

Dynamische toegangscontrolelijsten per gebruiker configureren in ISE

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Configureer een nieuw aangepast gebruikerskenmerk op ISE](#)

[DACL configureren](#)

[Een interne gebruikersaccount configureren met het aangepaste kenmerk](#)

[Een AD-gebruikersaccount configureren](#)

[Attributen van AD naar ISE importeren](#)

[Autorisatieprofielen voor interne en externe gebruikers configureren](#)

[Autorisatiebeleid configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

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**.

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE' and 'Administration · Identity Management'. Below this, there are tabs for 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'Settings' tab is active. On the left, a sidebar menu shows 'User Custom Attributes' selected. The main content area displays a table of existing attributes:

Mandatory	Attribute Name	Data Type
	AllowPasswordChangeAfterLogin	String
	Description	String
	EmailAddress	String
	EnableFlag	String
	EnablePassword	String
	Firstname	String
	Lastname	String
✓	Name	String
	Password (CredentialPassword)	String

Below this table, there is a section for 'User Custom Attributes' with a table showing the configuration for the 'ACL' attribute:

Attribute Name	Description	Data Type	Parameters	Default Value	Mandatory
ACL	Attribute for ACL per us	String	String Max length	+	<input type="checkbox"/>

DACL configureren

Om downloadbare ACL's te configureren navigeert u naar **Beleid > Beleidselementen > Resultaten > Autorisatie > Downloadbare ACL'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**.

Downloadable ACL List > New Downloadable ACL

Downloadable ACL

* Name

Description

IP version IPv4 IPv6 Agnostic ⓘ

* DACL Content

1234567	permit ip any any
8910111	
2131415	
1617181	
9202122	
2324252	
6272829	
3031323	
3343536	
3738394	
0414243	
4445464	

✓ Check DACL Syntax

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**.

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Res...

[Network Access Users List](#) > New Network Access User

Network Access User

* Name testuserinternal

Status Enabled

Email

Passwords

Password Type: Internal Users

Password Re-Enter Password

* Login Password

Enable Password

> User Information

> Account Options

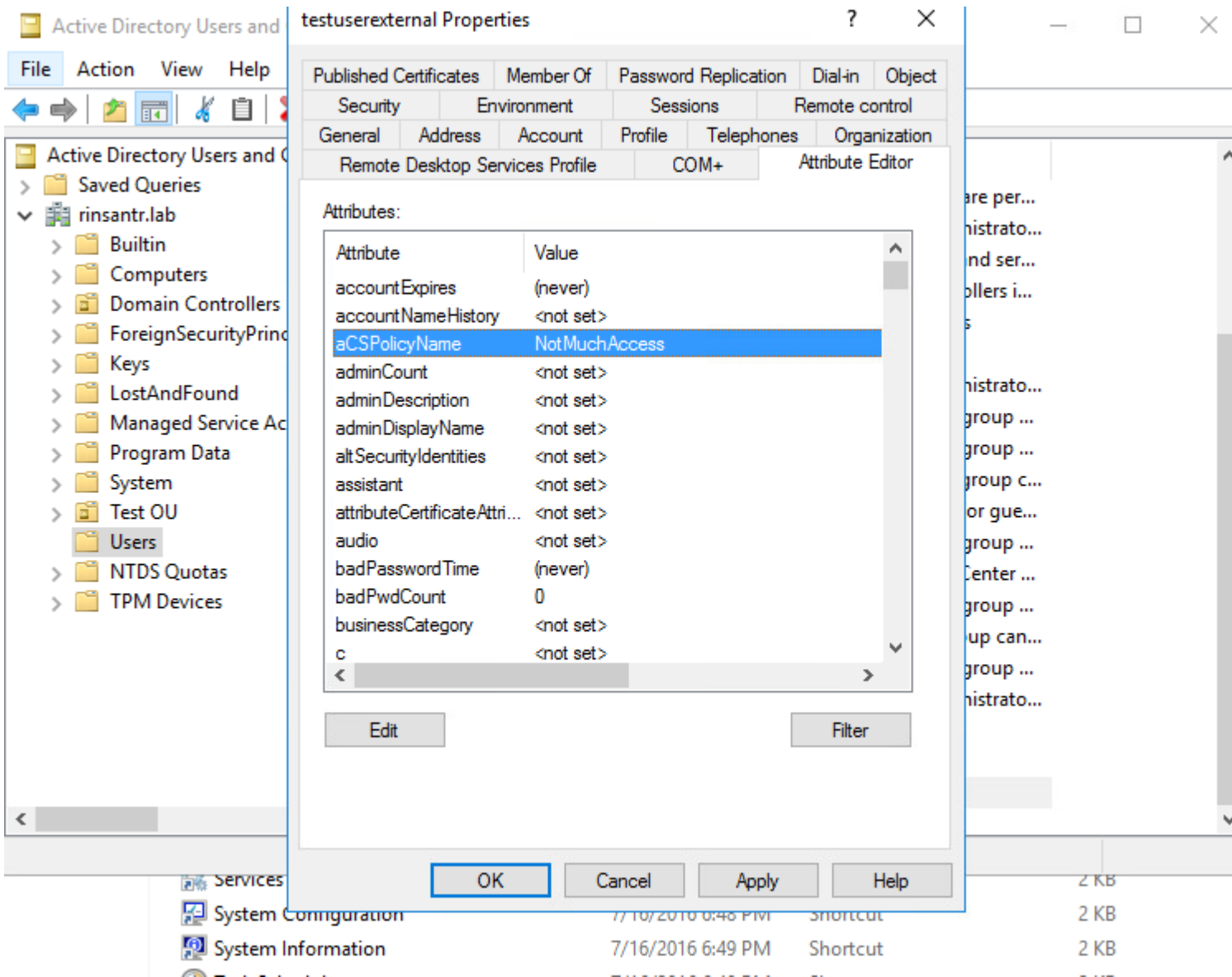
> Account Disable Policy

User Custom Attributes

⋮ ACL = 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

testuserexternal



Account

Retrieve Attributes...

<input type="checkbox"/>	Name	Type	Example Value
<input checked="" type="checkbox"/>	aCSPolicyName	STRING	NotMuchAccess
<input type="checkbox"/>	accountExpires	STRING	9223372036854775807
<input type="checkbox"/>	badPasswordTime	STRING	0
<input type="checkbox"/>	badPwdCount	STRING	0
<input type="checkbox"/>	cn	STRING	testuserexternal
<input type="checkbox"/>	codePage	STRING	0
<input type="checkbox"/>	countryCode	STRING	0
<input type="checkbox"/>	dSCorePropagationData	STRING	16010101000000.0Z
<input type="checkbox"/>	displayName	STRING	testuserexternal
<input type="checkbox"/>	distinguishedName	STRING	CN=testuserexternal,CN=User



External Identity Sources

- <
- > Certificate Authentication F
- Active Directory
 - RiniAD
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers
- Social Login

[Edit](#) [+ Add](#) [Delete Attribute](#)

<input type="checkbox"/>	Name	Type	Default	Internal Name
<input type="checkbox"/>	aCSPolicyName	STRING		aCSPolicyName

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**.

Dictionaryes

Conditions

Results

Authentication	>
Authorization	∨
Authorization Profiles	
Downloadable ACLs	
Profiling	>
Posture	>
Client Provisioning	>

[Authorization Profiles](#) > New Authorization Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile  Cisco ∨ ⊕

Service Template

Track Movement ⓘ

Agentless Posture ⓘ

Passive Identity Tracking ⓘ

∨ Common Tasks

DACL Name

InternalUser:...

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.

Dictionaryes

Conditions

Results

Authentication	>
Authorization	∨
Authorization Profiles	
Downloadable ACLs	
Profiling	>
Posture	>
Client Provisioning	>

[Authorization Profiles](#) > New Authorization Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile  Cisco ∨ ⊕

Service Template

Track Movement ⓘ

Agentless Posture ⓘ

Passive Identity Tracking ⓘ

∨ Common Tasks

DACL Name

[RiniAD:aCSF](#)

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.

				Results
Status	Rule Name	Conditions		Profiles
<input type="text" value="Search"/>				
✓	Basic Authenticated Access Internal User	AND	<ul style="list-style-type: none"> Network Access-AuthenticationStatus EQUALS AuthenticationPassed Radius-User-Name EQUALS testuserinternal 	InternalUserAttributeTe... x
✓	Basic Authenticated Access External User	AND	<ul style="list-style-type: none"> Network Access-AuthenticationStatus EQUALS AuthenticationPassed RiniAD-ExternalGroups EQUALS rinsantr.lab/Users/Test Group 	ExternalUserAttributeT... x
✓	Default			DenyAccess x

Verifiëren

Gebruik dit gedeelte om te controleren of de configuratie werkt.

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

Interne gebruiker:

Jan 18, 2021 03:27:11.5...	✓		#ACSACL#-IP-...
Jan 18, 2021 03:27:11.5...	✓		testuserinternal B4:96:91:26:E0:2B Intel-Device


Externe gebruiker:

Jan 18, 2021 03:39:33.3...	✓		#ACSACL#-IP-...
Jan 18, 2021 03:39:33.3...	✓		testuserexternal B4:96:91:26:E0:2B Intel-Device

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:

Overview

Event	5200 Authentication succeeded
Username	testuserexternal
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 Access User
Authorization Result	ExternalUserAttributeTest

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

Interne gebruiker:

EnableFlag	Enabled
ACL	NotMuchAccess
RADIUS Username	testuserinternal

Externe gebruiker:

aCSPolicyName	NotMuchAccess
RADIUS Username	testuserexternal

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

kenmerk als deel van Access-Accept wordt verzonden.

cisco-av-pair

ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-NotMuchAccess-60049cbb

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

Jan 18, 2021 03:39:33.3...



#ACSACL#-IP-Not

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

Overview

Event

5232 DACL Download Succeeded

Username

#ACSACL#-IP-NotMuchAccess-60049cbb

Endpoint Id

Endpoint Profile

Authorization Result

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

cisco-av-pair

ip:inacl#1=permit ip any any

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.