Dynamische toegangscontrolelijsten per gebruiker configureren in ISE

Inhoud

Inleiding

Dit document beschrijft de configuratie van een dynamische toegangscontrolelijst (dACL) per gebruiker voor gebruikers die aanwezig zijn in een type identiteitsarchief.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van beleidsconfiguratie op Identity Services Engine (ISE).

Gebruikte componenten

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

- Identity Services Engine 3.0
- Microsoft Windows Active Directory 2016

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

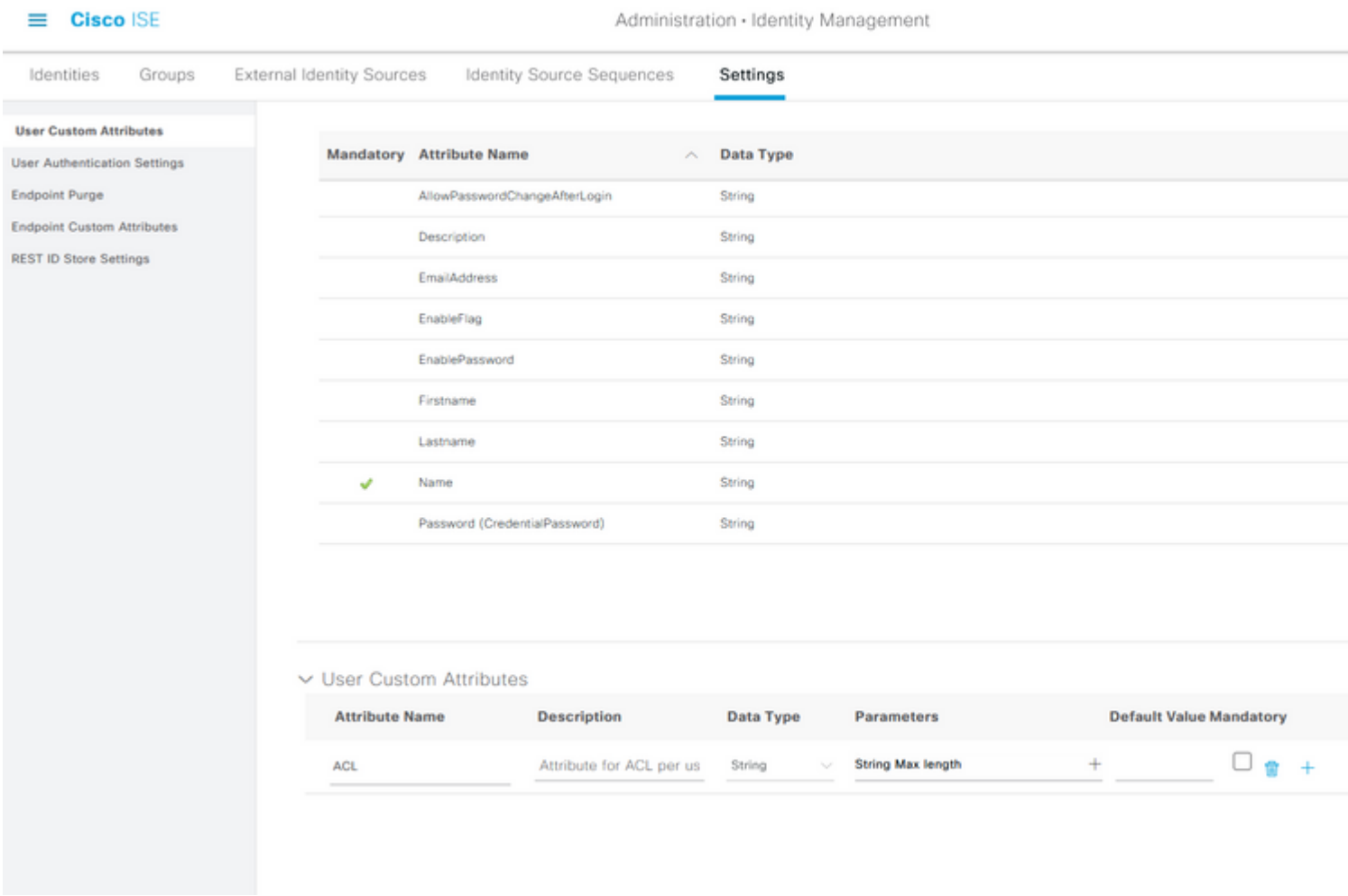
De configuratie van een dynamische toegangscontrolelijst per gebruiker is voor gebruikers die aanwezig zijn in het interne identiteitsarchief van ISE of in een extern identiteitsarchief.

Configureren

Per-gebruiker dACL kan worden geconfigureerd voor elke gebruiker in de interne winkel die een aangepast gebruikerskenmerk gebruikt. Voor een gebruiker in de Active Directory (AD), kan elke eigenschap van type string worden gebruikt om hetzelfde te bereiken. Deze sectie verschaft informatie die vereist is om de eigenschappen van zowel ISE als AD te kunnen configureren, samen met de configuratie die vereist is op ISE voor het werken met deze functie.

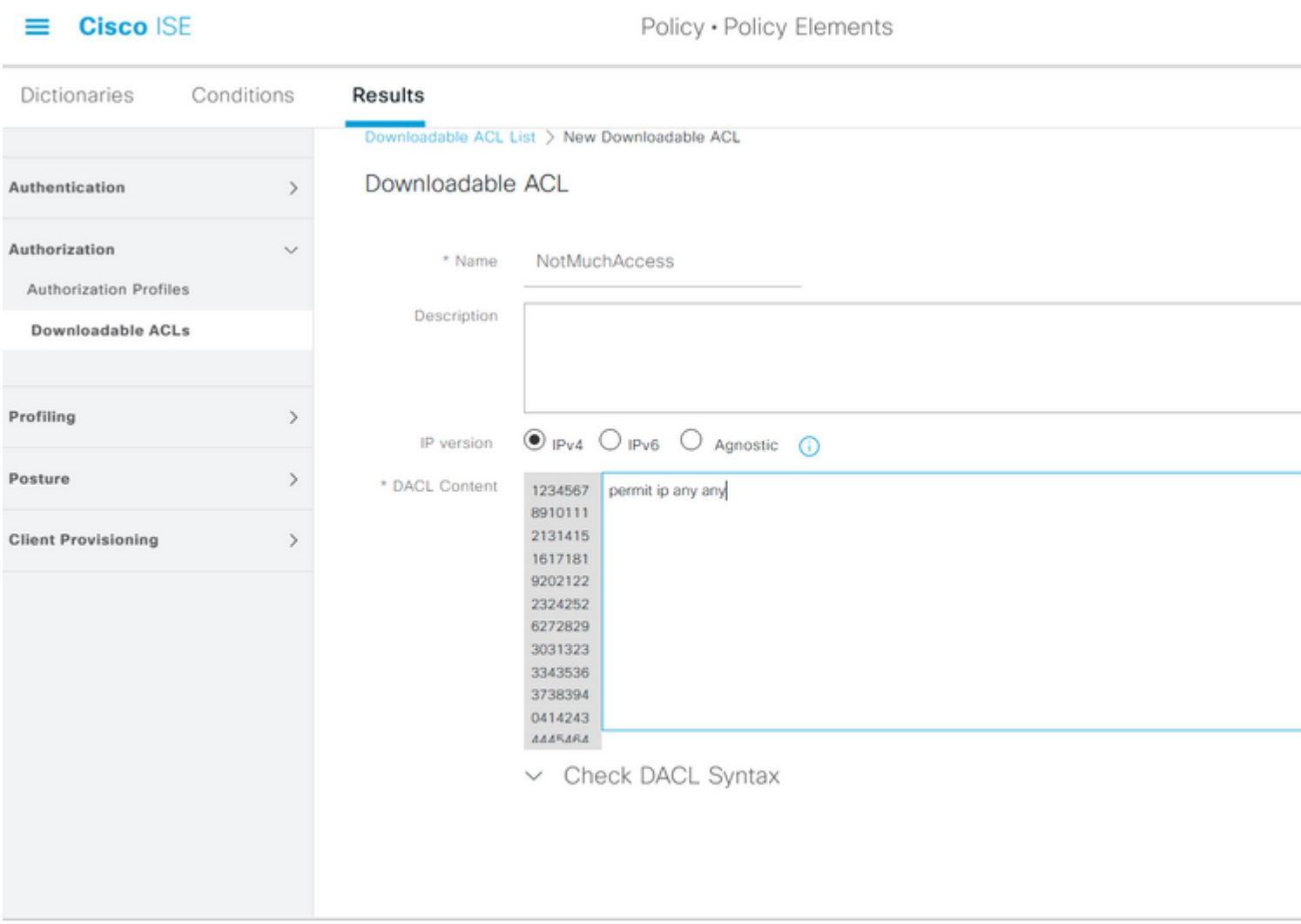
Configureer een nieuw aangepast gebruikerskenmerk op ISE

Ga naar **Beheer > Identity Management > Instellingen > Aangepaste gebruikerskenmerken**. Klik op de knop **+**, zoals in de afbeelding, om een nieuw kenmerk toe te voegen en de wijzigingen op te **slaan**. In dit voorbeeld is de naam van het aangepaste kenmerk **ACL**.



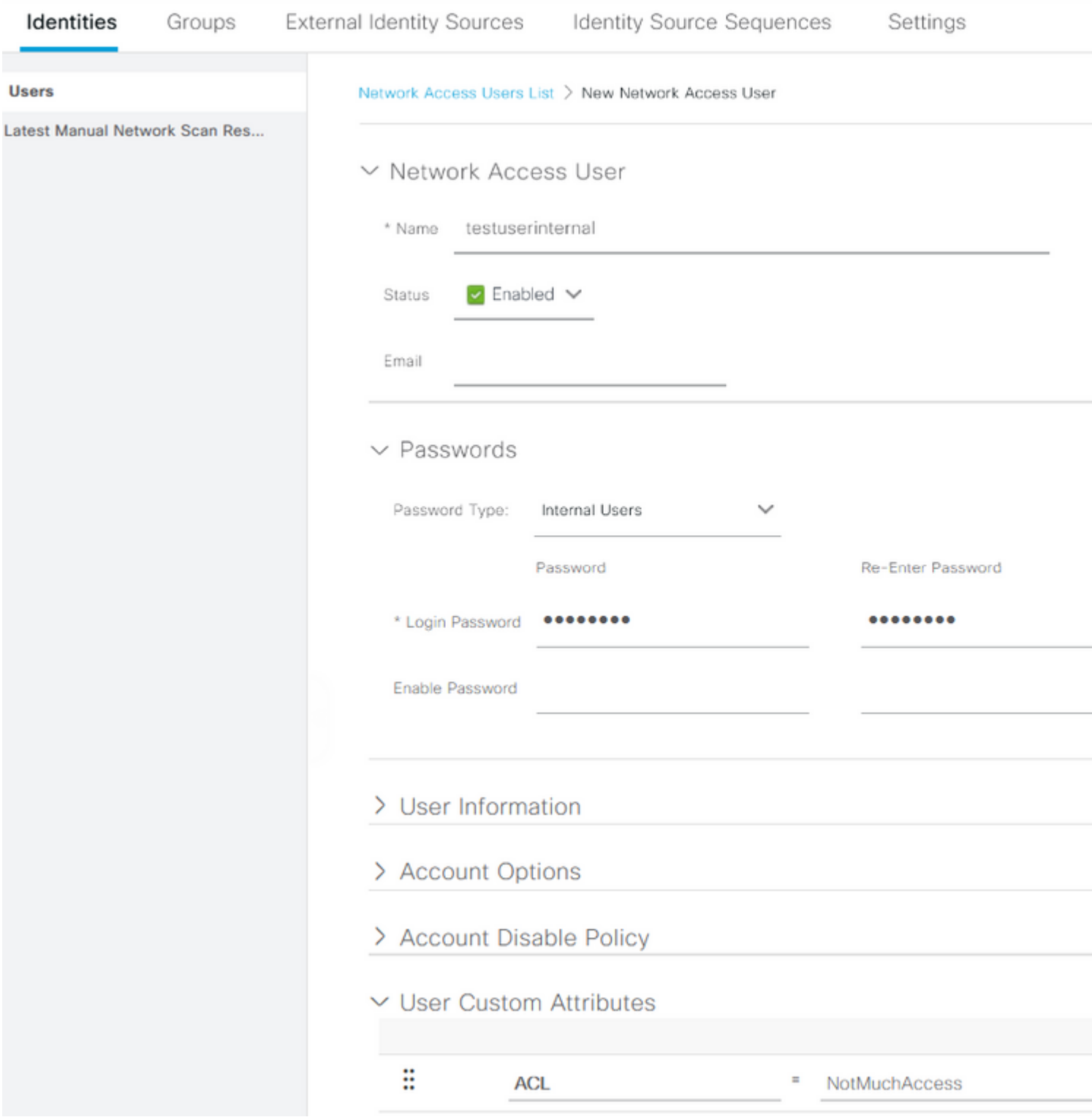
DACL configureren

Om downloadbare ACLâ€™s te configureren navigeert u naar **Beleid > Beleidselementen > Resultaten > Autorisatie > Downloadbare ACLâ€™s**. Klik op Add (Toevoegen). Geef een naam, inhoud van de dACL op en **sla** de wijzigingen op. Zoals in het beeld wordt getoond, is de naam van dACL **NotMuchAccess**.



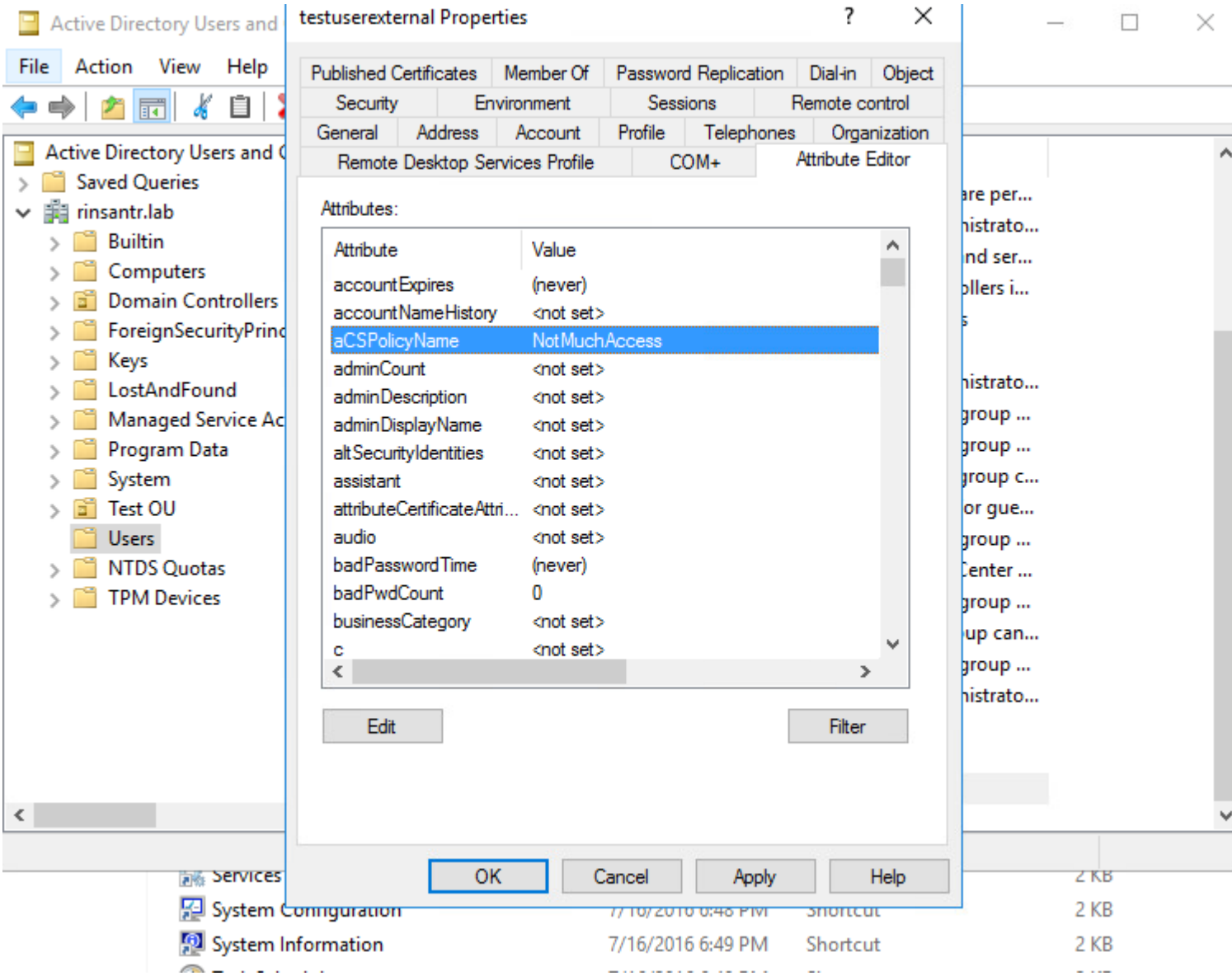
Een interne gebruikersaccount configureren met het aangepaste kenmerk

Ga naar **Beheer > Identity Management > Identity > Gebruikers > Add**. Maak een gebruiker en vorm de aangepaste attribuutwaarde met de naam van de dACL die de gebruiker moet krijgen wanneer geautoriseerd. In dit voorbeeld is de naam van dACL **NotMuchAccess**.



Een AD-gebruikersaccount configureren

Navigeer in de Active Directory naar de eigenschappen van de gebruikersaccount en ga vervolgens naar het tabblad **Attribute Editor**. Zoals in de afbeelding wordt getoond, is **CSPpolicyName** het kenmerk dat wordt gebruikt om de dACL-naam te specificeren. Echter, zoals eerder vermeld, elke eigenschap die een string waarde kan accepteren kan ook gebruikt worden.



Attributen van AD naar ISE importeren

Om het attribuut te gebruiken dat op AD is geconfigureerd, moet ISE het importeren. Om het kenmerk te importeren, navigeer je naar **Beheer > Identity Management > Externe Identity Sources > Active Directory > [Join point geconfigureerd] >** tabblad **Attributen**. Klik op **Add** en **selecteer** vervolgens **Attributen uit Directory**. Geef de naam van de gebruikersaccount op in de advertentie en klik vervolgens op **Kenmerken ophalen**. Selecteer het kenmerk dat voor de dACL is ingesteld, klik op **OK** en klik vervolgens op **Opslaan**. Zoals in de afbeelding wordt getoond, is CSPpolicyName het kenmerk.

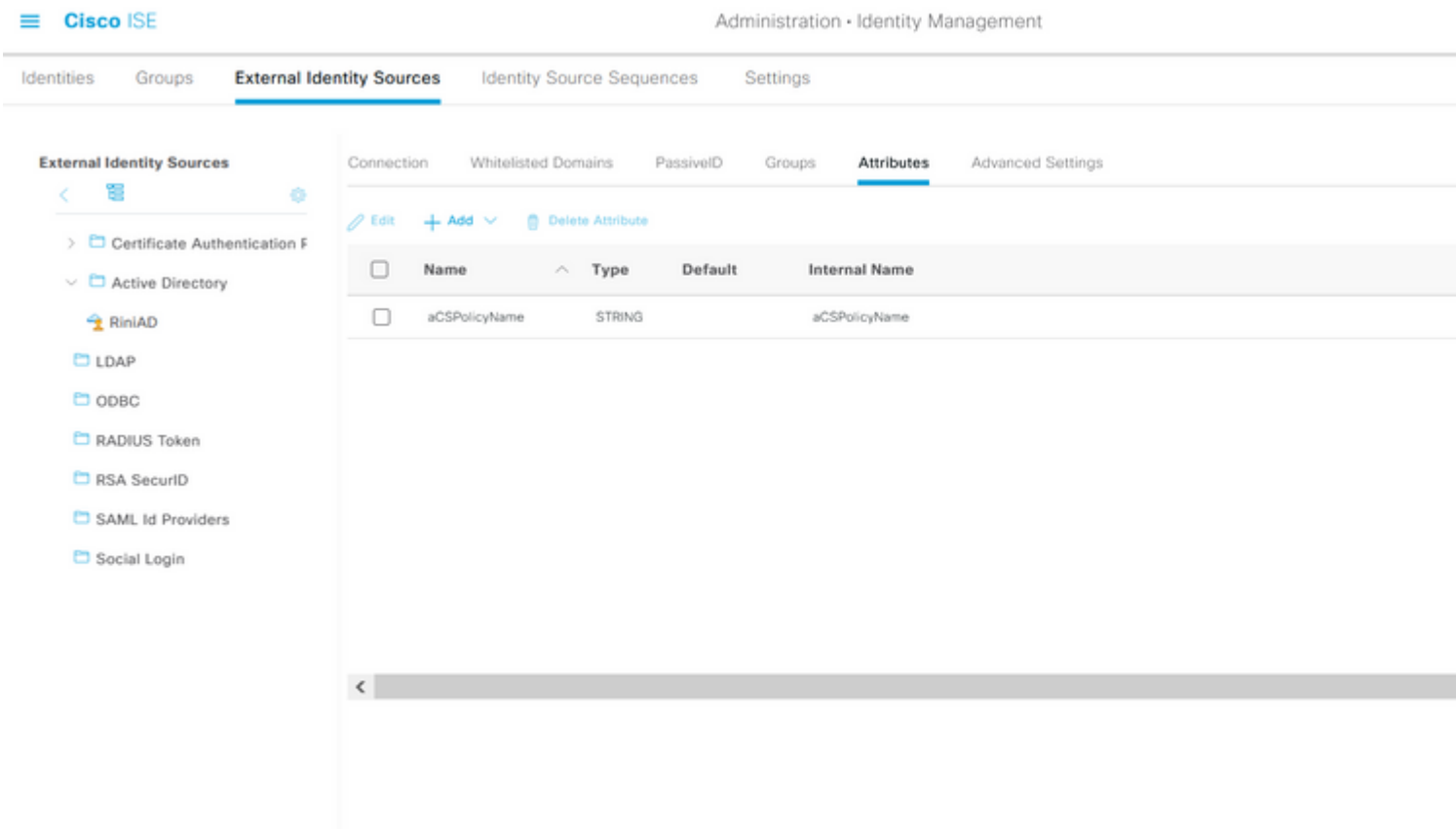
Directory Attributes

Only attributes selected below will be available for use as policy conditions in policy rules.

* Sample User or Machine Account: testuserexternal

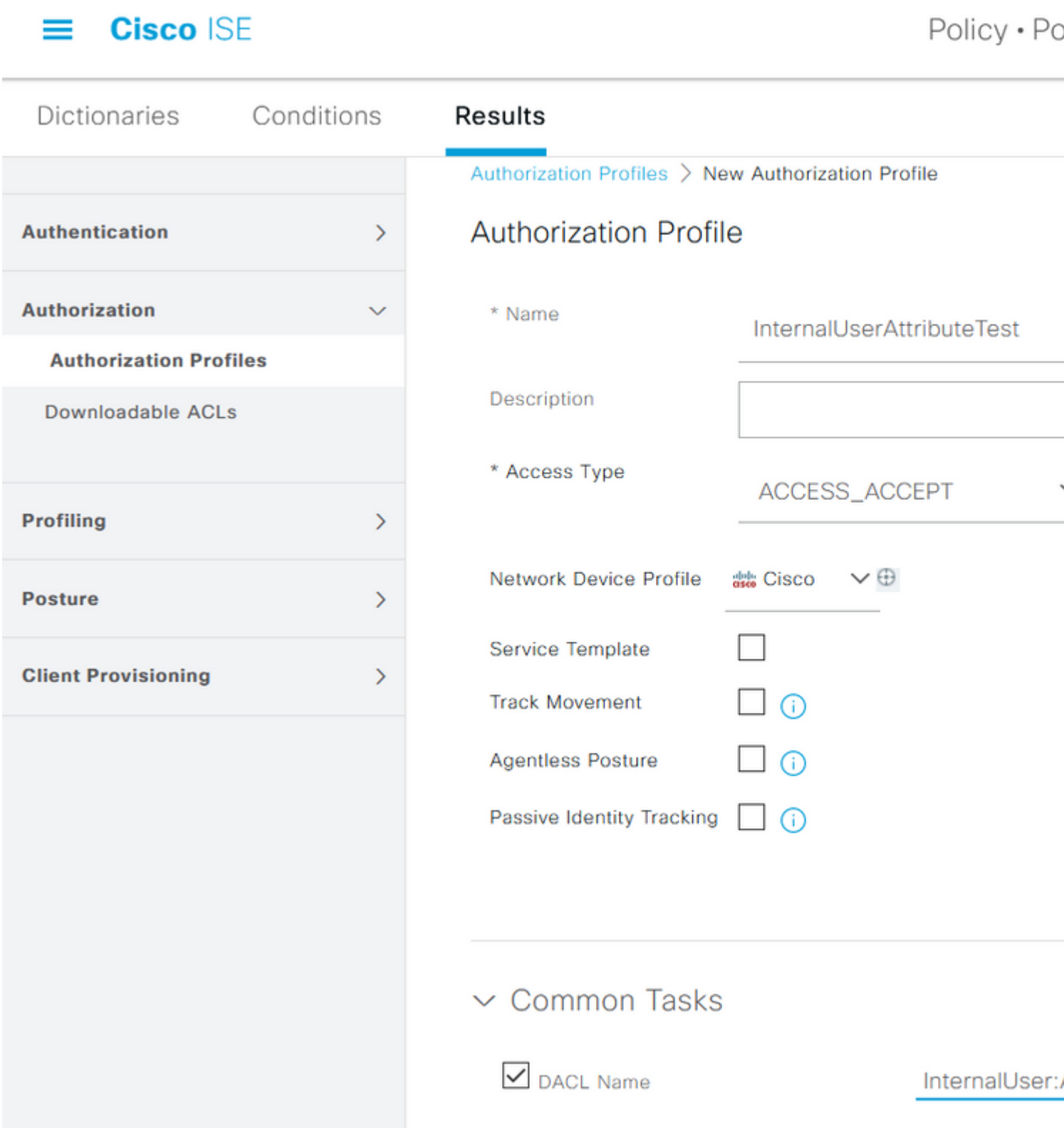
Retrieve Attributes...

Name	Type	Example Value
aCSPolicyName	STRING	NotMuchAccess
accountExpires	STRING	9223372036854775807
badPasswordTime	STRING	0
badPwdCount	STRING	0
cn	STRING	testuserexternal
codePage	STRING	0
countryCode	STRING	0
dSCorePropagationData	STRING	16010101000000.0Z
displayName	STRING	testuserexternal
distinguishedName	STRING	CN=testuserexternal,CN=User

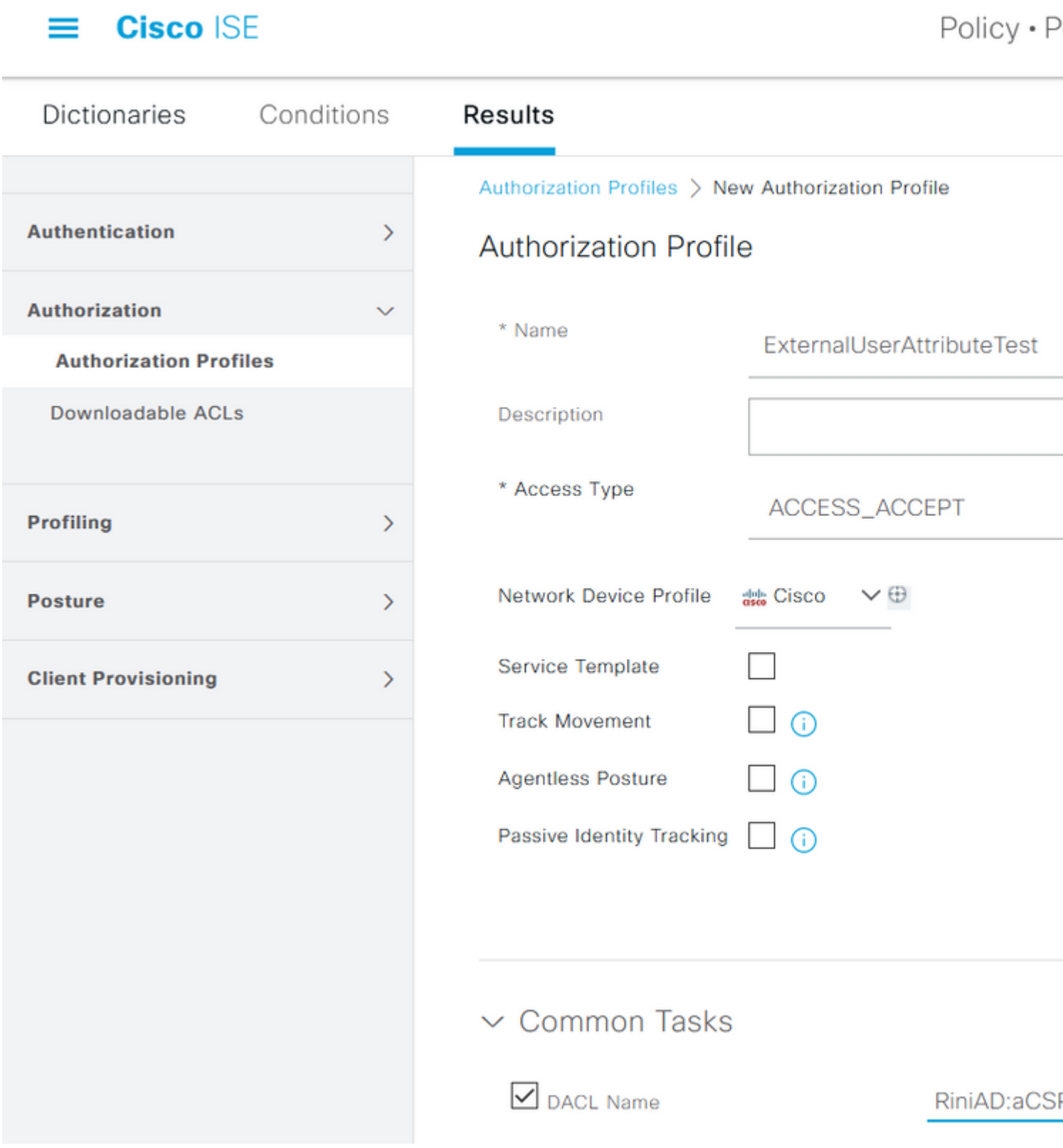


Autorisatieprofielen voor interne en externe gebruikers configureren

Om de profielen van de Vergunning te vormen, navigeer aan **Beleid > Elementen van het Beleid > Resultaten > Vergunning > Profielen van de Vergunning**. Klik op Add (Toevoegen). Geef een naam en kies de dACL-naam als **Interne gebruiker:<naam van aangepast kenmerk gemaakt>** voor interne gebruiker. Zoals in de afbeelding, voor interne gebruiker, wordt het profiel **InternalUserAttributeTest** geconfigureerd met de dACL geconfigureerd als **InternalUser:ACL**.

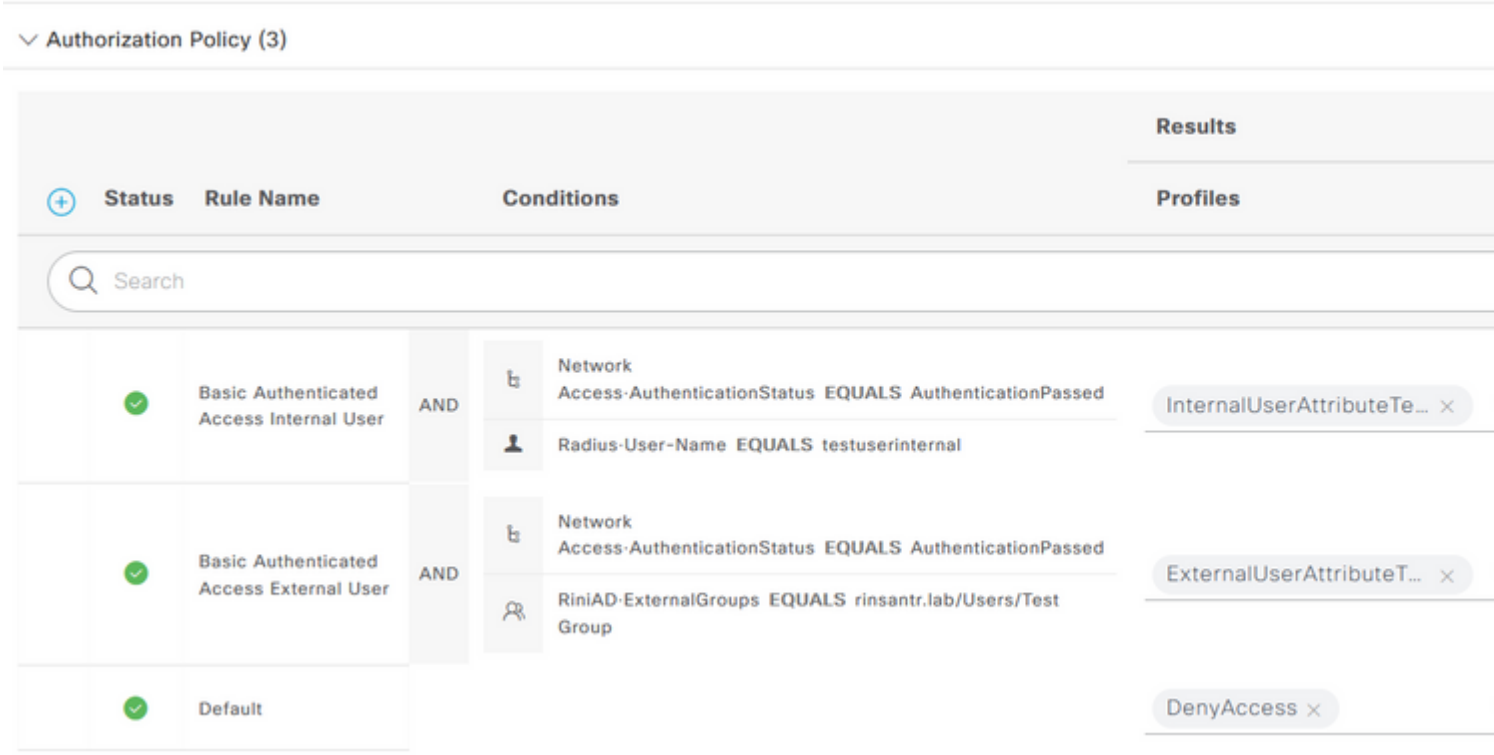


Voor externe gebruiker, gebruik **<Join point name>:<attribuut geconfigureerd op AD>** als dACL-naam.
In dit voorbeeld wordt het profiel **ExternalUserAttributeTest** geconfigureerd met de dACL die is geconfigureerd als **RiniAD:aCSPpolicyName** waarbij RiniAD de naam Join Point is.



Autorisatiebeleid configureren

Het autorisatiebeleid kan worden geconfigureerd bij **Policy > Policy Sets** op basis van de groepen waarin de externe gebruiker aanwezig is op de AD en ook op basis van de gebruikersnaam in het ISE interne identiteitsarchief. In dit voorbeeld is **testuserexternal** een gebruiker die aanwezig is in de groep **rinsantr.lab/Gebruikers/Test Group** en **testuserinternal** is een gebruiker die aanwezig is in het ISE-identiteitsarchief.

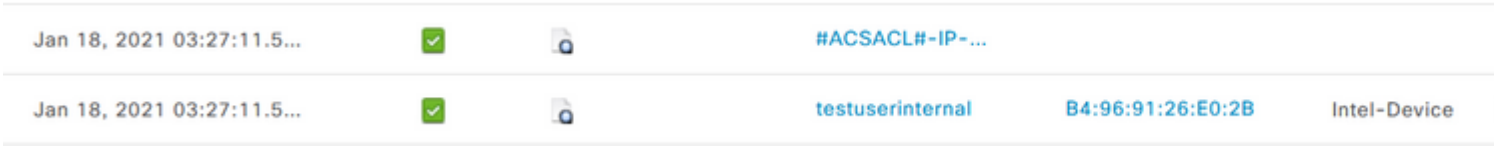


Verifiëren

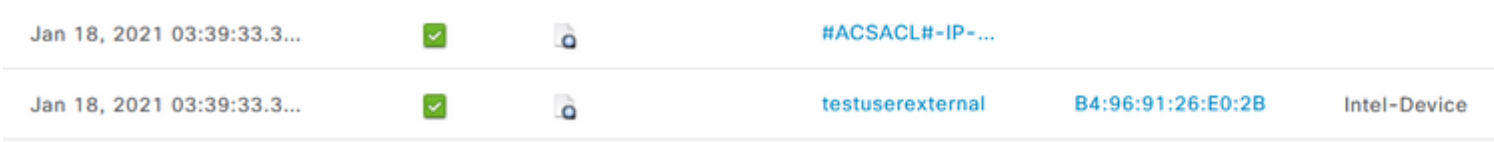
Gebruik dit gedeelte om te controleren of de configuratie werkt.

Controleer de actieve RADIUS-logbestanden om de gebruikersverificaties te verifiëren.

Interne gebruiker:



Externe gebruiker:



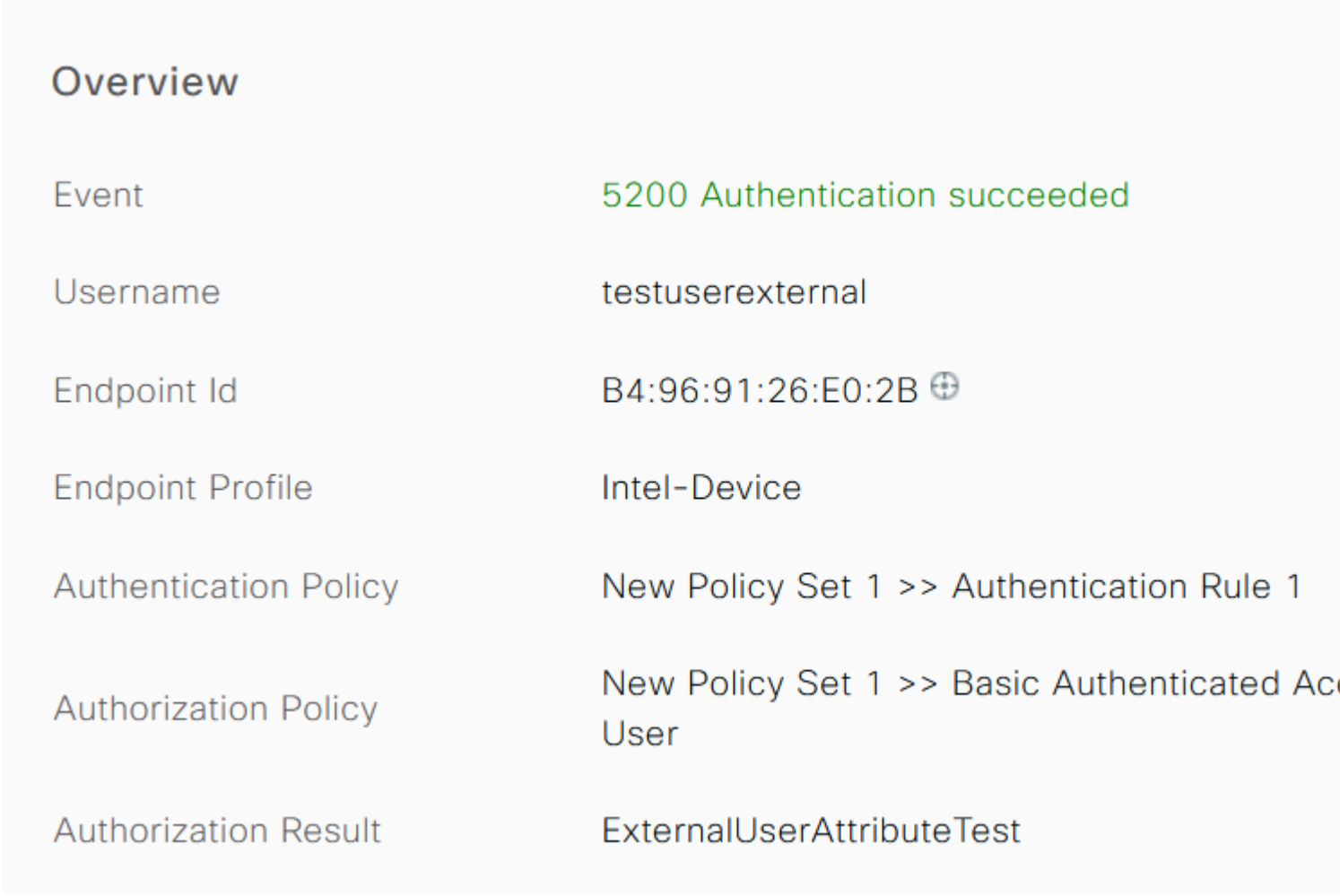
Klik op het pictogram vergrootglas op de succesvolle gebruikersverificaties om te controleren of de verzoeken het juiste beleid hebben gedrukt in het gedeelte Overzicht van de gedetailleerde bewegende logbestanden.

Interne gebruiker:

Overview

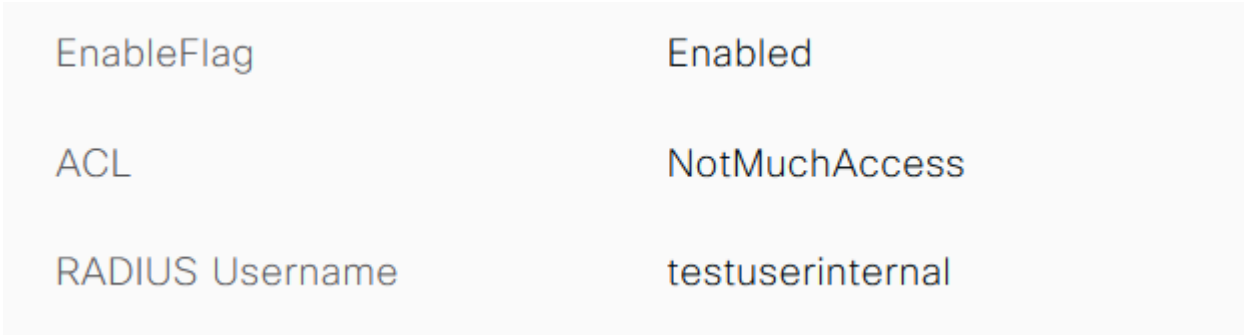
Event	5200 Authentication succeeded
Username	testuserinternal
Endpoint Id	B4:96:91:26:E0:2B
Endpoint Profile	Intel-Device
Authentication Policy	New Policy Set 1 >> Authentication Rule 1
Authorization Policy	New Policy Set 1 >> Basic Authenticated Ac
Authorization Result	InternalUserAttributeTest

Externe gebruiker:

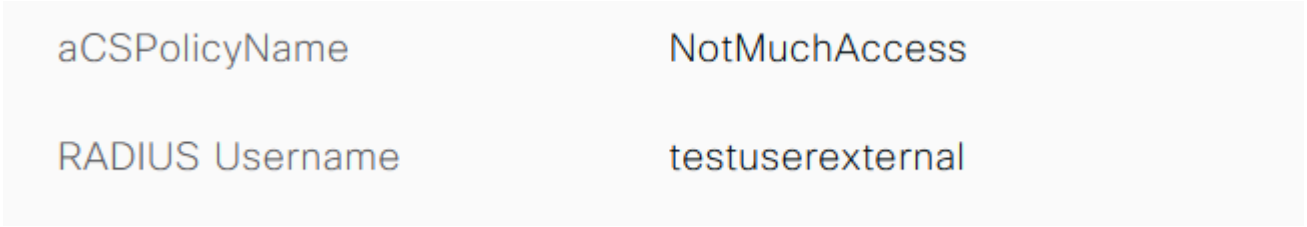


Controleer in de sectie Andere kenmerken van de gedetailleerde bewegende logbestanden of de gebruikerskenmerken zijn hersteld.

Interne gebruiker:

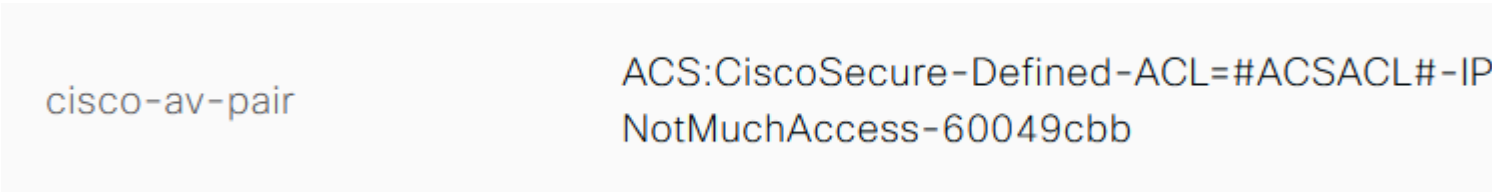


Externe gebruiker:



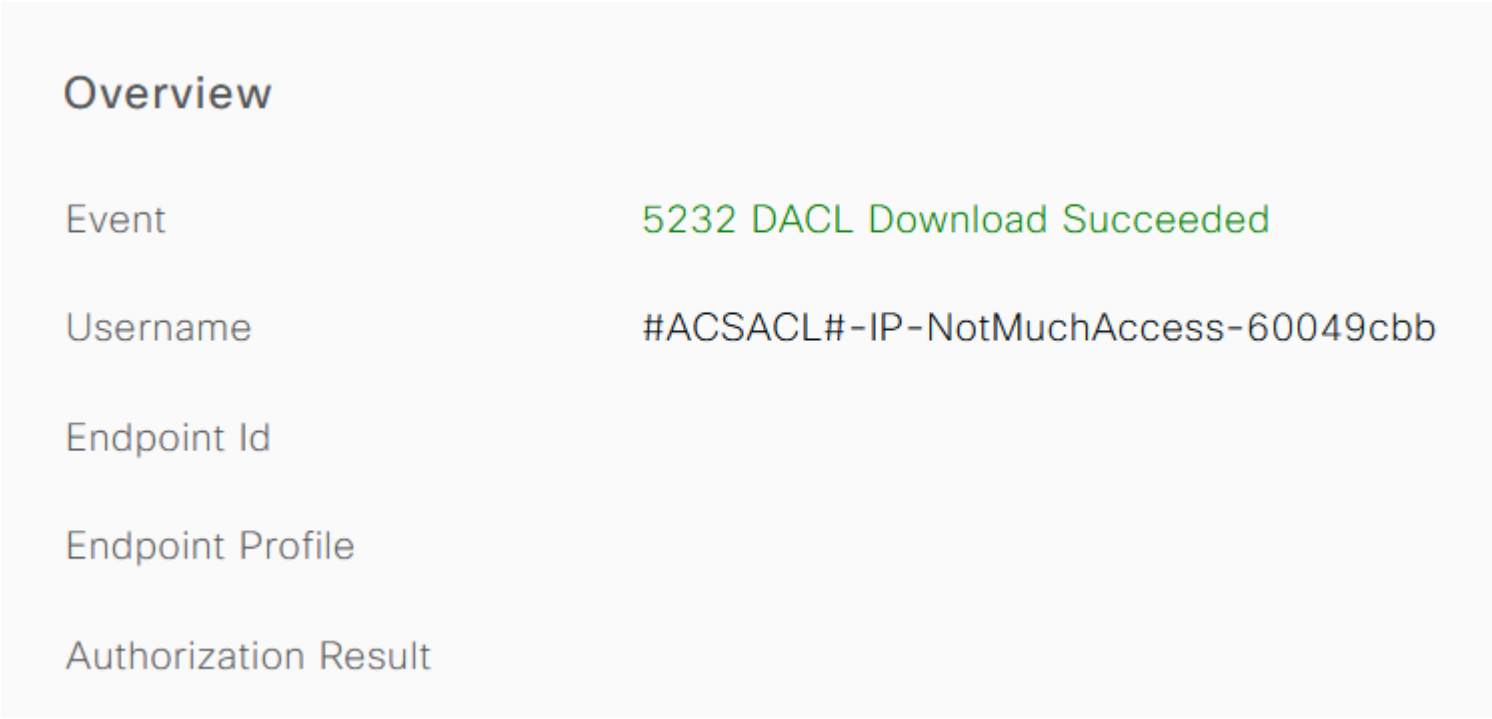
Controleer de sectie Resultaat van de gedetailleerde bewegende logbestanden om te verifiëren of het dACL-

kenmerk als deel van Access-Accept wordt verzonden.



Controleer ook de actieve RADIUS-logbestanden om te controleren of de dACL wordt gedownload na de gebruikersverificatie.

Klik op het vergrootglaspictogram op het succesvolle dACL-downloadlogboek en controleer het gedeelte Overzicht om de dACL-download te bevestigen.



Controleer de resultaatsectie van dit gedetailleerde rapport om de inhoud van dACL te verifiëren.

Problemen oplossen

Er is momenteel geen specifieke informatie beschikbaar om deze configuratie problemen op te lossen.

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.