

# Configuración de listas de control de acceso dinámico por usuario en ISE

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Configuración de un nuevo atributo de usuario personalizado en ISE](#)

[Configurar dACL](#)

[Configuración de una cuenta de usuario interna con el atributo personalizado](#)

[Configurar una cuenta de usuario de AD](#)

[Importar el atributo de AD a ISE](#)

[Configurar perfiles de autorización para usuarios internos y externos](#)

[Configurar directivas de autorización](#)

[Verificación](#)

[Troubleshoot](#)

---

## Introducción

Este documento describe la configuración de una lista de control de acceso dinámico (dACL) por usuario para los usuarios presentes en un tipo de almacén de identidades.

## Prerequisites

### Requirements

Cisco recomienda conocer la configuración de políticas en Identity Services Engine (ISE).

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Identity Services Engine 3.0
- Microsoft Windows Active Directory 2016

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

La configuración de una lista de control de acceso dinámico por usuario es para usuarios presentes en el almacén de identidades interno de ISE o en un almacén de identidades externo.

## Configurar

La dACL por usuario se puede configurar para cualquier usuario del almacén interno que utilice un atributo de usuario personalizado. Para un usuario de Active Directory (AD), se puede utilizar cualquier atributo de tipo cadena para lograr lo mismo. Esta sección proporciona la información necesaria para configurar los atributos tanto en ISE como en AD, junto con la configuración necesaria en ISE para que esta función funcione.

### Configuración de un nuevo atributo de usuario personalizado en ISE

Vaya a Administration > Identity Management > Settings > User Custom Attributes. Haga clic en el botón +, como se muestra en la imagen, para agregar un nuevo atributo y guardar los cambios. En este ejemplo, el nombre del atributo personalizado es ACL.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb navigation is Administration > Identity Management > Settings > User Custom Attributes. The page title is 'User Custom Attributes'. On the left, there is a sidebar with navigation options: User Custom Attributes, User Authentication Settings, Endpoint Purge, Endpoint Custom Attributes, and REST ID Store Settings. The main content area shows 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 the table, there is a section for adding a new attribute. It shows a table with columns: Attribute Name, Description, Data Type, Parameters, and Default Value Mandatory. The 'ACL' attribute is being added with the following details:

Attribute Name	Description	Data Type	Parameters	Default Value Mandatory
ACL	Attribute for ACL per us	String	String Max length	+

At the bottom right, there are 'Save' and 'Reset' buttons.

### Configurar dACL

Para configurar las ACL descargables, navegue hasta Política > Elementos de Política > Resultados > Autorización > ACL descargables. Haga clic en Add (Agregar). Proporcione un nombre, el contenido de la dACL y guarde los cambios. Como se muestra en la imagen, el

nombre de la dACL es NotMuchAccess.

The screenshot shows the Cisco ISE configuration interface for a Downloadable ACL. The page title is "Policy • Policy Elements". In the top right corner, there are two warning icons: "Evaluation Mode 27 Days" and "License Warning". The left sidebar contains a navigation menu with the following items: "Dictionaries", "Conditions", "Results", "Authentication", "Authorization", "Downloadable ACLs", "Profiling", "Posture", and "Client Provisioning". The "Results" tab is active, and the breadcrumb path is "Downloadable ACL List > New Downloadable ACL". The main content area is titled "Downloadable ACL" and contains the following fields:

- \* Name: NotMuchAccess
- Description: (empty text box)
- IP version:  IPv4  IPv6  Agnostic
- \* DACL Content: A list of IP addresses on the left and a text box on the right containing "permit ip any any". The list includes: 1234567, 8910111, 2131415, 1617181, 9202122, 2324252, 6272829, 3031323, 3343536, 3738394, 0414243, and .A.A.A.A.A.A.
- Check DACL Syntax: (checkbox)

A "Submit" button is located at the bottom right of the configuration area.

## Configuración de una cuenta de usuario interna con el atributo personalizado

Vaya a Administration > Identity Management > Identities > Users > Add. Cree un usuario y configure el valor del atributo personalizado con el nombre de la dACL que el usuario necesita obtener cuando se le autoriza. En este ejemplo, el nombre de la dACL es 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

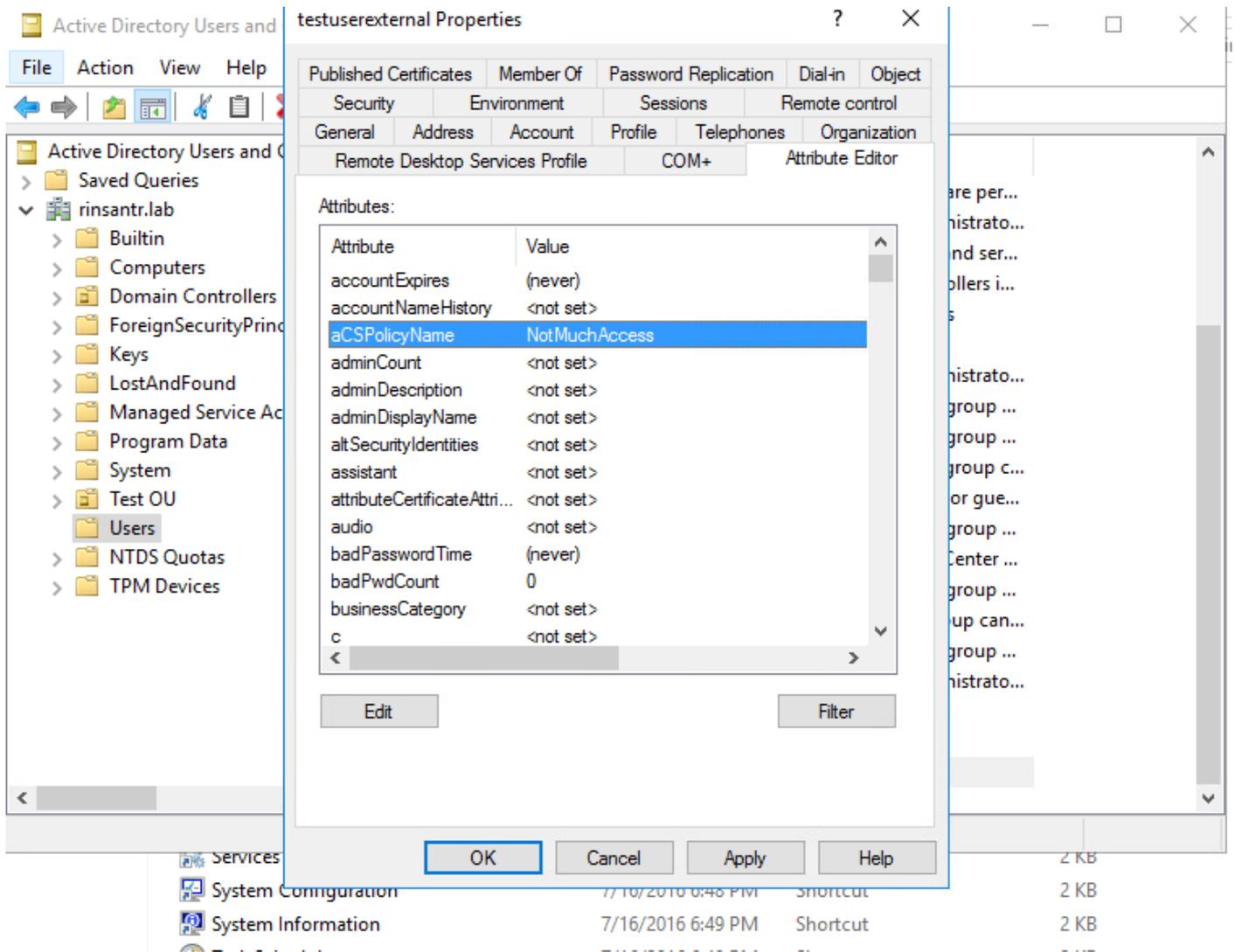
> Account Disable Policy

User Custom Attributes

ACL = NotMuchAccess

## Configurar una cuenta de usuario de AD

En Active Directory, desplácese hasta las propiedades de la cuenta de usuario y, a continuación, vaya a la ficha Attribute Editor. Como se muestra en la imagen, aCSPolicyName es el atributo utilizado para especificar el nombre dACL. Sin embargo, como se ha mencionado anteriormente, también se puede utilizar cualquier atributo que pueda aceptar un valor de cadena.



## Importar el atributo de AD a ISE

Para utilizar el atributo configurado en AD, ISE debe importarlo. Para importar el atributo, navegue hasta Administration > Identity Management > External Identity Sources > Active Directory > [Join point configured] > Attributes. Haga clic en Agregar y luego en Seleccionar atributos del directorio. Proporcione el nombre de cuenta de usuario en AD y, a continuación, haga clic en Recuperar atributos. Seleccione el atributo configurado para la dACL, haga clic en Aceptar y, a continuación, haga clic en Guardar. Como se muestra en la imagen, aCSPolicyName es el atributo.

# 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...

<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=Users,DC=rinsantr,DC=lab

Cancel OK

Cisco ISE Administration · Identity Management

External Identity Sources

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

Attributes

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

Save Reset

## Configurar perfiles de autorización para usuarios internos y externos

Para configurar los perfiles de autorización, navegue hasta Policy > Policy Elements > Results > Authorization > Authorization Profiles. Haga clic en Add (Agregar). Proporcione un nombre y elija el nombre dACL como InternalUser:<name of custom attribute created> para el usuario interno.

Como se muestra en la imagen, para el usuario interno, el perfil InternalUserAttributeTest se configura con el dACL configurado como InternalUser:ACL.

The screenshot shows the Cisco ISE web interface. At the top left is the Cisco ISE logo. At the top right, it says "Policy • Policy Elements". Below this is a navigation bar with "Dictionaries", "Conditions", and "Results" (which is selected). The main content area is titled "Authorization Profiles > New Authorization Profile". The "Authorization Profile" configuration form includes the following fields:

- \* Name: InternalUserAttributeTest
- Description: (empty text box)
- \* Access Type: ACCESS\_ACCEPT (dropdown menu)
- Network Device Profile: Cisco (dropdown menu)
- Service Template:
- Track Movement:  (with info icon)
- Agentless Posture:  (with info icon)
- Passive Identity Tracking:  (with info icon)

Below the form is a section titled "Common Tasks" with a checkbox for "DACL Name" which is checked. The value for this field is "InternalUser:ACL" (dropdown menu).

Para el usuario externo, utilice <Join point name>:<attribute configured on AD> como el nombre dACL. En este ejemplo, el perfil ExternalUserAttributeTest se configura con la dACL configurada como RiniAD:aCSPolicyName, donde RiniAD es el nombre del punto de unión.

Dictionaryes    Conditions    **Results**

Authorization Profiles > New Authorization Profile

## Authorization Profile

\* Name ExternalUserAttributeTest

Description

\* Access Type ACCESS\_ACCEPT ▼

Network Device Profile Cisco ▼ ⊕

Service Template

Track Movement  ⓘ

Agentless Posture  ⓘ

Passive Identity Tracking  ⓘ

---

▼ Common Tasks

DACL Name RiniAD:aCSPolicyName| ▼

## Configurar directivas de autorización

Las políticas de autorización se pueden configurar en Policy > Policy Sets en función de los grupos en los que el usuario externo está presente en AD y también en función del nombre de usuario en el almacén de identidad interna de ISE. En este ejemplo, testuserexternal es un usuario presente en el grupo rinsantr.lab/Users/Test Group y testuserinternal es un usuario presente en el almacén de identidades internas de ISE.

Authorization Policy (3)

				Results	
Status	Rule Name	Conditions	Profiles	Security Groups	
+	Search				
✓	Basic Authenticated Access Internal User	AND Network Access-AuthenticationStatus EQUALS AuthenticationPassed Radius-User-Name EQUALS testuserinternal	InternalUserAttributeTe... x	+	Select from list
✓	Basic Authenticated Access External User	AND Network Access-AuthenticationStatus EQUALS AuthenticationPassed RiniAD-ExternalGroups EQUALS rinsantr.lab/Users/Test Group	ExternalUserAttributeT... x	+	Select from list
✓	Default		DenyAccess x	+	Select from list

## Verificación

Utilice esta sección para verificar si la configuración funciona.

Verifique los registros en vivo de RADIUS para verificar las autenticaciones de usuario.

Usuario interno:

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	New Polic...	New Polic...	InternalUs...

Usuario externo:

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	New Polic...	New Polic...	ExternalUs...

Haga clic en el icono de lupa de las autenticaciones de usuario correctas para verificar si las solicitudes cumplen las políticas correctas en la sección Descripción general de los registros en directo detallados.

Usuario interno:

## 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 Access Internal User
Authorization Result	InternalUserAttributeTest

### Usuario externo:

## 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 External User
Authorization Result	ExternalUserAttributeTest

Verifique la sección Otros Atributos de los logs en vivo detallados para verificar si los atributos de usuario han sido recuperados.

### Usuario interno:

EnableFlag	Enabled
ACL	NotMuchAccess
RADIUS Username	testuserinternal

Usuario externo:

aCSPolicyName	NotMuchAccess
RADIUS Username	testuserexternal

Verifique la sección Resultado de los registros en vivo detallados para verificar si el atributo dACL se envía como parte de Access-Accept.

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

Además, verifique los registros en vivo de RADIUS para verificar si la dACL se descarga después de la autenticación del usuario.

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



[#ACSACL#-IP-NotMuchAccess-60049cbb](#)

Haga clic en el icono de lupa en el registro de descarga de dACL exitosa y verifique la sección Descripción General para confirmar la descarga de dACL.

## Overview

Event	5232 DACL Download Succeeded
Username	#ACSACL#-IP-NotMuchAccess-60049cbb
Endpoint Id	
Endpoint Profile	
Authorization Result	

Consulte la sección Resultado de este informe detallado para verificar el contenido de la dACL.

cisco-av-pair

ip:inacl#1=permit ip any any

## Troubleshoot

Actualmente no hay información específica disponible para resolver problemas de esta configuración.

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).