de gebruikerseigenschappen van Microsoft Entra ID en SAML-kenmerken.

Naam	naamruimte	bronkenmerk
e-mailadres	Geen waarde	user.userprincipalname
voornaam	Geen waarde	user.givenname
achternaam	Geen waarde	user.surname

Zorg ervoor dat u het veld Naamruimte voor elke claim wist, zoals hieronder wordt weergegeven:

Namespace	Enter a namespace URI
-----------	--

6. Zodra de secties Attributen en claims zijn ingevuld, wordt de laatste sectie SAML-ondertekeningscertificaat ingevuld. Sla de volgende waarden op zoals ze in het CRES-portaal zijn vereist:

- Sla de inlog-URL op.

You'll need to configure the application to link with Microsoft Entra ID.

Login URL

<https://login.microsoftonline.com/>

- Selecteer de link Certificaat (Base64) Downloaden.

Certificate (Base64)

Download

Cisco Email Encryption Service

1. Meld u als beheerder aan bij het organisatieportaal van de Secure Email Encryption Service.
2. Selecteer op het tabblad Accounts het tabblad Accounts beheren en klik op uw accountnummer.
3. Blader op het tabblad Details naar de verificatiemethode en selecteer SAML 2.0.

Sign In Settings

Websafe and Add-In
Authentication Method
Admin Portal
Authentication Method

☐ CRES ☒ SAML 2.0
☒ CRES ☐ SAML 2.0

4.- Vul de kenmerken als volgt in:

- Naam alternatief e-mailkenmerk voor eenmalige aanmelding: e-mailadres
- Entiteits-ID SSO-serviceprovider*: <https://res.cisco.com/>
- Klantenservice-URL voor eenmalige aanmelding*: Deze link wordt verstrekt door Entra ID, onder
- SSO-afmeldings-URL: leeg laten

5.- Klik op SAML activeren.

Verifiëren

Er verschijnt een nieuw venster waarin wordt bevestigd dat na een succesvolle aanmelding de SAML-verificatie is ingeschakeld. Klik op Next (Volgende). Het leidt u door naar de inlogpagina van uw Identity Provider. Log in met uw SSO-referenties. Na een succesvolle aanmelding kunt u het venster sluiten. Klik op Save (Opslaan).

Problemen oplossen

Als het venster u niet heeft doorgestuurd naar de aanmeldpagina van uw identiteitsprovider, wordt een traceringsgeretourneerd die u de fout geeft. Controleer de Attributen en claims, zorg ervoor dat deze is geconfigureerd met dezelfde naam als in de sectie CRES-verificatiemethode. Het e-mailadres van de gebruiker dat wordt gebruikt in de SAML-aanmelding moet overeenkomen met het e-mailadres in CRES. Gebruik geen aliassen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.