Microsoft Entra ID SSO External Authentication for DMP configureren

Inhoud

Inleiding

In dit document wordt beschreven hoe u Microsoft Entra ID voor eenmalige aanmelding configureert voor verificatie naar het Cisco Domain Protection-portaal.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben over deze onderwerpen:

- Cisco Domain Protection
- Microsoft Entra ID
- Zelf ondertekende of CA ondertekende (optioneel) X.509 SSL-certificaten in PEM-formaat

Gebruikte componenten

- Beheerderstoegang tot Cisco Domain Protection
- 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

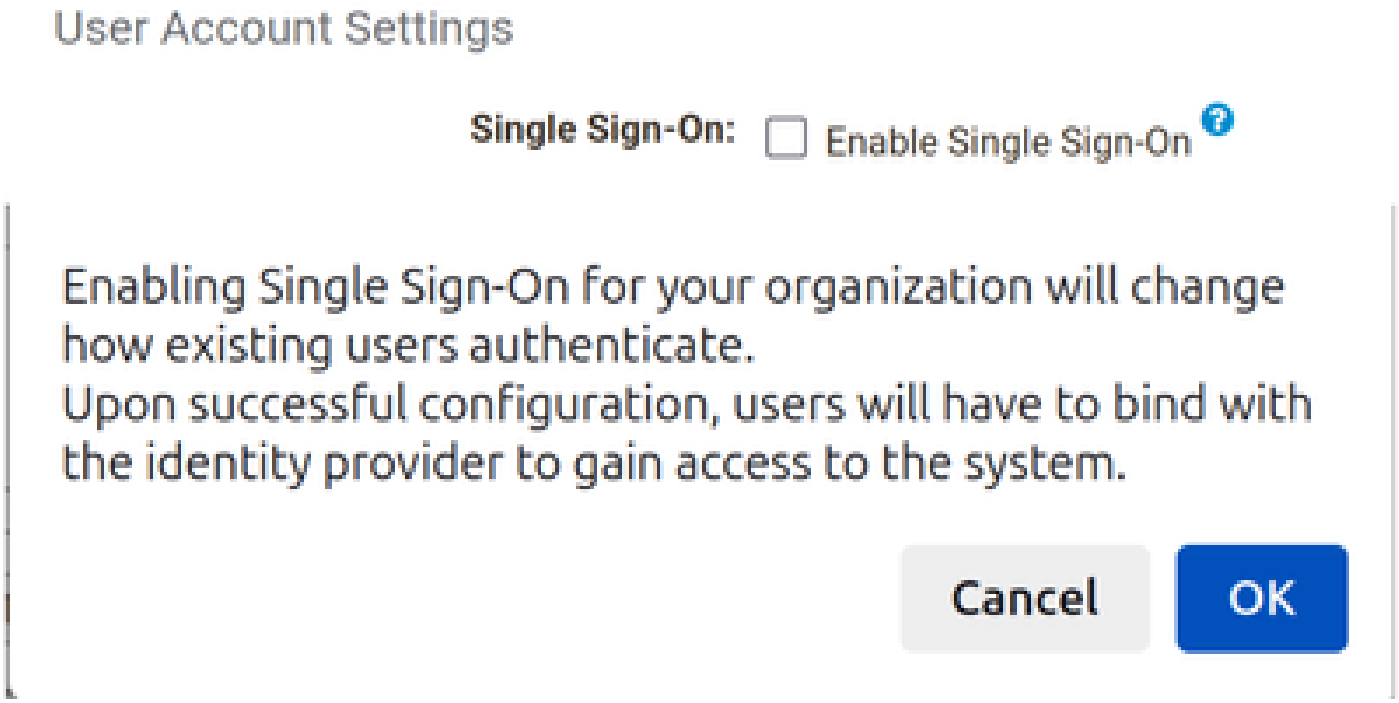
- Cisco Domain Protection maakt het mogelijk dat eindgebruikers zich via het SAML 2.0-protocol bij SSO aanmelden.
- Microsoft Entra SSO biedt toegang tot uw software-as-a-service (SaaS)-apps, cloud-apps of on-premises apps vanaf elke locatie met eenmalige aanmelding.
- Cisco Domain Protection kan worden ingesteld als een beheerde identiteitstoepassing die is verbonden met Microsoft Entra met verificatiemethoden die multi-factor-verificatie bevatten, omdat alleen-wachtwoord-verificatie 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

Cisco Domain Protection (deel 1)

1. Meld u aan bij het beheerportaal voor Cisco Domain Protection en navigeer naar Beheer > Organisatie. Klik op de knop Organisatiedetails bewerken, zoals in de afbeelding wordt weergegeven:

2. Navigeer naar het gedeelte Gebruikersaccountinstellingen en klik op Enkelvoudige aanmelding inschakelen. Er verschijnt een bericht zoals weergegeven in de afbeelding:

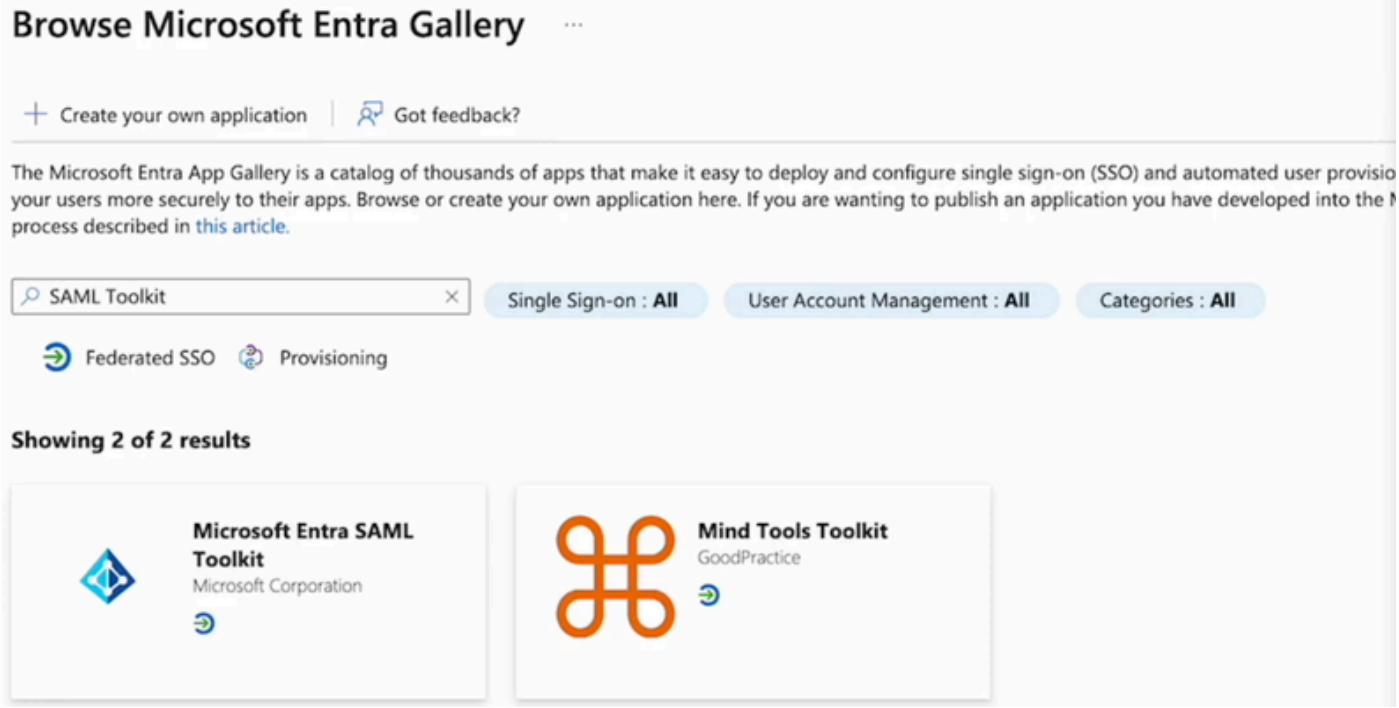


3. Klik op de knop OK en kopieer de URL-parameters Entity ID en Assertion Consumer Service (ACS). Deze parameters moeten worden gebruikt in Microsoft Entra ID Basic SAML-verificatie. Ga later terug voor het instellen van de parameters Name Identifier Format, SAML 2.0 Endpoint en Public Certificate.

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

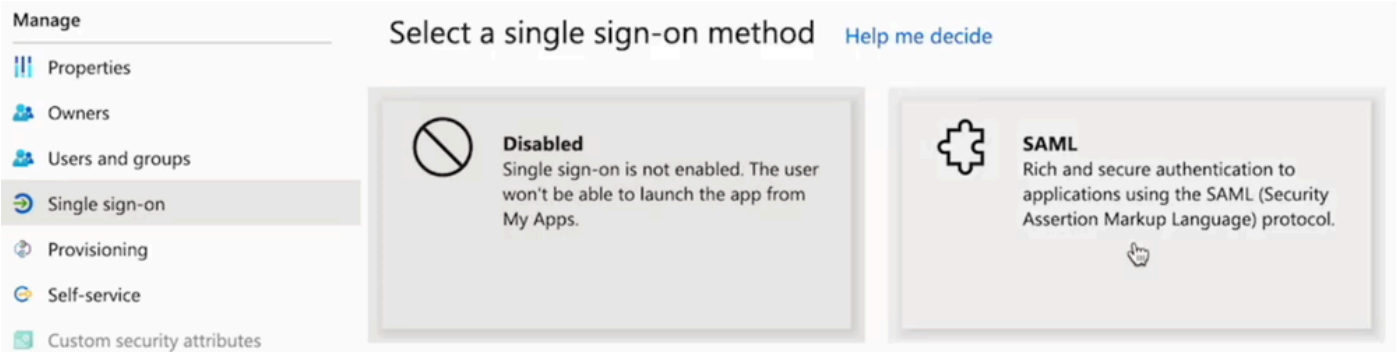
Microsoft Entra ID

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:



2. Noem het met een betekenisvolle waarde en klik op Maken. Bijvoorbeeld aanmelden voor domeinbescherming.

3. Navigeer naar het linkerzijpaneel onder het gedeelte Beheer. Klik op Eenmalige aanmelding en selecteer SAML.



4. Klik in het paneel Basisconfiguratie van SAML op Bewerken en vul de parameters in:

- Identificatiecode (Entiteit-ID): dmp.cisco.com
- Beantwoord-URL (Bewering Consumer Service-URL): https://<dmp_id>.dmp.cisco.com/auth/saml/callback
- Aanmelden URL: https://<dmp_id>.dmp.cisco.com/auth/saml/callback
- 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.

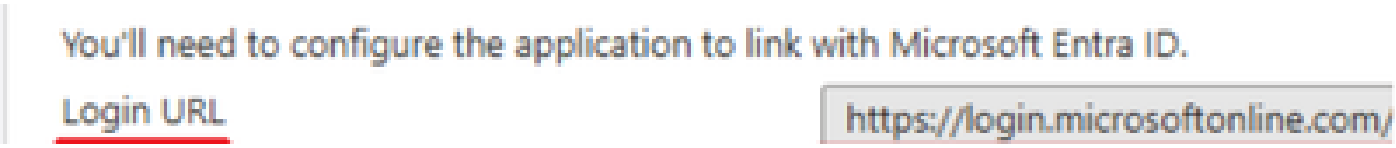
- Stel het veld Bronattribuut in op user.userprincipalname. Hierbij wordt ervan uitgegaan dat de waarde van user.userprincipalname een geldig e-mailadres vertegenwoordigt. Als dit niet het geval is, stelt u Bron in op user.primary authoritative email.
- Klik onder het paneel Extra claims op Bewerken 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:

6. Zodra de secties Attributen en claims zijn ingevuld, wordt de laatste sectie SAML-ondertekeningscertificaat ingevuld.

- Sla de inlog-URL op.

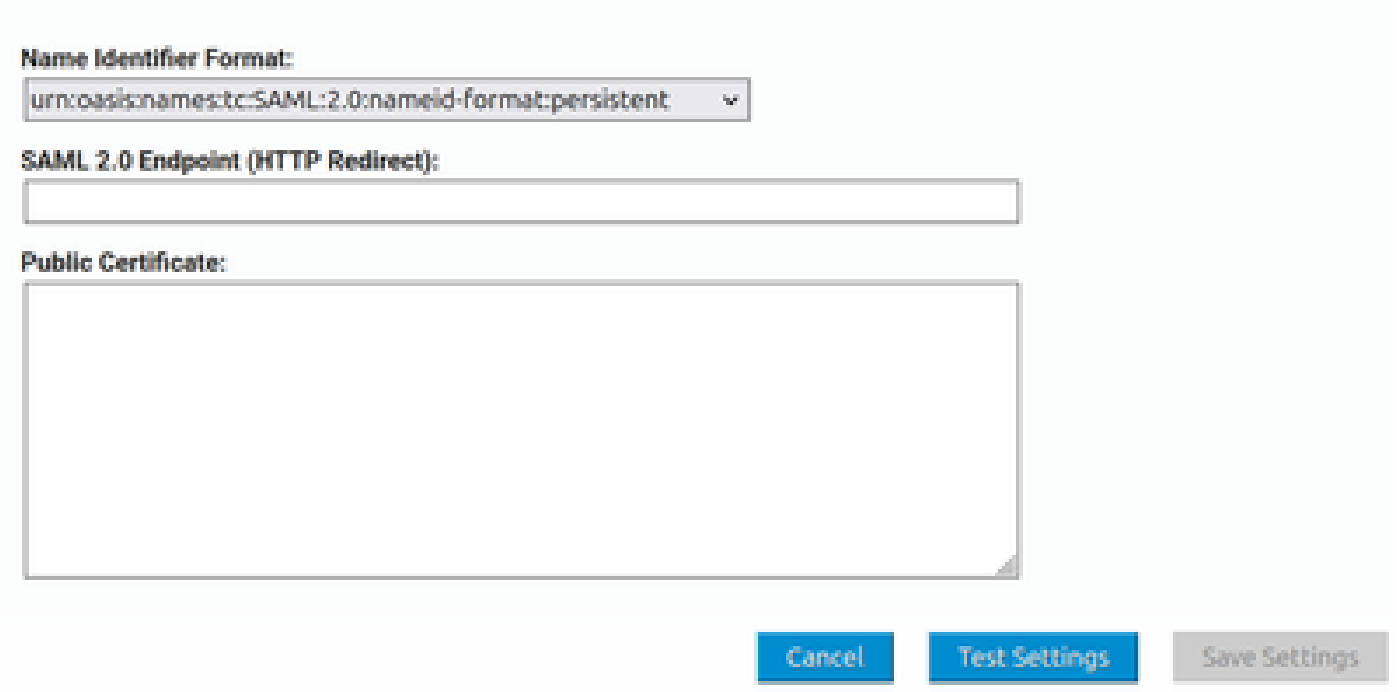


- Bewaar het certificaat (Base64).

Cisco Domain Protection (deel 2)

Ga terug naar Cisco Domain Protection > Single Sign-On sectie inschakelen.

- Name Identifier Format: urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
- SAML 2.0-eindpunt (HTTP-omleiding): aanmeldings-URL verstrekt door Microsoft Entra ID
- Publiek certificaat: certificaat (Base64) verstrekt door Microsoft Entra ID



Verifiëren

Klik op Testinstellingen. 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 Instellingen opslaan.

Problemen oplossen

`Error - Error parsing X509 certificate`

- Zorg ervoor dat het certificaat in Base64 staat.

`Error - Please enter a valid URL`

- Controleer of de aanmeldings-URL van Microsoft Entra ID juist is.

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.