

LDAP configureren in Intersight virtuele applicatie

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Configuratie van LDAP Basic Settings](#)

[Gebruikers en groepen configureren](#)

[Groepen configureren](#)

[Gebruikers configureren](#)

[Configuratie van LDAPS \(Secure LDAP\)](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Fout 1. Onjuiste toegangsgegevens](#)

[Fout 2. Fout bij binden van gegevens](#)

[Fout 3. Kan geen gebruiker vinden](#)

[Fout 4. Onjuist certificaat](#)

[Fout 5. Encryptie inschakelen wordt gebruikt met een beveiligde poort](#)

[Fout 6. Verbindingsparameters onjuist](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft het proces om LDAP-verificatie te configureren in een Intersight Private Virtual Applicatie (PVA).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Lichtgewicht Directory Access Protocol (LDAP).
- Intersight Private virtuele applicatie.
- Domain Name Server (DNS).

Gebruikte componenten

- Intersight Private virtuele applicatie.
- Microsoft Active Directory.
- DNS-server.

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

LDAP is een protocol dat wordt gebruikt om toegang te krijgen tot bronnen via een directory via het netwerk. Deze directory's slaan informatie op over gebruikers, organisaties en resources. LDAP biedt een standaardmanier om toegang te krijgen tot die informatie en deze te beheren, die kan worden gebruikt voor authenticatie- en autorisatieprocessen.

Dit document toont het configuratieproces om externe verificatie via LDAP toe te voegen aan een Intersight PVA.

Configureren

Configuratie van LDAP Basic Settings

1. Ga naar Systeem > Instellingen > VERIFICATIE > LDAP/AD.
2. Klik op LDAP configureren.
3. Voer de vereiste informatie in. Overweeg de volgende aanbevelingen:
 1. De naam wordt willekeurig ingesteld en heeft geen invloed op de configuratie.
 2. Voor de BaseDN en BindDN, kopieer en plak de corresponderende waarden van uw Active Directory (AD) configuratie.
 3. De standaardwaarde voor groepskenmerk is lid.



Opmerking: In andere UCS-beheertools, zoals UCSM of CIMC, is het groepskenmerk ingesteld op memberOf. In Intersight wordt aanbevolen om het als lid te laten.

4. Voer het wachtwoord in voor deze LDAP-provider.
5. Schakel Nesting Group Search toggle in als u een recursieve zoekfunctie in uw AD wilt toestaan voor alle groepen vanaf root en hun ingesloten groepen.
6. Laat Encryptie uitgeschakeld voor een reguliere LDAP-configuratie. Als er een beveiligde LDAP nodig is, moet u deze inschakelen en ervoor zorgen dat de sectie Configuration of LDAPS (Secure LDAP) wordt beoordeeld voor de aanvullende

stappen die u moet configureren.

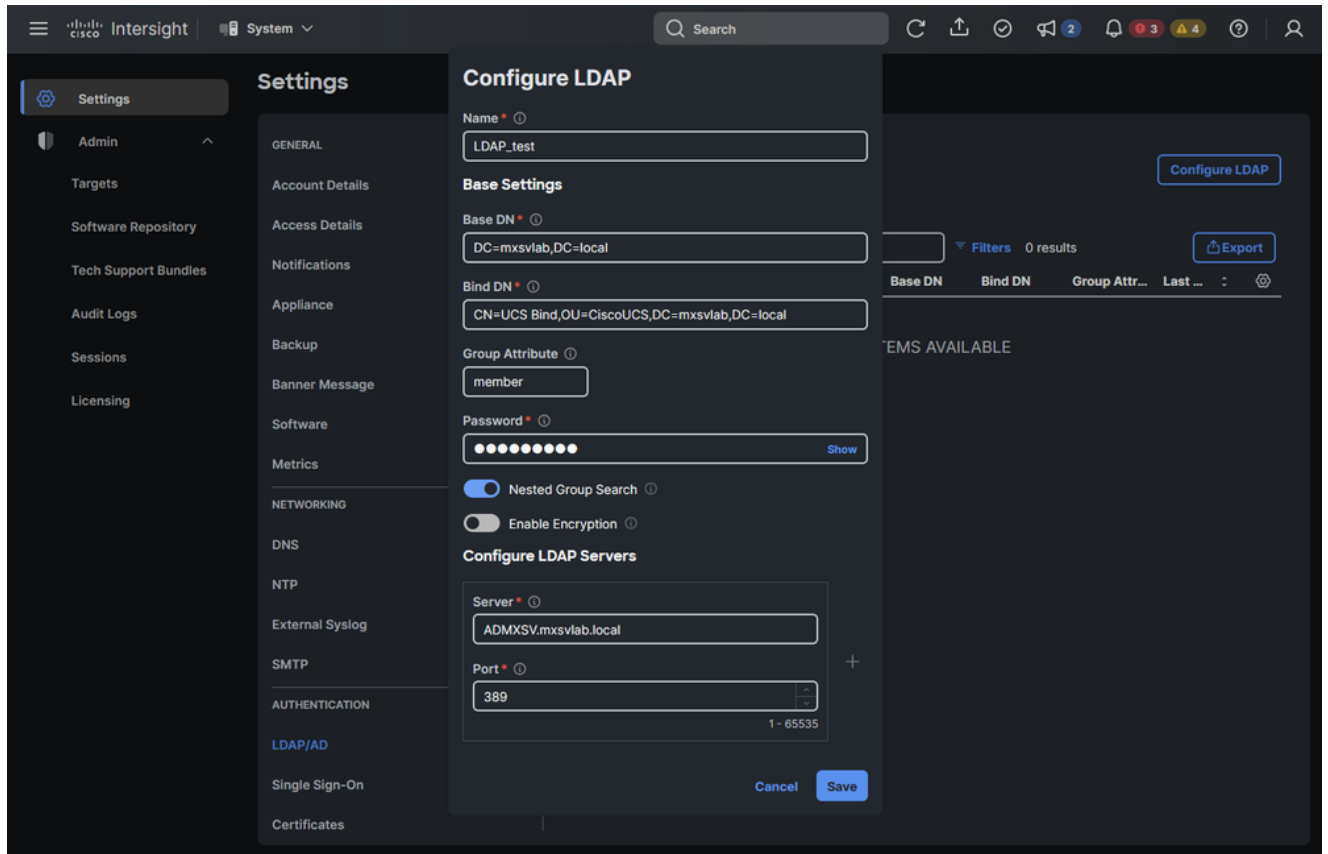
4. Voeg de configuratie voor één LDAP-server toe:

1. In Server introduceer de IP of hostname van de LDAP-server.

 Voorzichtig: Als hostname wordt gebruikt, zorg ervoor dat de DNS in staat is om die hostname correct in kaart te brengen.

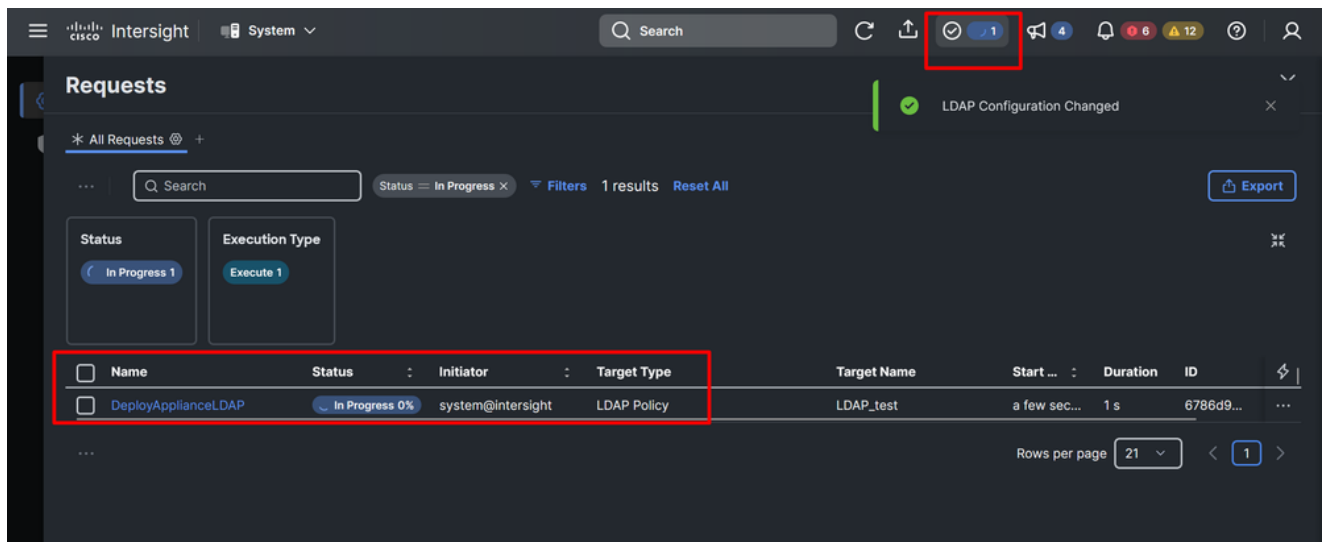
2. De standaard en aanbevolen poort voor LDAP is 389 .

5. Klik op Save (Opslaan).



Configuratievoorbeeld voor basis LDAP-instellingen

6. Bewaak de workflow ImplementyApplianceLDAP vanuit de Verzoeken in de bovenste balk.



Implementatieaanvraag

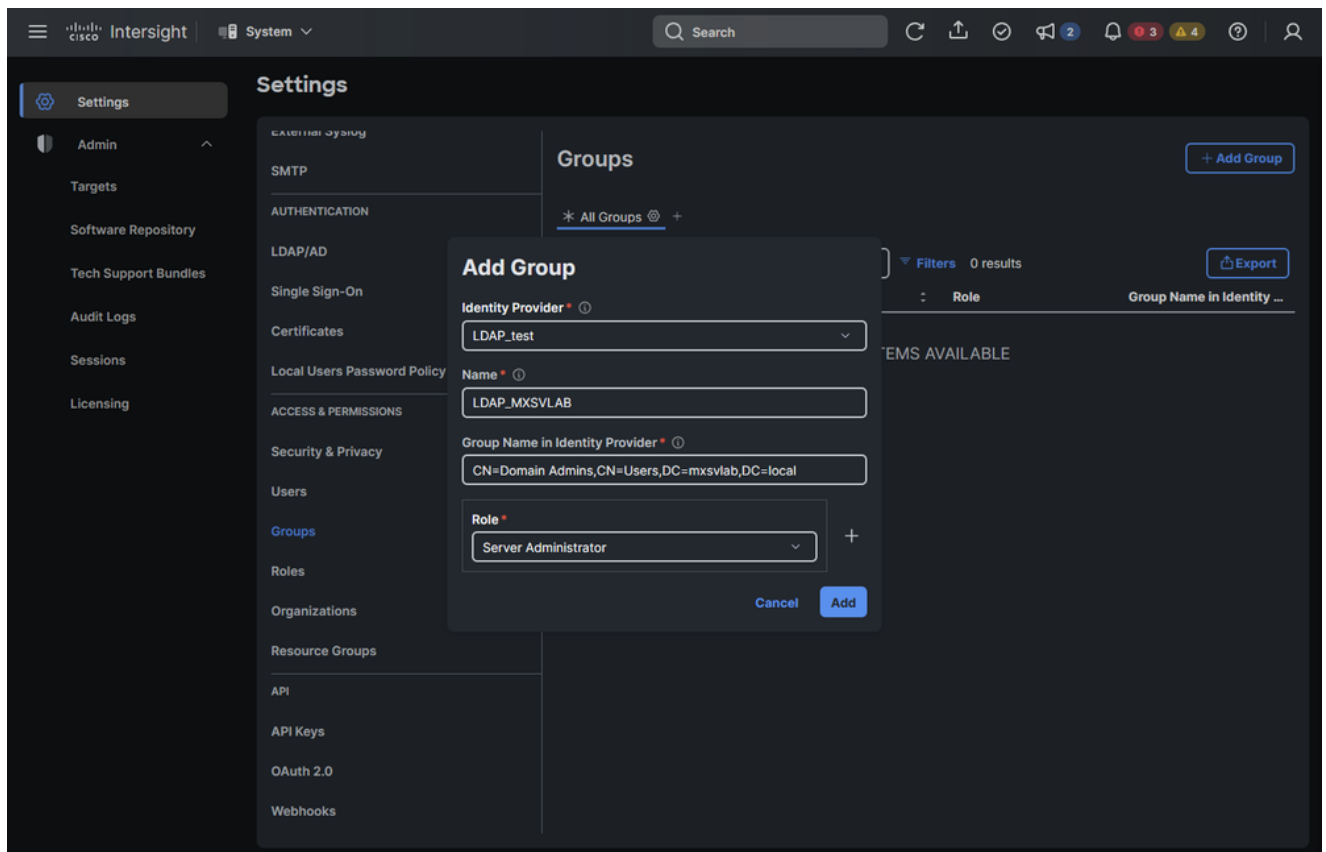
Gebruikers en groepen configureren

Wanneer de workflow ImplementyApplianceLDAP is voltooid, kunt u Groepen of individuele Gebruikers configureren.

Als u besluit Groepen te gebruiken, wordt de autorisatie verleend aan alle gebruikers die tot die Groep behoren. Als u individuele gebruikers gebruikt, dan moet u elke gebruiker met zijn eigen autorisatiefunctie toevoegen.

Groepen configureren

1. Navigeren naar systeem > Instellingen > TOEGANG EN TOESTEMMING > Groepen.
2. Klik op Groep toevoegen.
3. Selecteer de identiteitsprovider. Het is de naam die u instelt in de sectie LDAP Basic Settings configureren.
4. Stel een naam in voor de groep.
5. Voer de waarde in voor Groepsnaam in Identity Provider. Het moet overeenkomen met de configuraties van de groep in uw LDAP-server.
6. Selecteer de rol afhankelijk van het toegangsniveau dat u aan de gebruikers in deze groep wilt bieden. Zie [Rollen en Privileges in Intersight](#).



Configuratievoorbeeld voor een groep

Gebruikers configureren

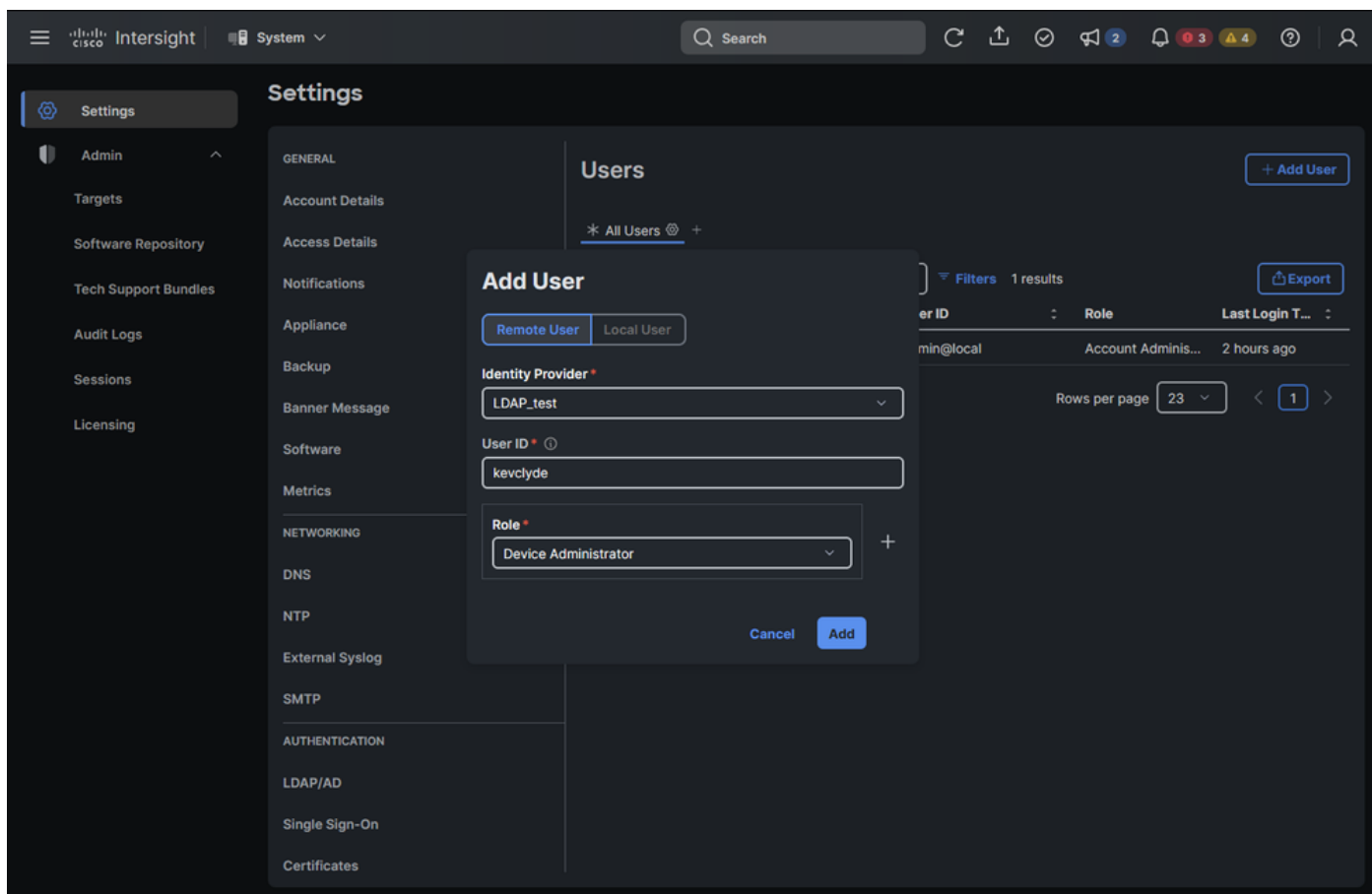
Als u liever individuele gebruikers configureren in plaats van groepen, volg dan deze instructies:

1. Ga naar Systeem > Instellingen > TOEGANG EN TOESTEMMING > Gebruikers.
2. Klik op Gebruiker toevoegen.
3. Selecteer externe gebruiker.
4. Selecteer de identiteitsprovider. Het is de naam die u instelt in de sectie LDAP Basic Settings configureren.
5. Stel een gebruikers-id in.



Tip: Als u de gebruikersnaam als inlogmethode wilt gebruiken, kopieert u in het veld Gebruikersnaam de waarde die in uw LDAP-server is ingesteld als rekennaam. Als u de e-mail wilt gebruiken, zorg er dan voor dat u de e-mail van de gebruiker instelt in het kenmerk mail op de LDAP-server.

6. Selecteer de rol afhankelijk van het toegangsniveau dat u aan de gebruiker wilt bieden. Zie [Rollen en Privileges in Intersight](#).

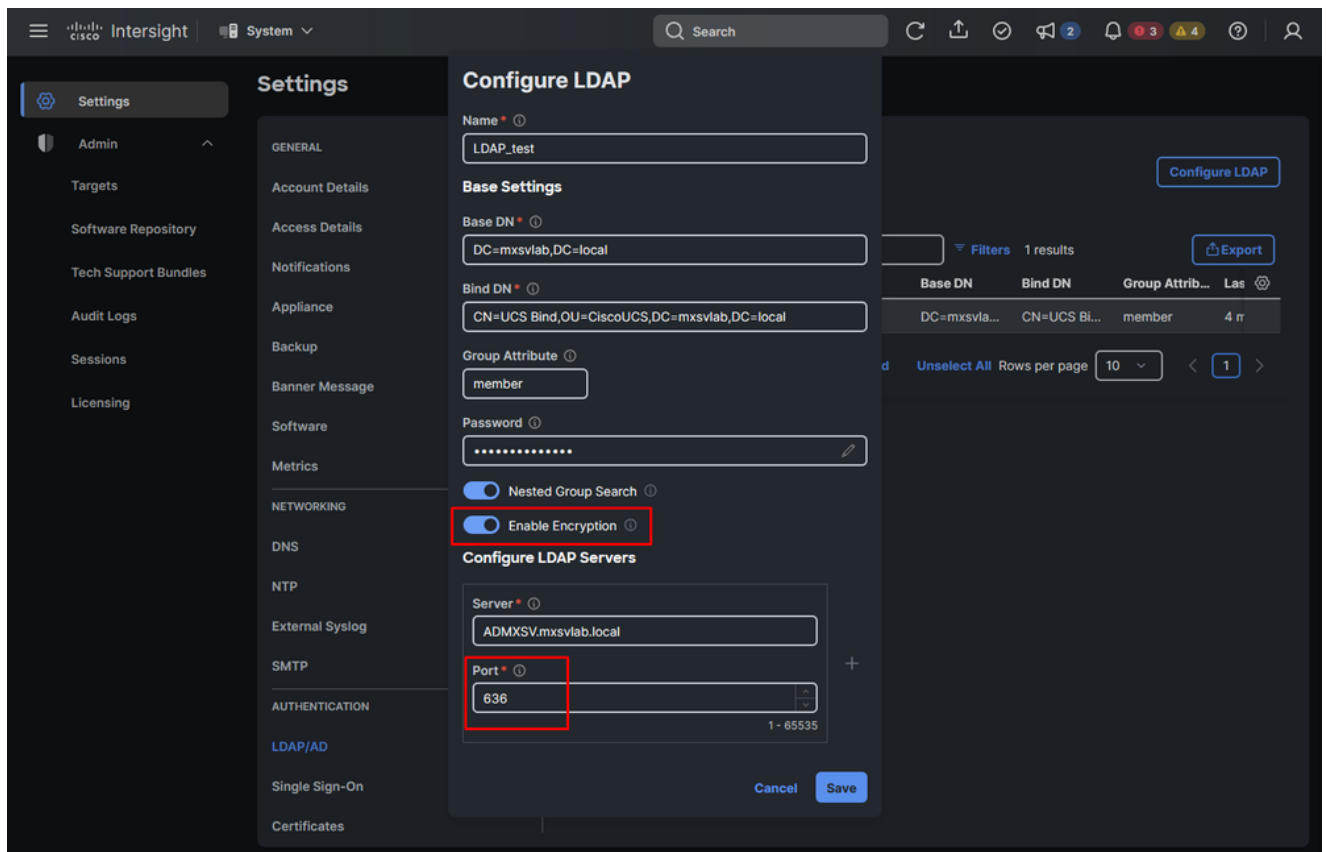


Configuratievoorbeeld voor een gebruiker

Configuratie van LDAPS (Secure LDAP)

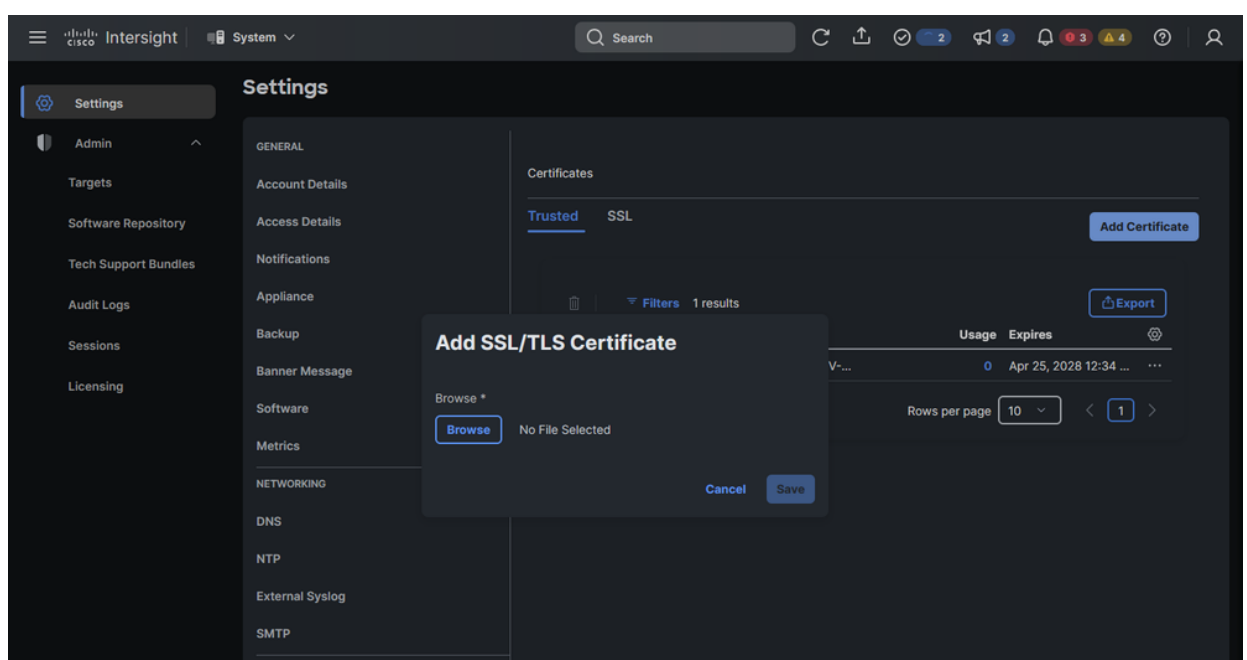
Als u wilt dat uw LDAP communicatie wordt beveiligd met encryptie, moet u een certificaat hebben ondertekend door uw CA. Zorg ervoor dat u deze wijzigingen in de configuratie toepast:

1. Voltooi de stappen vanaf Configuration of LDAP Basic Settings maar zorg ervoor dat de schuifschakelaar Encryption naar rechts inschakelt (Stap 3.g).
2. Zorg ervoor dat de gebruikte poort ofwel 636 of 3269 is, de poorten die LDAPS ondersteunen (beveiligd). Alle andere poorten ondersteunen LDAP via TLS.



Configuratie-wijzigingen voor Secure LDAP

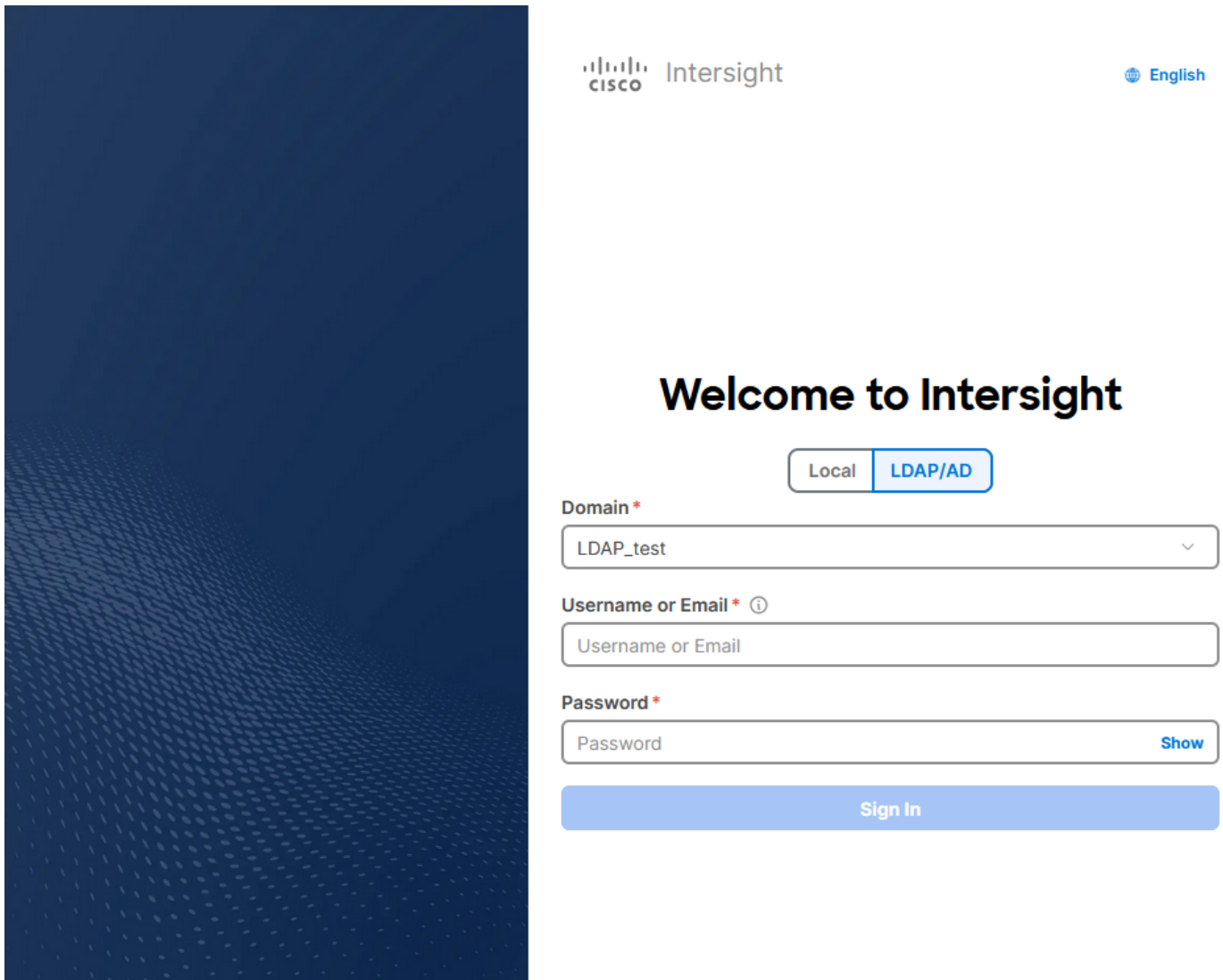
3. Sla de configuratie op en wacht tot de workflow ImplementationApplianceLDAP klaar is.
4. Voeg een certificaat toe met de volgende stappen:
 1. Navigeren naar Systeem > Instellingen > VERIFICATIE > Certificaten > Vertrouwd.
 2. Klik op Add Certificate (Certificaat toevoegen).
 3. Klik op Bladeren en selecteer een .pem-bestand dat het certificaat bevat dat is afgegeven door uw CA.



Configuratie om een certificaat toe te voegen

Verifiëren

Navigeer in uw browser naar uw Intersight Virtual Appliance URL. Het scherm toont nu een optie om in te loggen met LDAP-referenties:

The screenshot shows the Intersight login page. On the left is a large dark blue decorative panel with a subtle pattern. The right side is white. At the top right, there is the Cisco Intersight logo and a language selector set to 'English'. The main heading is 'Welcome to Intersight'. Below this are two tabs: 'Local' and 'LDAP/AD', with 'LDAP/AD' being the active tab. The login form includes a 'Domain' dropdown menu with 'LDAP_test' selected, a 'Username or Email' text input field, and a 'Password' text input field with a 'Show' toggle. A blue 'Sign In' button is at the bottom of the form.

LDAP-configuratie ingeschakeld vanaf het inlogscher

Problemen oplossen

Als de login mislukt, geven de foutmeldingen aanwijzingen over wat er fout kan zijn.

Fout 1. Onjuiste toegangsgegevens

Notification Details



LDAP login failed.

LDAP Authentication failed with the given credentials, LDAP Result Code 49. Check your username or password and try again.

Close

Foutmelding voor fout wachtwoord fout

Deze fout betekent dat de toegangsgegevens onjuist zijn.

1. Controleer of de gebruikersnaam en het wachtwoord juist zijn.

Fout 2. Fout bij binden van gegevens

Notification Details



LDAP login failed.

LDAP Authentication failed with the given bind credentials, LDAP Result Code 49. Check your BindDN and Bind password and try again.

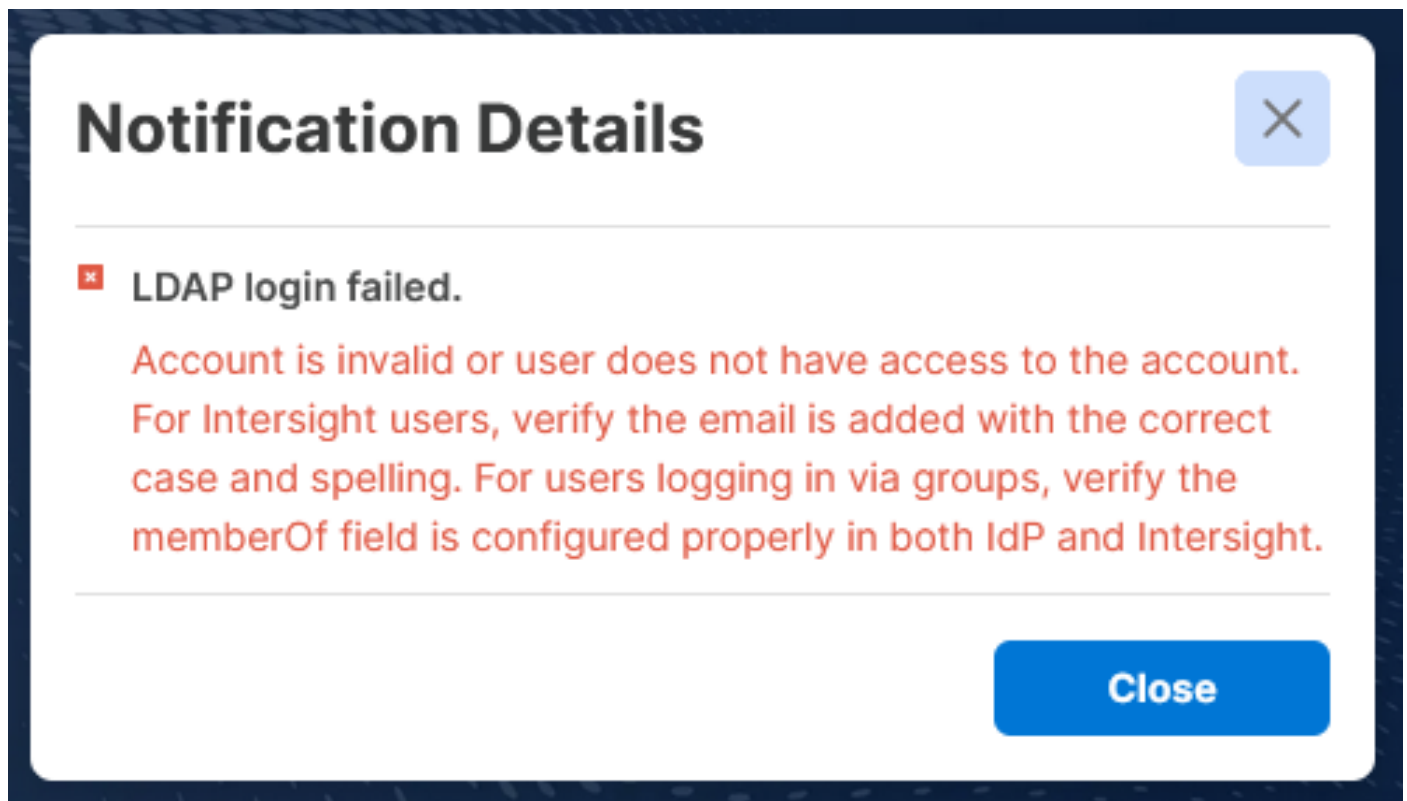
Close

Foutmelding voor verkeerde bindgegevens

Deze fout betekent dat de bind gegevens onjuist zijn.

1. Controleer de bindDN.
2. Controleer het bind wachtwoord dat in de LDAP-instellingen is ingesteld.

Fout 3. Kan geen gebruiker vinden



Foutmelding voor gebruiker niet gevonden

Dit wordt geactiveerd wanneer de zoekactie op de LDAP-server geen geautoriseerde gebruikers teruggeeft. Controleer of de volgende instellingen correct zijn:

1. Controleer BaseDN. De parameters die worden gebruikt om de gebruiker te zoeken, zijn onjuist.
2. Zorg ervoor dat het groepskenmerk is ingesteld op lid in plaats van lidOf.
3. Controleer of de groepsnaam in Identity Provider in de configuratie Groepen juist is. Dit geldt alleen als de vergunning via Groepen wordt verleend.
4. Controleer of de e-mail van de gebruiker correct is ingesteld in het e-mailveld in de AD-configuratie voor de gebruiker. Dit is alleen van toepassing als de vergunning aan individuele gebruikers wordt verleend.

Fout 4. Onjuist certificaat

Notification Details



✖ LDAP login failed.

LDAP login failed: Start TLS failed, x509: Certificate signed by unknown authority, LDAP Result Code 200. Check your CA certificate in the Trusted Certificates and try again.

Close

Foutmelding voor onjuist certificaat

Als versleutelde LDAP is ingeschakeld:

1. Controleer of het certificaat is geconfigureerd en het bevat het juiste volledige certificaat.

Fout 5. Encryptie inschakelen wordt gebruikt met een beveiligde poort

Notification Details



✖ LDAP login failed.

LDAP Authentication failed with the given bind credentials, LDAP Result Code 0. Check your BindDN and Bind password and try again.

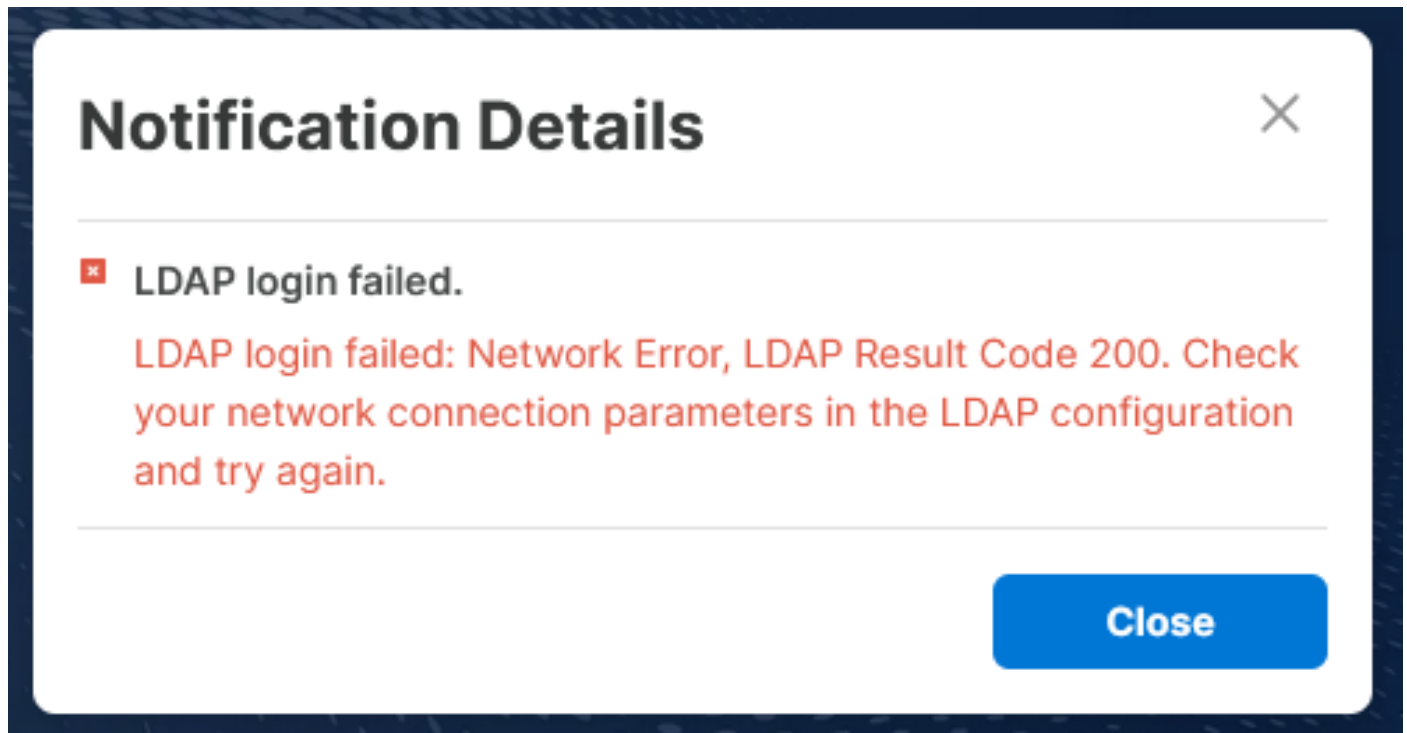
Close

Foutmelding voor Encryptie inschakelen is uitgeschakeld

Deze fout verschijnt wanneer Encryptie inschakelen niet is ingeschakeld maar er een poort voor beveiligde LDAP is geconfigureerd.

1. Zorg ervoor dat u poort 389 gebruikt als encryptie niet is ingeschakeld.

Fout 6. Verbindingsparameters onjuist



Foutmelding voor verkeerde poort

Deze fout betekent dat het niet mogelijk was om een succesvolle verbinding met de LDAP-server te maken. Verifieer:

1. De DNS-server moet de hostnaam van de LDAP-server oplossen naar de juiste IP.
2. Intersight-apparaat kan de LDAP-server bereiken.
3. Zorg ervoor dat poort 389 wordt gebruikt voor niet-versleutelde LDAP, 636 of 3269 voor beveiligde LDAP (LDAPS) en alle andere poorten voor TLS (activeer de codering en stel een certificaat in).

Gerelateerde informatie

- [De Cisco Intersight virtuele applicatie integreren met LDAP \(video\)](#)
- [LDAP-instellingen configureren in Intersight-applicatie](#)
- [Rollen en privileges in Intersight](#)
- [Monsterconfiguratie voor LDAP in UCSM](#)

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.