

Konfigurieren benutzerspezifischer dynamischer Zugriffskontrolllisten in der ISE

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Konfigurieren eines neuen benutzerdefinierten Benutzerattributs auf der ISE](#)

[dACL konfigurieren](#)

[Konfigurieren eines internen Benutzerkontos mit dem benutzerdefinierten Attribut](#)

[AD-Benutzerkonto konfigurieren](#)

[Attribut von AD in ISE importieren](#)

[Autorisierungsprofile für interne und externe Benutzer konfigurieren](#)

[Autorisierungsrichtlinien konfigurieren](#)

[Überprüfung](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird die Konfiguration einer benutzerspezifischen Dynamic Access Control List (dACL) für Benutzer in einem Identitätsspeicher beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse der Richtlinienkonfiguration auf der Identity Services Engine (ISE) verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Identity Services Engine 3.0
- Microsoft Windows Active Directory 2016

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Die Konfiguration einer benutzerspezifischen dynamischen Zugriffskontrollliste richtet sich an Benutzer, die

entweder im internen ISE-Identitätsspeicher oder in einem externen Identitätsspeicher vorhanden sind.

Konfigurieren

Die benutzerspezifische dACL kann für jeden Benutzer im internen Speicher konfiguriert werden, der ein benutzerdefiniertes Benutzerattribut verwendet. Für einen Benutzer im Active Directory (AD) kann ein beliebiges Attribut vom Typ Zeichenfolge verwendet werden, um dasselbe zu erreichen. Dieser Abschnitt enthält Informationen, die für die Konfiguration der ISE- und AD-Attribute erforderlich sind, sowie die Konfiguration, die für die Funktion auf der ISE erforderlich ist.

Konfigurieren eines neuen benutzerdefinierten Benutzerattributs auf der ISE

Navigieren Sie zu **Administration > Identity Management > Settings > User Custom Attributes**. Klicken Sie auf die Schaltfläche +, wie im Bild gezeigt, um ein neues Attribut hinzuzufügen und die Änderungen **zu speichern**. In diesem Beispiel lautet der Name des benutzerdefinierten Attributs **ACL**.

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is Administration > Identity Management > Settings > User Custom Attributes. The left sidebar shows the navigation menu with '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 the 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 konfigurieren

Um herunterladbare ACLs zu konfigurieren, navigieren Sie zu **Richtlinie > Richtlinienelemente > Ergebnisse > Autorisierung > Herunterladbare ACLs**. Klicken Sie auf Hinzufügen. Geben Sie einen Namen und den Inhalt der dACL an, und **speichern Sie** die Änderungen. Wie in der Abbildung dargestellt, lautet der Name der 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

Konfigurieren eines internen Benutzerkontos mit dem benutzerdefinierten Attribut

Navigieren Sie zu **Administration > Identity Management > Identities > Users > Add**. Erstellen Sie einen Benutzer, und konfigurieren Sie den benutzerdefinierten Attributwert mit dem Namen der dACL, die der Benutzer bei der Autorisierung abrufen muss. In diesem Beispiel lautet der Name der 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

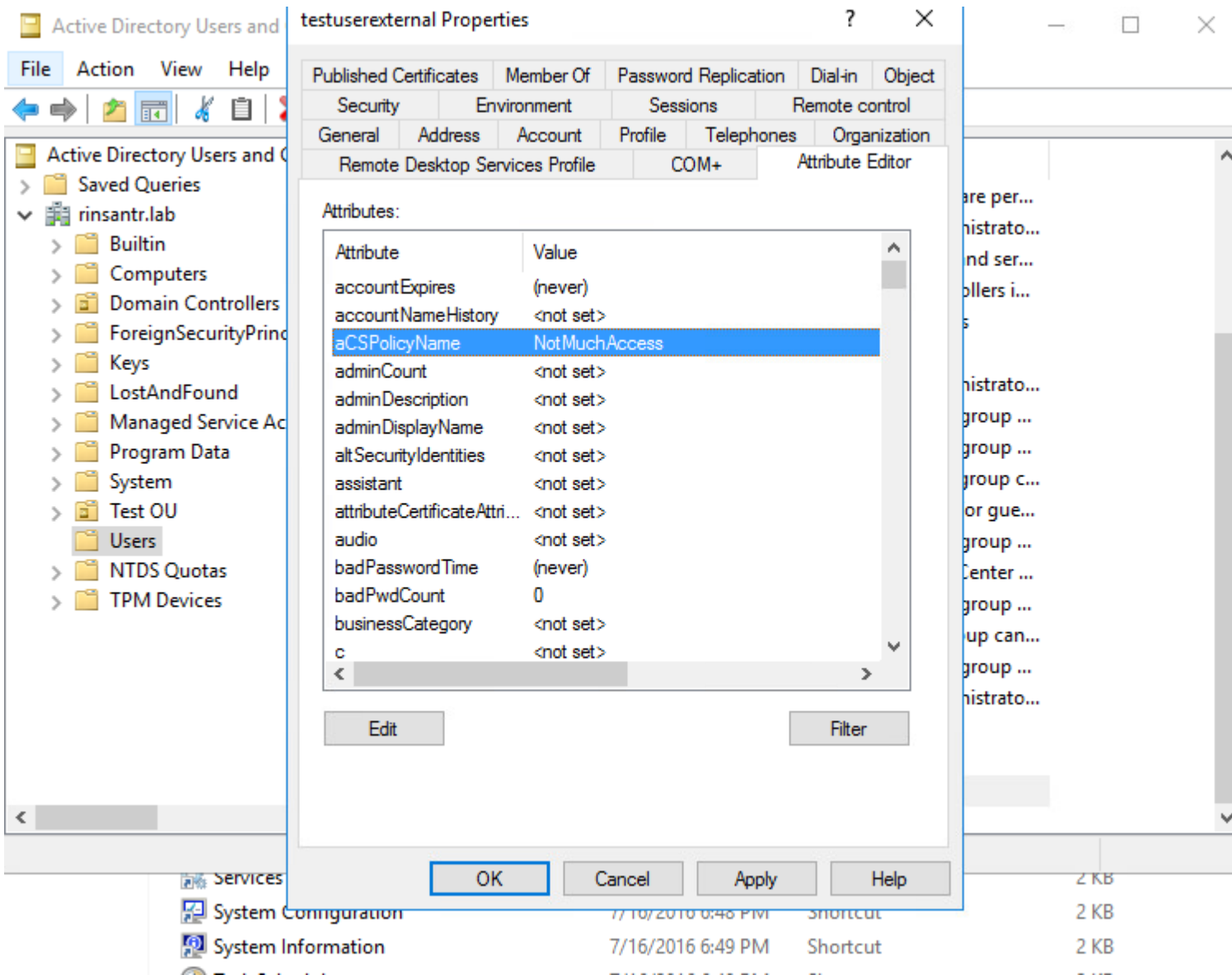
> Account Disable Policy

User Custom Attributes

ACL = NotMuchAccess

AD-Benutzerkonto konfigurieren

Navigieren Sie im Active Directory zu den Benutzerkontoeigenschaften, und wechseln Sie dann zur Registerkarte **Attribute-Editor**. Wie im Bild gezeigt, ist **aCSPolicyName** das Attribut, mit dem der dACL-Name angegeben wird. Wie bereits erwähnt, kann jedoch auch jedes Attribut verwendet werden, das einen Zeichenfolgenwert akzeptieren kann.



Attribut von AD in ISE importieren

Um das für AD konfigurierte Attribut zu verwenden, muss es von der ISE importiert werden. Um das Attribut zu importieren, navigieren Sie zu **Administration > Identity Management > External Identity Sources > Active Directory > [Join point configured] > Attributes** tab. Klicken Sie auf **Hinzufügen** und dann auf **Attribute aus Verzeichnis auswählen**. Geben Sie im AD den Namen des Benutzerkontos an, und klicken Sie dann auf **Attribute abrufen**. Wählen Sie das für die DACL konfigurierte Attribut aus, klicken Sie auf **OK** und dann auf **Speichern**. Wie im Bild gezeigt, ist aCSPolicyName das Attribut.

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

Autorisierungsprofile für interne und externe Benutzer konfigurieren

Um Autorisierungsprofile zu konfigurieren, navigieren Sie zu **Policy > Policy Elements > Results > Authorization > Authorization Profiles**. Klicken Sie auf Hinzufügen. Geben Sie einen Namen an, und wählen Sie den dACL-Namen **InternalUser:<name of custom attribute created>** für den internen Benutzer aus. Wie im Bild gezeigt, wird für interne Benutzer das Profil **InternalUserAttributeTest** konfiguriert, wobei dACL als **InternalUser:ACL** konfiguriert ist.

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:...

Verwenden Sie für externe Benutzer **<Join point name>:<attribute configured on AD>** als dACL-Namen. In diesem Beispiel wird das Profil **ExternalUserAttributeTest** mit der dACL konfiguriert, die als **RiniAD:aCSPolicyName** konfiguriert ist, wobei RiniAD der Name des Join-Punkts ist.

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

DAACL Name

[RiniAD:aCSF](#)

Autorisierungsrichtlinien konfigurieren

Autorisierungsrichtlinien können unter **Richtlinie > Richtliniensätze** konfiguriert werden, basierend auf den Gruppen, in denen der externe Benutzer im AD vorhanden ist, und basierend auf dem Benutzernamen im internen ISE-Identitätsspeicher. In diesem Beispiel ist **testuserexternal** ein Benutzer in der Gruppe **rinsantr.lab/Users/Test Group**, und **testuserinternal** ist ein Benutzer im internen ISE-Identitätsspeicher.

Authorization Policy (3)

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

Überprüfung

In diesem Abschnitt können Sie überprüfen, ob die Konfiguration funktioniert.

Überprüfen Sie die RADIUS-Live-Protokolle, um die Benutzerauthentifizierungen zu überprüfen.

Interner Benutzer:

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


Externer Benutzer:

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

Klicken Sie auf das Lupensymbol für die erfolgreichen Benutzerauthentifizierungen, um zu überprüfen, ob die Anforderungen die richtigen Richtlinien im Abschnitt "Übersicht" der detaillierten Live-Protokolle erreichen.


Interner Benutzer:

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

Externer Benutzer:

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 Ac User
Authorization Result	ExternalUserAttributeTest

Überprüfen Sie im Abschnitt "Other Attributes" (Andere Attribute) der detaillierten Live-Protokolle, ob die Benutzerattribute abgerufen wurden.

Interner Benutzer:

EnableFlag	Enabled
ACL	NotMuchAccess
RADIUS Username	testuserinternal

Externer Benutzer:

aCSPolicyName	NotMuchAccess
RADIUS Username	testuserexternal

Überprüfen Sie im Abschnitt "Ergebnis" der detaillierten Live-Protokolle, ob das dACL-Attribut als Teil

von Access-Accept gesendet wird.

cisco-av-pair

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

Überprüfen Sie außerdem die RADIUS-Live-Protokolle, um zu überprüfen, ob die dACL nach der Benutzerauthentifizierung heruntergeladen wurde.

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



#ACSACL#-IP-Not

Klicken Sie im Download-Protokoll der dACL auf das Lupensymbol, und überprüfen Sie den Abschnitt Overview (Übersicht), um den dACL-Download zu bestätigen.

Overview

Event

5232 DACL Download Succeeded

Username

#ACSACL#-IP-NotMuchAccess-60049cbb

Endpoint Id

Endpoint Profile

Authorization Result

Im Abschnitt "Ergebnis" dieses detaillierten Berichts können Sie den Inhalt der dACL überprüfen.

cisco-av-pair

ip:inacl#1=permit ip any any

Fehlerbehebung

Es sind derzeit keine spezifischen Informationen zur Fehlerbehebung für diese Konfiguration verfügbar.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.