Configurar listas de controle de acesso dinâmico por usuário no ISE

Contents

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 Ative Diretory 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

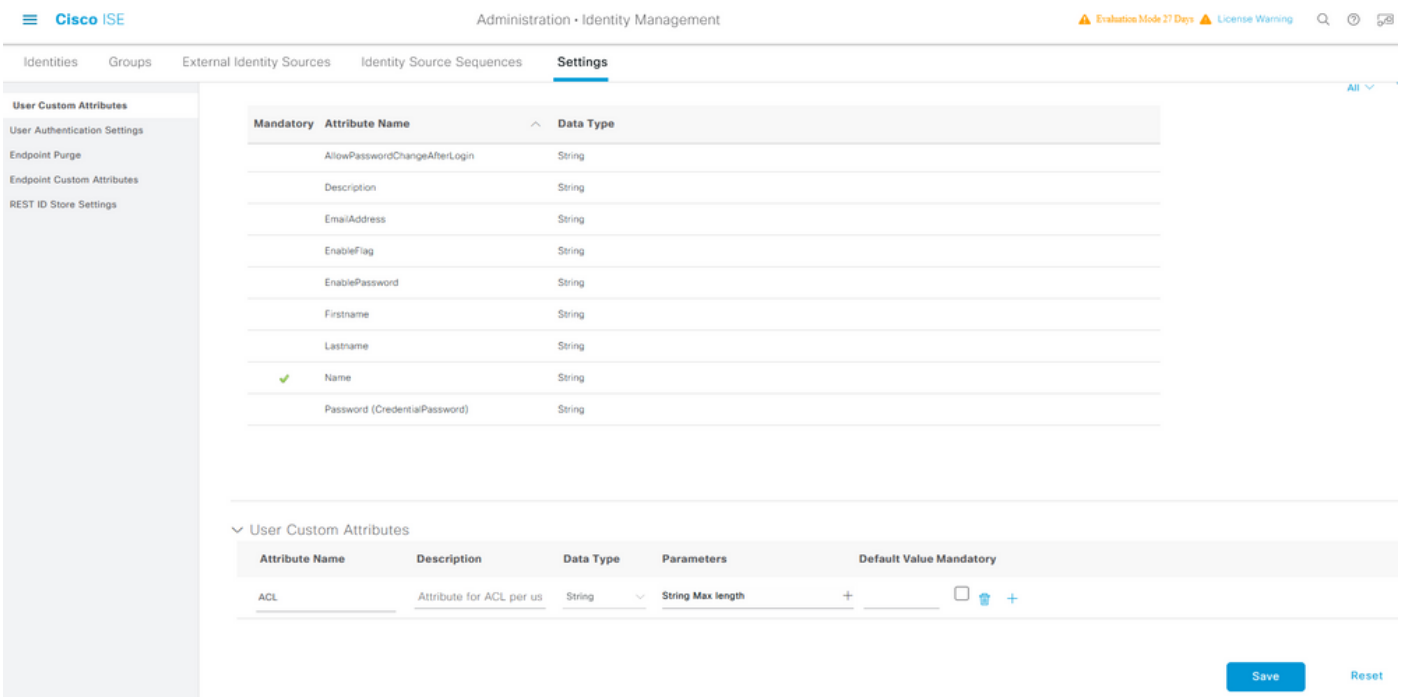
A configuração de uma Lista de controle de acesso dinâmico por usuário é para usuários presentes no armazenamento de identidade interno do ISE ou em um armazenamento de identidade externo.

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

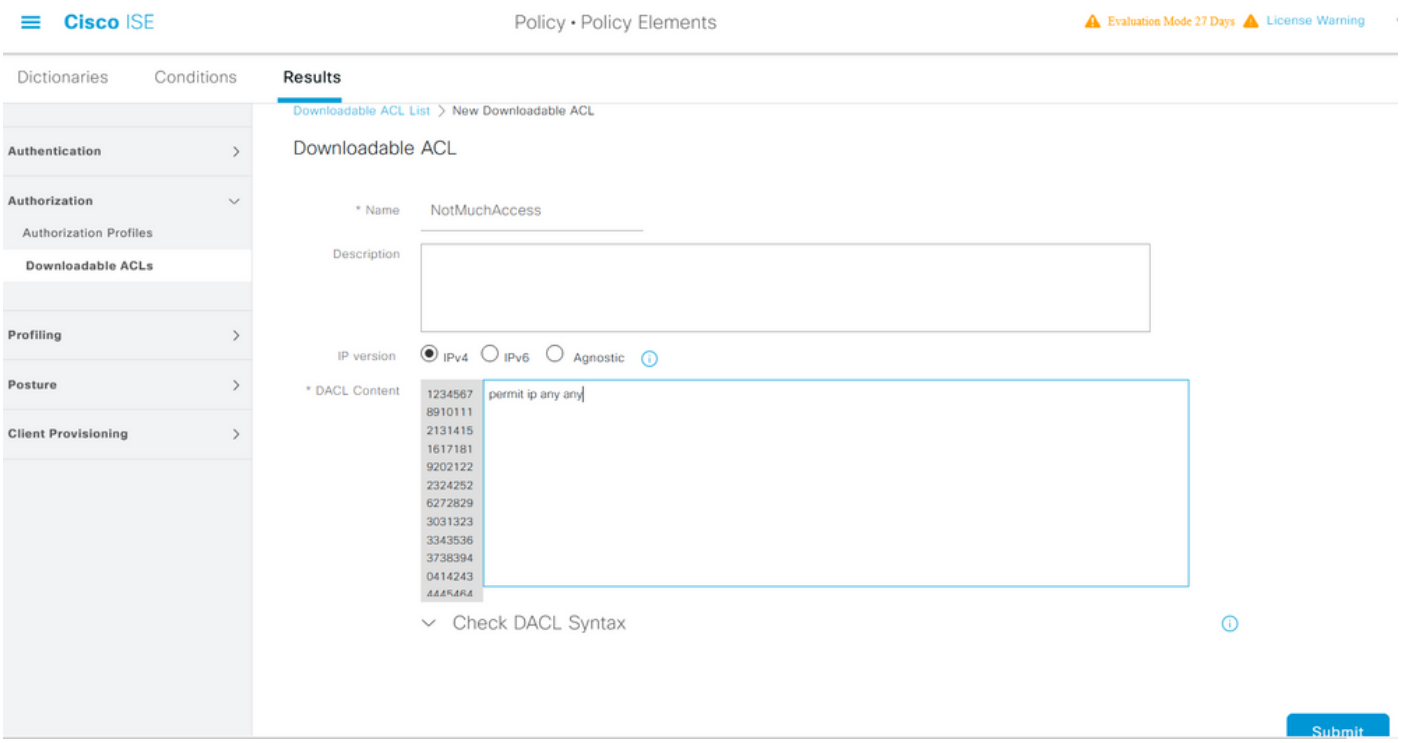
Navegue até Administração > Gerenciamento de identidades > Configurações > Atributos personalizados do usuário. Clique no botão +, conforme mostrado na imagem, para adicionar um novo atributo e salvar as alterações. Neste exemplo, o nome do atributo personalizado é ACL.



Configurar dACL

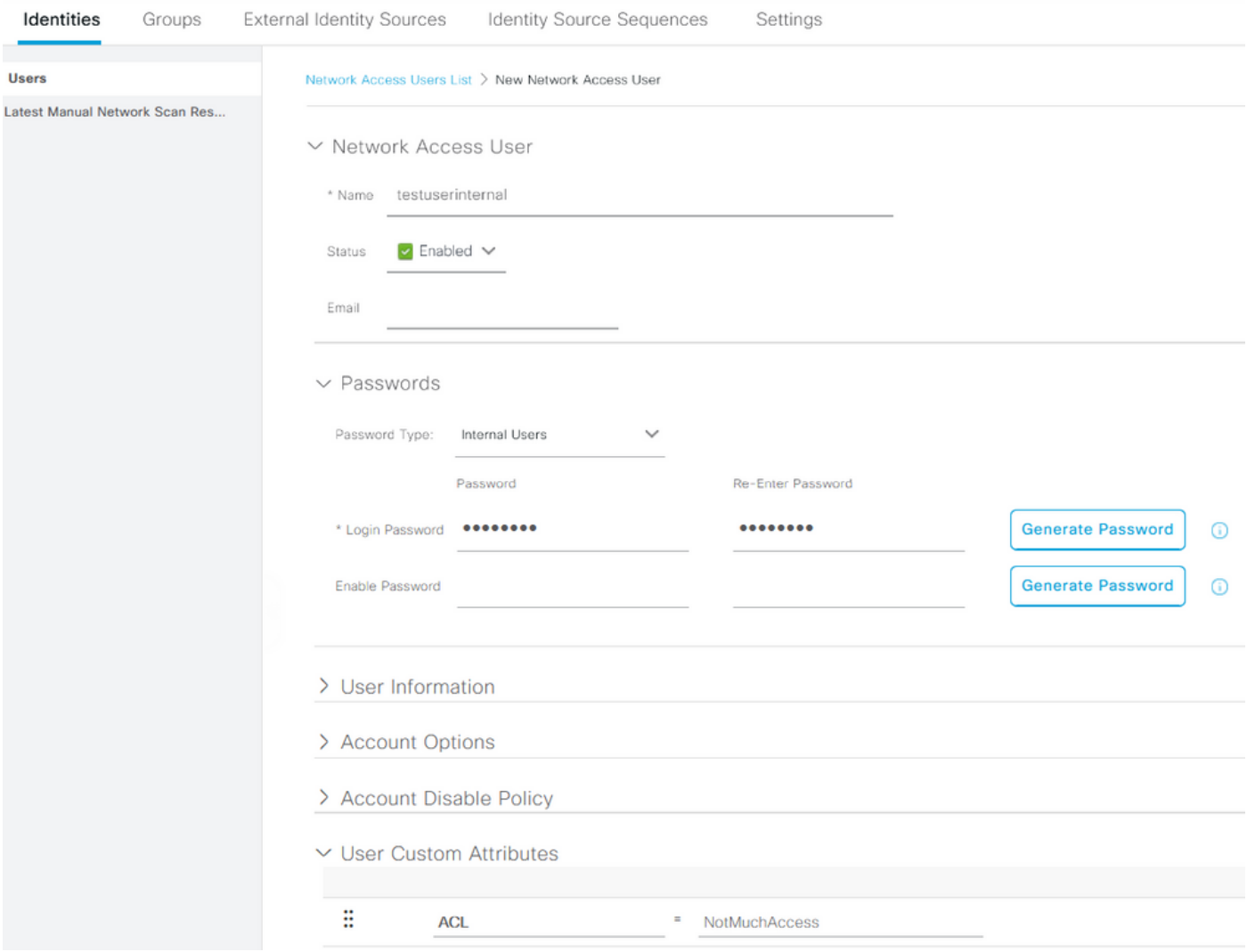
Para configurar ACLs para download, navegue para Policy > Policy Elements > Results >

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.



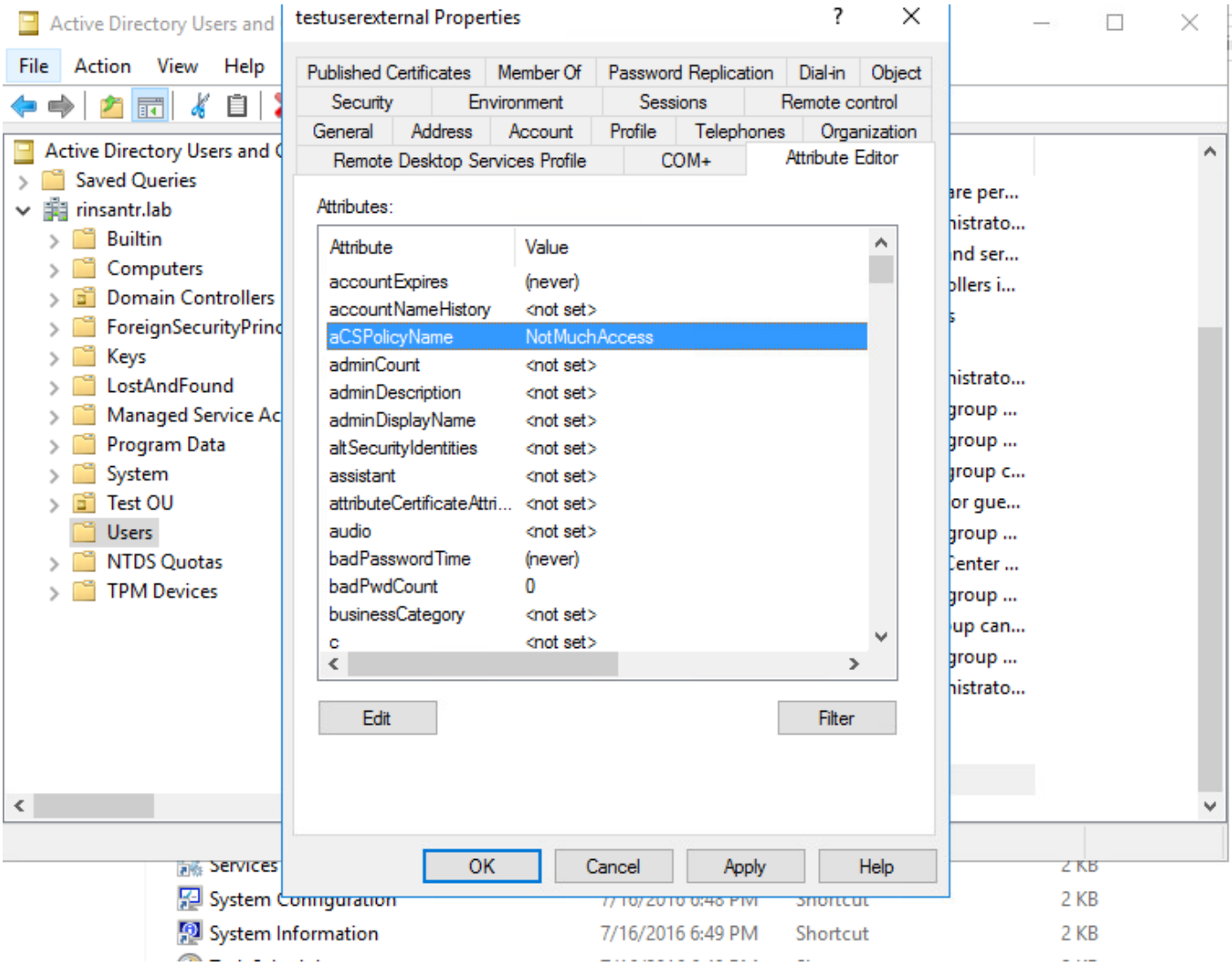
Configurar uma conta de usuário interno com o atributo personalizado

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.



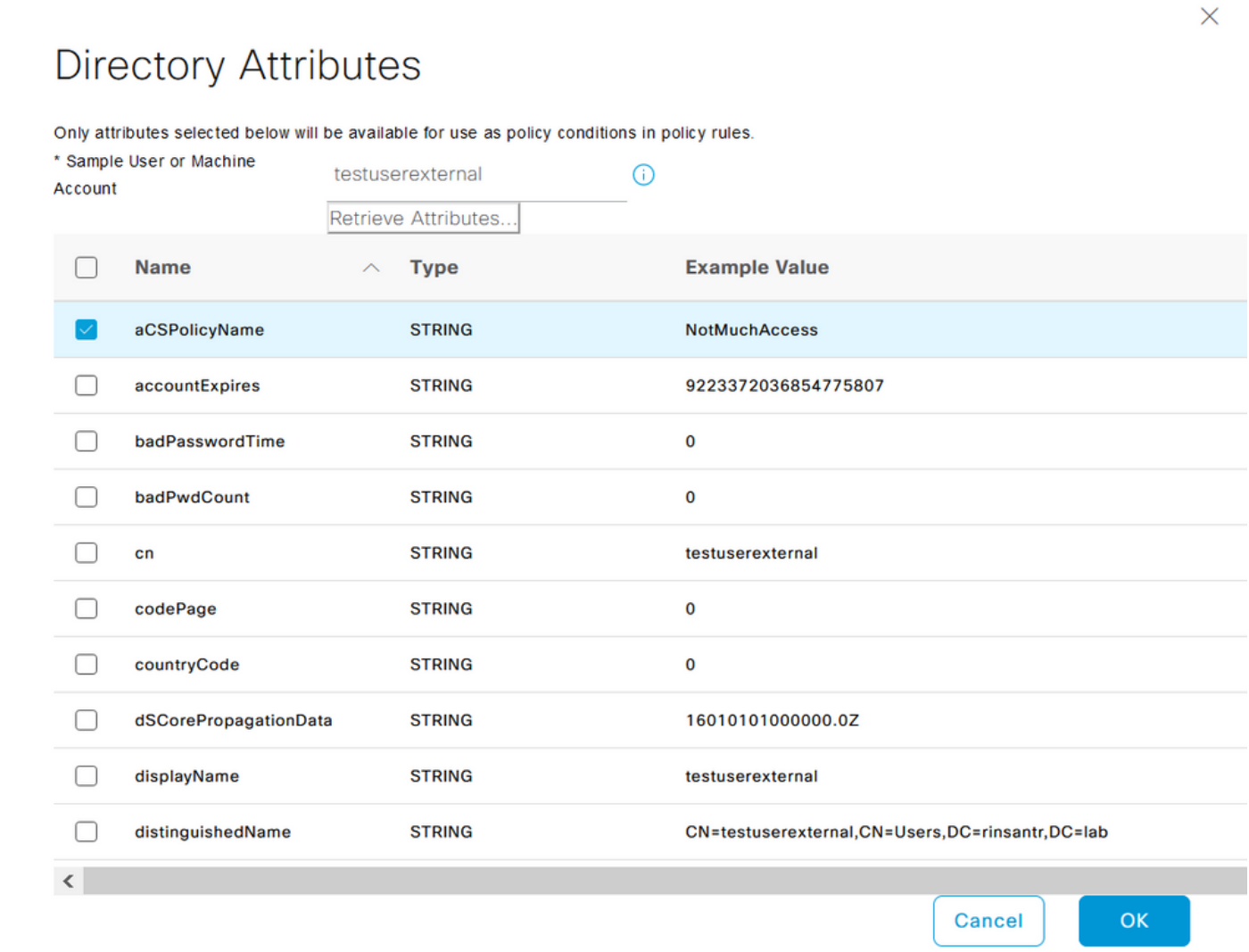
Configurar uma conta de usuário do AD

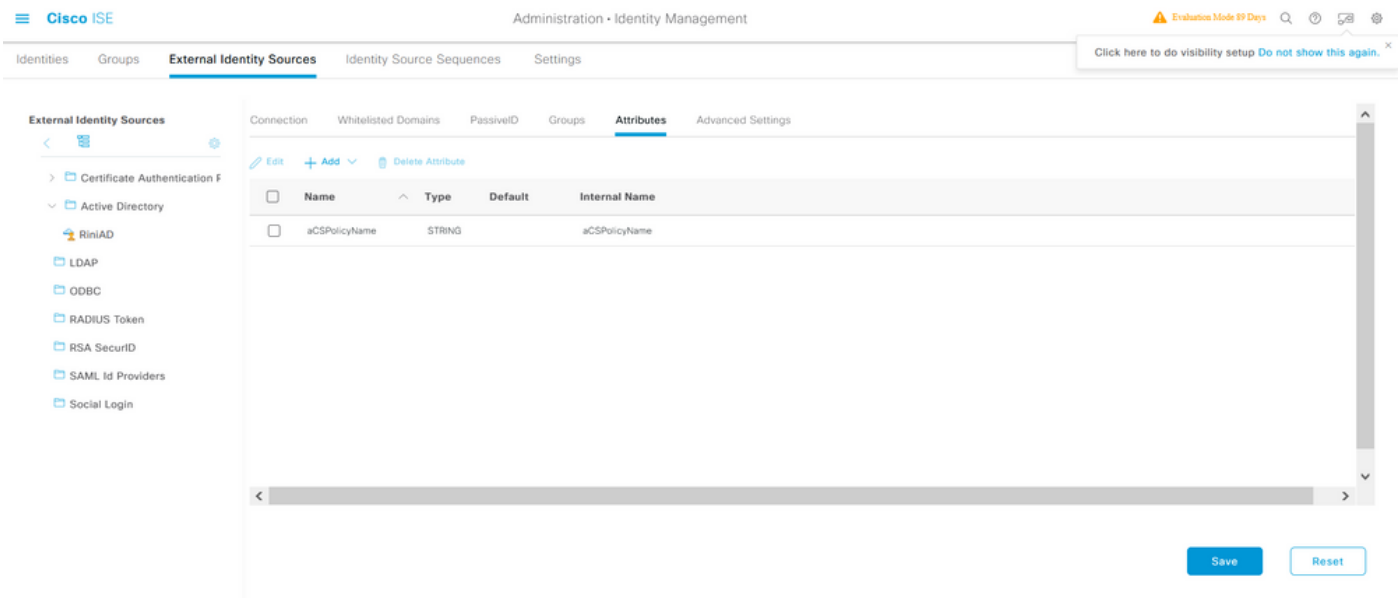
No Ative Diretory, navegue até as propriedades da conta de usuário e depois até a guia Editor de atributos. Como mostrado na imagem, aCSPolicyName é o atributo usado para especificar o nome dACL. No entanto, como mencionado anteriormente, qualquer atributo que possa aceitar um valor de string também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

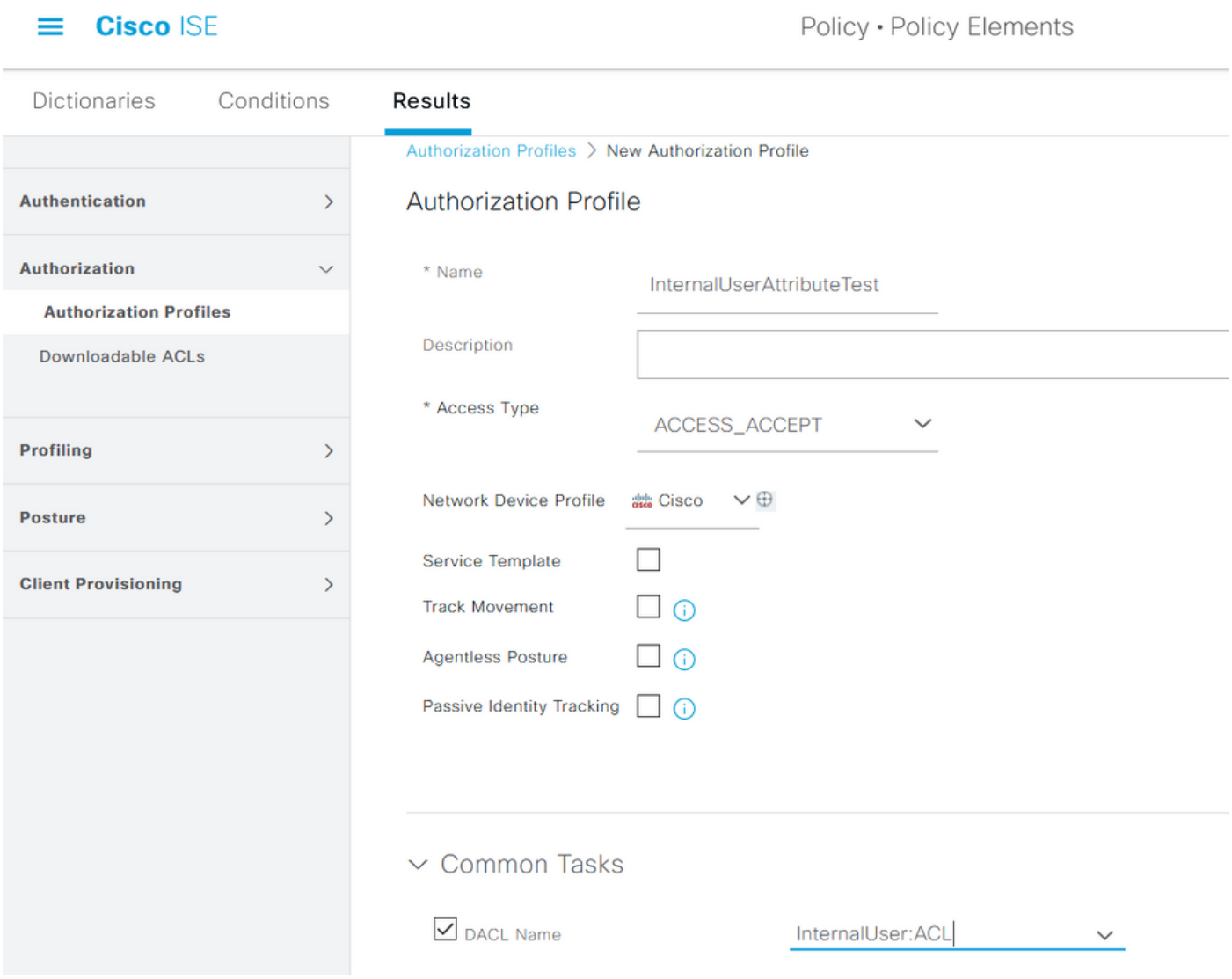




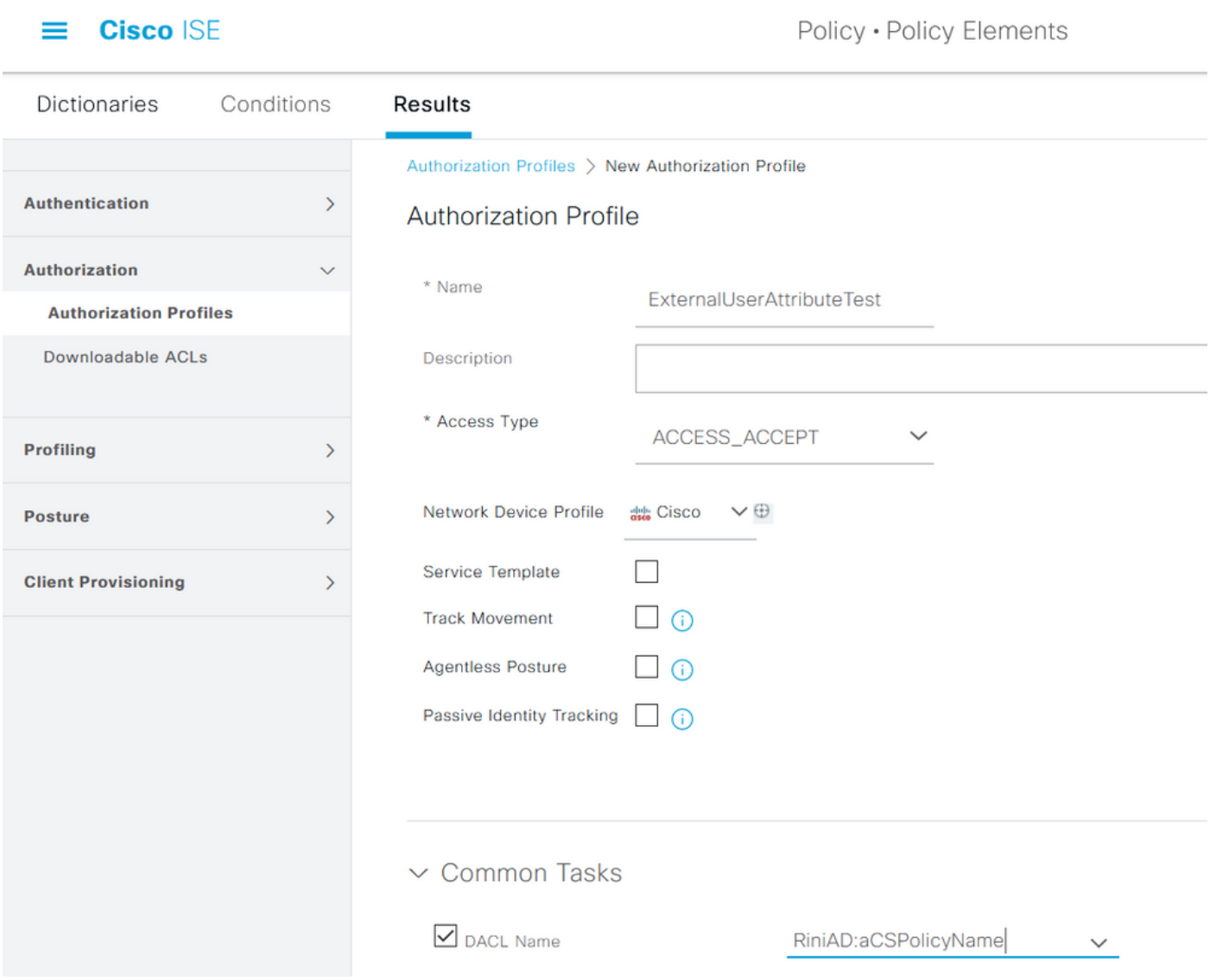
Configurar perfis de autorização para usuários internos e externos

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.

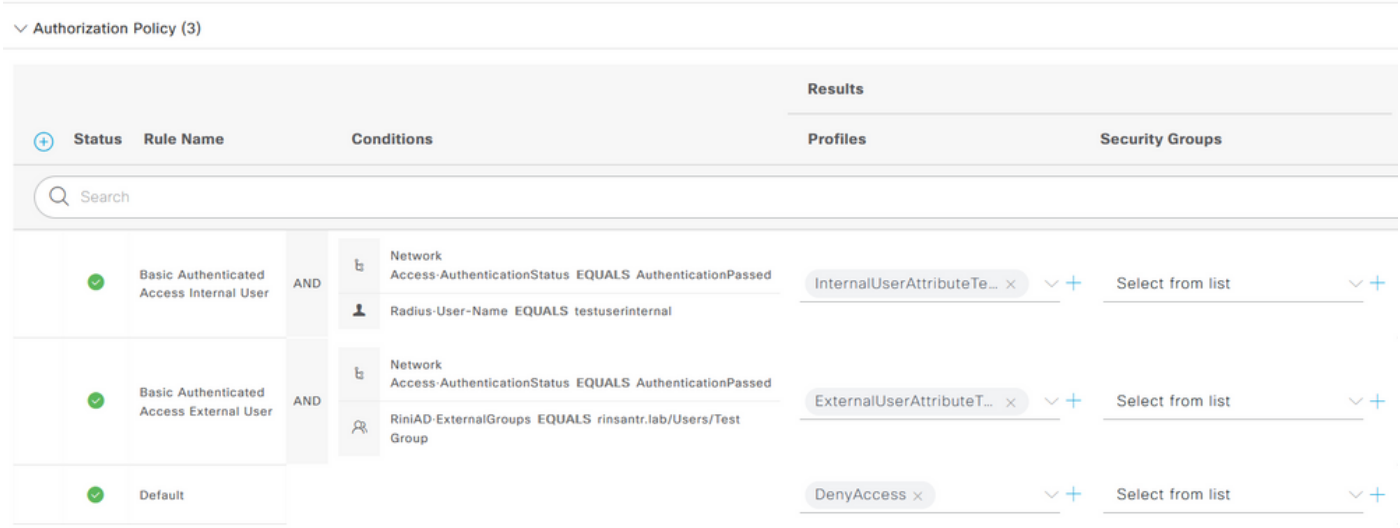


Para o usuário externo, use <Join point name>:<attribute configured on AD> como o nome dACL. Neste exemplo, o perfil ExternalUserAttributeTest é configurado com o dACL configurado como RiniAD:aCSPolicyName, onde RiniAD é o nome do ponto Join.



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.

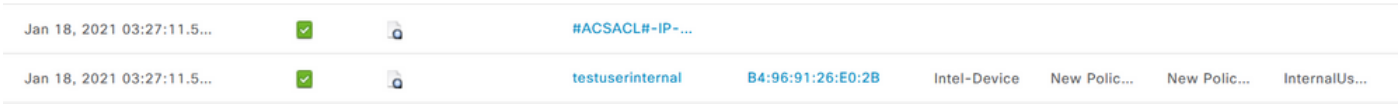


Verificar

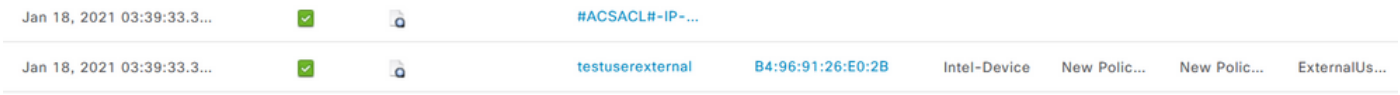
Use esta seção para verificar se a configuração funciona.

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

Usuário interno:

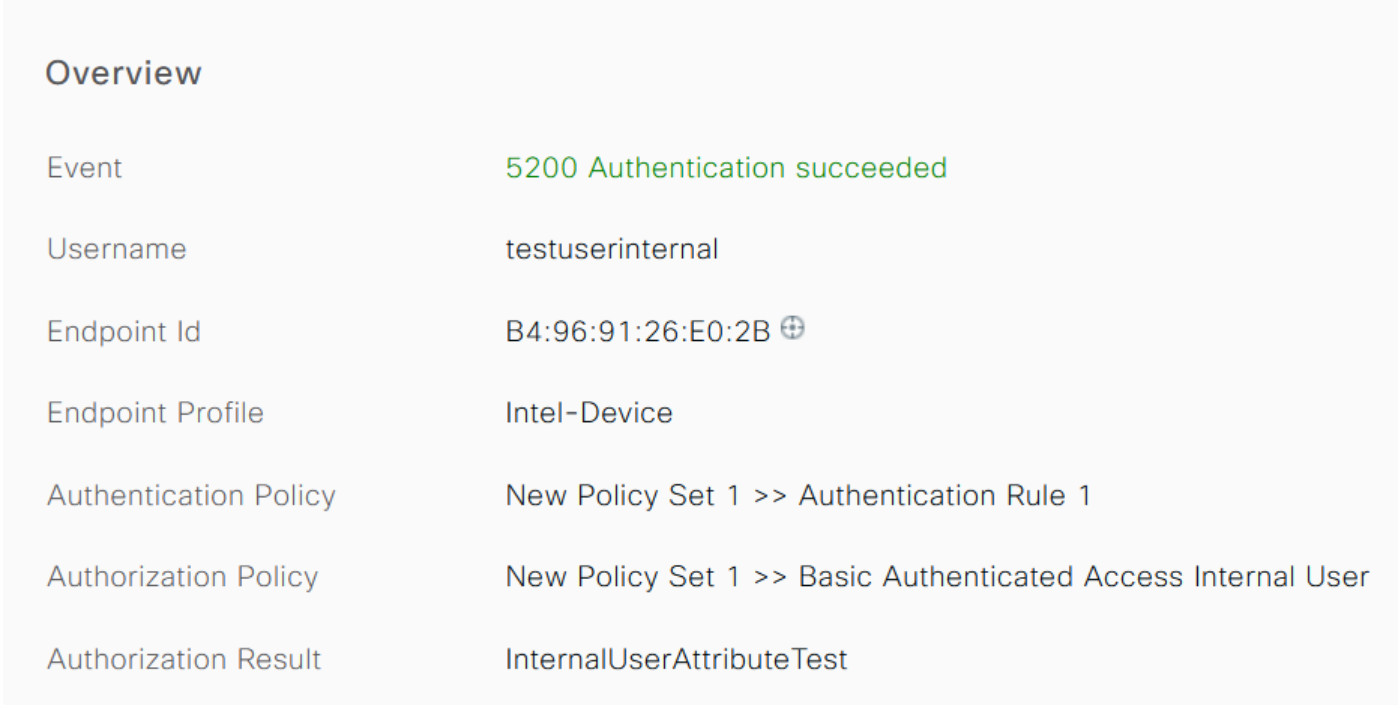


Usuário externo:

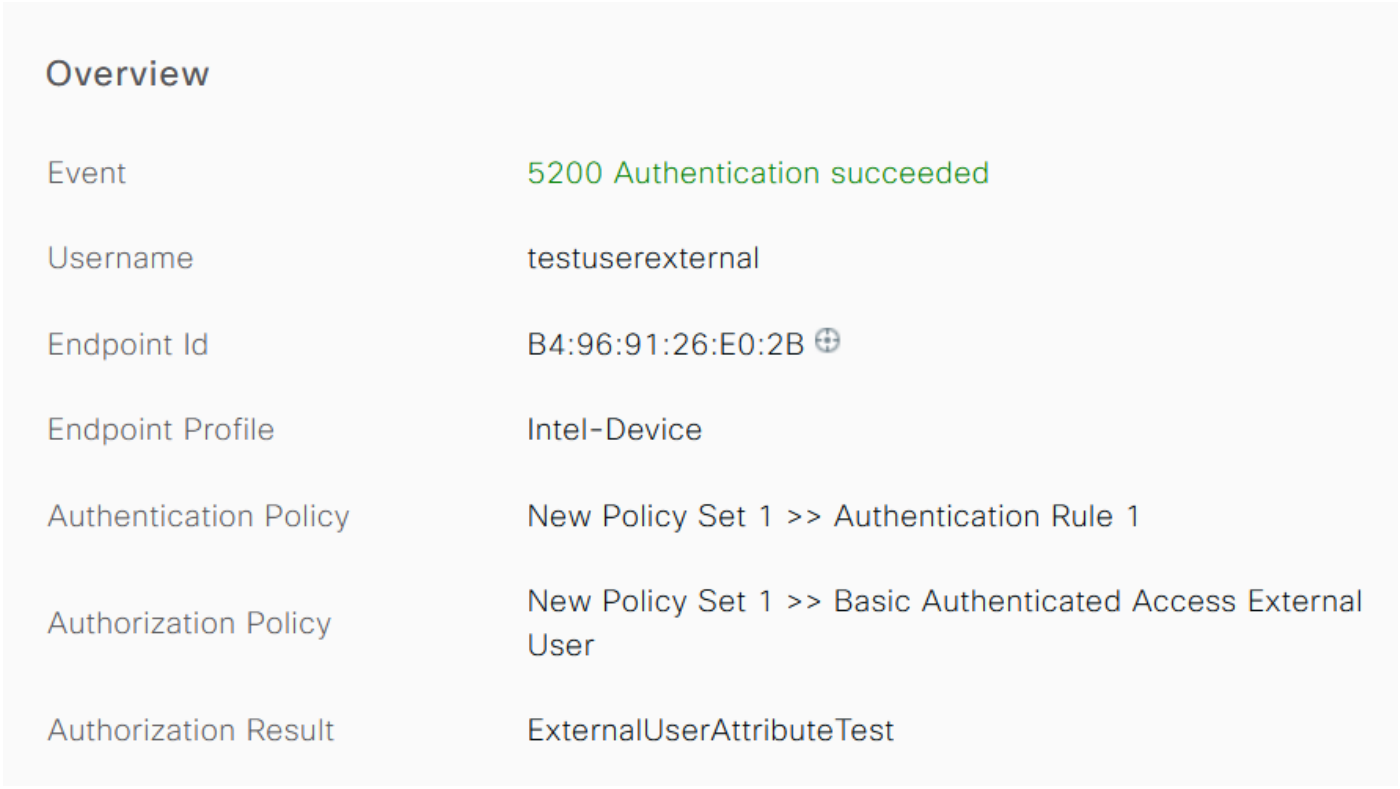


Clique no ícone de lupa nas autenticações de usuário bem-sucedidas para verificar se as solicitações atingem as políticas corretas na seção Visão geral dos logs ao vivo detalhados.

Usuário interno:



Usuário externo:



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:

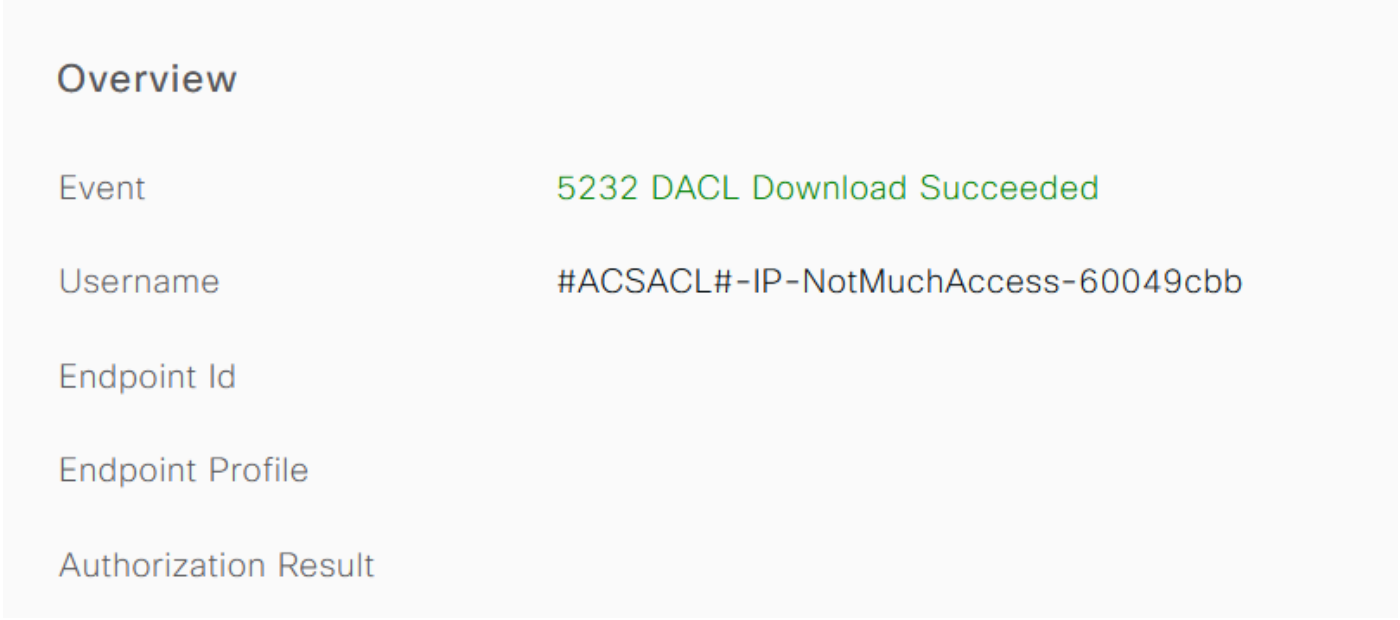
aCSPolicyName	NotMuchAccess
RADIUS Username	testuserexternal

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.

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



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

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.