Beveiligde bescherming tegen e-mailbedreigingen: verificatie met meerdere factoren en toegangscontroles

Inhoud

Inleiding

In dit document worden de mogelijkheden beschreven die Cisco Email Threat Defense (ETD) biedt om beheerderstoegang tot de beheerconsole te beheren.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van deze onderwerpen om ETD-verificatie met Duo te configureren:

- Een Cisco ETD-abonnement
- Cisco Security Cloud Control (SCC)
- Een verificatieoplossing voor verbeterde beveiliging, in dit geval Cisco Duo.

Gebruikte componenten

Dit document is beperkt tot Email Treat Defense en Secure Cloud Control.

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

Dit document richt zich op de manier waarop Cisco ETD gebruikmaakt van Cisco SCC en integreert met Cisco Duo om veilige verificatie en granulaire toegangscontrole te leveren.

In moderne cloudgebaseerde oplossingen is toegangscontrole een van de meest kritieke componenten voor het waarborgen van gegevensbeveiliging, naleving van regelgeving en operationele integriteit. Ongeautoriseerde toegang, met name tot beheerdersaccounts, kan leiden tot ernstige gevolgen, zoals gecompromitteerde systemen, datalekken en serviceonderbrekingen.

Cisco biedt robuuste beveiligingsmogelijkheden in zijn cloudportfolio, waaronder Multifactor Authentication (MFA)-technologie, die een integraal onderdeel is van services zoals Cisco ETD. MFA voegt een kritische verificatiestap toe die verder gaat dan traditionele wachtwoorden en vereist dat gebruikers zich authenticeren via een extra factor, zoals een goedkeuring van een mobiele applicatie, beveiligingstoken of biometrische verificatie.

Om het authenticatieproces van de beheerder te stroomlijnen en te versterken, maakt ETD gebruik van Cisco SCC, een gecentraliseerde authenticatie- en beleidsbeheerservice.

Via SCC krijgt ETD toegang tot een breed scala aan beveiligingsfuncties, waaronder:

- MFA-handhaving om risico's op diefstal van referenties te beperken.
- Integratie met externe identiteitsproviders zoals Cisco Duo, Microsoft Entra ID, Okta en anderen om flexibele verificatieworkflows en federatie van bedrijfsidentiteiten te ondersteunen.
- Gecentraliseerde beleidsadministratie, waardoor consistente toegangsregels voor Cisco-cloudservices mogelijk zijn.

Met name Cisco Duo breidt deze mogelijkheden uit door geavanceerd toegangsbeheer op basis van beleidsregels toe te voegen. Met behulp van SCC als integratiekanaal kan ETD gedetailleerde besturingselementen van Duo, zoals bron-IP-beperkingen, healthchecks van apparaten en op gebruikersgroepen gebaseerde regels, rechtstreeks toepassen op beheerderstoegang.

Organisaties kunnen bijvoorbeeld een beleid definiëren dat alleen toegang biedt vanuit specifieke vertrouwde netwerkbereiken. Elke poging tot verbinding buiten de geautoriseerde IP-lijst kan automatisch worden geblokkeerd, zoals wordt geïllustreerd in de bijbehorende diagrammen. Deze combinatie van MFA + contextueel beleid maakt een diepgaande defensieaanpak mogelijk, waardoor wordt gewaarborgd dat zelfs als de geloofsbrieven in het gedrang komen, aanvallers nog steeds geen toegang hebben tot het systeem, tenzij ze ook aan aanvullende beveiligingscriteria voldoen.

Door Cisco ETD, Cisco SCC en Cisco Duo samen te voegen, kunnen bedrijven een veilig, schaalbaar en gebruiksvriendelijk toegangscontrolemodel implementeren, dat aansluit bij de beste praktijken in de branche en tegelijkertijd de bescherming voor kritieke cloudservices verbetert.

Scenario's

Met ETD kunnen verschillende scenario's voor verificatie en toegangscontrole worden geïmplementeerd om de administratieve toegang te beveiligen:

1. Embedded MFA – Gebruik de ingebouwde MFA van Cisco of integreer Microsoft MFA.
2. Cisco SCC met Cisco Duo – Combineer de gecentraliseerde authenticatie van Cisco SCC met de geavanceerde MFA-mogelijkheden van Duo.
3. Cisco SCC met een externe identiteitsleverancier (bijvoorbeeld Microsoft Entra ID) – Verleng het verificatiebeleid door te integreren met oplossingen voor bedrijfsidentiteit.

Dit document beschrijft de configuratiestappen voor Scenario 2: Cisco SCC met Cisco Duo, hoewel het proces kan worden aangepast voor andere technologieën.

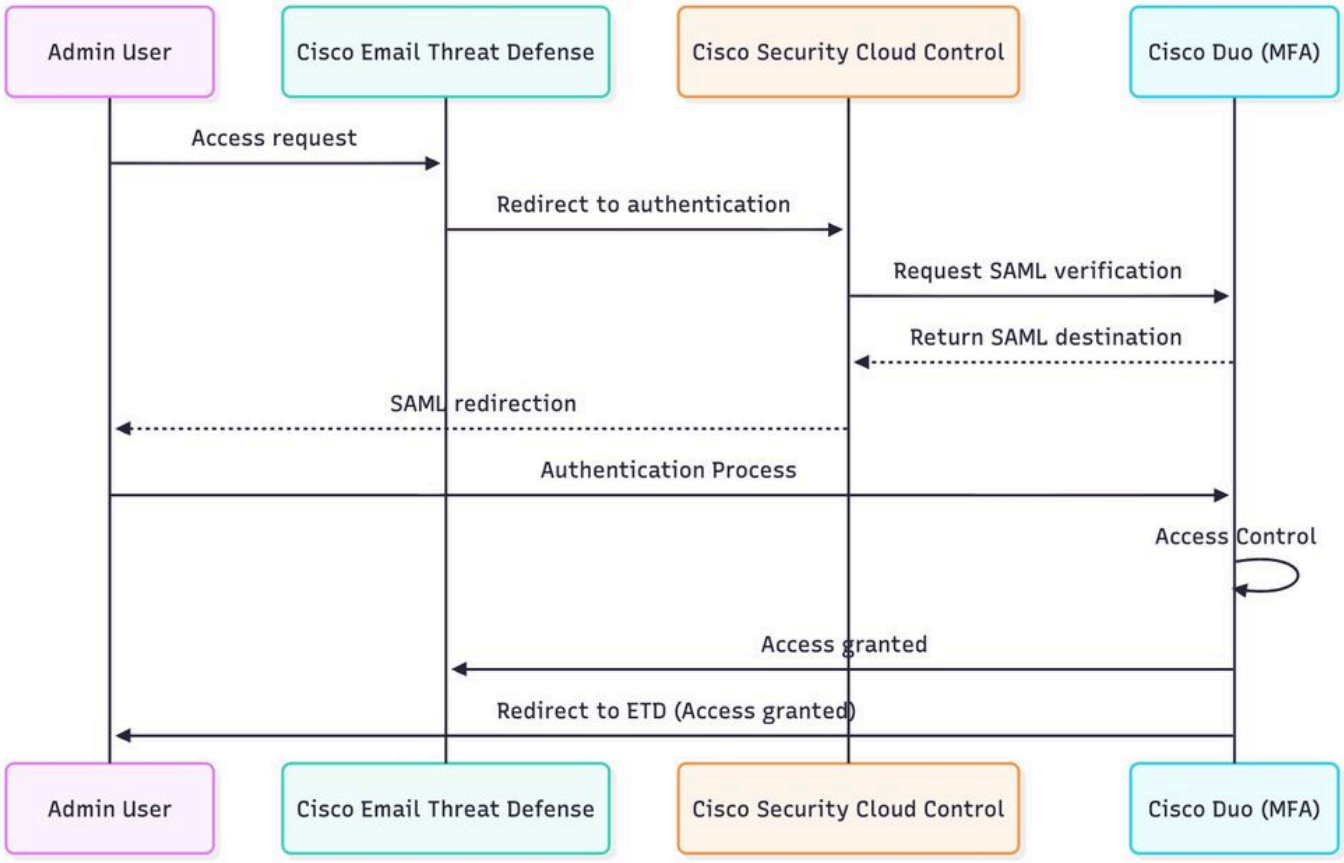
Opmerking: Dit document biedt een overzicht van de basisstappen die nodig zijn om toegangscontrole in te schakelen in Email Threat Defense (ETD) met behulp van de multifactor-authenticatiemogelijkheden van Cisco Duo. De implementatie van Duo-integratie helpt de beveiliging te verbeteren door ervoor te zorgen dat alleen geautoriseerde gebruikers toegang hebben tot het platform. Voor uitgebreide richtlijnen, configuratieopties en geavanceerde implementatiescenario's raadpleegt u de officiële productdocumentatie:

– voor gecentraliseerd beveiligingsbeleid en toegangsbeheer.

Cisco Duo– voor gedetailleerde instructies over de configuratie van multifactorverificatie en best practices.

Cisco SCC-configuratie

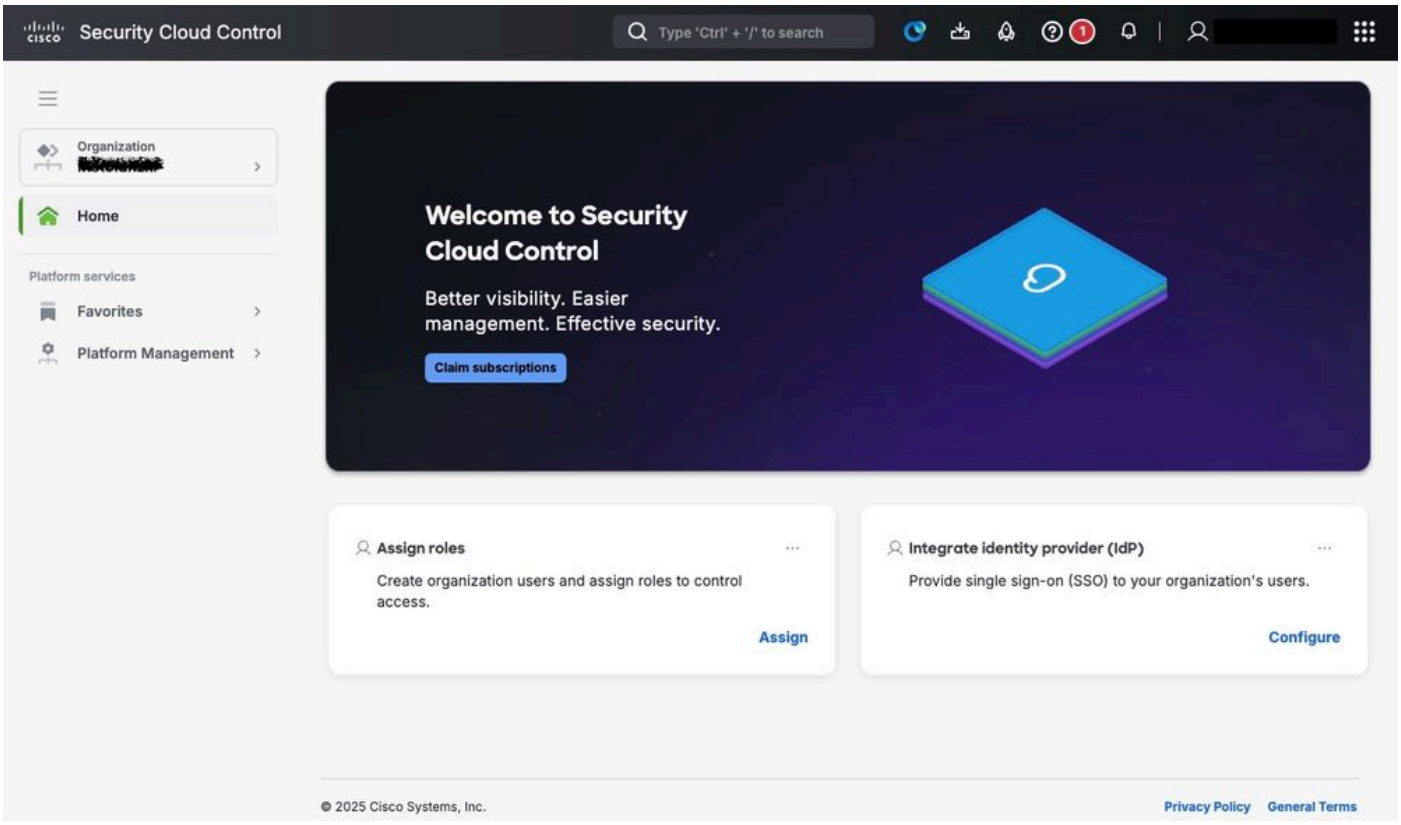
Om Cisco ETD te integreren met Cisco Duo, is de eerste stap het configureren van het verificatiedomein in Cisco SCC. Dit stelt de vertrouwensrelatie vast die Cisco SCC in staat stelt om met externe identiteit en MFA-providers te werken.



Diagram

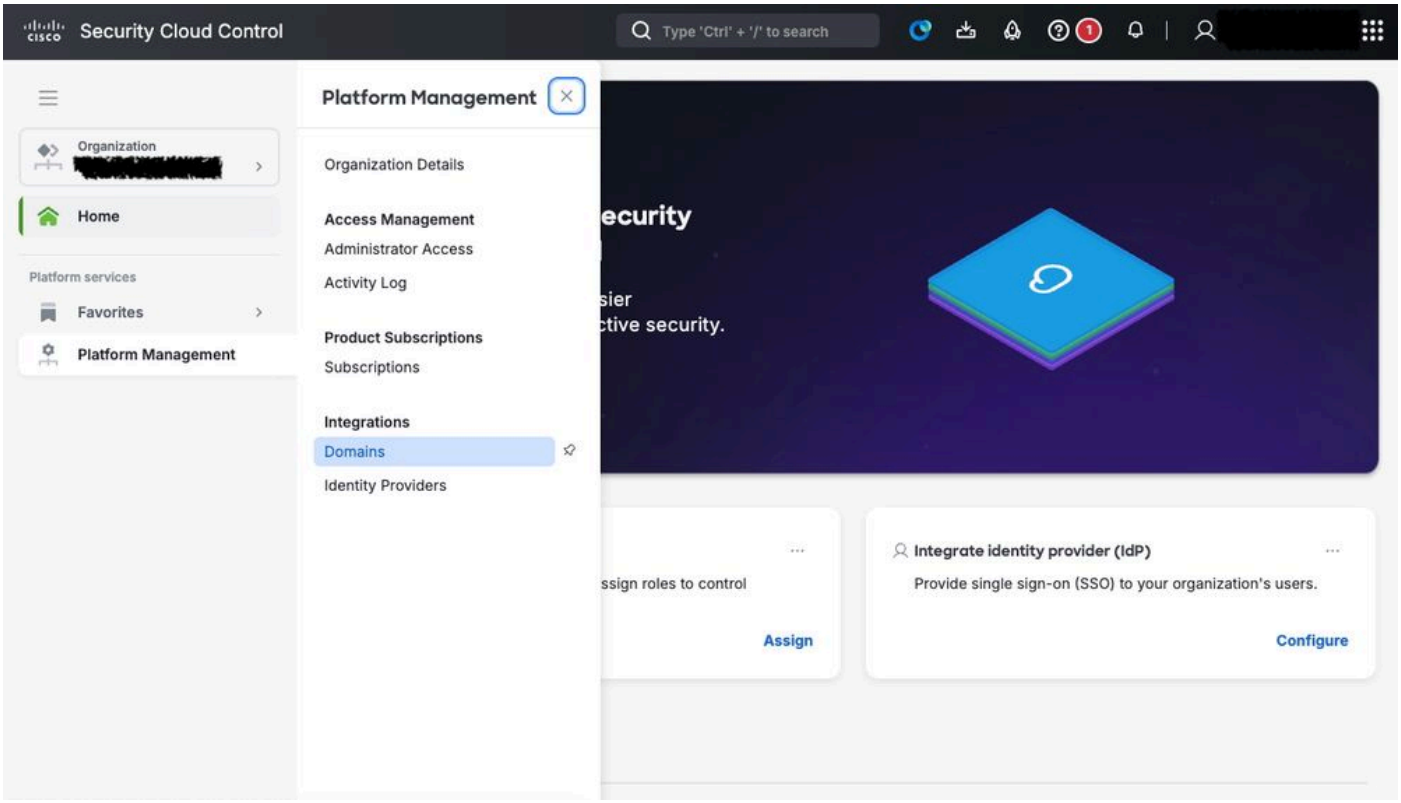
Stap 1. Toegang tot de Cisco SCC-console.

Meld u aan bij het Cisco SCC-portaal https://security.cisco.com/.



Stap 2. Navigeer naar Domeinbeheer.

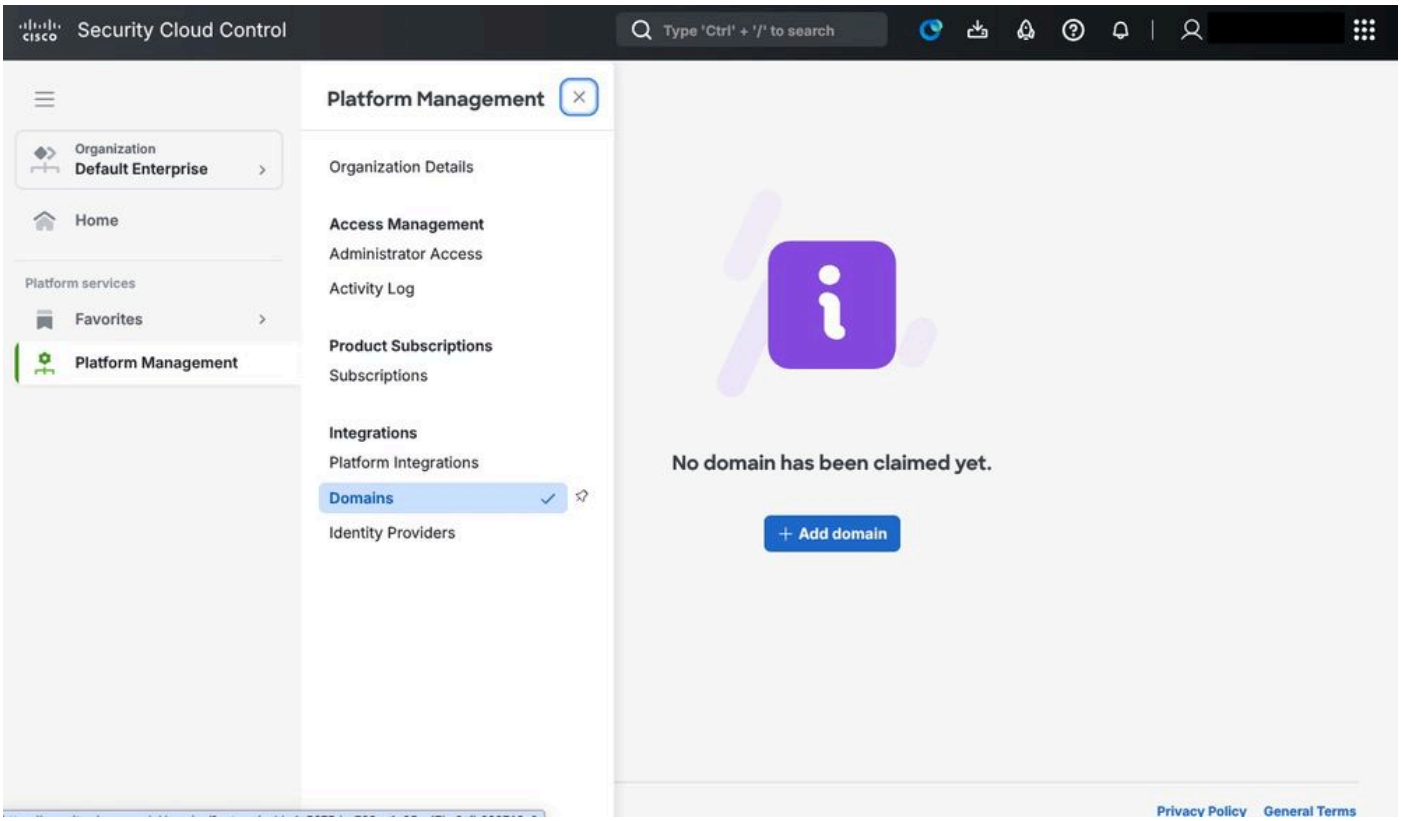
Navigeer in het hoofdmenu naar Platformbeheer > Domeinen.



Secure Cloud Control Domeinconfiguratie

Stap 3. Voeg een nieuw domein toe.

Klik op Domein toevoegen om te beginnen met het registreren van uw verificatiedomein.

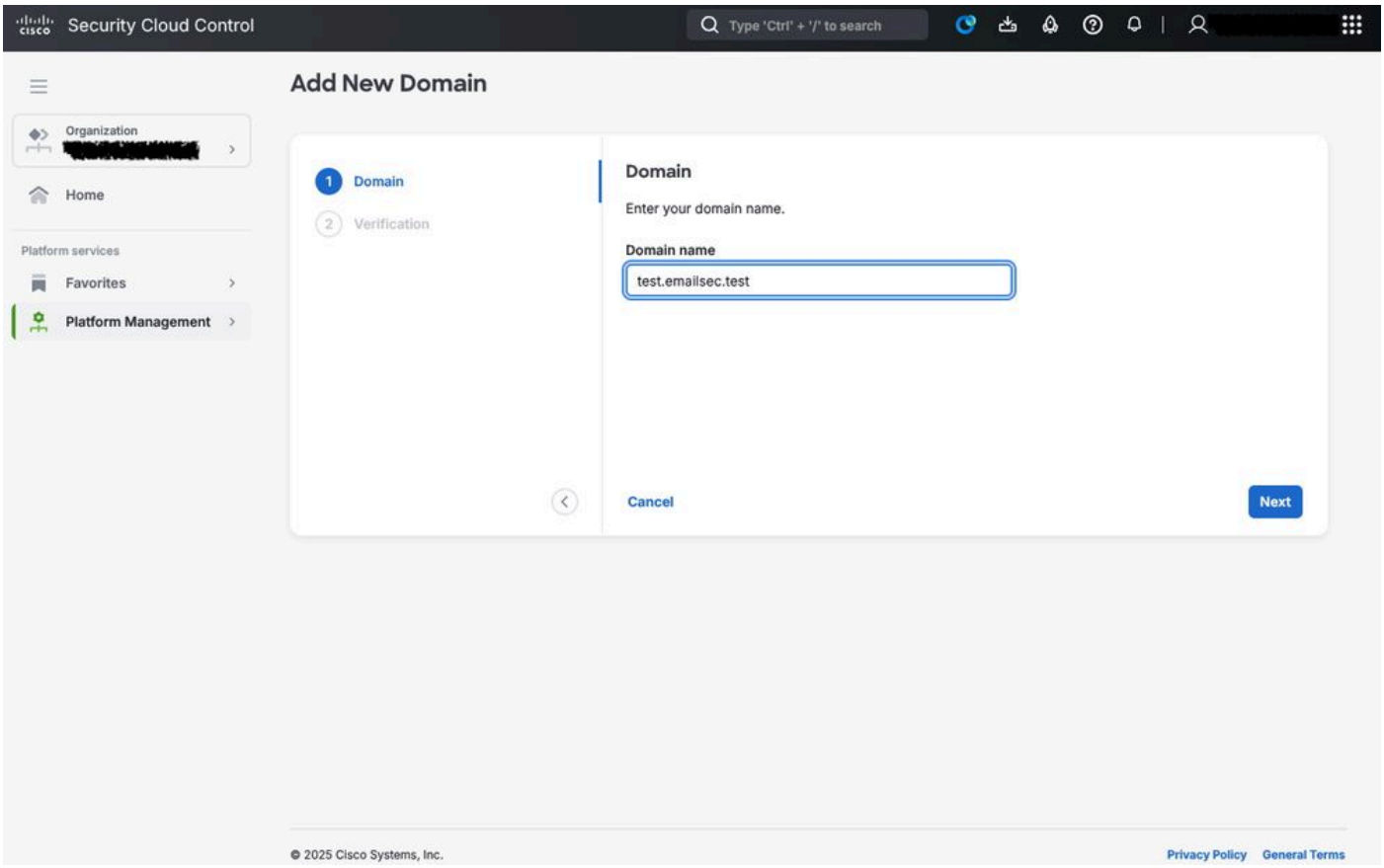


Security Cloud Control: domein

Stap 4. Geef de domeininformatie op.

Vul het formulier in met de details van het domein dat wordt gebruikt voor authenticatie. Dit omvat doorgaans:

- De domeinnaam (bijvoorbeeld test.emailsec.test)
- Contactgegevens (administratief en technisch)
- Authenticatieparameters, afhankelijk van de gekozen identiteitsprovider



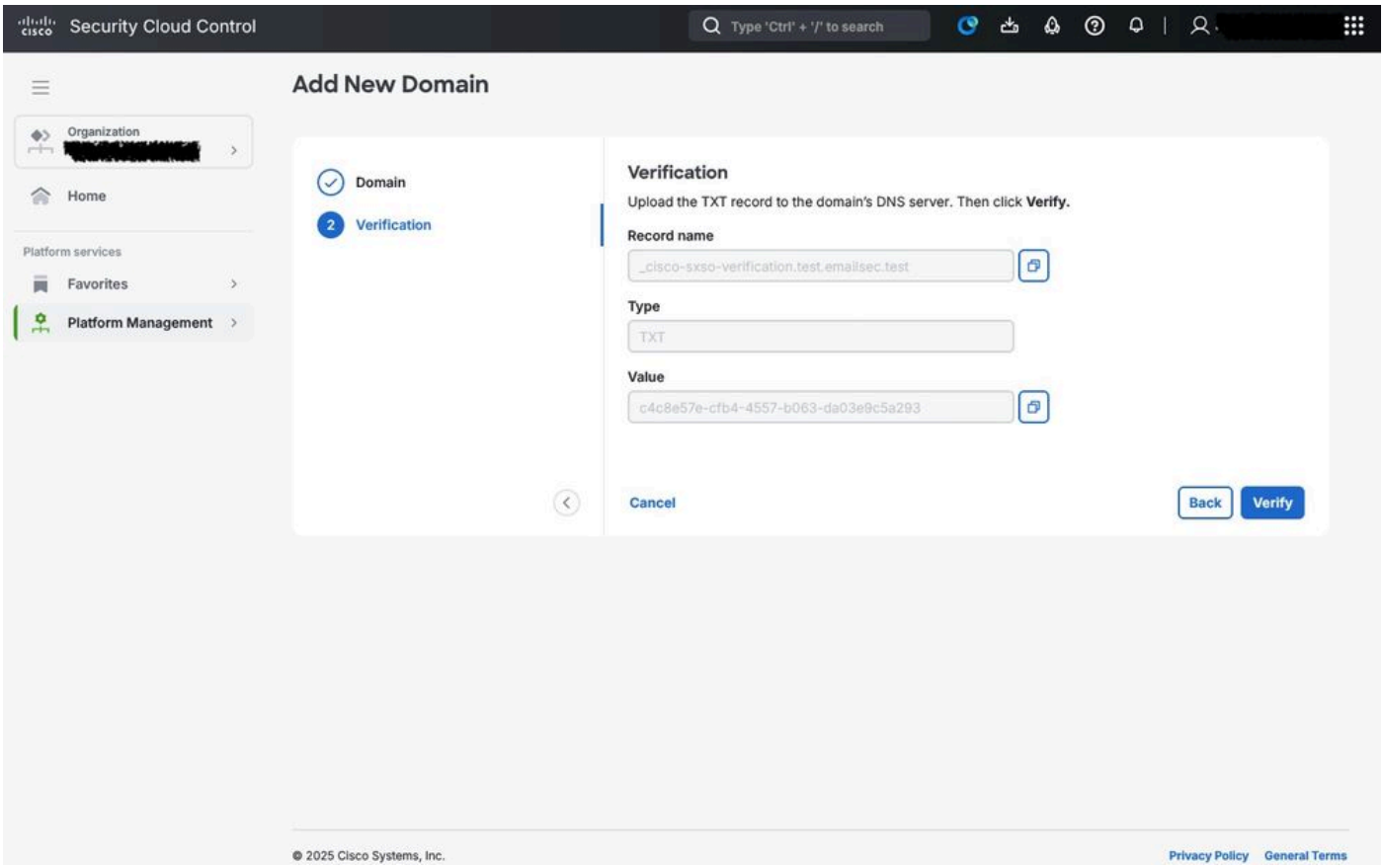
Stap 5. Domeinverificatie via DNS.

Zodra het domein is geregistreerd, vereist Cisco een bewijs van eigendom.

- Een verificatierecord wordt verstrekt door CSCC
- Deze record moet worden toegevoegd aan de DNS-configuratie van uw domein (meestal als een TXT-record)
- Cisco Secure Cloud valideert automatisch de DNS-vermelding om te bevestigen dat het domein bij uw organisatie hoort

---

⚠ Let op: het verificatieproces moet met succes zijn voltooid voordat u verder kunt gaan met de integratie. Afhankelijk van de DNS-propagatie duurt de validatie enkele minuten tot enkele uren.



ETD verbinden met Cisco Duo met Cisco SCC

Zodra het domein van de beheerder met succes is geconfigureerd (wat dient als basis voor het toepassen van strengere toegangscontroles en het beheren van bevoegdheden), is de volgende stap het integreren van de gecontracteerde MFA-service.

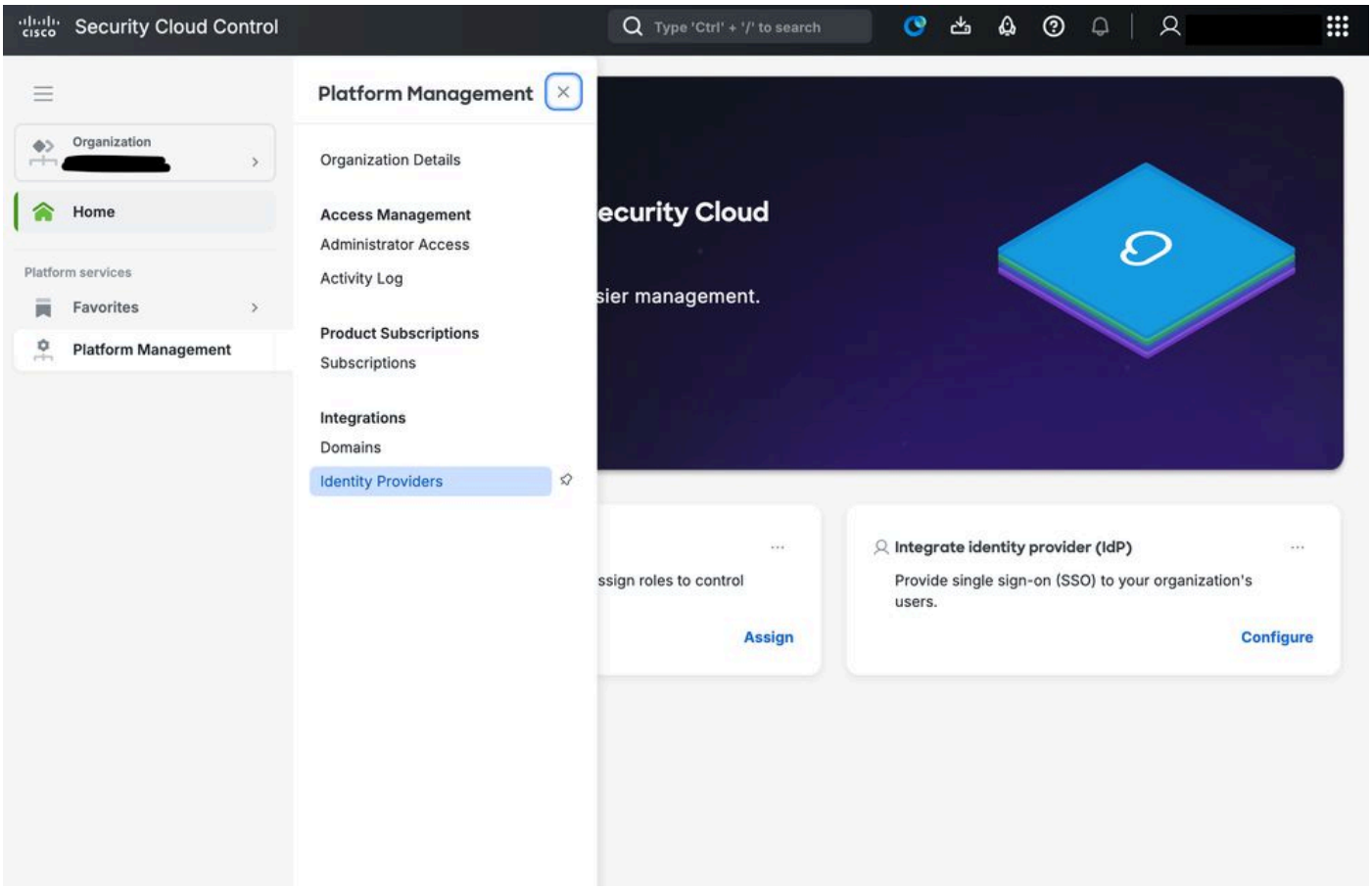
In dit scenario wordt Cisco Duo geïmplementeerd als de primaire oplossing voor toegangscontrole, beveiligde aanmelding en MFA-verificatie. Deze integratie verbetert de beveiligingspositie van de omgeving door beheerders te verplichten hun identiteit te verifiëren door middel van meerdere verificatiestappen, waardoor het risico van ongeoorloofde toegang wordt verminderd en de naleving van het beveiligingsbeleid van de organisatie wordt gewaarborgd.

Cisco Duo en Cisco Cloud Control Integratie

Stap 1. Toegang tot de Cisco SCC-console.

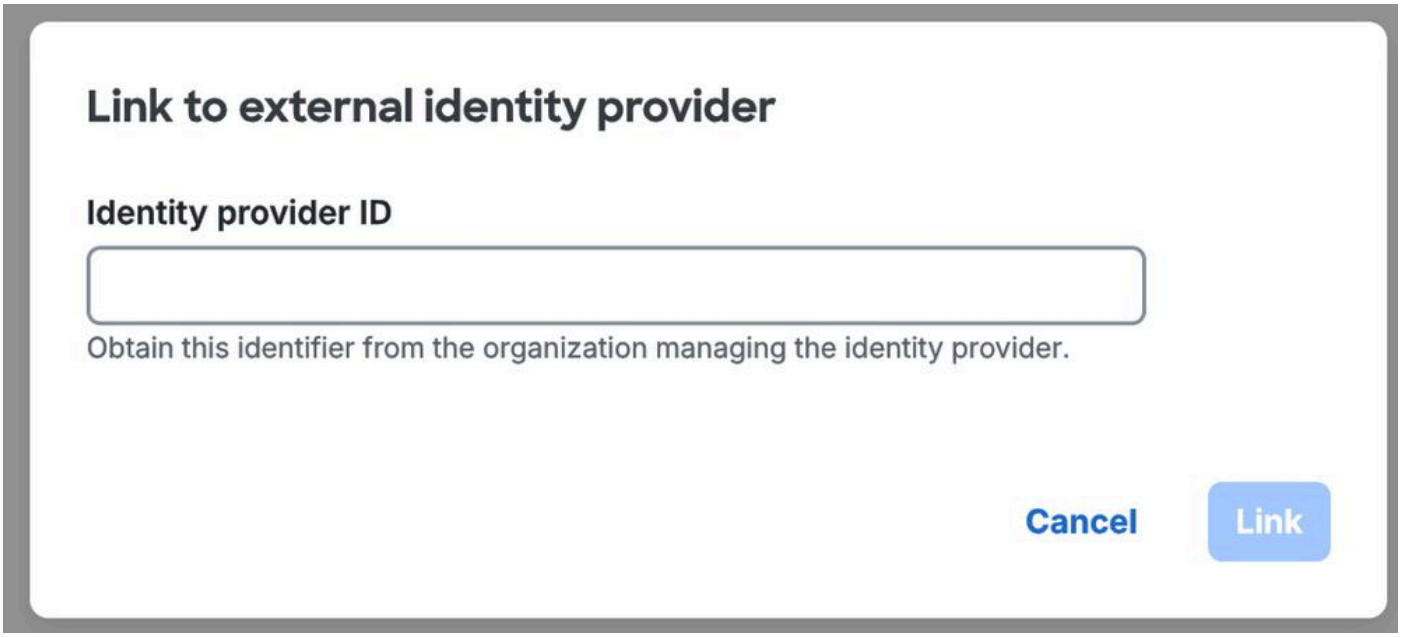
Meld u aan bij de Cisco Security Cloud Control portal https://security.cisco.com/.

Navigeer naar Platform Management en klik op Identity Providers.



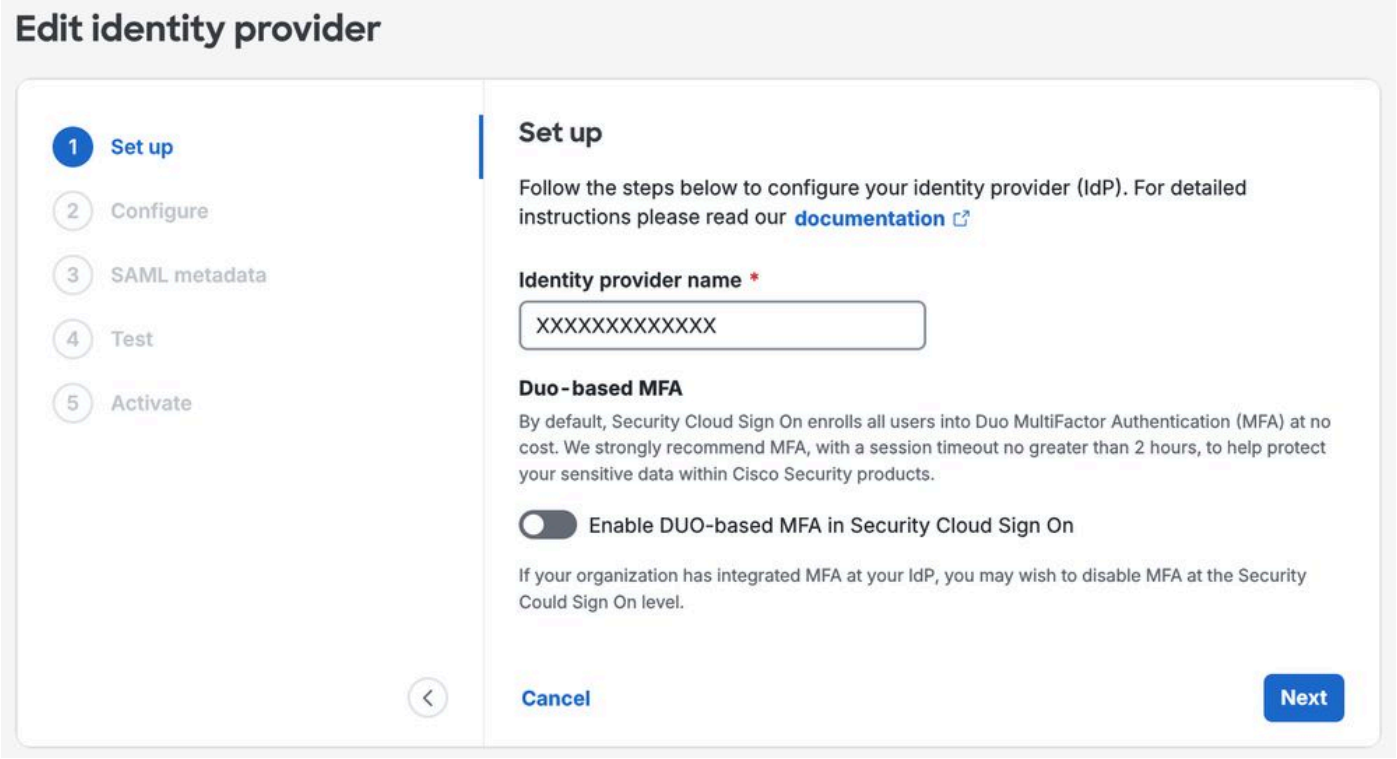
SCC IDP-configuratie

Gebruik een aangepaste naam om de identiteitsprovider te identificeren.



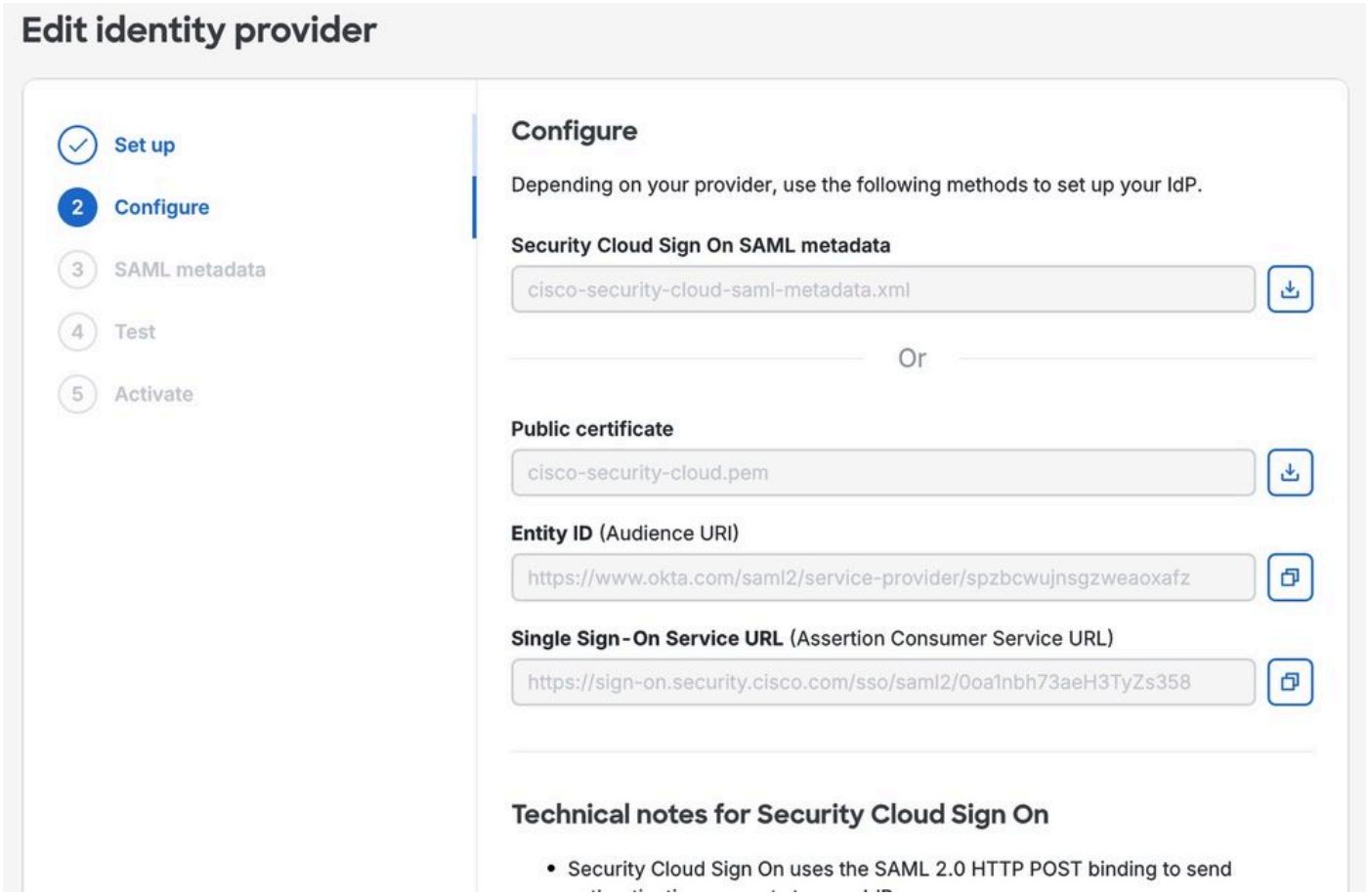
Nu begint de setup. Op dit moment krijgt u toegang tot Cisco SCC en Cisco Duo.

Stap 2. Schakel in SCC MFA op basis van DUO inschakelen in Security Cloud inschakelen, zoals in de afbeelding wordt weergegeven, uit en klik op Volgende.

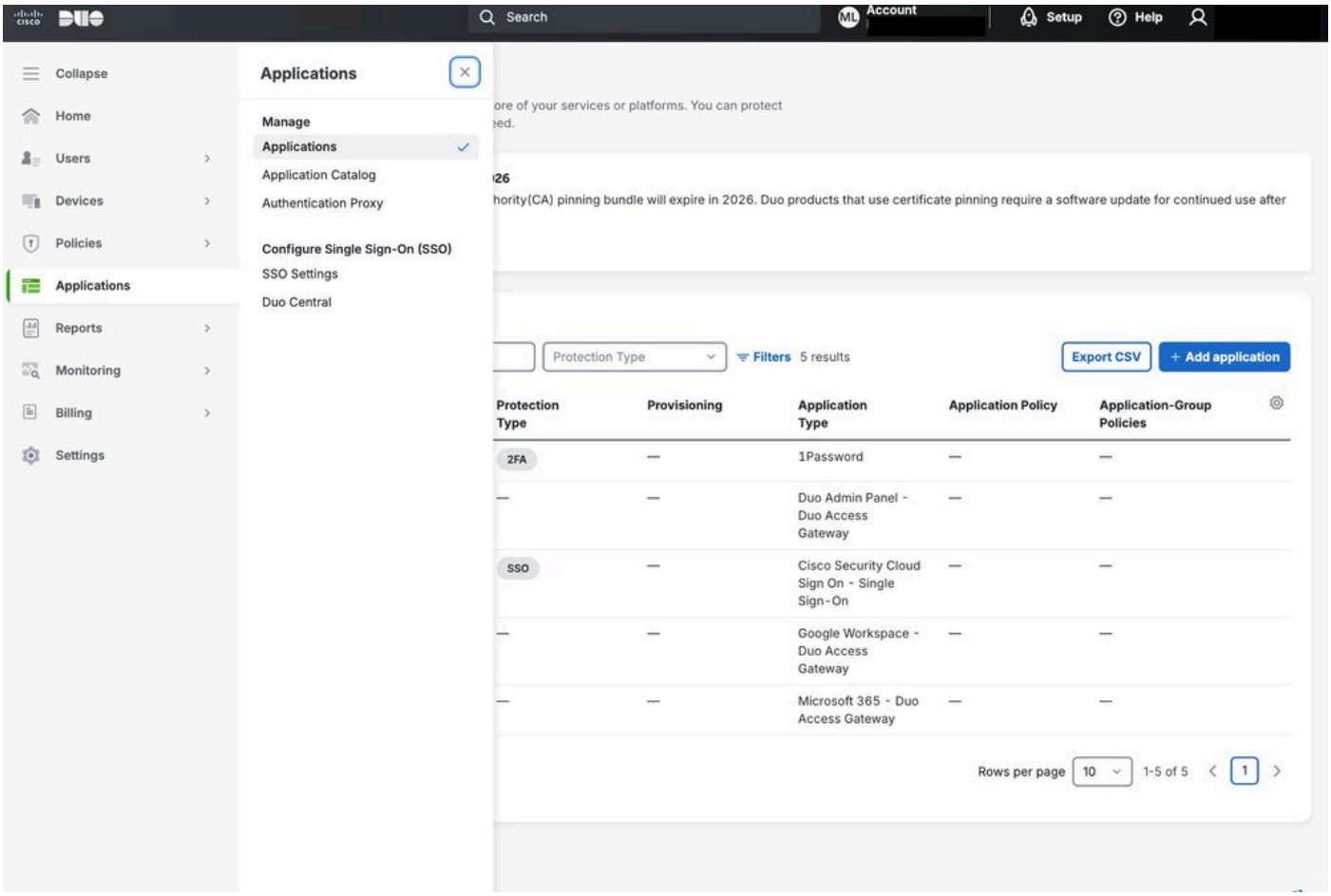


Configuratie van identiteitsprovider

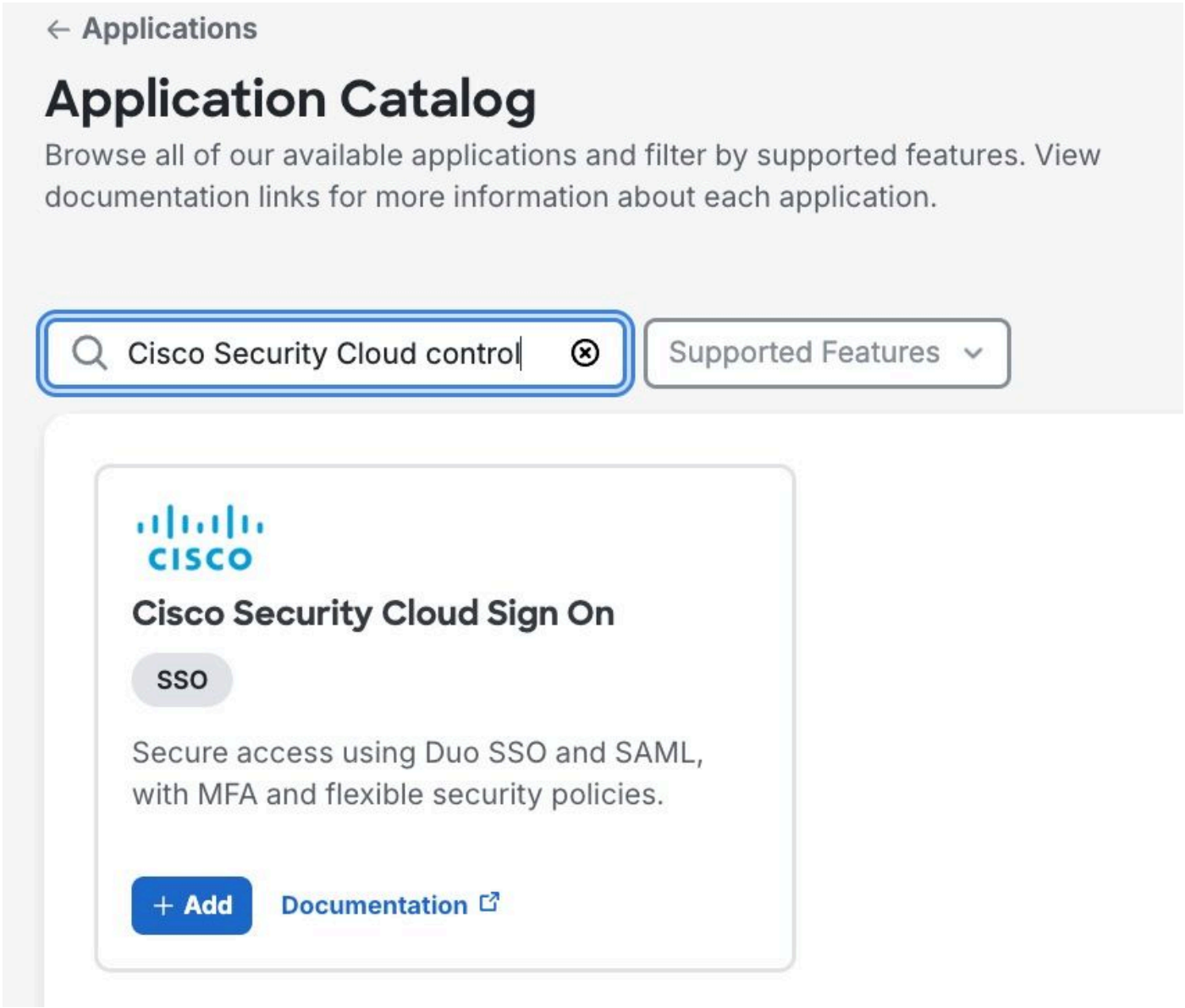
Stap 3. De relevante gegevens worden gemaakt en deze worden gebruikt tijdens de Cisco Duo-configuratie.
Zorg ervoor dat u alle vereiste waarden en bijbehorende gegevens kopieert en op een veilige locatie opslaat.
Deze gegevens zijn essentieel voor toekomstige integratiestappen, dus zorg ervoor dat ze alleen toegankelijk zijn voor bevoegd personeel en worden beschermd in overeenstemming met het beveiligingsbeleid van uw organisatie.



Stap 4. Open Cisco Duo, ga naar de sectie Toepassingen en klik op Toepassing toevoegen.

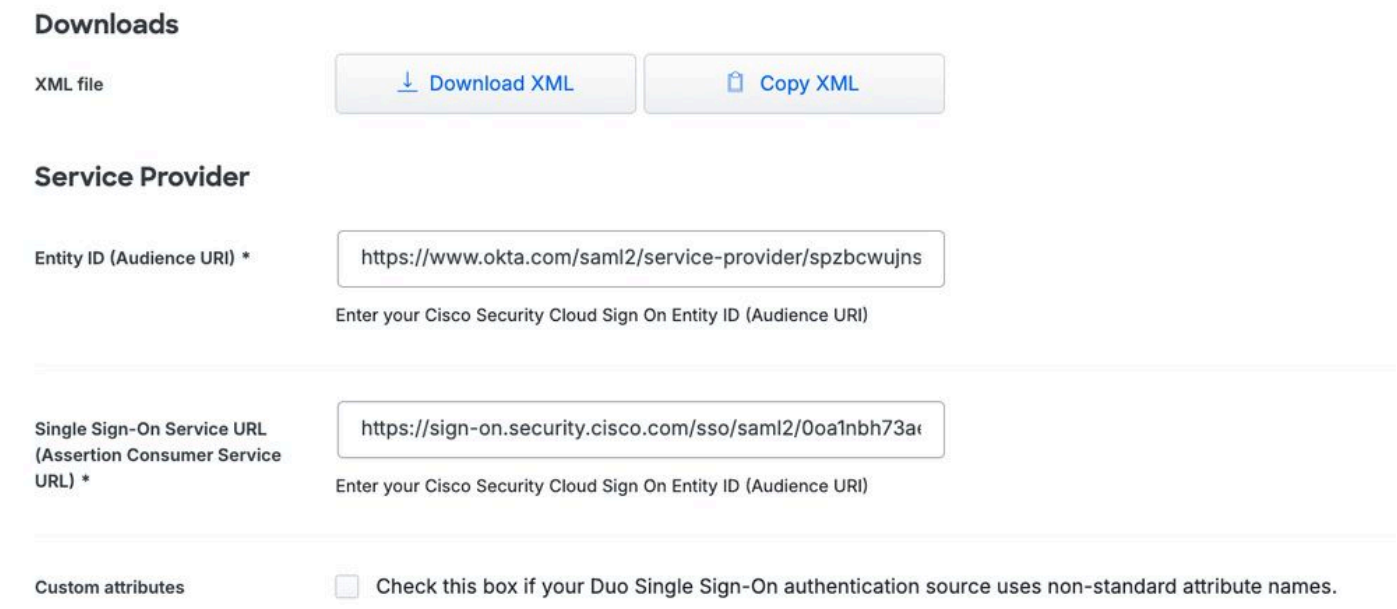


Zoek in het menu naar Cisco Security Cloud en klik op Toevoegen om de integratie te starten.

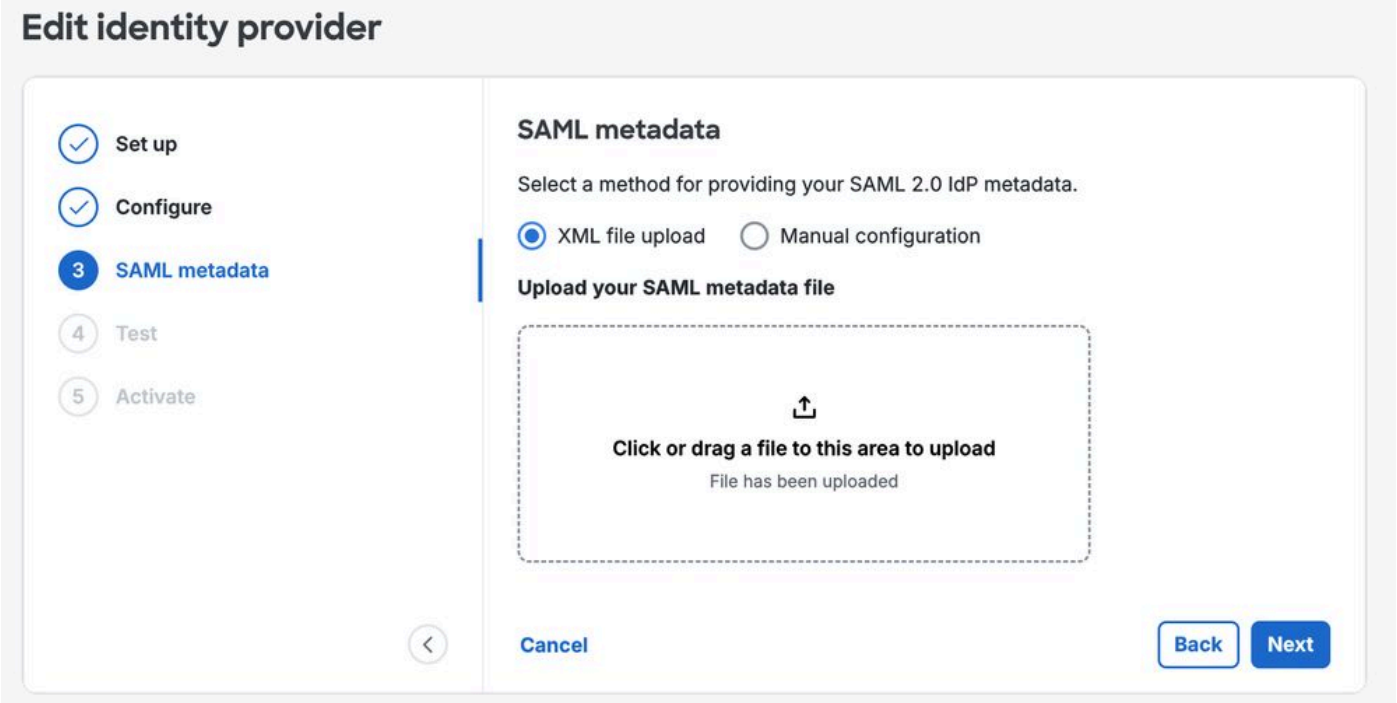


Stap 5. Configureer de relevante informatie in de Cisco Duo-toepassing.

Kopieer de Entiteit-ID en Singles Sign-On Service-URL van Cisco SCC naar Cisco Duo.



Stap 6. Download de XML en upload het bestand naar Cisco SCC.



Opmerking: de overige parameters die in de toepassing kunnen worden geconfigureerd vanaf de Cisco Duo-console, moeten worden aangepast aan uw specifieke vereisten. Gedetailleerde uitleg voor elk van deze instellingen is te vinden in de officiële Cisco Duo-documentatie. Voorbeelden van configureerbare parameters zijn de toegewezen toepassingsnaam, de set gebruikers waarop het beleid van toepassing is en andere aanpassingsopties die de beveiligingscontroles kunnen aanpassen om aan de behoeften van uw organisatie te voldoen.

Beleidsconfiguratie in Cisco Duo voor Cisco ETD

In dit stadium zijn alle componenten verbonden en de volgende stap is het configureren van een beleid dat van toepassing is op het verificatieproces van de beheerder binnen de Cisco ETD-console.

In dit voorbeeld ligt de focus specifiek op toegangscontrole op basis van IP-adres. Cisco Duo biedt echter veel andere opties voor toegangscontrole.

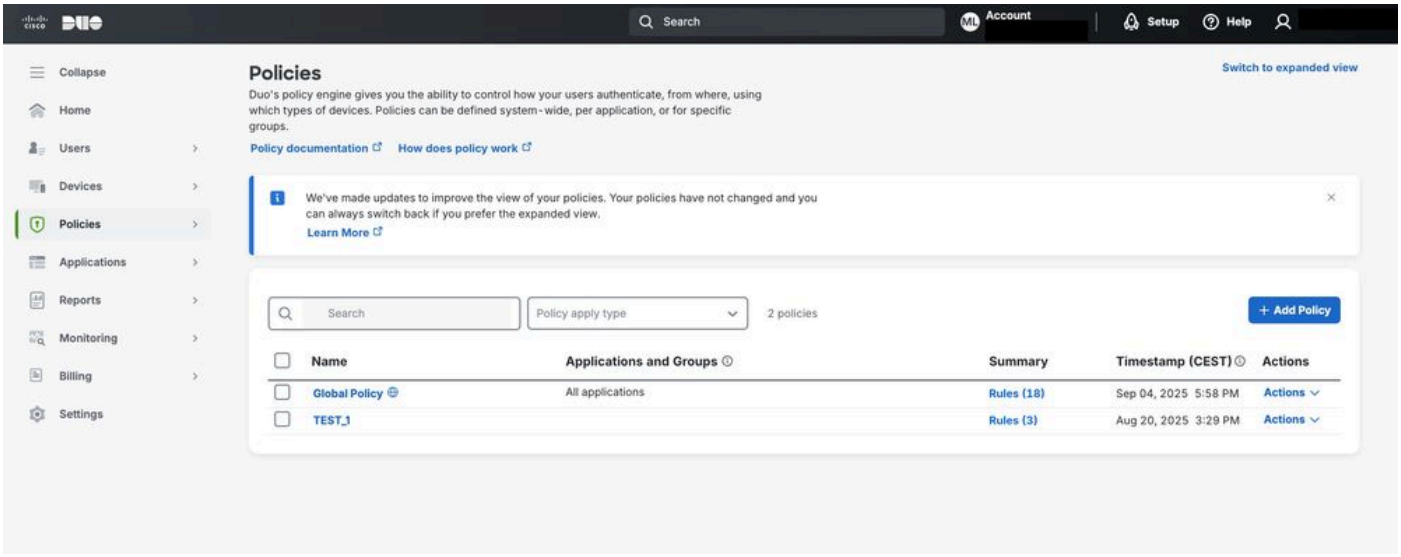
Er kan een nieuw beleid worden gemaakt en aan de toepassing worden toegewezen, waardoor de gewenste verificatieregels en beveiligingsbeperkingen voor aanmeldingen door beheerders kunnen worden gehandhaafd.

Voor meer gedetailleerde informatie over alle beschikbare besturingselementen en configuratieopties in Cisco Duo raadpleegt u de officiële documentatie van Cisco Duo.

Deze bron biedt uitgebreide richtlijnen voor installatie, aanpassing en best practices om het beveiligingsbeleid te helpen optimaliseren.

Door naar de sectie Beleid in Cisco Duo te navigeren, kan een beleid worden gemaakt en toegewezen aan de Cisco ETD-verbinding via Cisco Duo.

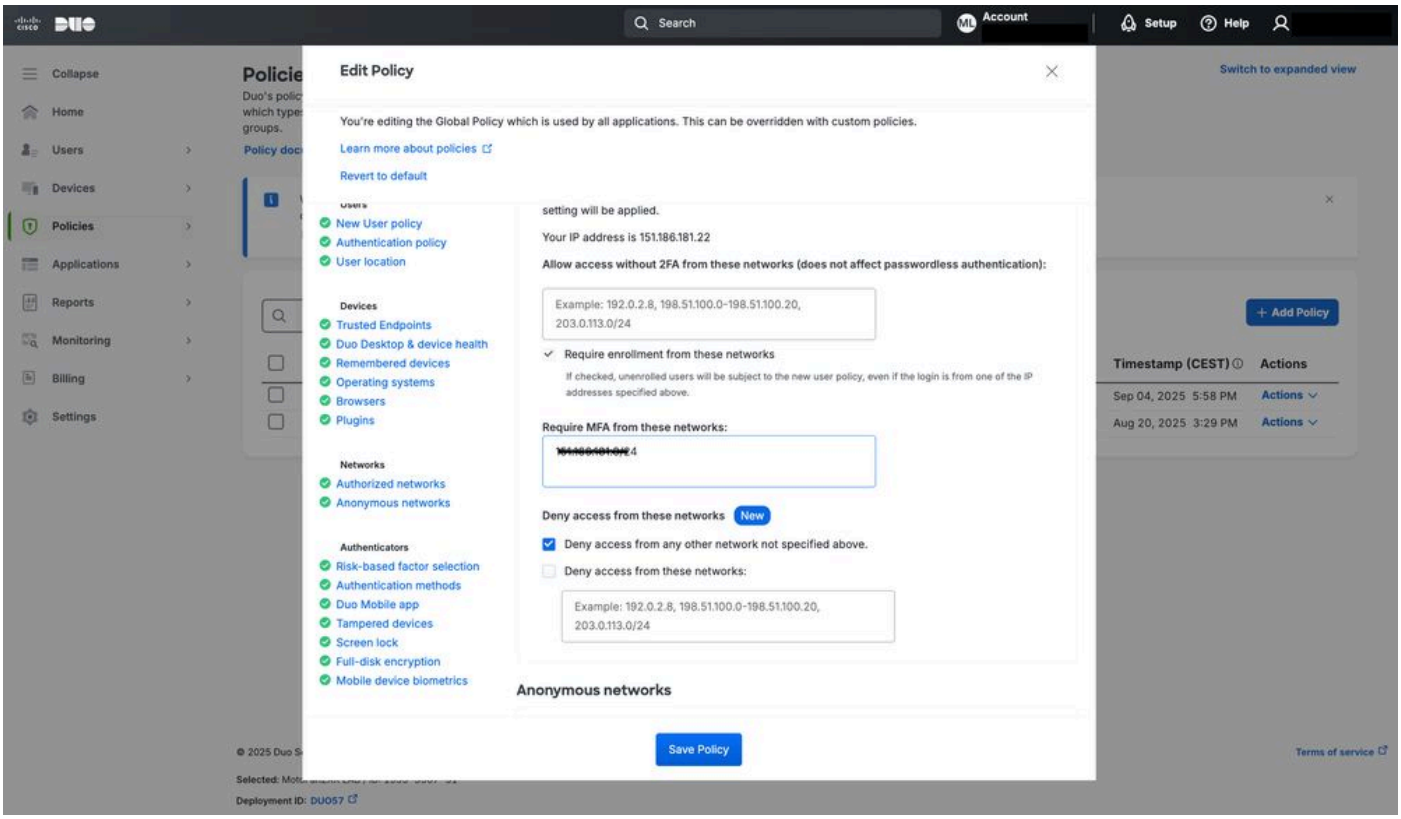
Dit beleid kan per gebruiker of groep worden toegepast, afhankelijk van de toegangsvereisten.



Cisco Duo

In dit voorbeeld wordt, zoals in het image wordt getoond, de IP-brontoegangscontrole ingeschakeld door de sectie Geautoriseerde netwerken te configureren.

Deze configuratie biedt alleen toegang vanaf bepaalde vertrouwde IP-bereiken, waardoor de beveiliging voor Cisco ETD wordt verbeterd.



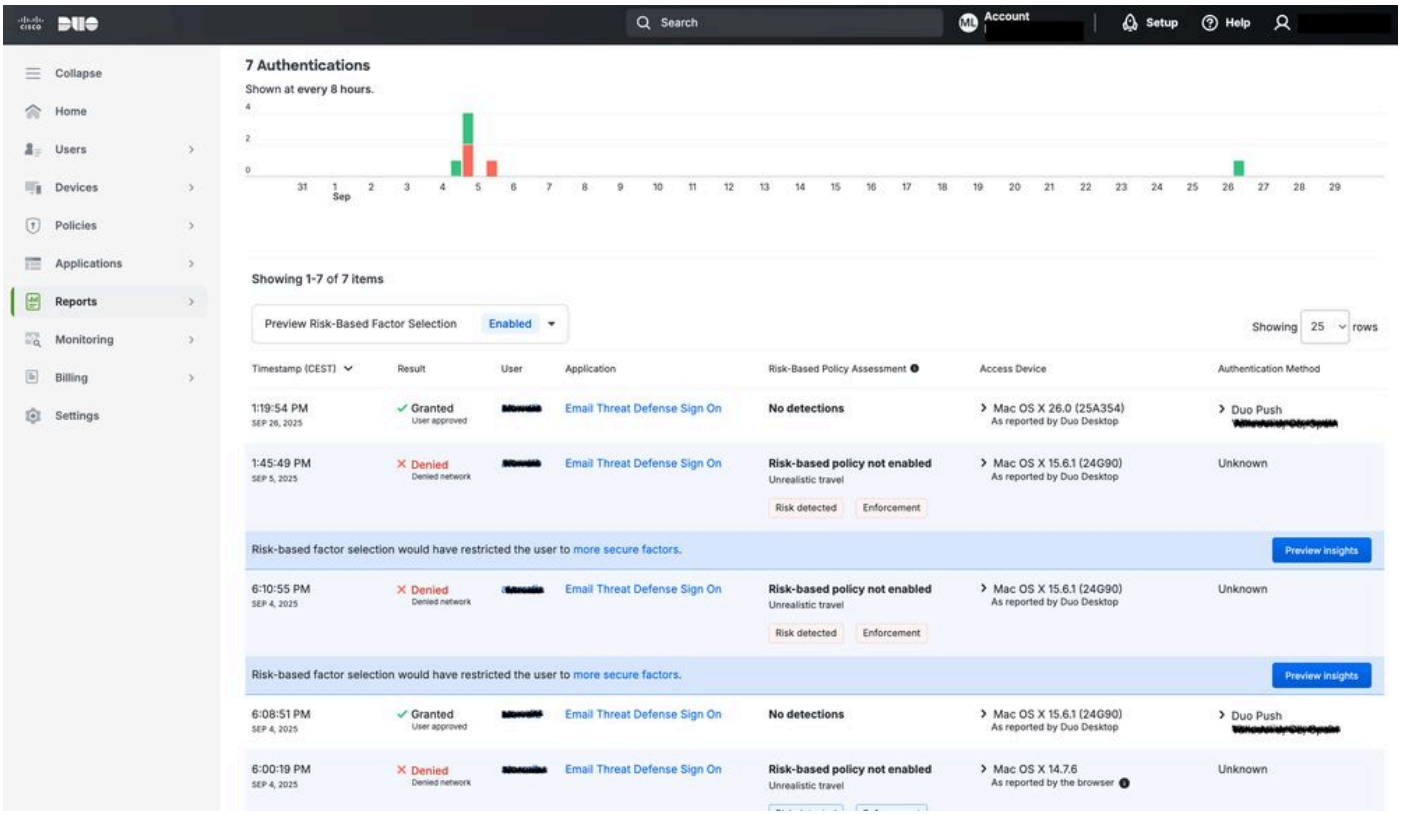
Configuratie Cisco Duo-beleid

conclusies

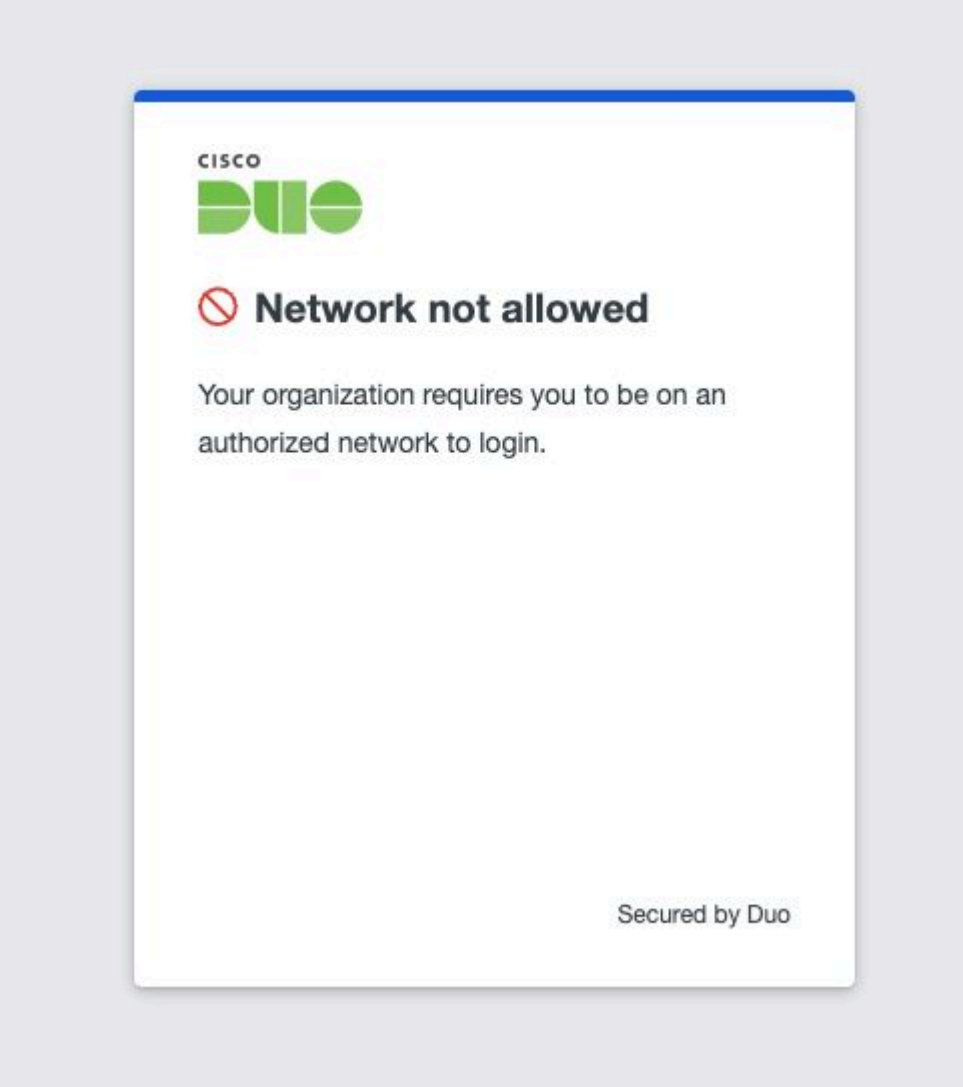
Cisco ETD biedt flexibele opties om beheerderstoegang te beschermen door middel van MFA en integratie met identiteitsproviders.
Door Cisco SCC te combineren met Cisco Duo kunnen organisaties een sterker verificatiebeleid implementeren, het risico op ongeoorloofde toegang verminderen en zich afstemmen op best practices uit de branche voor veilig cloudservicebeheer.

Naast MFA kunnen beheerders gebruikmaken van beleidsgebaseerde controles van Cisco Duo om de toegang te beperken op basis van specifieke criteria, zoals het IP-adres van de bron. Bijvoorbeeld, zoals geïllustreerd in de volgende afbeelding, wordt een toegangspoging van een IP-adres buiten het geautoriseerde bereik automatisch geblokkeerd door het systeem. Dit zorgt ervoor dat alleen verzoeken afkomstig van vertrouwde netwerken zijn toegestaan, waardoor een extra beschermingslaag tegen potentiële aanvallen wordt toegevoegd.

Door IP-gebaseerde toegangscontrole en MFA te implementeren, bereiken organisaties een defensieve aanpak waarbij identiteitsverificatie wordt gecombineerd met validatie van netwerklocaties om kritieke beheerinterfaces in de cloud te beveiligen.



Cisco Duo-rapporten



Resultaat netwerkbesturing

Waarschuwing: Het is belangrijk om te begrijpen dat deze wijziging van invloed is op alle toepassingen die hetzelfde verificatiedomein gebruiken; niet alleen ETD, maar ook andere producten die afhankelijk zijn van hetzelfde verificatieproces, zoals toegang tot de Cisco Secure Access-console.

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.