Configuración de listas de control de acceso dinámico por usuario en ISE

Contenido

- Introducción
- Prerequisites
  - Requirements
  - Componentes Utilizados
- Antecedentes
- Configurar
  - Configuración de un nuevo atributo de usuario personalizado en ISE
  - Configurar dACL
  - Configuración de una cuenta de usuario interna con el atributo personalizado
  - Configurar una cuenta de usuario de AD
  - Importar el atributo de AD a ISE
  - Configurar perfiles de autorización para usuarios internos y externos
  - Configurar directivas de autorización
- Verificación
- Troubleshoot

Introducción

Este documento describe la configuración de una lista de control de acceso dinámico (dACL) por usuario para los usuarios presentes en un tipo de almacén de identidades.

Prerequisites

Requirements

Cisco recomienda conocer la configuración de políticas en Identity Services Engine (ISE).

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Identity Services Engine 3.0
- Microsoft Windows Active Directory 2016

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

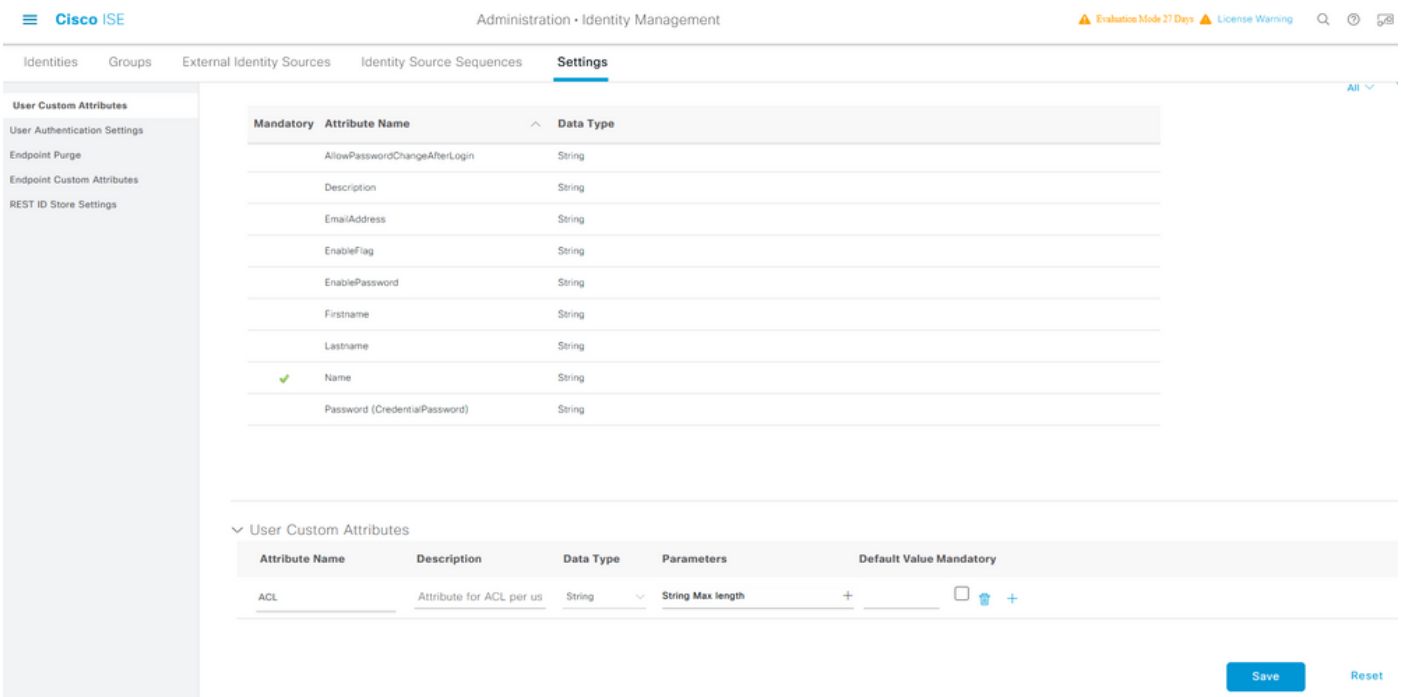
La configuración de una lista de control de acceso dinámico por usuario es para usuarios presentes en el almacén de identidades interno de ISE o en un almacén de identidades externo.

Configurar

La dACL por usuario se puede configurar para cualquier usuario del almacén interno que utilice un atributo de usuario personalizado. Para un usuario de Active Directory (AD), se puede utilizar cualquier atributo de tipo cadena para lograr lo mismo. Esta sección proporciona la información necesaria para configurar los atributos tanto en ISE como en AD, junto con la configuración necesaria en ISE para que esta función funcione.

Configuración de un nuevo atributo de usuario personalizado en ISE

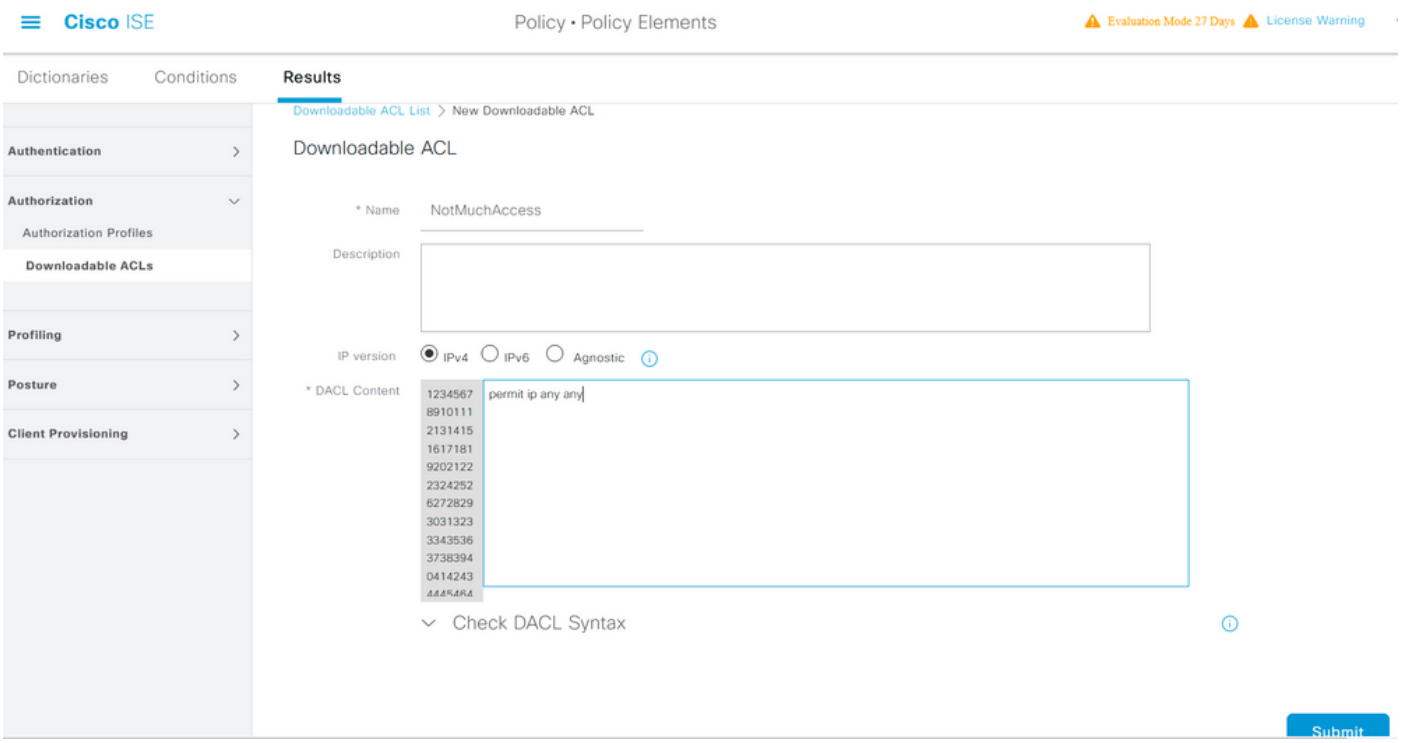
Vaya a Administration > Identity Management > Settings > User Custom Attributes. Haga clic en el botón +, como se muestra en la imagen, para agregar un nuevo atributo y guardar los cambios. En este ejemplo, el nombre del atributo personalizado es ACL.



Configurar dACL

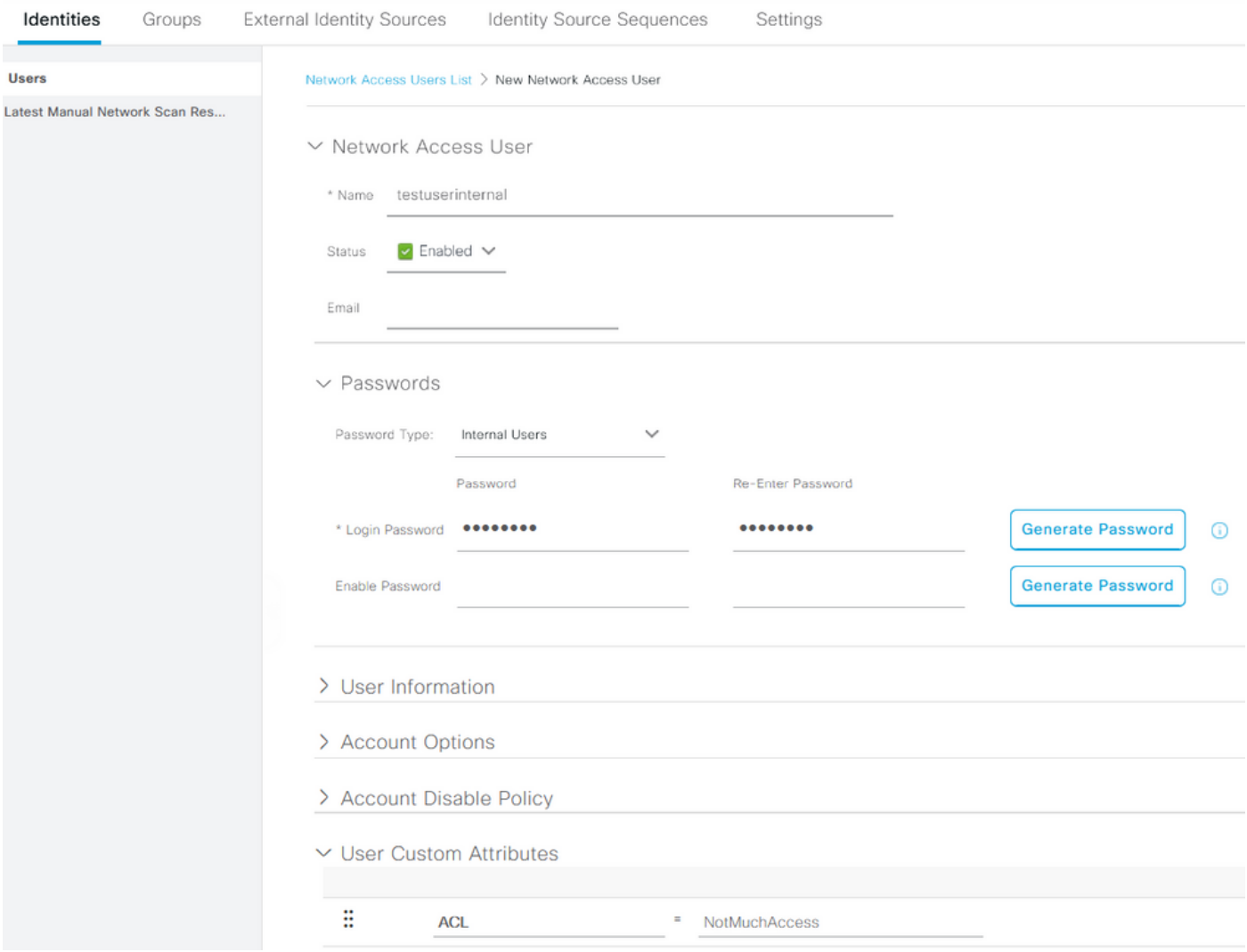
Para configurar las ACL descargables, navegue hasta Política > Elementos de Política > Resultados > Autorización > ACL descargables. Haga clic en Add (Agregar). Proporcione un nombre, el contenido de la dACL y guarde los cambios. Como se muestra en la imagen, el

nombre de la dACL es NotMuchAccess.



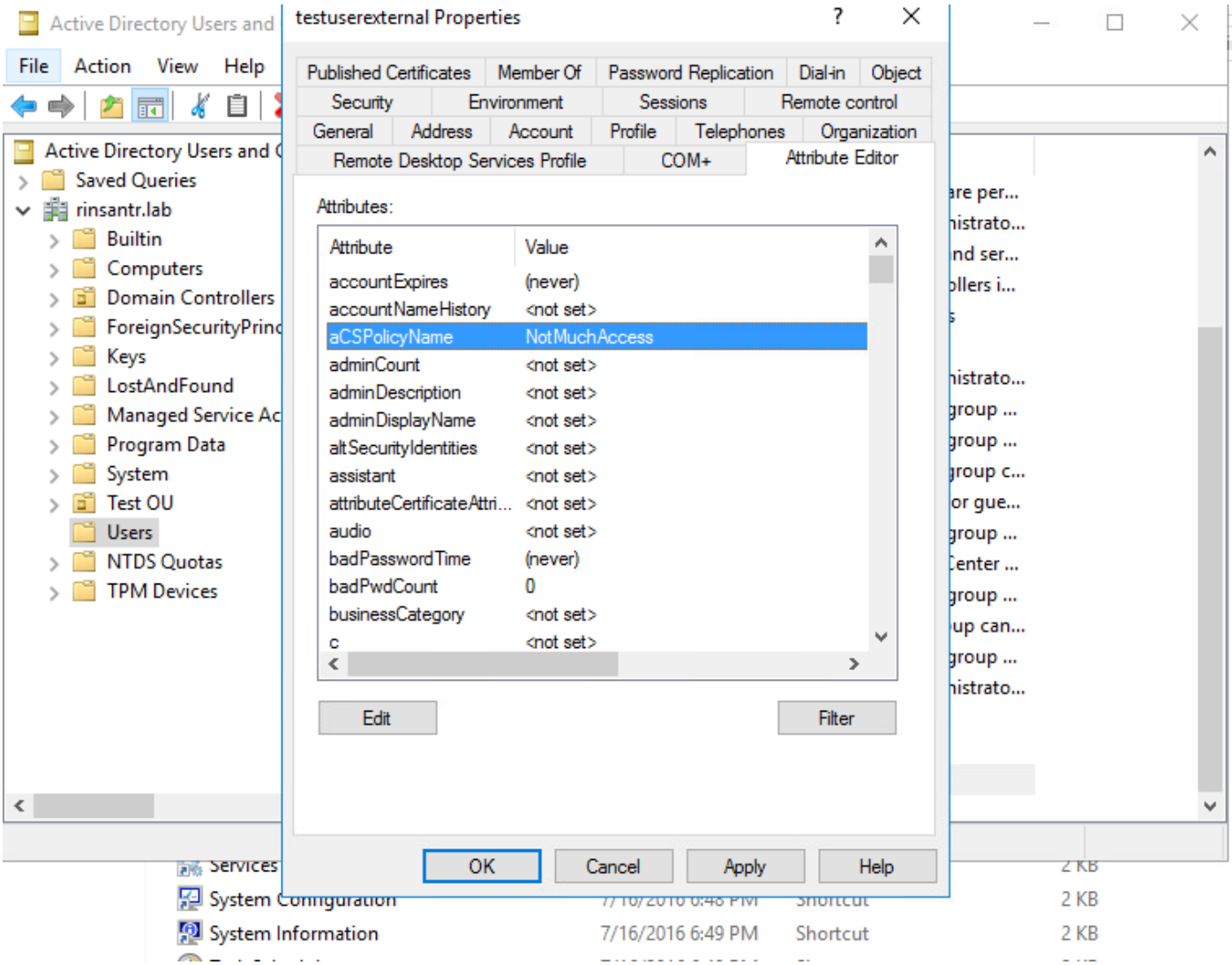
Configuración de una cuenta de usuario interna con el atributo personalizado

Vaya a Administration > Identity Management > Identities > Users > Add. Cree un usuario y configure el valor del atributo personalizado con el nombre de la dACL que el usuario necesita obtener cuando se le autoriza. En este ejemplo, el nombre de la dACL es NotMuchAccess.



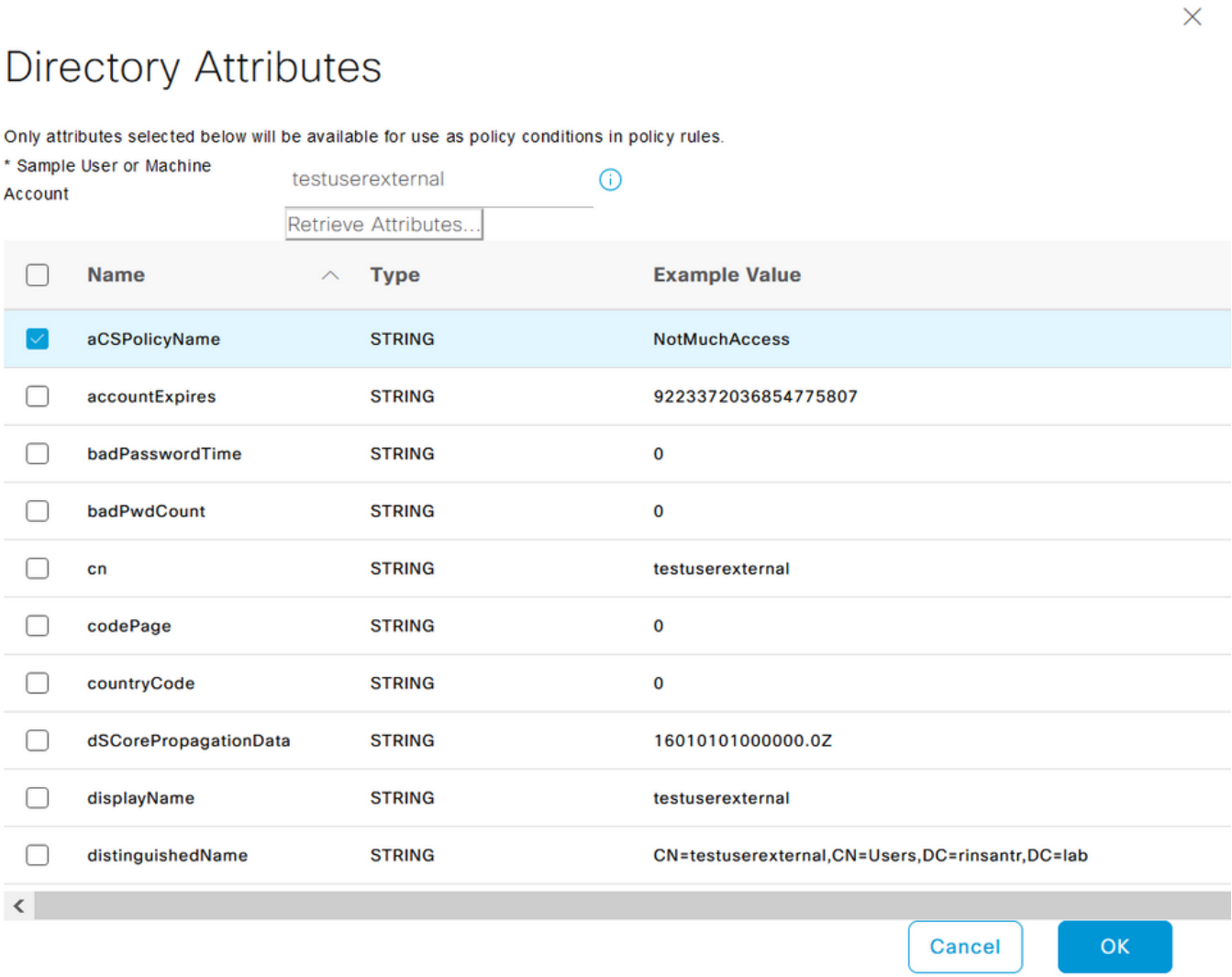
Configurar una cuenta de usuario de AD

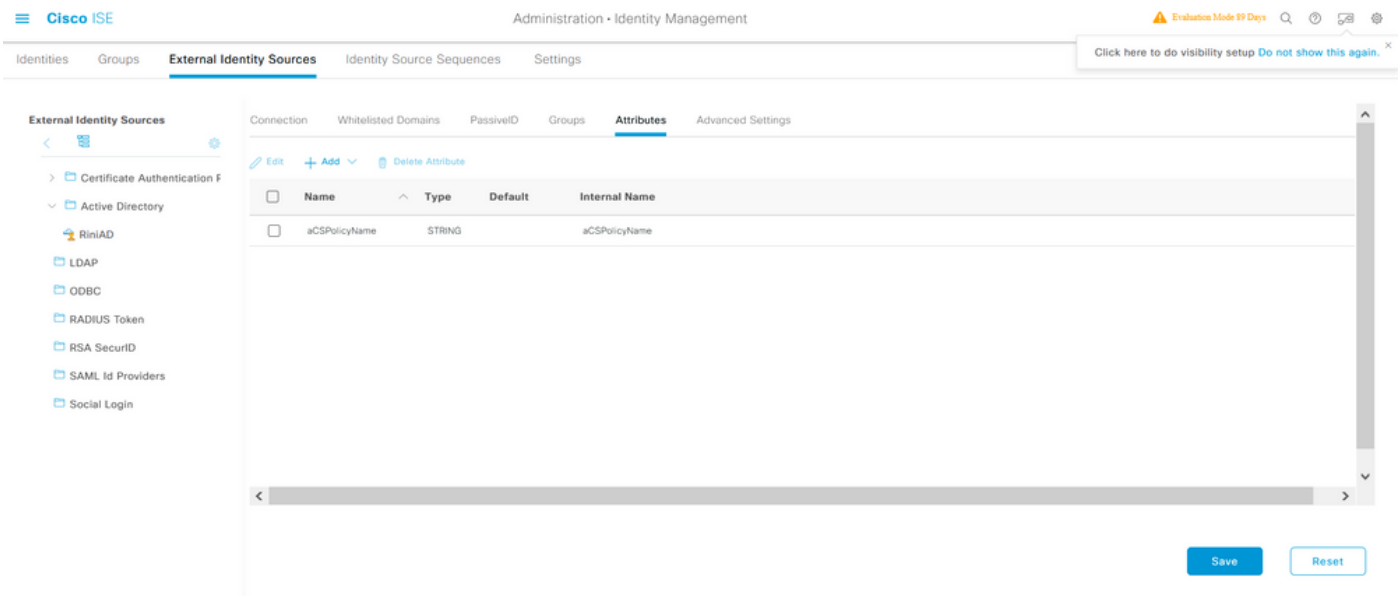
En Active Directory, desplácese hasta las propiedades de la cuenta de usuario y, a continuación, vaya a la ficha Attribute Editor. Como se muestra en la imagen, aCSPolicyName es el atributo utilizado para especificar el nombre dACL. Sin embargo, como se ha mencionado anteriormente, también se puede utilizar cualquier atributo que pueda aceptar un valor de cadena.



Importar el atributo de AD a ISE

Para utilizar el atributo configurado en AD, ISE debe importarlo. Para importar el atributo, navegue hasta Administration > Identity Management > External Identity Sources > Active Directory > [Join point configured] > Attributes. Haga clic en Agregar y luego en Seleccionar atributos del directorio. Proporcione el nombre de cuenta de usuario en AD y, a continuación, haga clic en Recuperar atributos. Seleccione el atributo configurado para la dACL, haga clic en Aceptar y, a continuación, haga clic en Guardar. Como se muestra en la imagen, aCSPolicyName es el atributo.

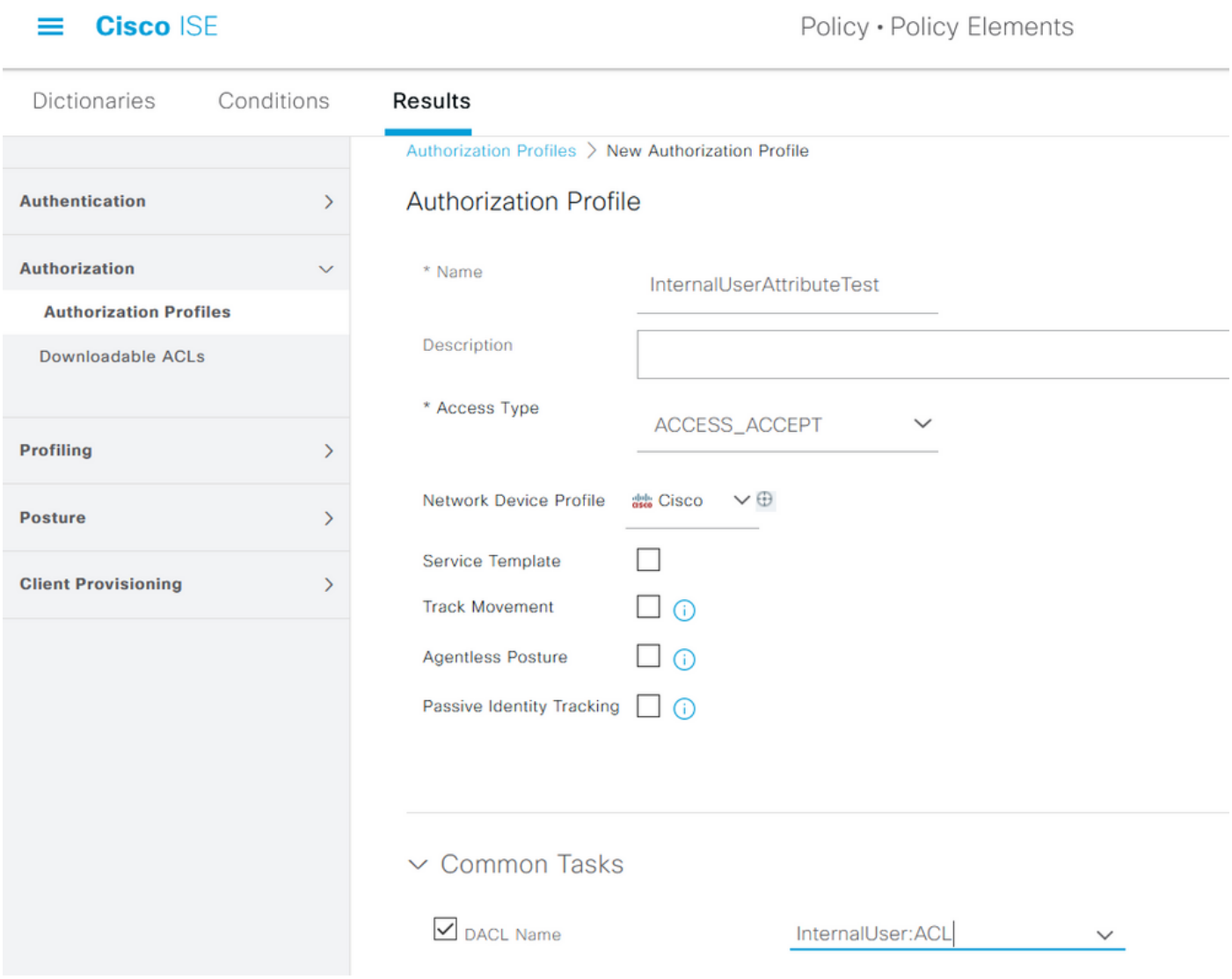




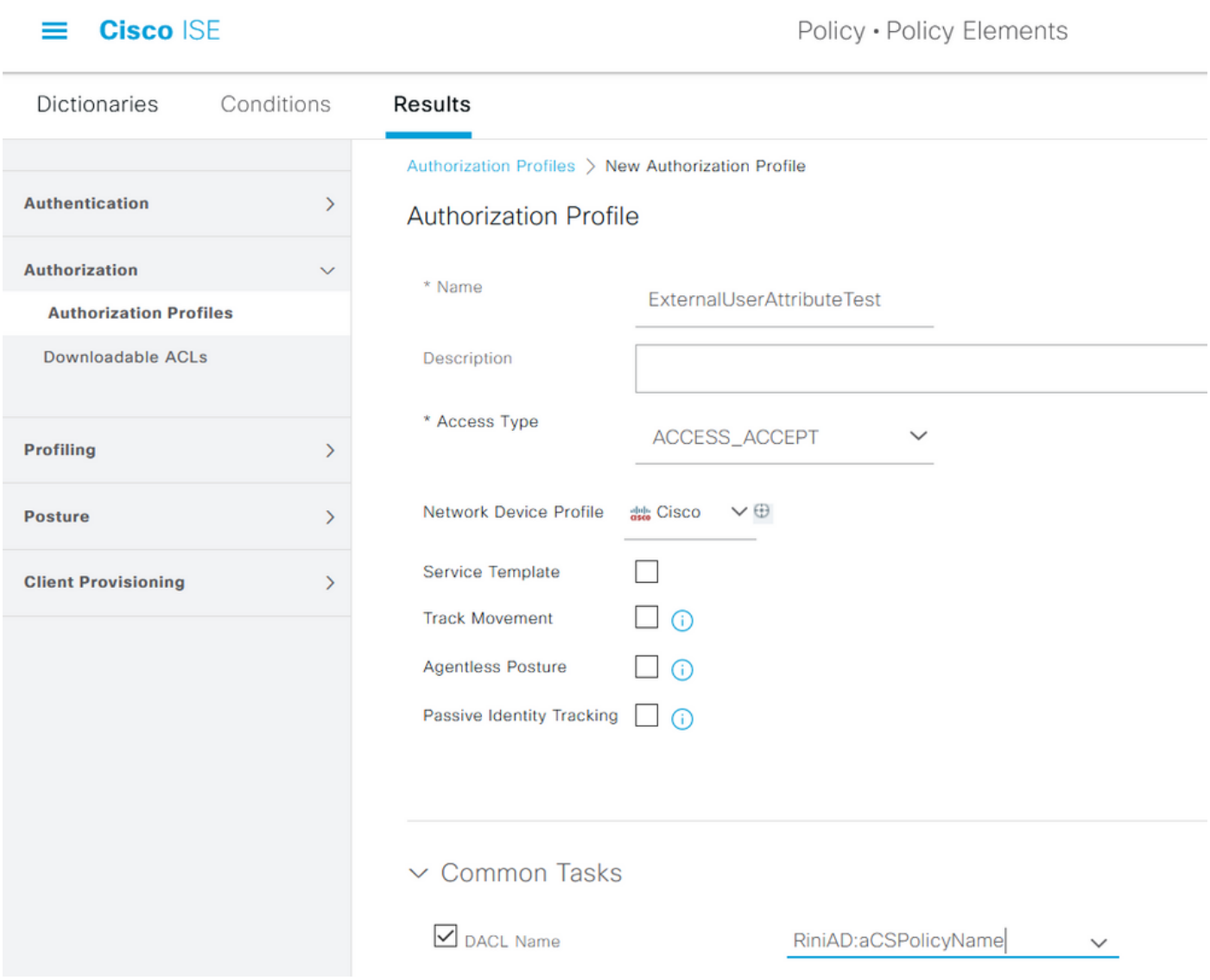
Configurar perfiles de autorización para usuarios internos y externos

Para configurar los perfiles de autorización, navegue hasta Policy > Policy Elements > Results > Authorization > Authorization Profiles. Haga clic en Add (Agregar). Proporcione un nombre y elija el nombre dACL como InternalUser:<name of custom attribute created> para el usuario interno.

Como se muestra en la imagen, para el usuario interno, el perfil InternalUserAttributeTest se configura con el dACL configurado como InternalUser:ACL.

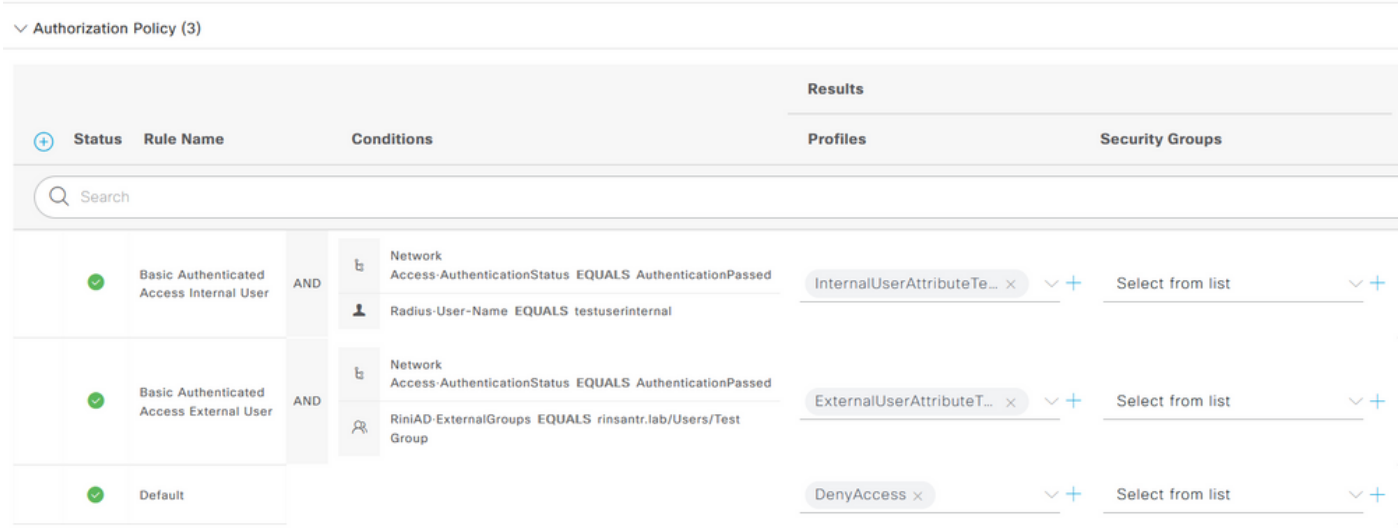


Para el usuario externo, utilice <Join point name>:<attribute configured on AD> como el nombre dACL. En este ejemplo, el perfil ExternalUserAttributeTest se configura con la dACL configurada como RiniAD:aCSPolicyName, donde RiniAD es el nombre del punto de unión.



Configurar directivas de autorización

Las políticas de autorización se pueden configurar en Policy > Policy Sets en función de los grupos en los que el usuario externo está presente en AD y también en función del nombre de usuario en el almacén de identidad interna de ISE. En este ejemplo, testuserexternal es un usuario presente en el grupo rinsantr.lab/Users/Test Group y testuserinternal es un usuario presente en el almacén de identidades internas de ISE.

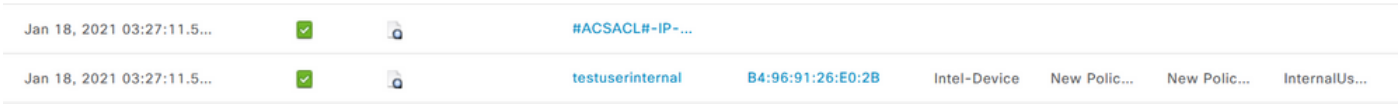


Verificación

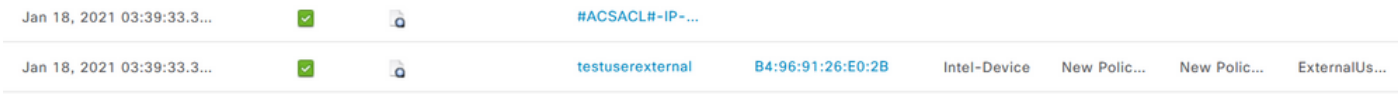
Utilice esta sección para verificar si la configuración funciona.

Verifique los registros en vivo de RADIUS para verificar las autenticaciones de usuario.

Usuario interno:



Usuario externo:



Haga clic en el icono de lupa de las autenticaciones de usuario correctas para verificar si las solicitudes cumplen las políticas correctas en la sección Descripción general de los registros en directo detallados.

Usuario 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

Usuario 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 la sección Otros Atributos de los logs en vivo detallados para verificar si los atributos de usuario han sido recuperados.

Usuario interno:

EnableFlag	Enabled
ACL	NotMuchAccess
RADIUS Username	testuserinternal

Usuario externo:

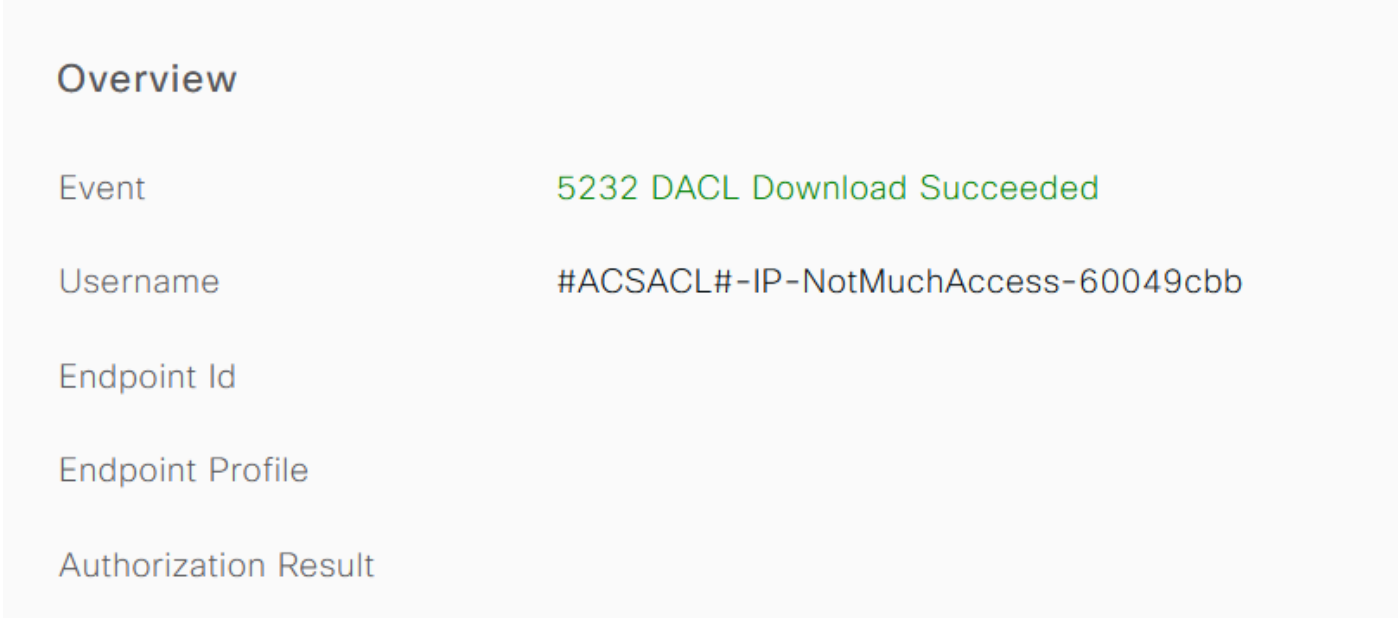
aCSPolicyName	NotMuchAccess
RADIUS Username	testuserexternal

Verifique la sección Resultado de los registros en vivo detallados para verificar si el atributo dACL se envía como parte de Access-Accept.

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

Además, verifique los registros en vivo de RADIUS para verificar si la dACL se descarga después de la autenticación del usuario.

Haga clic en el icono de lupa en el registro de descarga de dACL exitosa y verifique la sección Descripción General para confirmar la descarga de dACL.



Consulte la sección Resultado de este informe detallado para verificar el contenido de la dACL.

Troubleshoot

Actualmente no hay información específica disponible para resolver problemas de esta configuración.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).