Configuratievoorbeeld van ISE Administration Portal Access met AD-Credentials

Inhoud

Inleiding

Dit document beschrijft een configuratievoorbeeld voor het gebruik van Microsoft Active Directory (AD) als een externe identiteitswinkel voor beheertoegang tot de Cisco Identity Services Engine (ISE) beheerGUI.

Voorwaarden

Cisco raadt kennis van de volgende onderwerpen aan:

- Configuratie van Cisco ISE versies 1.1.x of hoger
- Microsoft AD

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ISE versie 1.1.x
- Windows Server 2008 release 2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

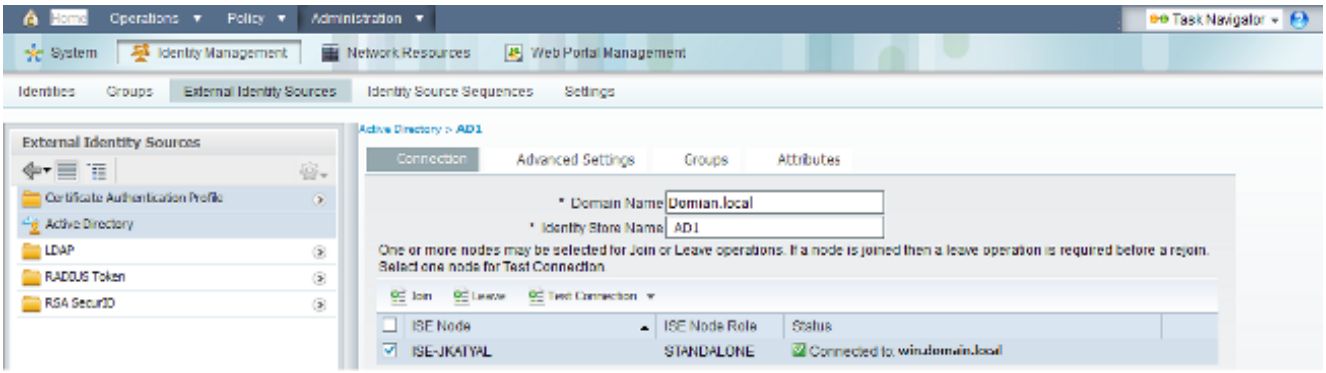
opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Gebruik deze sectie om te configureren voor het gebruik van Microsoft AD als een externe identiteitswinkel voor beheertoegang tot de Cisco ISE Management GUI.

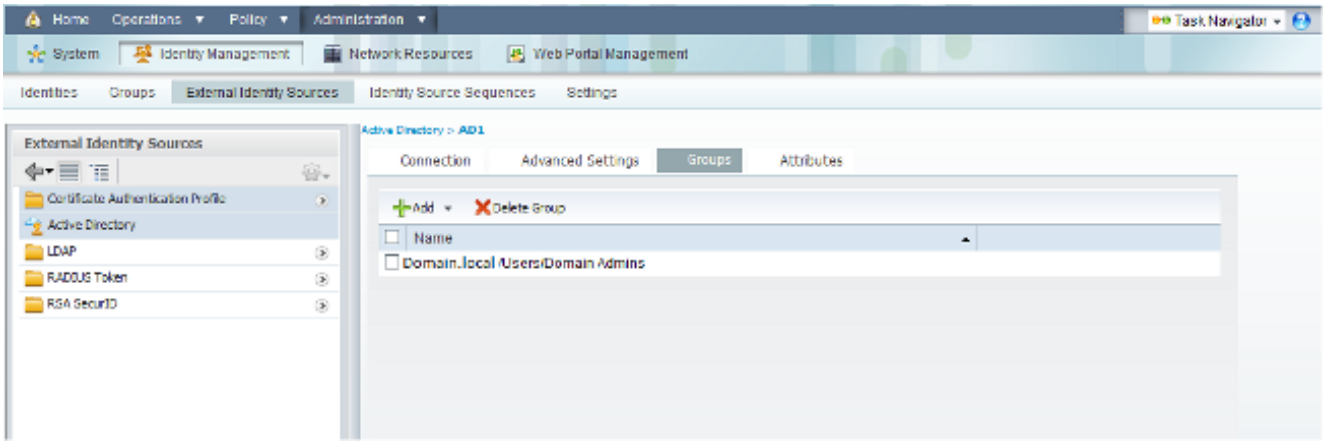
Doe mee met ISE naar AD

1. Navigeer naar **Administratie > identiteitsbeheer > Externe Bronnen > Actieve Map**.
2. Voer de AD Domain Name and Identity Store Name in en klik vervolgens op **Join**.
3. Voer de referenties in van de AD-account die wijzigingen in computerobjecten kan toevoegen en aanbrengen, en klik op **Configuratie opslaan**.



Map-groepen selecteren

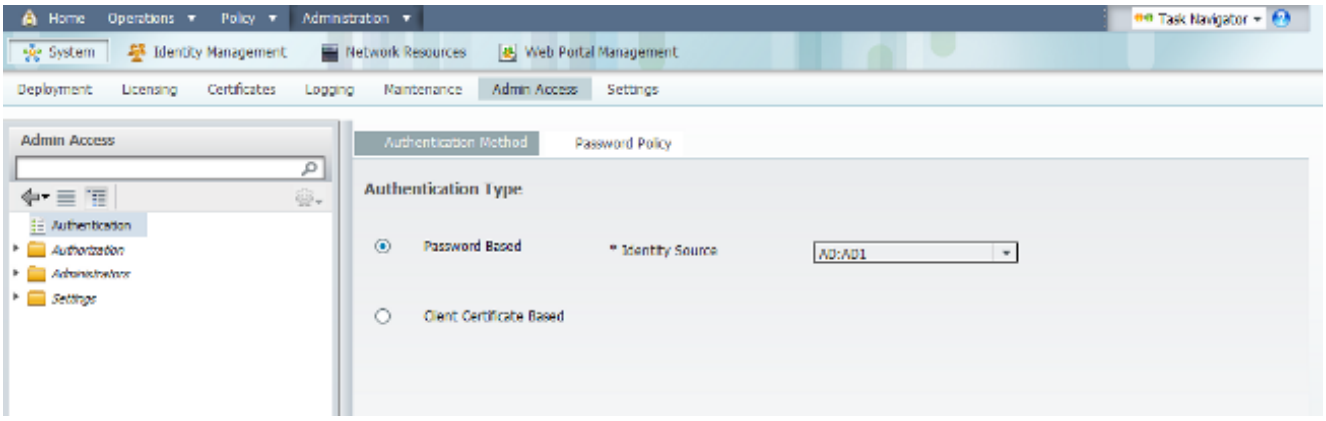
1. Navigeer naar **Administratie > identiteitsbeheer > Externe Identiteitsbronnen > Actieve Map > Groepen > Toevoegen > Selecteer groepen formuliermap**.
2. Importeer ten minste één AD-groep waartoe de beheerder behoort.



Administratieve toegang voor AD inschakelen

Voltooi deze stappen om op een wachtwoord gebaseerde verificatie voor AD mogelijk te maken:

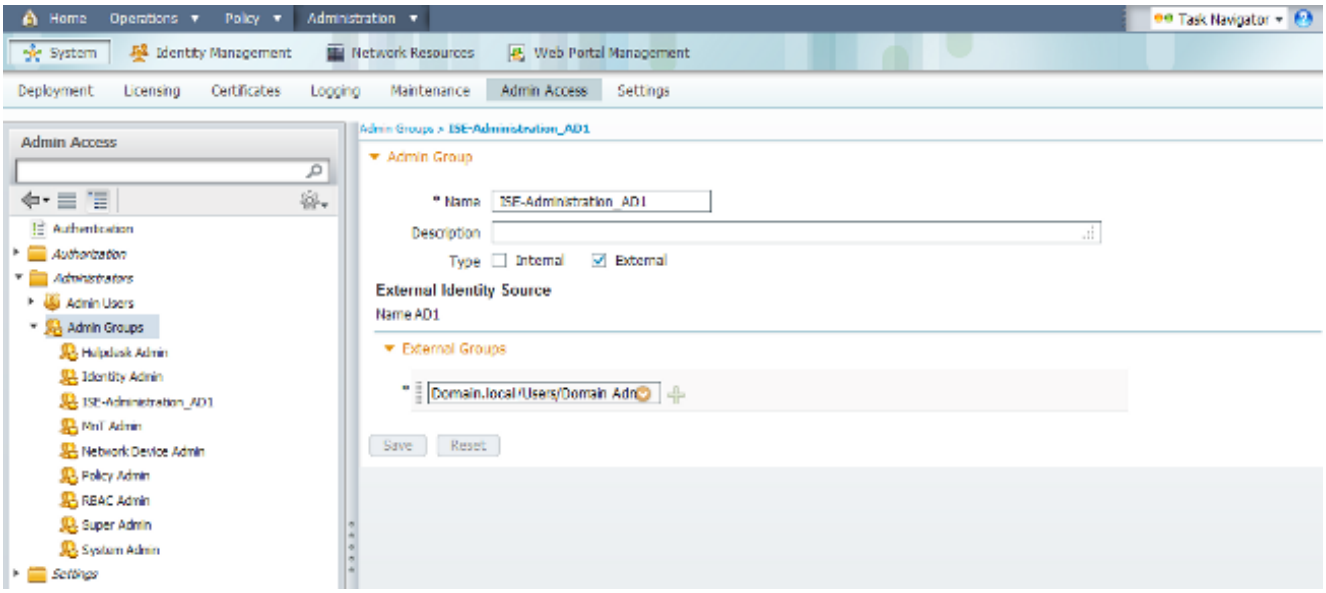
1. Navigeer naar **Administratie > Systeem > Admin Access > Verificatie**.
2. Selecteer in het tabblad **Verificatiemethode** de optie **Wachtwoord gebaseerd**.
3. Selecteer **AD** in het vervolgkeuzemenu **Identity** Source.
4. Klik op **Wijzigingen opslaan**.



Toewijzing van Admin-groep naar AD-groep configureren

Defineert een Cisco ISE Admin Group en zet deze in kaart aan een AD-groep. Dit staat een vergunning toe om de Rol Based Access Control (RBAC) machtigingen voor de beheerder te bepalen op basis van groepslidmaatschap in AD.

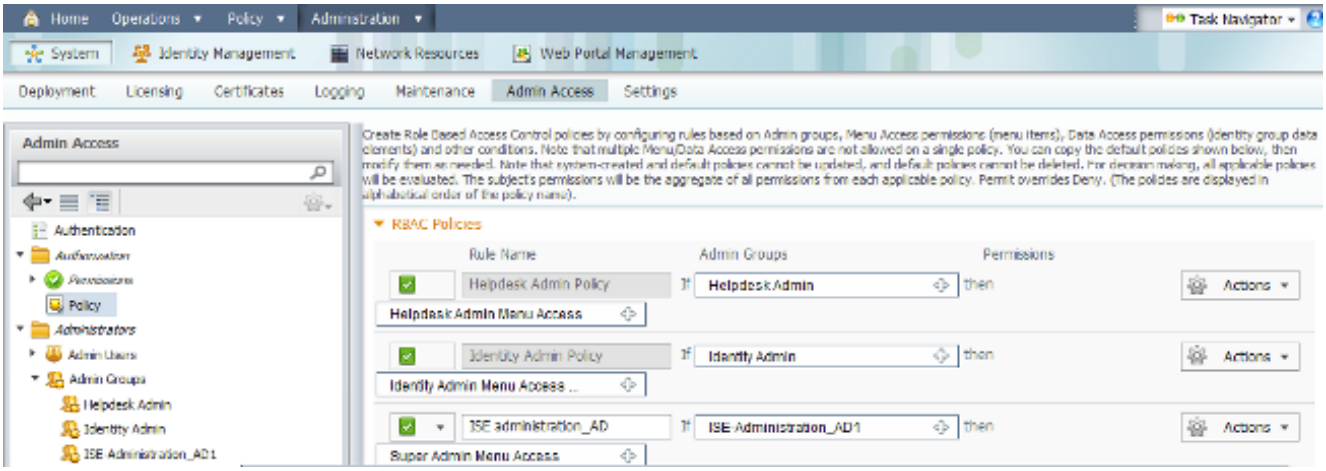
1. Navigeer naar **Administratie > Systeem > Admin Access > Beheerders > Admin Groepen**.
2. Klik op **Add** in de tabelkop om het nieuwe configuratievenster van de Admin Group te bekijken.
3. Voer de naam in voor de nieuwe Admin-groep.
4. Controleer in het veld Type het vakje **Externe** controle.
5. Selecteer in het vervolgkeuzemenu **Externe Groepen** de AD-groep waaraan u deze Admin-groep wilt toewijzen, zoals gedefinieerd in het gedeelte Map selecteren.
6. Klik op **Wijzigingen opslaan.**



RBAC-toegangsrechten voor de Admin-groep instellen

Voltooi deze stappen om RBAC-toegangsrechten toe te kennen aan de Admin-groepen die in de vorige sectie zijn gemaakt:

1. Navigeer naar **Administratie > Systeem > Admin Access > autorisatie > Beleid**.
2. Selecteer in het vervolgkeuzemenu **Handelingen** rechts de optie **Nieuw beleid invoegen hieronder** om een nieuw beleid toe te voegen.
3. Maak een nieuwe regel die **ISE_administration_AD** wordt genoemd, stel deze in kaart met de Admin Group die in de sectie Toegang voor AD van het Bevoegd wordt gedefinieerd, en verdeel het recht.Opmerking: In dit voorbeeld wordt de Admin Group die **Super Admin** wordt genoemd toegewezen, wat aan de standaard admin account gelijkwaardig is.
4. Klik op **Wijzigingen opslaan** en de bevestiging van de opgeslagen wijzigingen wordt weergegeven in de rechterbenedenhoek van de GUI.



Toegang tot ISE met AD-Credentials

Voltooi deze stappen om toegang te krijgen tot ISE met AD-referenties:

1. Uitloggen van de administratieve GUI.
2. Selecteer **AD1** in het vervolgkeuzemenu **Identity** Source.
3. Voer de gebruikersnaam en het wachtwoord in uit de AD-database en log in.

Opmerking: ISE is standaard ingeschakeld voor de interne gebruikerswinkel als AD onbereikbaar is of de gebruikte accountnummers niet in AD bestaan. Dit vergemakkelijkt het snel inloggen als u de interne winkel gebruikt terwijl AD voor administratieve toegang is ingesteld.

Verifiëren

Om te bevestigen dat uw configuratie correct werkt, verifieert u de geauthenticeerde gebruikersnaam aan de rechterbovenhoek van de ISE GUI.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Gebruikershandleiding voor Cisco Identity Services Engine, release 1.1 - Onderhoudskenmerken en beheerderstoegang
- Technische ondersteuning en documentatie – Cisco Systems