

Configure Per-User Dynamic Access Control Lists in ISE

Contents

- [Introduction](#)
- [Prerequisites](#)
- [Requirements](#)
- [Components Used](#)
- [Background Information](#)
- [Configure](#)
- [Configure a New Custom User Attribute on ISE](#)
- [Configure dACL](#)
- [Configure an Internal User Account with the Custom Attribute](#)
- [Configure a AD User Account](#)
- [Import the Attribute from AD to ISE](#)
- [Configure Authorization Profiles for Internal and External Users](#)
- [Configure Authorization Policies](#)
- [Verify](#)
- [Troubleshoot](#)

Introduction

This document describes the configuration of a per-user Dynamic Access Control List (dACL) for users present in a type of identity store.

Prerequisites

Requirements

Cisco recommends that you have knowledge of policy configuration on Identity Services Engine (ISE).

Components Used

The information in this document is based on these software and hardware versions:

- Identity Services Engine 3.0
- Microsoft Windows Active Directory 2016

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

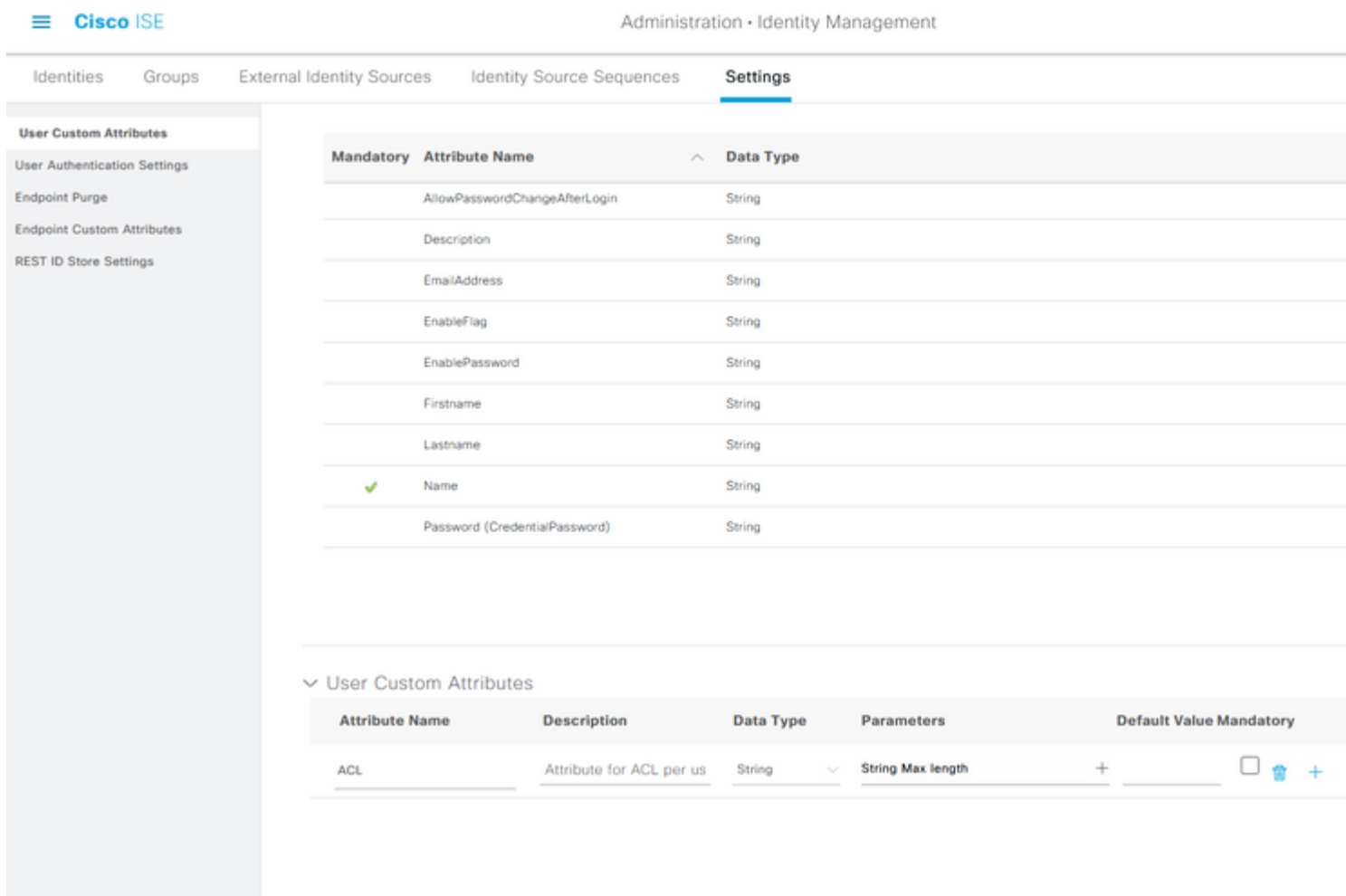
The configuration of a per-user Dynamic Access Control List is for users present in either the ISE internal identity store or an external identity store.

Configure

Per-user dACL can be configured for any user in the internal store that uses a custom user attribute. For a user in the Active Directory (AD), any attribute of type string can be used to achieve the same. This section provides information required to configure the attributes both on ISE and AD along with the configuration required on ISE for this feature to work.

Configure a New Custom User Attribute on ISE

Navigate to **Administration > Identity Management > Settings > User Custom Attributes**. Click the + button, as shown in the image, to add a new attribute and **save** the changes. In this example, the name of the custom attribute is **ACL**.



Configure dACL

In order to configure downloadable ACLs, navigate to **Policy > Policy Elements > Results > Authorization > Downloadable ACLs**. Click **Add**. Provide a name, content of the dACL, and **save** the changes. As shown in the image, the name of the dACL is **NotMuchAccess**.

[Dictionaries](#) [Conditions](#) **Results**

[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

Configure an Internal User Account with the Custom Attribute

Navigate to **Administration > Identity Management > Identities > Users > Add**. Create a user and configure the custom attribute value with the name of the dACL that the user needs to get when authorized. In this example, the name of the dACL is **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

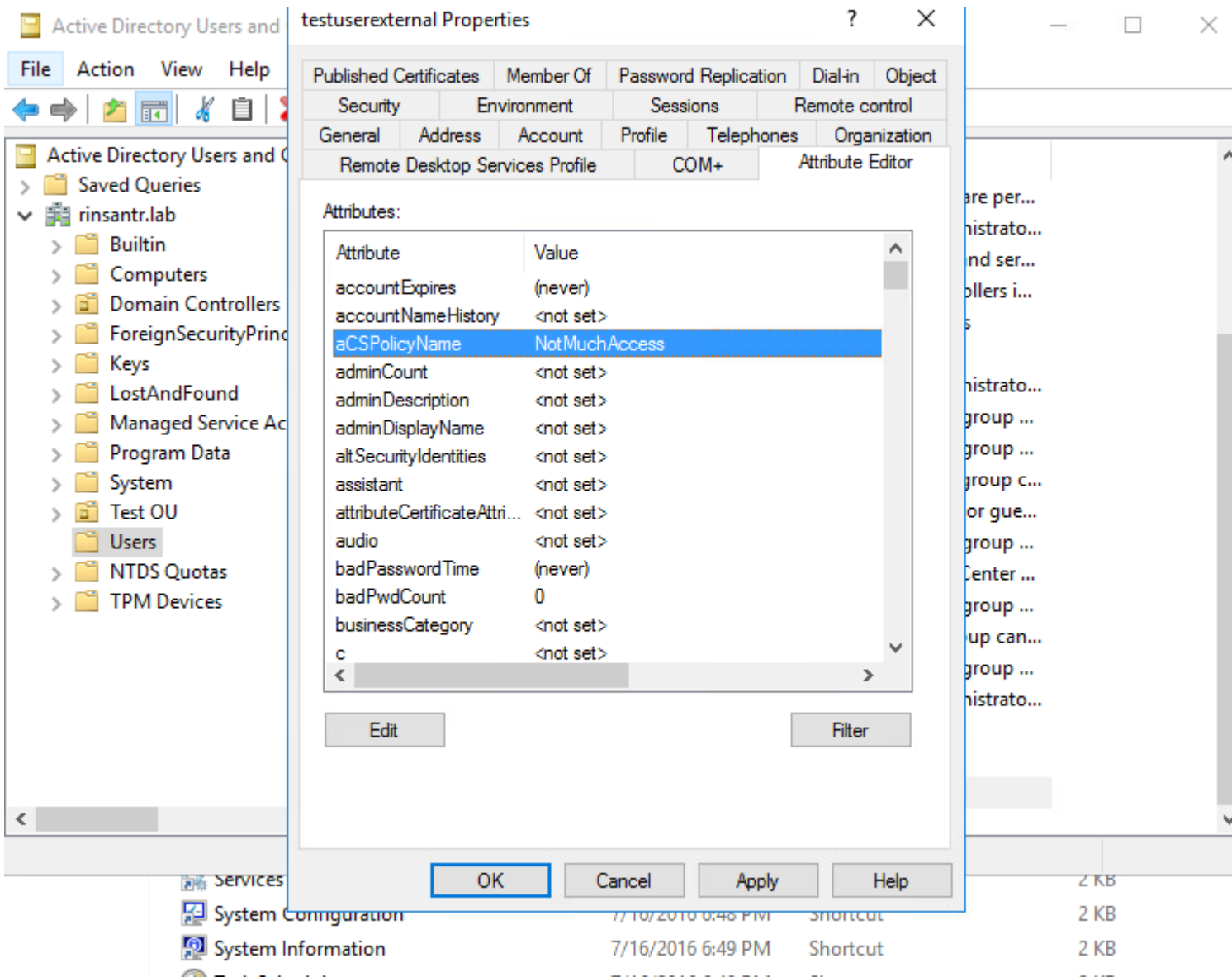
> Account Disable Policy

User Custom Attributes

⋮ ACL = NotMuchAccess

Configure a AD User Account

On the Active Directory, navigate to the user account properties and then on to the **Attribute Editor** tab. As shown in the image, **aCSPolicyName** is the attribute used to specify the dACL name. However, as mentioned earlier, any attribute which can accept a string value can be used as well.



Import the Attribute from AD to ISE

To use the attribute configured on AD, ISE needs to import it. In order to import the attribute, navigate to **Administration > Identity Management > External Identity Sources > Active Directory > [Join point configured] > Attributes** tab. Click **Add** and then **Select Attributes From Directory**. Provide the user account name on the AD and then click **Retrieve Attributes**. Select the attribute configured for the dACL, click **OK** and then click **Save**. As shown in the image, aCSPolicyName is the attribute.

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

  Add  Delete Attribute

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

Configure Authorization Profiles for Internal and External Users

In order to configure Authorization Profiles, navigate to **Policy > Policy Elements > Results > Authorization > Authorization Profiles**. Click **Add**. Provide a name and choose the dACL name as **InternalUser:<name of custom attribute created>** for internal user. As shown in the image, for internal user, the profile **InternalUserAttributeTest** is configured with the dACL configured as **InternalUser:ACL**.

Dictionary

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:...

For external user, use <Join point name>:<attribute configured on AD> as the dACL name. In this example, the profile **ExternalUserAttributeTest** is configured with the dACL configured as **RiniAD:aCSPolicyName** where RiniAD is the Join point name.

Dictionarys

Conditions

Results

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

[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:aCSF](#)

Configure Authorization Policies

Authorization policies can be configured at **Policy > Policy Sets** based on the groups in which the external user is present on the AD and also based on the username in the ISE internal identity store. In this example, **testuserexternal** is a user present in the group **rinsantr.lab/Users/Test Group** and **testuserinternal** is a user present in the ISE internal identity store.

Authorization Policy (3)

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

Verify

Use this section to verify if the configuration works.

Check the RADIUS live logs to verify the user authentications.

Internal user:

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


External user:

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

Click the magnifying glass icon on the successful user authentications to verify if the requests hit the correct policies in the Overview section of the detailed live logs.

Internal user:

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

External user:

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

Check the Other Attributes section of the detailed live logs to verify if the user attributes have been retrieved.

Internal user:

EnableFlag	Enabled
ACL	NotMuchAccess
RADIUS Username	testuserinternal

External user:

aCSPolicyName	NotMuchAccess
RADIUS Username	testuserexternal

Check the Result section of the detailed live logs to verify if the dACL attribute is sent as a part of Access-

Accept.

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

Also, check the RADIUS live logs to verify if the dACL is downloaded after the user authentication.

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



#ACSACL#-IP-Not

Click the magnifying glass icon on the successful dACL download log and verify the Overview section to confirm the dACL download.

Overview

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

Check the Result section of the this detailed report to verify the contents of the dACL.

cisco-av-pair

ip:inacl#1=permit ip any any

Troubleshoot

There is currently no specific information available to troubleshoot this configuration.