在ISE中配置每用户动态访问控制列表

目录

简介

本文档介绍如何为身份存储类型中的用户配置每用户动态访问控制列表(dACL)。

先决条件

要求

思科建议您了解身份服务引擎(ISE)上的策略配置。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 身份服务引擎3.0
- Microsoft Windows Active Directory 2016

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

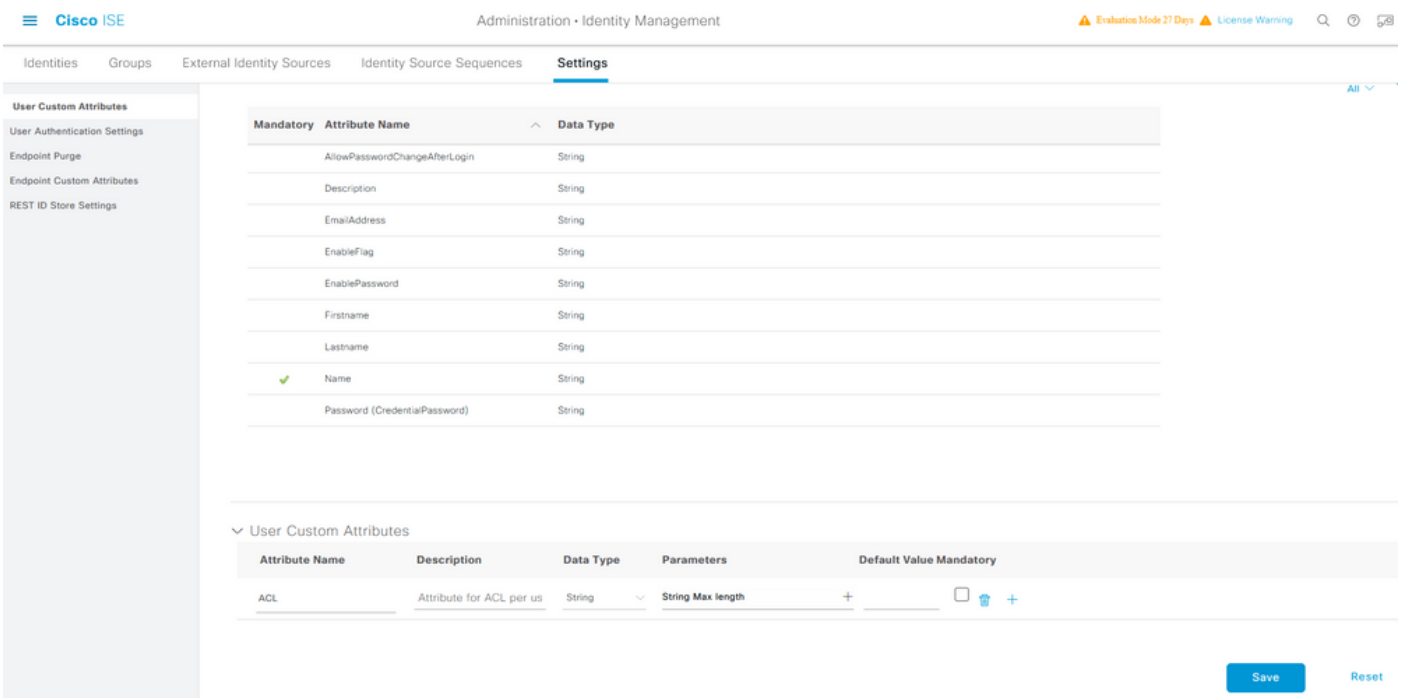
每用户动态访问控制列表的配置适用于ISE内部身份库或外部身份库中的用户。

配置

可为使用自定义用户属性的内部存储中的任何用户配置每用户dACL。对于Active Directory(AD)中的用户，可以使用任何类型字符串的属性来实现相同目的。本部分提供在ISE和AD上配置属性所需的信息以及ISE上使用此功能所需的配置。

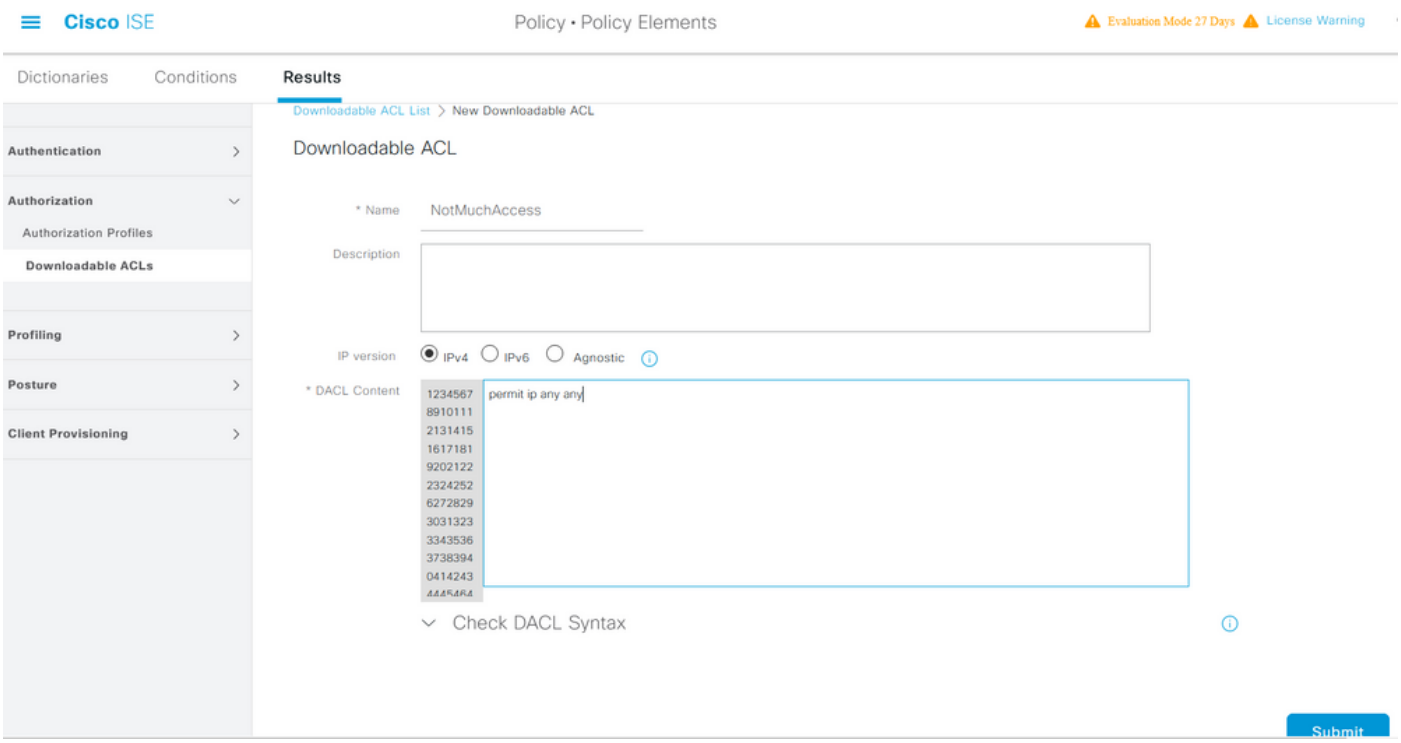
在ISE上配置新的自定义用户属性

导航到管理>身份管理>设置>用户自定义属性。单击+按钮（如图所示），添加新的属性并保存更改。在本示例中，自定义属性的名称为ACL。



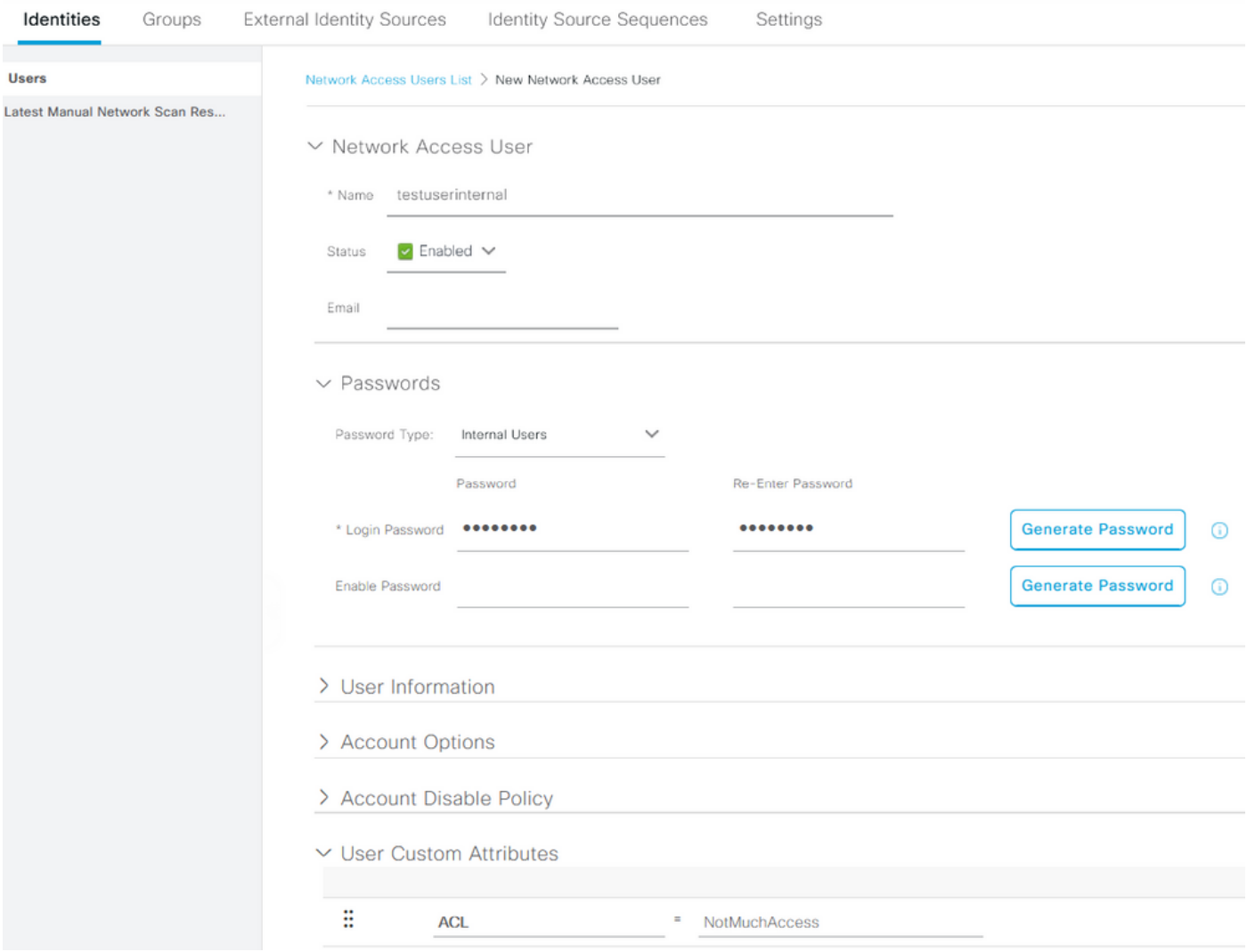
配置dACL

要配置可下载ACL，请导航到Policy > Policy Elements > Results > Authorization > Downloadable ACLs。单击 Add。提供dACL的名称、内容并保存更改。如图所示，dACL的名称为NotManyAccess。



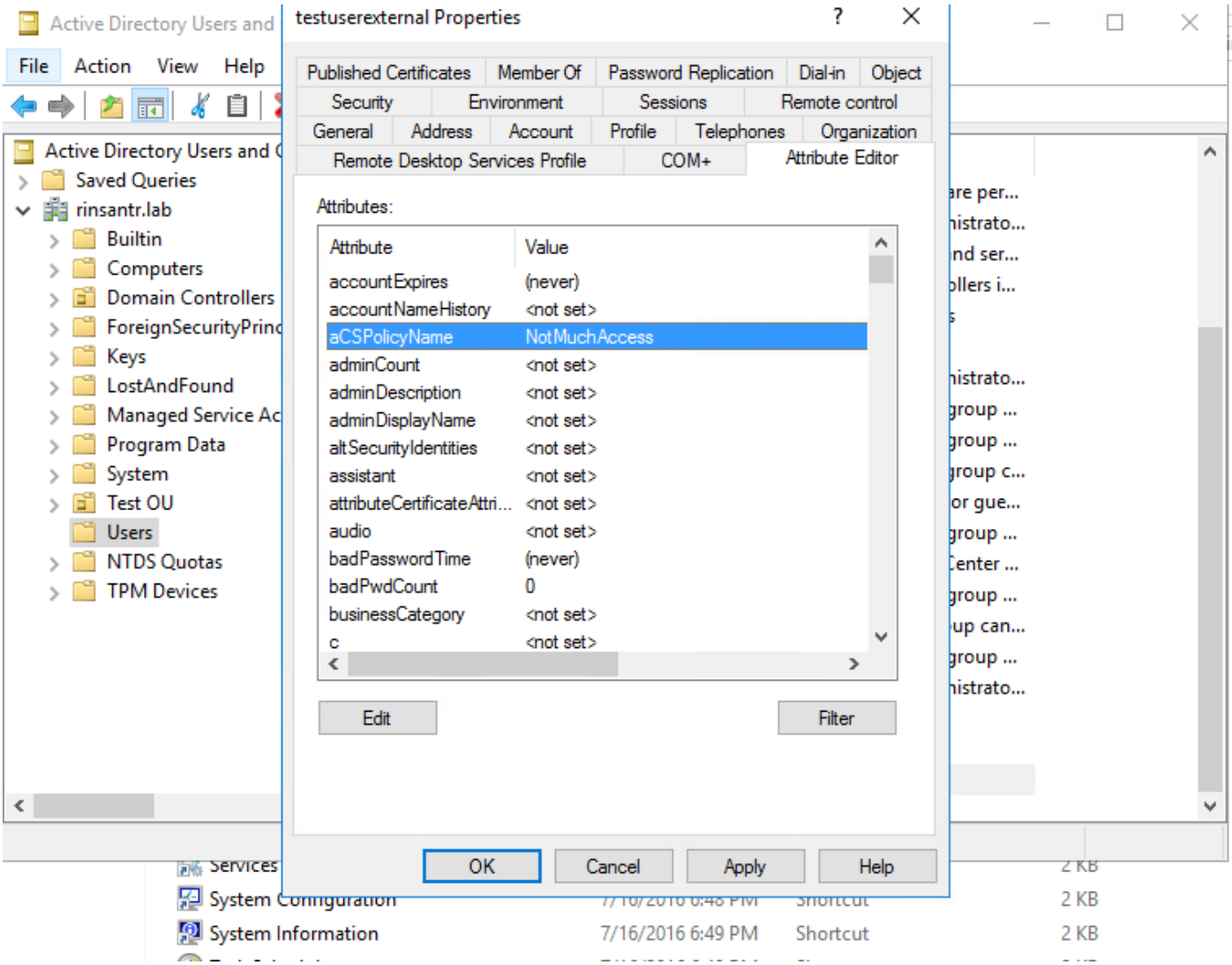
使用自定义属性配置内部用户帐户

导航到管理>身份管理>身份>用户>添加。创建用户并使用用户获得授权时需要获取的dACL名称配置自定义属性值。在本示例中，dACL的名称为NotMuchAccess。



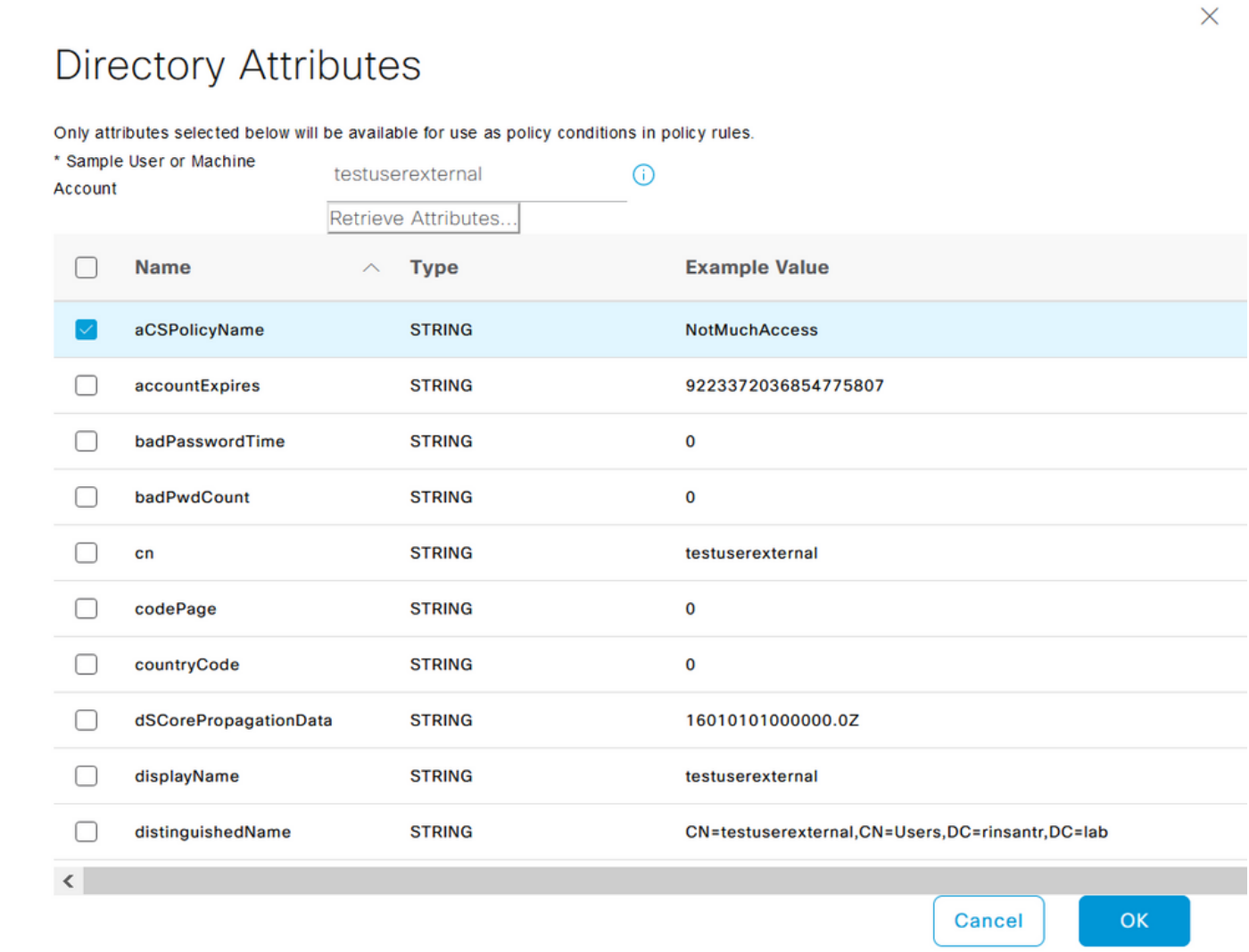
配置AD用户帐户

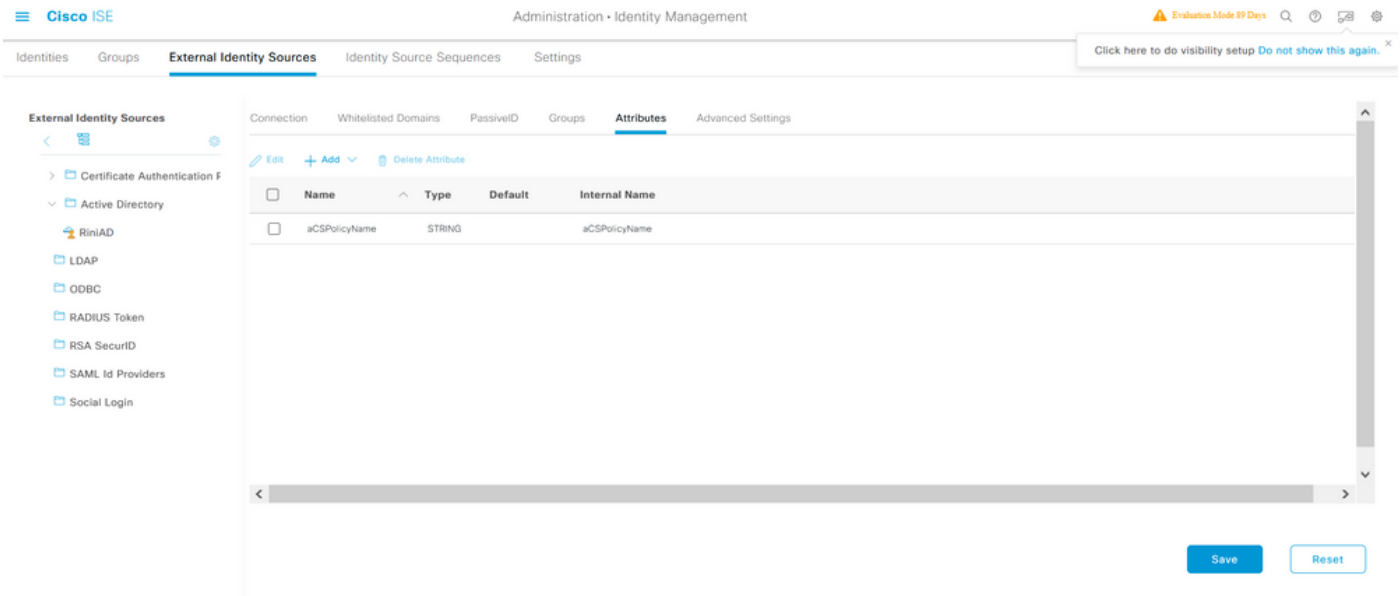
在Active Directory上，导航到用户帐户属性，然后导航到属性编辑器选项卡。如图所示，aCSPolicyName是用于指定dACL名称的属性。但是，如前所述，也可以使用任何可以接受字符串值的属性。



将属性从AD导入ISE

要使用在AD上配置的属性，ISE需要导入它。要导入属性，请导航到管理>身份管理>外部身份源> Active Directory > [配置的加入点] >属性选项卡。单击Add，然后单击Select Attributes from Directory。 在AD上提供用户帐户名称，然后点击检索属性。 选择为dACL配置的属性，单击OK，然后单击Save。如图所示，aCSPolicyName是属性。

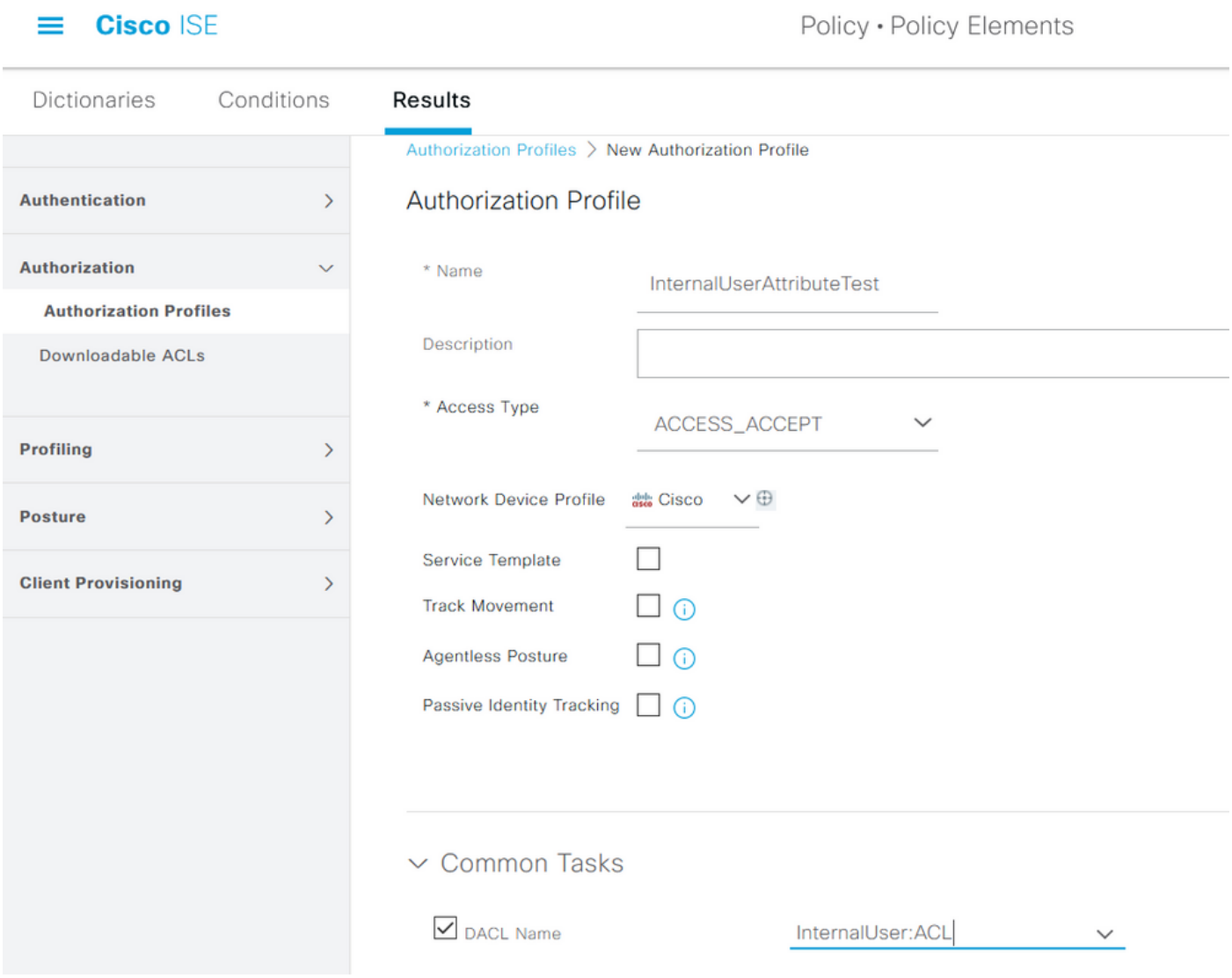




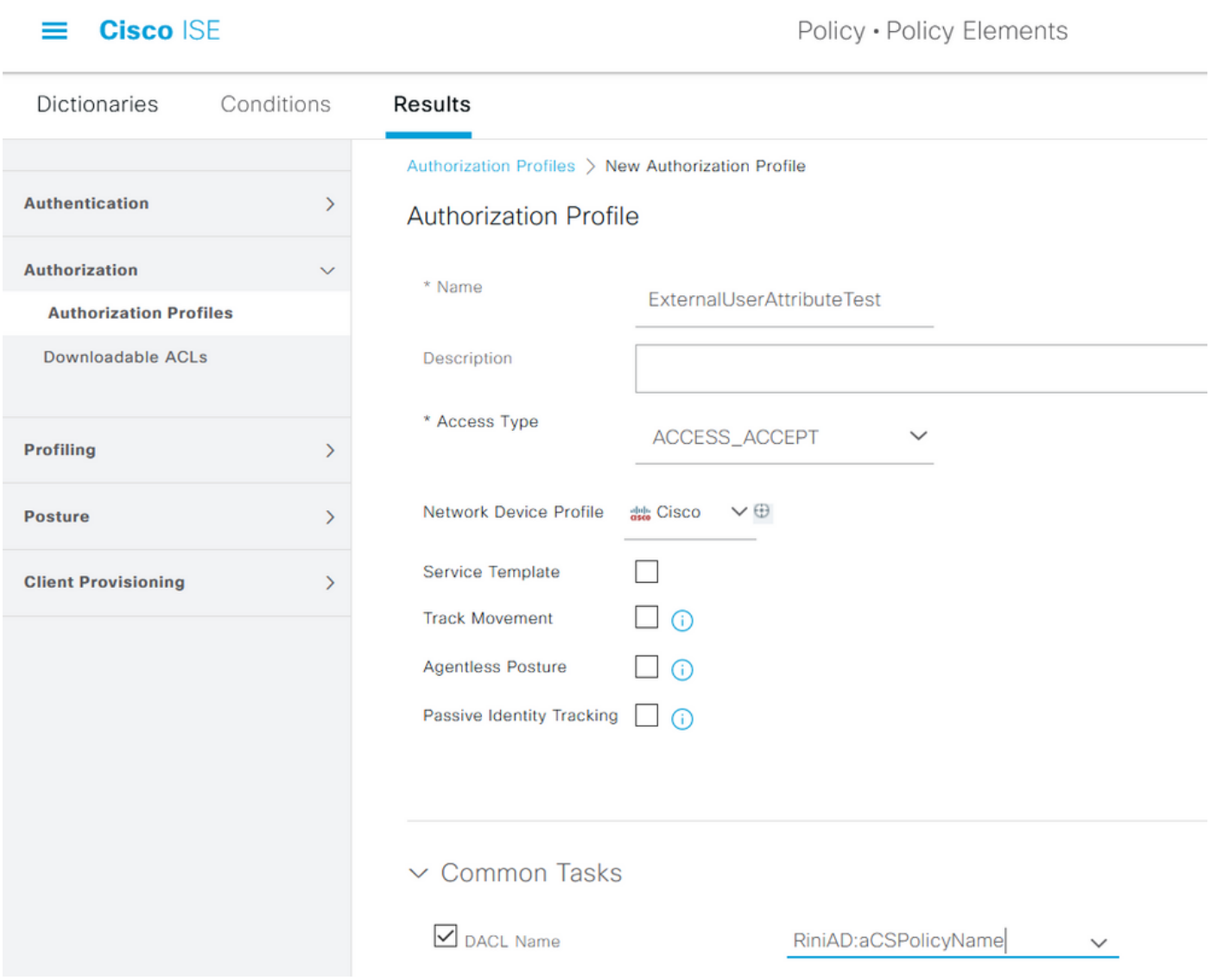
为内部和外部用户配置授权配置文件

要配置授权配置文件，请导航到Policy > Policy Elements > Results > Authorization > Authorization Profiles。单击 Add。提供名称，并为内部用户选择dACL名称InternalUser:<name of custom attribute created>。如图所示，对于内部用户，配置文件InternalUserAttributeTest使用配置为

InternalUser:ACL的dACL进行配置。

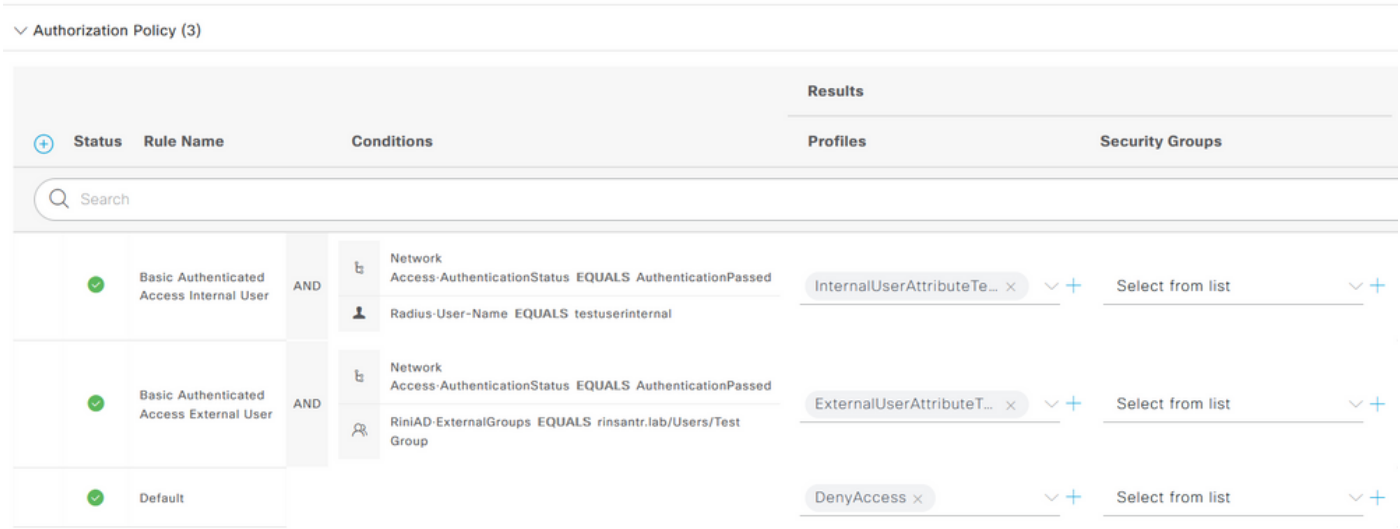


对于外部用户，请使用<Join point name>:<attribute configured on AD> 作为dACL名称。在本示例中，配置文件ExternalUserAttributeTest使用配置为RiniAD:aCSPolicyName的dACL进行配置，其中RiniAD是加入点名称。



配置授权策略

授权策略可以在Policy > Policy Sets中配置，具体取决于外部用户在AD上所处的组，也基于ISE内部身份库中的用户名。在本示例中，testuserexternal是组rinsantr.lab/Users/Test Group中的用户，而testuserinternal是ISE内部身份存储库中的用户。

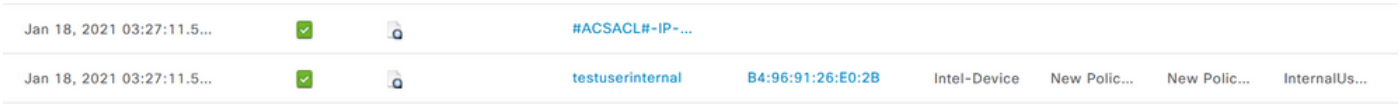


验证

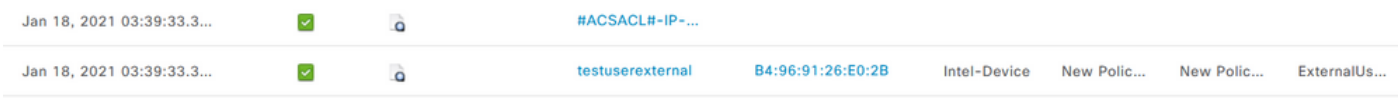
使用此部分验证配置是否有效。

检查RADIUS实时日志以验证用户身份验证。

内部用户:

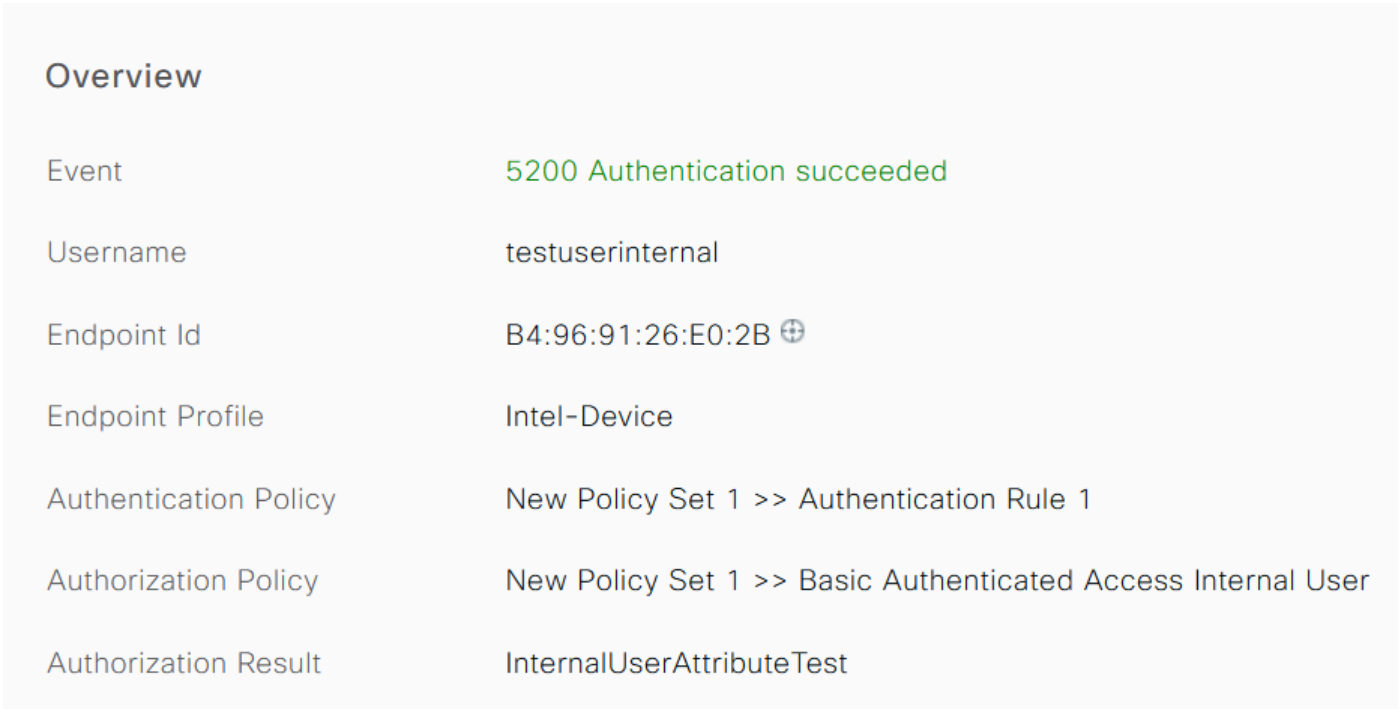


外部用户:



点击成功用户身份验证上的放大镜图标，以验证请求是否满足详细实时日志的Overview部分中的正确策略。

内部用户:



外部用户:

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

检查详细实时日志的其他属性部分，验证是否已检索到用户属性。

内部用户:

EnableFlag	Enabled
ACL	NotMuchAccess
RADIUS Username	testuserinternal

外部用户:

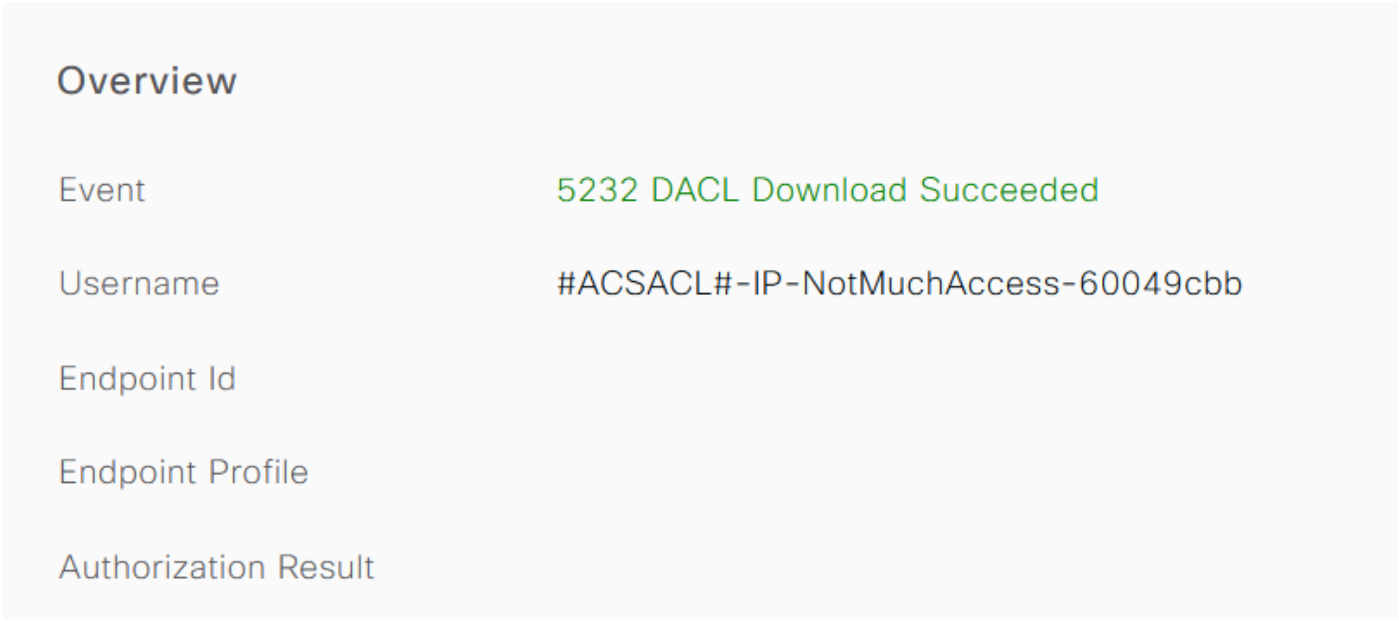
aCSPolicyName	NotMuchAccess
RADIUS Username	testuserexternal

检查详细实时日志的结果部分，以验证dACL属性是否作为Access-Accept的一部分发送。

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

此外，检查RADIUS实时日志以验证是否在用户身份验证后下载dACL。

点击成功的dACL下载日志上的放大镜图标，并验证Overview部分以确认dACL下载。



检查此详细报告的结果部分以验证dACL的内容。

故障排除

当前没有故障排除此配置的特定可用资料。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。