ACS 5.x en hoger - Integratie met Microsoft AD configureren

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie voor het integreren van Microsoft Active Directory met Cisco Secure Access Control System (ACS) 5.x en hoger. ACS gebruikt Microsoft Active Directory (AD) als een externe identiteitsopslag om resources zoals gebruikers, machines, groepen en eigenschappen op te slaan. ACS bevestigt deze middelen tegen AD.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- Windows Active Directory Domain om te worden gebruikt, moet volledig worden geconfigureerd en gebruiksklaar zijn.
- Gebruik Microsoft Windows Server 2003 Domain, Microsoft Windows Server 2008 Domain of Microsoft Windows Server 2008 R2 Domain aangezien deze door ACS 5.x worden ondersteund.**Opmerking:** Integratie van Microsoft Windows Server 2008 R2-domein met ACS wordt ondersteund door ACS 5.2 en later.

Gebruikte componenten

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

- Cisco beveiligde ACS 5.3
- Microsoft Windows Server 2003-domein

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.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

Windows Active Directory biedt veel functies die in het dagelijkse netwerkgebruik worden gebruikt. De integratie van ACS 5.x met AD maakt het gebruik van bestaande AD-gebruikers, machines en hun groepstoewijzing mogelijk.

ACS 5.x geïntegreerd met AD biedt deze functies:

1. Machine-verificatie
2. Teruggave van kenmerken voor autorisatie
3. certificaatvernieuwing voor EAP-TLS-verificatie
4. Beperking aantal gebruikers- en machineaccount
5. Beperkingen van toegang machine
6. Controleer inbeltoegangsrechten
7. Terugbellen voor inbelgebruikers
8. Ondersteuning van inbellen

Configuratie

ACS 5.x Application Deployment Engine (ADE-OS) configureren

Zorg ervoor dat de **TimeZone, datum en tijd** op de ACS-overeenkomsten overeenkomen met die op de AD-primaire domeincontroller voordat u ACS 5.x in de AD integreert. Bepaal ook de DNS server op ACS om de domeinnaam van ACS 5.x op te lossen. Voltooi deze stappen om ACS 5.x Application Engine (ADE-OS) te configureren:

1. SSH aan het ACS-apparaat en voer de CLI-referenties in.
2. Geef de opdracht **kloktijd uit** in de configuratie-modus zoals getoond om de **TIMEZONE** op de ACS te configureren om deze op de domeincontroller af te stemmen.

   ```
   clock timezone Asia/Kolkata
   ```

   Opmerking: Asia/Kolkata is de tijdzone die in dit document wordt gebruikt. U kunt uw specifieke tijdzone vinden door exec mode **de** opdracht **van de tijdzones te tonen**.
3. Indien uw AD-domeincontroller gesynchroniseerd is met een NTP-server die in uw netwerk verblijft, wordt het sterk aanbevolen om dezelfde NTP-server op de ACS te gebruiken. Als u geen NTP-server hebt, sla dan over naar **stap 4**. Dit zijn de stappen om NTP-server te

configureren:NTP-server kan met het **ntp server <ip-adres van de NTP server>**-opdracht worden ingesteld in configuratie-modus zoals getoond.

```
ntp server 192.168.26.55
The NTP server was modified.
If this action resulted in a clock modification, you must restart ACS.
```

Raadpleeg [ACS 5.x: Cisco ACS-synchronisatie met NTP Server Configuration Voorbeeld] voor meer informatie over NTP-configuratie.

4. Om datum en tijd handmatig te configureren gebruikt u de **klokinstelling** opdracht in **exec-modus**. Hier wordt een voorbeeld getoond:

```
clock set Jun 8 10:36:00 2012
Clock was modified. You must restart ACS.
Do you want to restart ACS now? (yes/no) yes
Stopping ACS.
Stopping Management and View.....................
Stopping Runtime......
Stopping Database....
Cleanup.....
Starting ACS ....

To verify that ACS processes are running, use the
'show application status acs' command.
```

5. Controleer nu de **Time-zone, datum** en **tijd** bij de opdracht **Show kloktijd**. De uitvoer van de opdracht Kloktijd wordt hier weergegeven:

```
acs51/admin# show clock
Fri Jun  8 10:36:05 IST 2012
```

6. Configureer DNS op ACS met het **<ip-naam-server <ip-adres van de DNS>**-opdracht in **configuratiemodus** zoals hier wordt getoond:

```
ip name-server 192.168.26.55
```

Opmerking: Het DNS IP-adres is door de beheerder van uw Windows-domein beschikbaar.

7. Geef de opdracht **nslookup <domeinnaam>** uit om de bereikbaarheid van de domeinnaam zoals aangegeven te controleren.

```
acs51/admin#nslookup MCS55.com
Trying "MCS55.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60485
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
;MCS55.com.                     IN      ANY

;; ANSWER SECTION:
MCS55.com.              600     IN      A       192.168.26.55
MCS55.com.              3600    IN      NS      admin-zq2ttn9ux.MCS55.com.
MCS55.com.              3600    IN      SOA     admin-zq2ttn9ux.MCS55.com.
   hostmaster.MCS55.com. 635 900 600 86400 3600

;; ADDITIONAL SECTION:
admin-zq2ttn9ux.MCS55.com. 3600 IN      A       192.168.26.55

Received 136 bytes from 192.168.26.55#53 in 0 ms
```

Opmerking: Als het **gedeelte ANTWOORD** leeg is, neem dan contact op met de beheerder van het Windows-domein om te weten te komen welke DNS-server het juiste is.

8. Geef de opdracht **ip-domeinnaam <domeinnaam>** uit om **DOMAIN-NAME** op de ACS te configureren zoals hier wordt getoond:

```
ip domain-name MCS55.com
```

9. Geef de **hostname <hostname>** opdracht uit om **HOSTNAME** op de ACS te configureren zoals hier wordt getoond:

```
hostname acs51
```

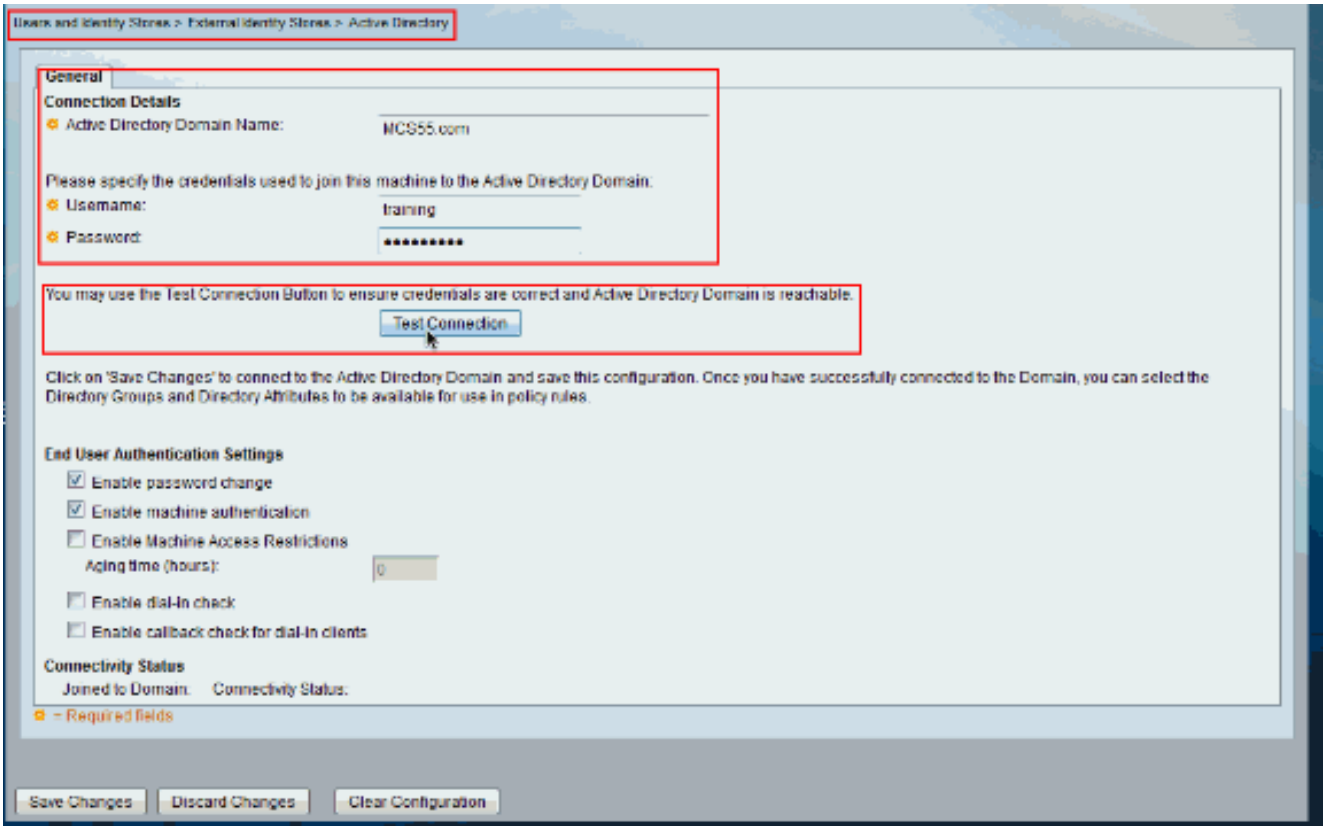
N.B.: Vanwege de beperkingen van het NETzien, moeten ACS-hostnamen minimaal 15 tekens bevatten.

10. Geef de opdracht **Schrijfgeheugen op** om de configuratie op ACS op te slaan.

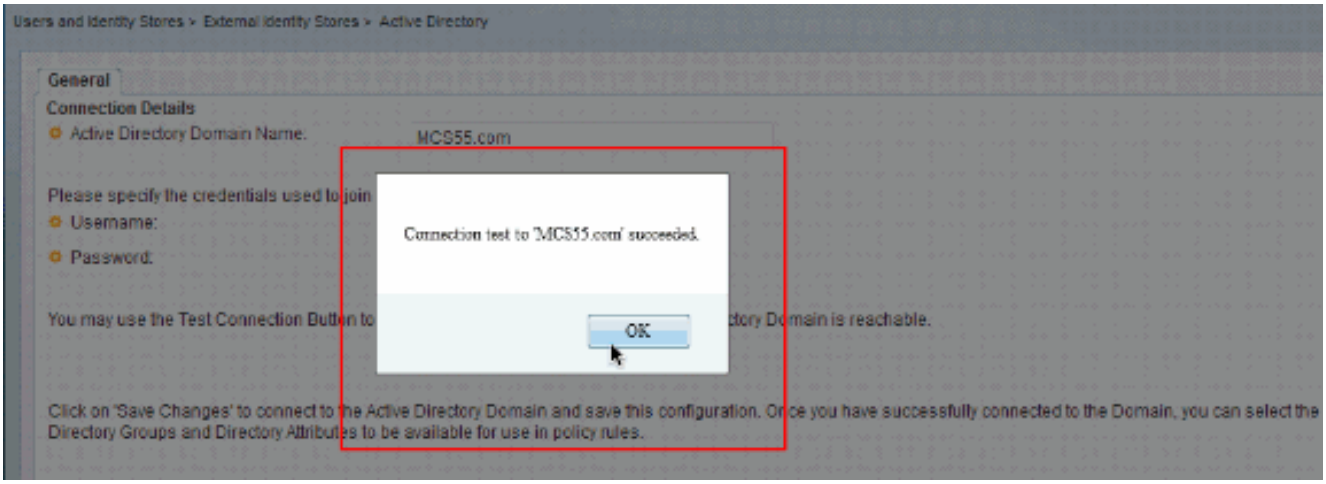
Samenvoegen ACS 5.x tot AD

Voltooi deze stappen om zich aan te sluiten bij ACS5.x tot AD:

1. Kies **gebruikers en identiteitsopslag > Externe identiteitsopslag > Actieve map** en geef de domeinnaam, AD-account (gebruikersnaam) en het wachtwoord op en klik op **Test Connection**.**Opmerking:** AD-account vereist voor domeintoegang in ACS moet een van de volgende kenmerken hebben:Voeg werkstations toe aan het juiste domein van de gebruiker in het betreffende domein.Maak Computer Objects of verwijder Computer Objects toestemming op corresponderende computercontainer waar de ACS-machineaccount is gemaakt voordat u de ACS-machine naar het domein sluit.**Opmerking:** Cisco raadt u aan het uitsluitingsbeleid voor de ACS-account uit te schakelen en de AD-infrastructuur te configureren om signaleringen naar de beheerder te verzenden als er een fout wachtwoord voor die account wordt gebruikt. Dit komt doordat als u een fout wachtwoord invoert, ACS het rekenschap van de machine niet aanmaakt of wijzigt wanneer het nodig is en daarom mogelijk alle authenticaties ontkent.**Opmerking:** De Windows AD-account, dat ACS-bestanden naar het AD-domein voegt, kan in de eigen organisatie-eenheid (OU) worden geplaatst. Deze account is aangemaakt of heeft een beperking waardoor de naam van het apparaat moet overeenkomen met de naam van de AD-account.

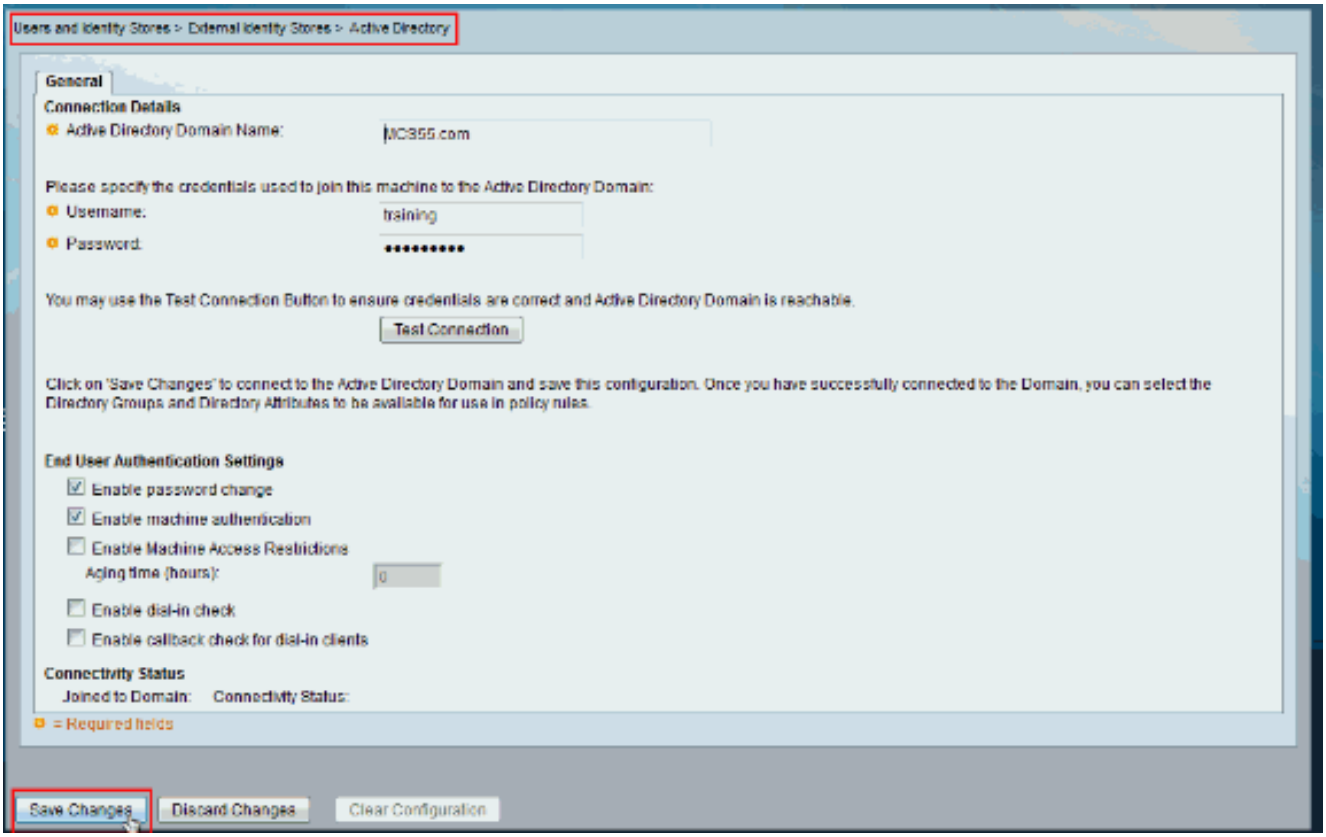


2. Dit screenshot laat zien dat de testverbinding met de AD succesvol is. Klik vervolgens op **OK**.



Opmerking: Centrify configuratie wordt beïnvloed en wordt soms losgekoppeld als er een trage reactie van de server is terwijl u de ACS verbinding met het AD-domein test. Maar het werkt prima voor de andere toepassingen.

3. Klik op **Wijzigingen opslaan** voor ACS om mee te doen met AD.



4. Zodra ACS met succes tot het AD Domein is toegetreden, toont het in de connectiviteitsstatus.

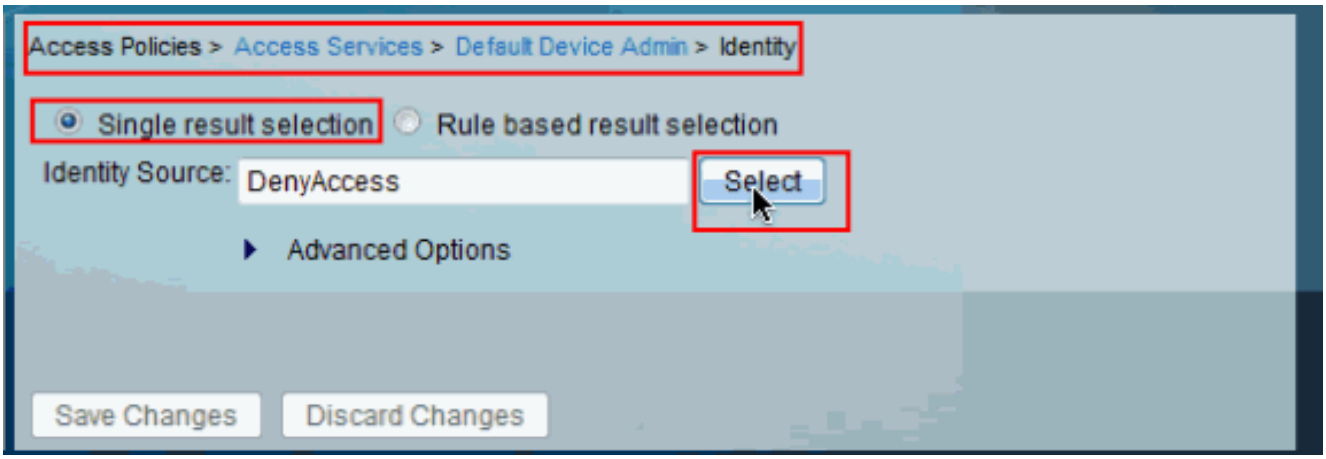
Opmerking: Wanneer u een AD-identiteitswinkel configureren maakt ACS ook:Een nieuw woordenboek voor die winkel met twee eigenschappen: Externe groepen en een ander kenmerk voor elke eigenschap die uit de map wordt opgeroepen.Een nieuw kenmerk, IdentityAccessBeperkt. U kunt handmatig een aangepaste voorwaarde voor deze eigenschap maken.Een aangepaste voorwaarde voor groepstoewijzing van de eigenschap ExternGroup; de naam van de douaneconditie is AD1:Extern Groepen en een andere maatvoorwaarde voor elke

eigenschap geselecteerd in de pagina van de Eigenschappen van de Map, bijvoorbeeld, AD1:cn.

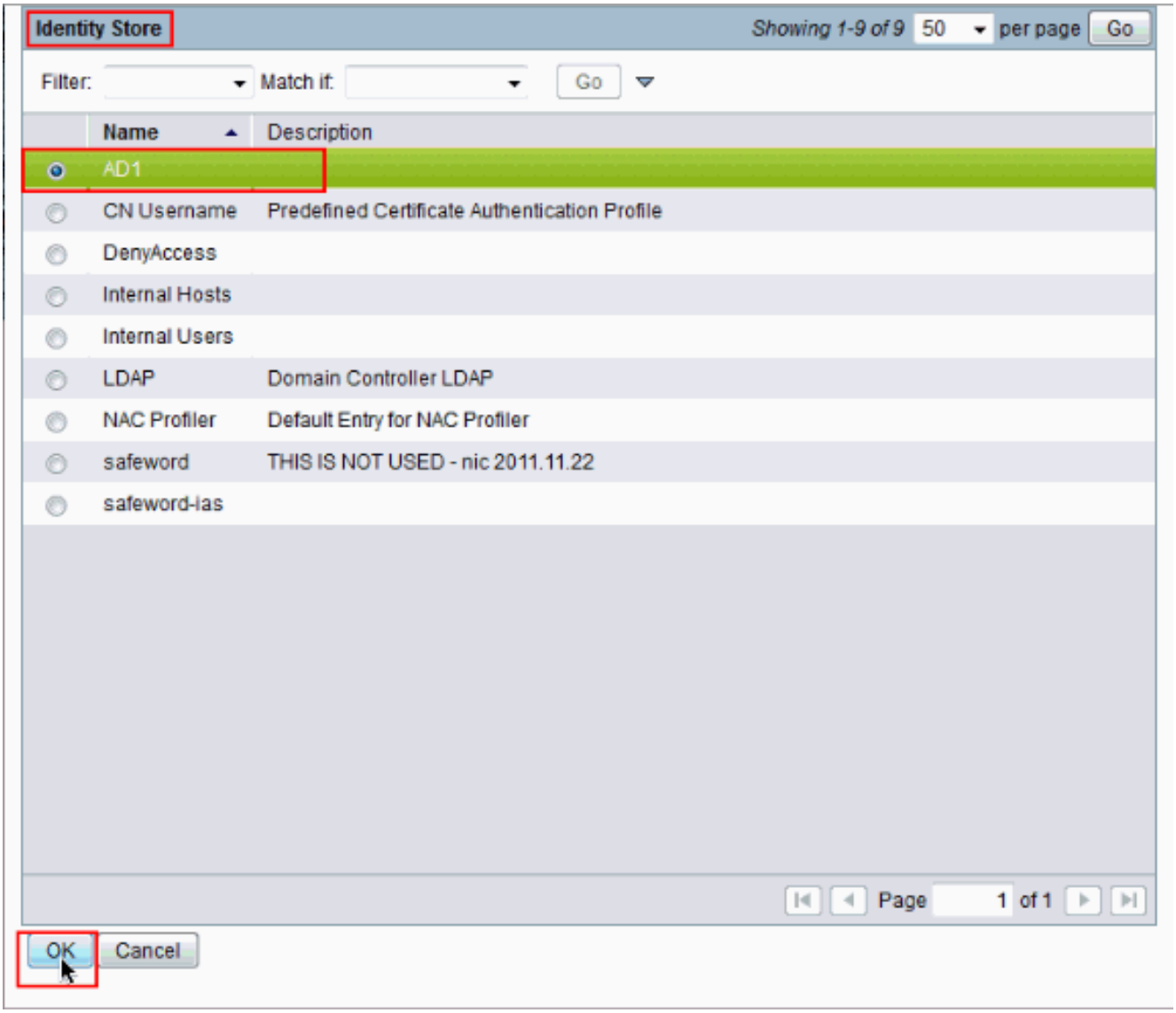
Toegangsservice configureren

Voltooi deze stappen om de configuratie van de toegangsservice te voltooien zodat ACS de nieuw geconfigureerd AD-integratie kan gebruiken.

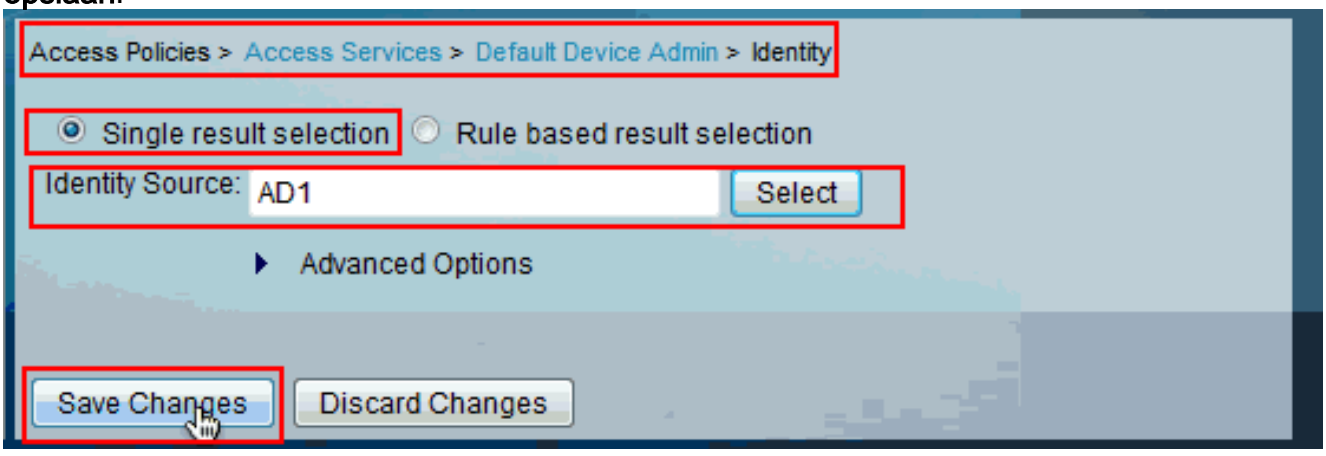
1. Kies de service vanuit welke u wilt dat de gebruikers worden geauthentiseerd vanuit AD en klik op **Identity**. Klik nu op **Selecteren** naast het veld Identity Source.



2. Kies **AD1** en klik op **OK**.



3. Klik op **Wijzigingen opslaan**.

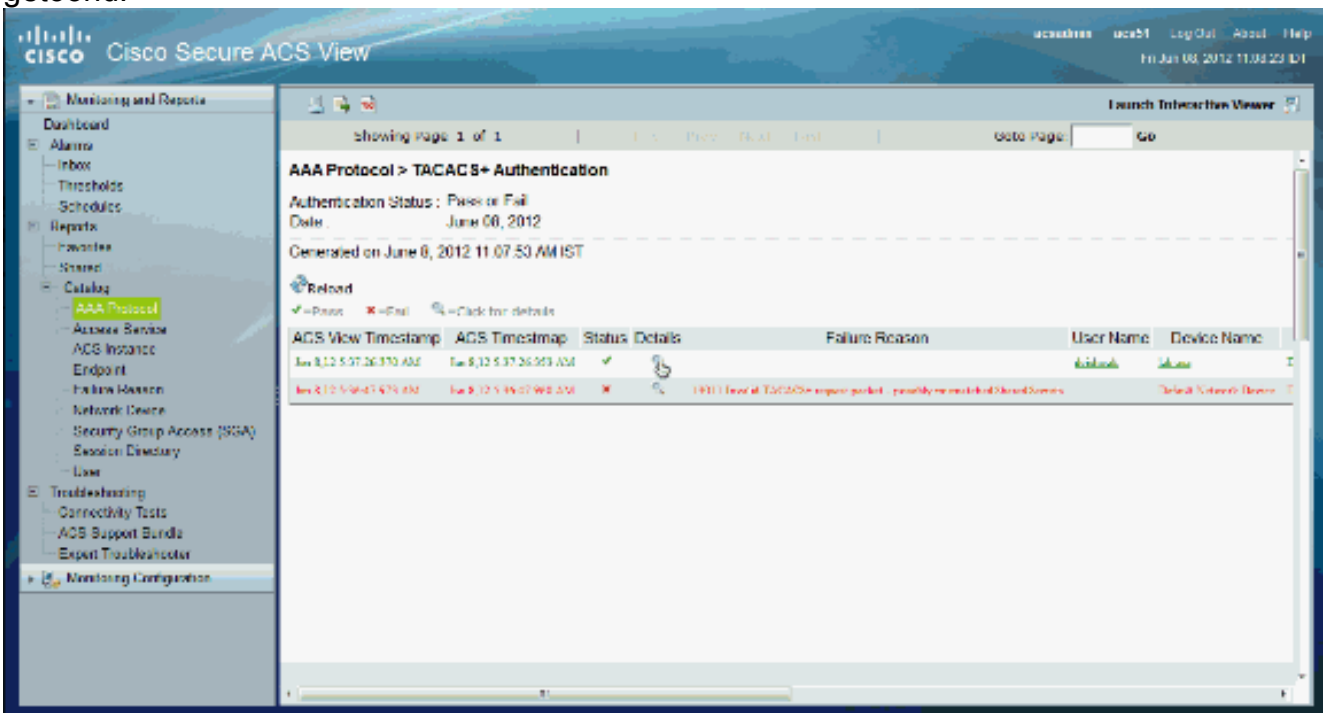


Verifiëren

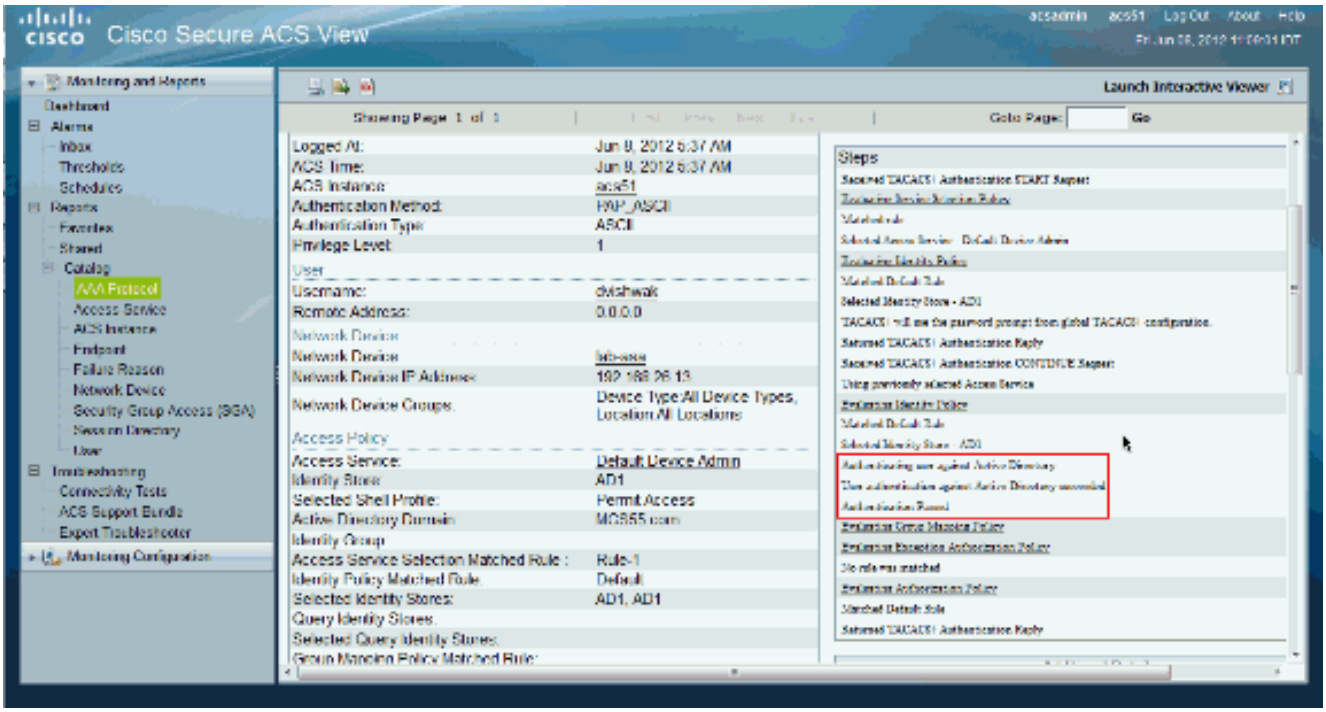
Om AD-verificatie te verifiëren, stuurde zij een verificatieaanvraag van een NAS met AD-referenties. Zorg ervoor dat de NAS op de ACS is geconfigureerd en dat het verzoek wordt verwerkt door de toegangsservice die in de vorige sectie is ingesteld.

1. Na succesvolle verificatie van NAS-loggen in de ACS-GUI en kies **monitoring en rapporten > AAA-protocol > TACACS+verificatie**. Identificeer de passerende authenticatie uit de lijst en

klik op het **vergrootglas** symbool zoals getoond.



2. U kunt verifiëren uit de stappen die ACS verificatieaanvraag naar AD heeft verzonden.



Gerelateerde informatie

- Cisco Secure Access Control-systeem
- Technische ondersteuning en documentatie – Cisco Systems