

# Configurazione di Access Control List dinamici per utente in ISE

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Configurazione di un nuovo attributo utente personalizzato in ISE](#)

[Configurazione di dACL](#)

[Configurare un account utente interno con l'attributo personalizzato](#)

[Configurare un account utente AD](#)

[Importare l'attributo da AD ad ISE](#)

[Configurazione dei profili di autorizzazione per utenti interni ed esterni](#)

[Configura criteri di autorizzazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

---

## Introduzione

In questo documento viene descritta la configurazione di un elenco di controllo di accesso dinamico (dACL) per utente per gli utenti presenti in un tipo di archivio identità.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza della configurazione delle policy su Identity Services Engine (ISE).

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Identity Services Engine 3.0
- Microsoft Windows Active Directory 2016

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

La configurazione di un elenco di controllo di accesso dinamico per utente è destinata agli utenti presenti nell'archivio di identità interno ISE o in un archivio di identità esterno.

## Configurazione

È possibile configurare dACL per utente per qualsiasi utente dell'archivio interno che utilizzi un attributo utente personalizzato. Per ottenere lo stesso risultato, è possibile utilizzare qualsiasi attributo di tipo stringa per un utente di Active Directory (AD). In questa sezione vengono fornite le informazioni necessarie per configurare gli attributi sia su ISE che su AD, nonché la configurazione richiesta su ISE per il corretto funzionamento di questa funzione.

### Configurazione di un nuovo attributo utente personalizzato in ISE

Passare a Amministrazione > Gestione delle identità > Impostazioni > Attributi utente personalizzati. Fare clic sul pulsante +, come illustrato nell'immagine, per aggiungere un nuovo attributo e salvare le modifiche. Nell'esempio, il nome dell'attributo personalizzato è ACL.

The screenshot shows the Cisco ISE Administration console interface. The top navigation bar includes 'Cisco ISE', 'Administration · Identity Management', and status indicators for 'Evaluation Mode 27 Days' and 'License Warning'. The main menu on the left lists 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'Settings' section is expanded to show 'User Custom Attributes'. A table lists existing attributes with columns for 'Mandatory', 'Attribute Name', and 'Data Type'. A new attribute 'ACL' is being added at the bottom, with a description 'Attribute for ACL per us', data type 'String', and parameters 'String Max length'. A 'Save' button is visible at the bottom right.

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

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

### Configurazione di dACL

Per configurare gli ACL scaricabili, selezionare Policy > Policy Elements > Results > Authorization > Downloadable ACLs (Policy > Elementi criterio > Risultati > Autorizzazione > ACL scaricabili).

Fare clic su Add. Fornire un nome e il contenuto dell'elenco di controllo di accesso (dACL) e salvare le modifiche. Come mostrato nell'immagine, il nome dell'ACL è NotMuchAccess.

The screenshot shows the Cisco ISE configuration page for a Downloadable ACL. The breadcrumb navigation is 'Downloadable ACL List > New Downloadable ACL'. The page title is 'Downloadable ACL'. The configuration fields are as follows:

- Name:** NotMuchAccess
- Description:** (Empty text box)
- IP version:**  IPv4,  IPv6,  Agnostic
- DACL Content:** permit ip any any

At the bottom right, there is a blue 'Submit' button. A 'Check DACL Syntax' link is also present below the content field.

## Configurare un account utente interno con l'attributo personalizzato

Passare a Amministrazione > Gestione delle identità > Identità > Utenti > Aggiungi. Creare un utente e configurare il valore dell'attributo personalizzato con il nome dell'elenco di controllo di accesso (dACL) che l'utente deve ottenere quando è autorizzato. Nell'esempio, il nome dell'ACL è 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

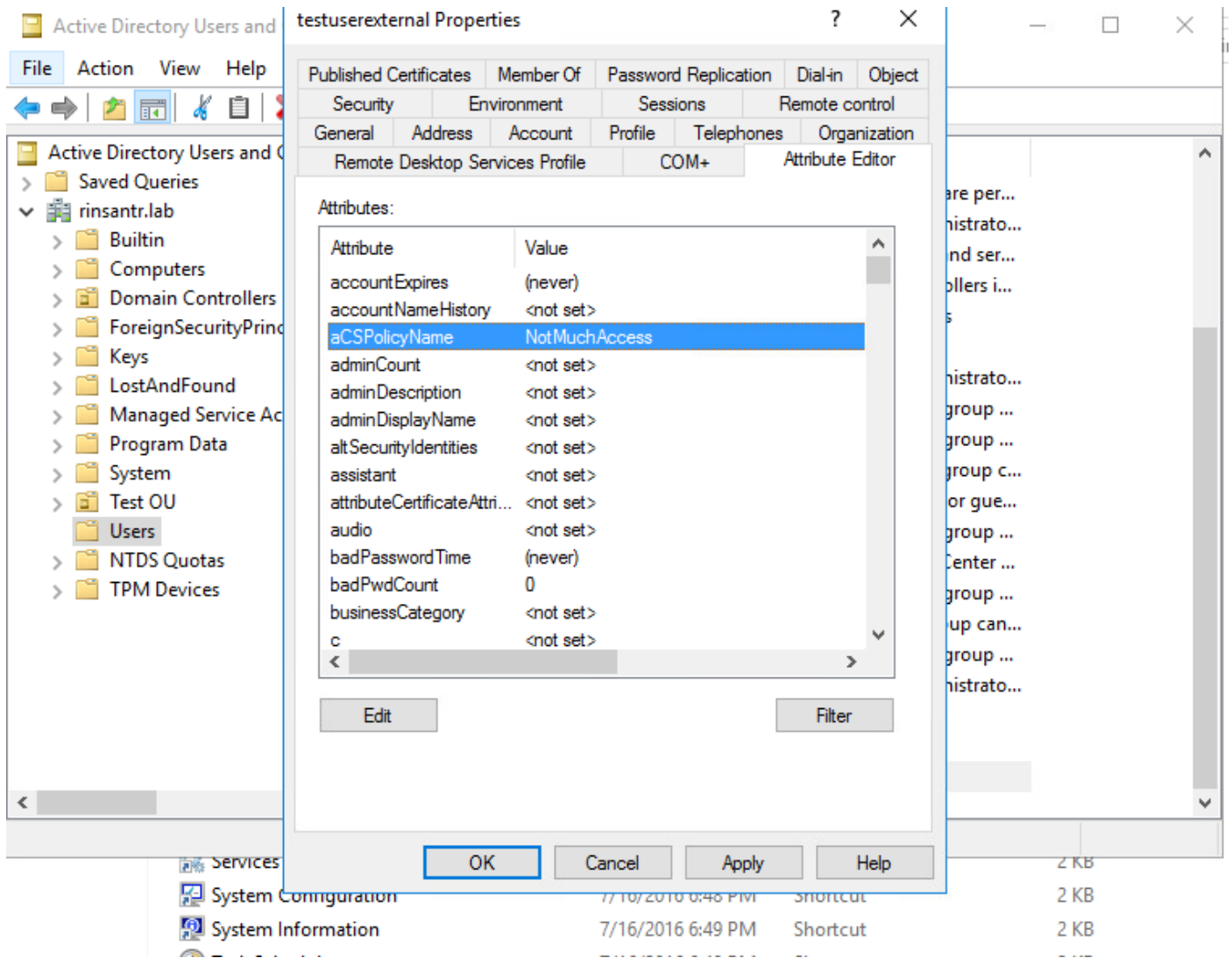
> Account Disable Policy

User Custom Attributes

ACL = NotMuchAccess

## Configurare un account utente AD

In Active Directory passare alle proprietà dell'account utente e quindi alla scheda Editor attributi. Come mostrato nell'immagine, aCSPolicyName è l'attributo utilizzato per specificare il nome dACL. Tuttavia, come accennato in precedenza, è possibile utilizzare anche qualsiasi attributo che accetta un valore stringa.



## Importare l'attributo da AD ad ISE

Per utilizzare l'attributo configurato in AD, ISE deve importarlo. Per importare l'attributo, selezionare Amministrazione > Gestione delle identità > Origini identità esterne > Active Directory > [Punto di join configurato] > scheda Attributi. Fare clic su Aggiungi, quindi su Seleziona attributi dalla directory. Specificare il nome dell'account utente in Active Directory e quindi fare clic su Recupera attributi. Selezionare l'attributo configurato per dACL, fare clic su OK, quindi su Salva. Come mostrato nell'immagine, aCSPolicyName è l'attributo.

# 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

Name	Type	Default	Internal Name
aCSPolicyName	STRING		aCSPolicyName

Save Reset

## Configurazione dei profili di autorizzazione per utenti interni ed esterni

Per configurare i profili di autorizzazione, selezionare Criterio > Elementi criteri > Risultati > Autorizzazione > Profili di autorizzazione. Fare clic su Add. Specificare un nome e scegliere il nome dACL InternalUser:<nome dell'attributo personalizzato creato> per l'utente interno. Come

mostrato nell'immagine, per gli utenti interni il profilo InternalUserAttributeTest è configurato con il dACL configurato come InternalUser:ACL.

The screenshot shows the Cisco ISE web interface for configuring a new Authorization Profile. The breadcrumb navigation is "Authorization Profiles > New Authorization Profile". The main heading is "Authorization Profile".

On the left, there is a navigation menu with the following items: Authentication, Authorization (expanded to show "Authorization Profiles" and "Downloadable ACLs"), Profiling, Posture, and Client Provisioning.

The configuration form includes the following fields:

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

Below the form, there is a section for "Common Tasks" with a checked checkbox for "DAACL Name" and a dropdown menu set to "InternalUser:ACL".

Per l'utente esterno, utilizzare <Nome punto di join>:<attributo configurato in AD> come nome di dACL. In questo esempio, il profilo ExternalUserAttributeTest è configurato con l'ACL dACL configurato come RiniAD:aCSPolicyName dove RiniAD è il nome del punto di join.

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  ▾

## Configura criteri di autorizzazione

I criteri di autorizzazione possono essere configurati in Criteri > Set di criteri in base ai gruppi in cui l'utente esterno è presente in Active Directory e anche in base al nome utente nell'archivio di identità interno ISE. Nell'esempio, testuserexternal è un utente presente nel gruppo rinsantr.lab/Users/Test Group e testuserinternal è un utente presente nell'archivio di identità interno 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	

## Verifica

Utilizzare questa sezione per verificare se la configurazione funziona.

Controllare i registri attivi RADIUS per verificare le autenticazioni utente.

Utente 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...


Utente esterno:

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...

Fare clic sull'icona della lente di ingrandimento sulle autenticazioni utente riuscite per verificare se le richieste hanno soddisfatto i criteri corretti nella sezione Panoramica dei log attivi dettagliati.


Utente 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

### Utente esterno:

## 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

Controllare la sezione Altri attributi dei log attivi dettagliati per verificare se gli attributi utente sono stati recuperati.

### Utente interno:

EnableFlag	Enabled
ACL	NotMuchAccess
RADIUS Username	testuserinternal

Utente esterno:

aCSPolicyName	NotMuchAccess
RADIUS Username	testuserexternal

Controllare la sezione Result dei log attivi dettagliati per verificare se l'attributo dACL viene inviato come parte di Access-Accept.

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

Controllare inoltre i log attivi RADIUS per verificare se l'ACL è stato scaricato dopo l'autenticazione dell'utente.

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



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

Fare clic sull'icona della lente di ingrandimento nel log di download di dACL riuscito e verificare la sezione Overview (Panoramica) per confermare il download di dACL.

## Overview

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

Controllare la sezione Result del report dettagliato per verificare il contenuto dell'ACL.

cisco-av-pair

ip:inacl#1=permit ip any any

## Risoluzione dei problemi

Non sono attualmente disponibili informazioni specifiche per risolvere i problemi relativi a questa configurazione.

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).