

Configurar listas de controle de acesso dinâmico por usuário no ISE

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Configurar um novo atributo de usuário personalizado no ISE](#)

[Configurar dACL](#)

[Configurar uma conta de usuário interno com o atributo personalizado](#)

[Configurar uma conta de usuário do AD](#)

[Importar o atributo do AD para o ISE](#)

[Configurar perfis de autorização para usuários internos e externos](#)

[Configurar Políticas de Autorização](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento descreve a configuração de uma lista de controle de acesso dinâmico (dACL - Dynamic Access Control List) por usuário para usuários presentes em um tipo de armazenamento de identidade.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento da configuração da política no Identity Services Engine (ISE).

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Identity Services Engine 3.0
- Microsoft Windows Active Directory 2016

As informações neste documento foram criadas a partir de dispositivos em um ambiente de

laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A configuração de uma Lista de controle de acesso dinâmico por usuário é para usuários presentes no armazenamento de identidade interno do ISE ou em um armazenamento de identidade externo.

Configurar

O dACL por usuário pode ser configurado para qualquer usuário no armazenamento interno que use um atributo de usuário personalizado. Para um usuário no Ative Diretory (AD), qualquer atributo do tipo cadeia de caracteres pode ser usado para obter o mesmo resultado. Esta seção fornece informações necessárias para configurar os atributos no ISE e no AD, juntamente com a configuração necessária no ISE para que esse recurso funcione.

Configurar um novo atributo de usuário personalizado no ISE

Navegue até Administração > Gerenciamento de identidades > Configurações > Atributos personalizados do usuário. Clique no botão +, conforme mostrado na imagem, para adicionar um novo atributo e salvar as alterações. Neste exemplo, o nome do atributo personalizado é 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 includes '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'. The 'Save' button is highlighted in blue.

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

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

Configurar dACL

Para configurar ACLs para download, navegue para Policy > Policy Elements > Results >

Authorization > Downloadable ACLs. Clique em Add. Forneça um nome, o conteúdo do dACL e salve as alterações. Como mostrado na imagem, o nome do dACL é NotMuchAccess.

The screenshot shows the Cisco ISE configuration page for a Downloadable ACL. The breadcrumb trail 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

Below the DACL content field, there is a 'Check DACL Syntax' option and a 'Submit' button.

Configurar uma conta de usuário interno com o atributo personalizado

Navegue até Administração > Gerenciamento de identidades > Identidades > Usuários > Adicionar. Crie um usuário e configure o valor do atributo personalizado com o nome do dACL que o usuário precisa obter quando autorizado. Neste exemplo, o nome do dACL é 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

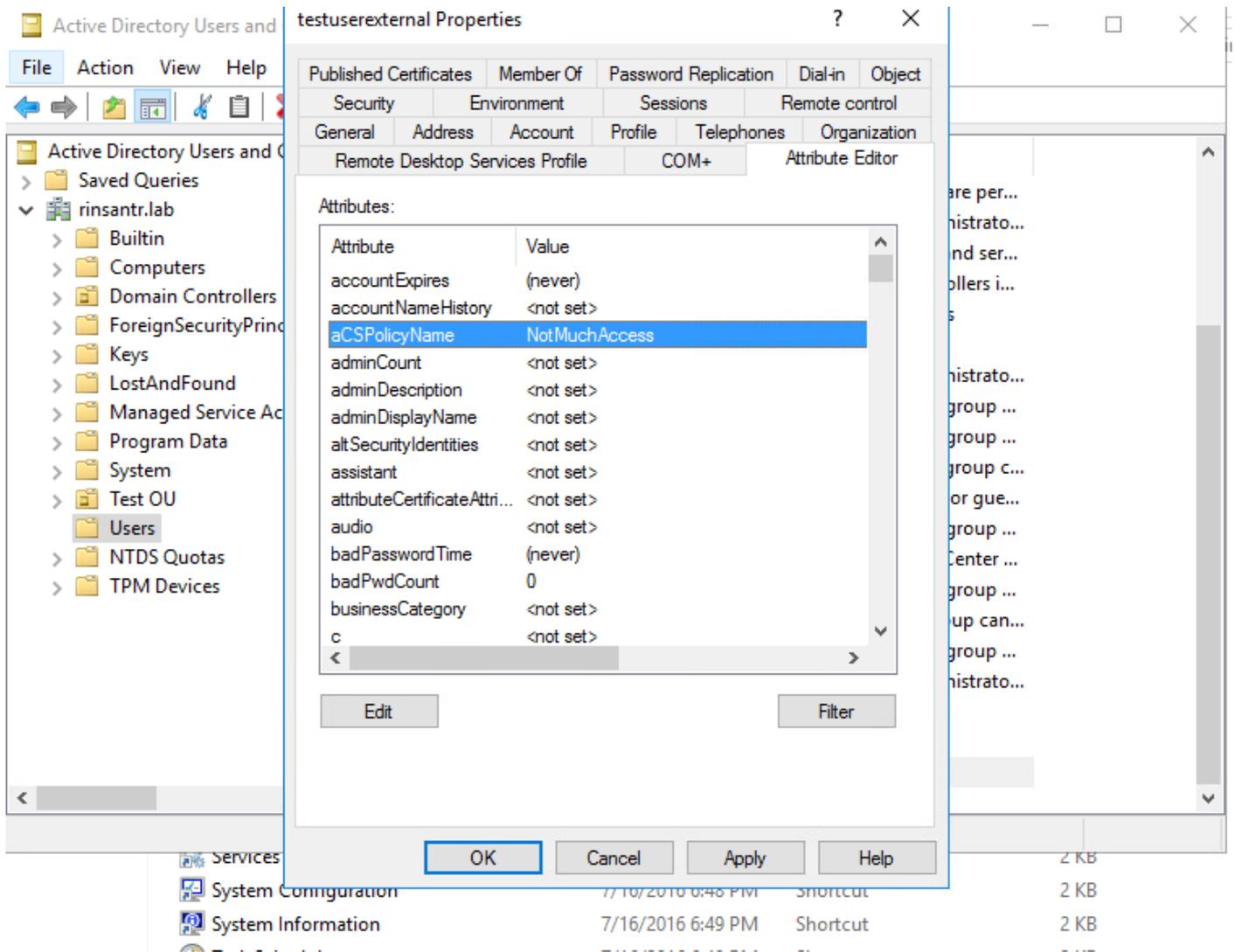
> Account Disable Policy

User Custom Attributes

ACL = NotMuchAccess

Configurar uma conta de usuário do AD

No Active Directory, navegue até as propriedades da conta de usuário e depois até a guia Editor de atributos. Como mostrado na imagem, aCSPolicyName é o atributo usado para especificar o nome dACL. No entanto, como mencionado anteriormente, qualquer atributo que possa aceitar um valor de string também pode ser usado.



Importar o atributo do AD para o ISE

Para usar o atributo configurado no AD, o ISE precisa importá-lo. Para importar o atributo, navegue para Administração > Gerenciamento de identidades > Fontes de identidade externas > Active Directory > [Ponto de ingresso configurado] > guia Atributos. Clique em Adicionar e em Selecionar atributos do diretório. Forneça o nome da conta de usuário no AD e clique em Recuperar atributos. Selecione o atributo configurado para o dACL, clique em OK e em Salvar. Como mostrado na imagem, aCSPolicyName é o 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

Click here to do visibility setup Do not show this again.

External Identity Sources

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

Attributes

Edit + Add Delete Attribute

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

Save

Reset

Configurar perfis de autorização para usuários internos e externos

Para configurar Perfis de autorização, navegue para Política > Elementos de política > Resultados > Autorização > Perfis de autorização. Clique em Add. Forneça um nome e escolha o nome dACL como InternalUser:<nome do atributo personalizado criado> para o usuário interno. Como

mostrado na imagem, para o usuário interno, o perfil InternalUserAttributeTest é configurado com o dACL configurado como InternalUser:ACL.

The screenshot shows the Cisco ISE interface for configuring a new Authorization Profile. The breadcrumb path 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), Authorization Profiles, Downloadable ACLs, Profiling, Posture, and Client Provisioning.

The main configuration area 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 main configuration, there is a section for "Common Tasks" which is expanded. It contains a checked checkbox for "DACL Name" and a dropdown menu with the value "InternalUser:ACL".

Para o usuário externo, use <Join point name>:<attribute configured on AD> como o nome dACL. Neste exemplo, o perfil ExternalUserAttributeTest é configurado com o dACL configurado como RiniAD:aCSPolicyName, onde RiniAD é o nome do ponto Join.

Dictionaryes
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:aCSPolicyName| ▼

Configurar Políticas de Autorização

As políticas de autorização podem ser configuradas em Política > Conjuntos de políticas com base nos grupos em que o usuário externo está presente no AD e também com base no nome de usuário no armazenamento de identidade interna do ISE. Neste exemplo, testuserexternal é um usuário presente no grupo rinsantr.lab/Users/Test Group e testuserinternal é um usuário presente no armazenamento de identidade interno do 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

Verificar

Use esta seção para verificar se a configuração funciona.

Verifique os logs RADIUS ativos para verificar as autenticações de usuário.

Usuário 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...

Usuário 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...

Clique no ícone de lupa nas autenticações de usuário bem-sucedidas para verificar se as solicitações atingem as políticas corretas na seção Visão geral dos logs ao vivo detalhados.

Usuário 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

Usuário 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 a seção Outros Atributos dos logs ao vivo detalhados para verificar se os atributos do usuário foram recuperados.

Usuário interno:

EnableFlag	Enabled
ACL	NotMuchAccess
RADIUS Username	testuserinternal

Usuário externo:

aCSPolicyName	NotMuchAccess
RADIUS Username	testuserexternal

Verifique a seção Resultado dos logs dinâmicos detalhados para verificar se o atributo dACL é enviado como parte de Access-Accept.

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

Além disso, verifique os logs RADIUS ao vivo para verificar se o dACL é baixado após a autenticação do usuário.

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



#ACSACL#-IP-NotMuchAccess-60049cbb

Clique no ícone de lupa no log de download do dACL e verifique a seção Visão geral para confirmar o download do dACL.

Overview

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

Verifique a seção Resultado deste relatório detalhado para verificar o conteúdo do dACL.

cisco-av-pair

ip:inacl#1=permit ip any any

Troubleshooting

No momento, não há informações específicas disponíveis para solucionar esse problema de configuração.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.