在ISE中配置每使用者動態訪問控制清單

目錄

簡介

本檔案將說明在身份儲存庫型別中存在的使用者的每使用者動態訪問控制清單(dACL)的配置。

必要條件

需求

思科建議您瞭解身份服務引擎(ISE)上的策略配置。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 身分識別服務引擎3.0
- Microsoft Windows Active Directory 2016

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

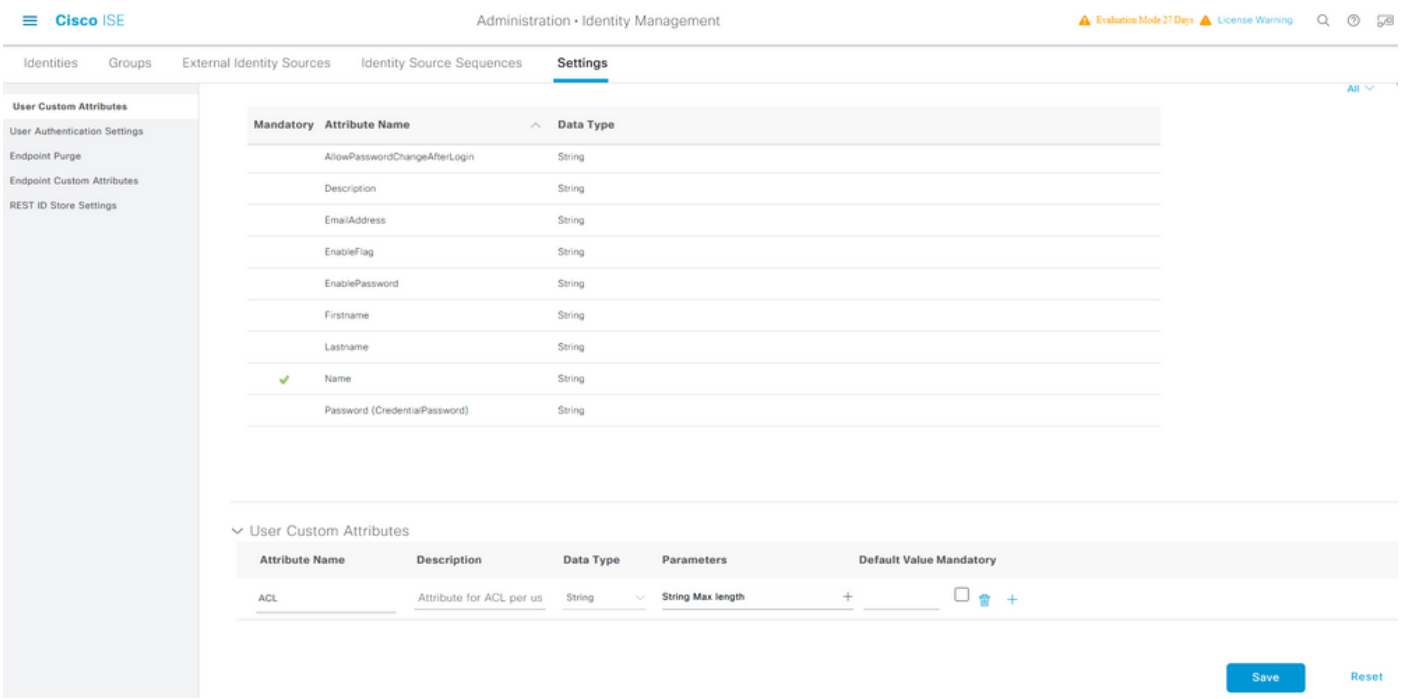
每個使用者的動態訪問控制清單的配置適用於ISE內部身份儲存或外部身份儲存中的使用者。

設定

可為內部儲存中使用自定義使用者屬性的任何使用者配置每使用者dACL。對於Active Directory(AD)中的使用者，可以使用字串型別的任何屬性來實現相同目的。本節提供在ISE和AD上配置屬性所需的資訊以及此功能在ISE上運行所需的配置。

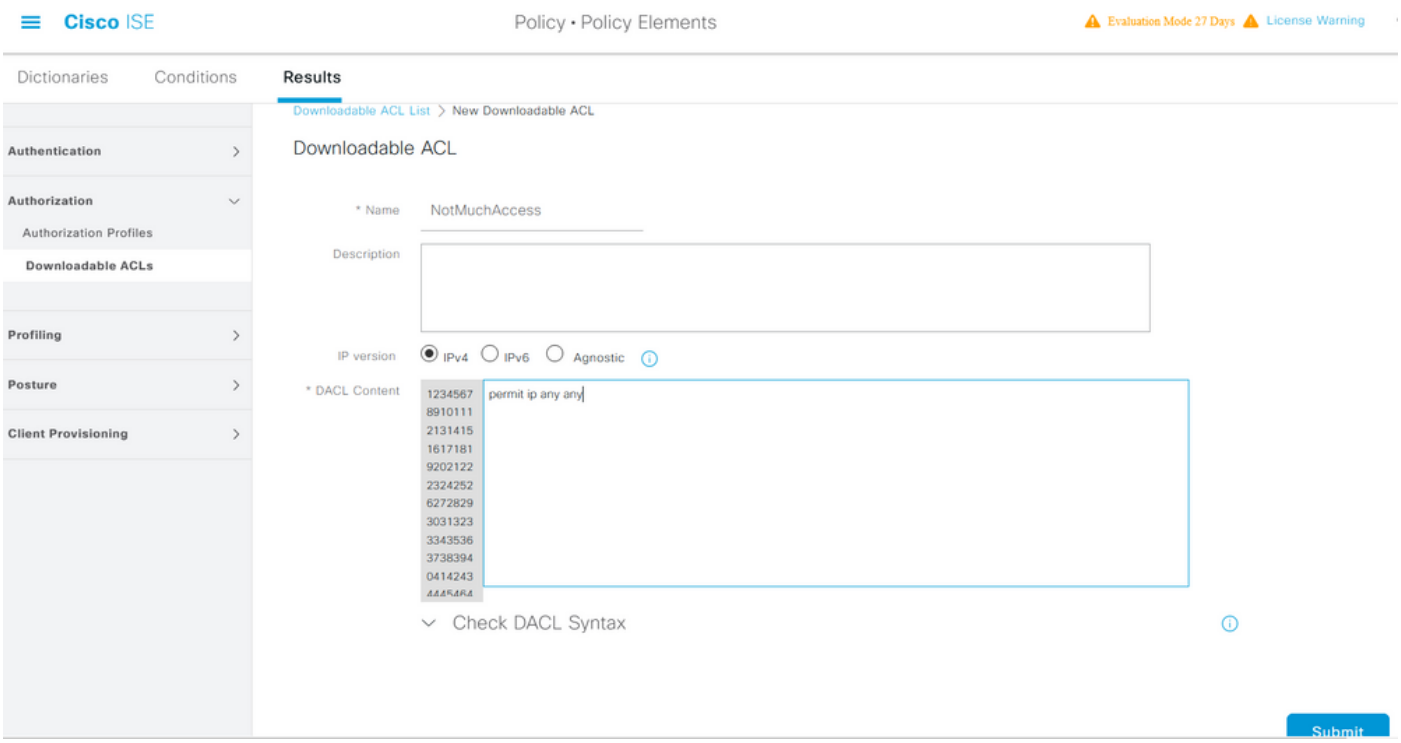
在ISE上配置新的自定義使用者屬性

導航到管理>身份管理>設定>使用者自定義屬性。按一下+按鈕（如圖所示），新增屬性並儲存變更。在本例中，自定義屬性的名稱為ACL。



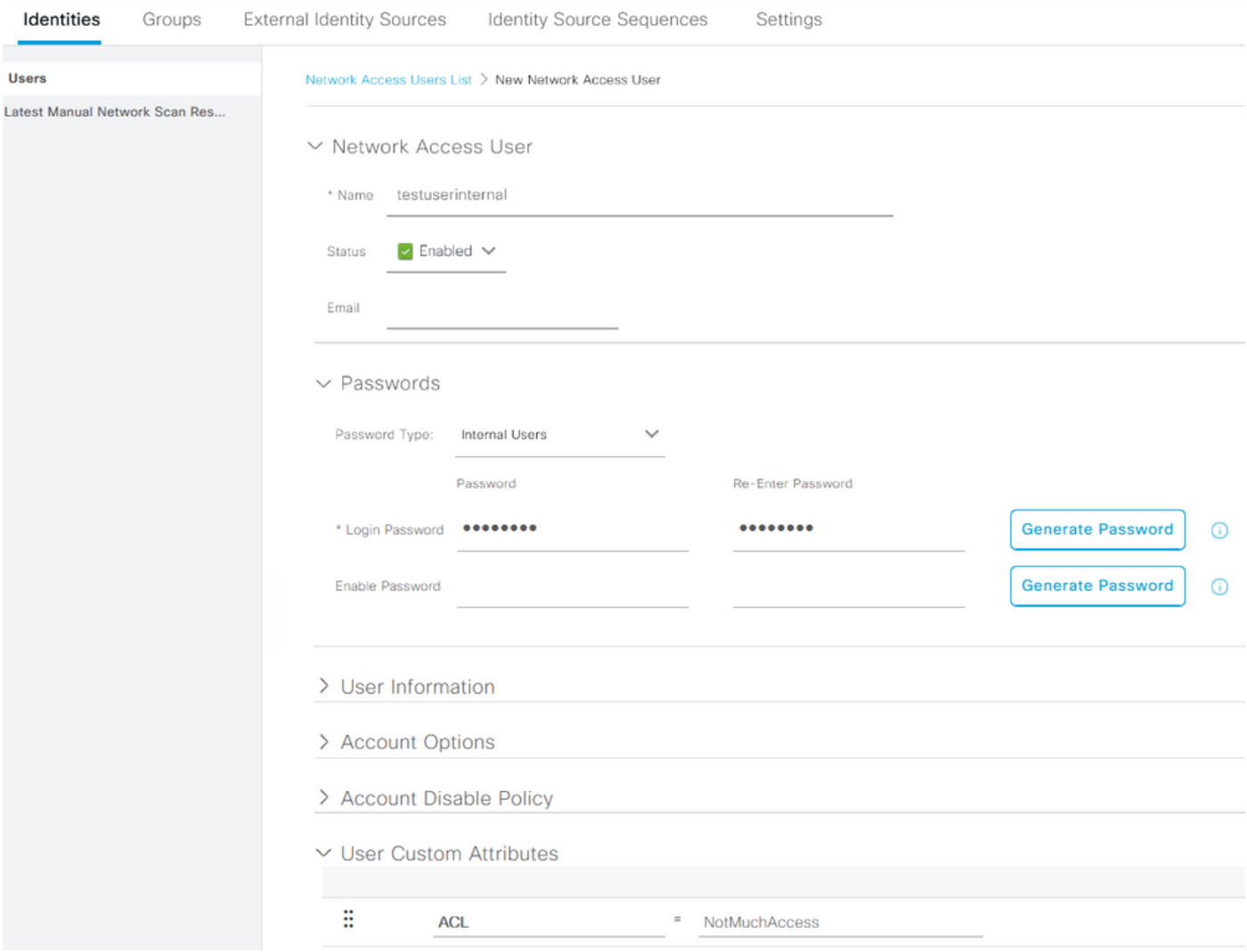
配置dACL

若要設定可下載ACL，請導覽至Policy > Policy Elements > Results > Authorization > Downloadable ACLs。按一下「Add」。提供dACL的名稱、內容並保存更改。如圖所示，dACL的名稱不是ManyAccess。



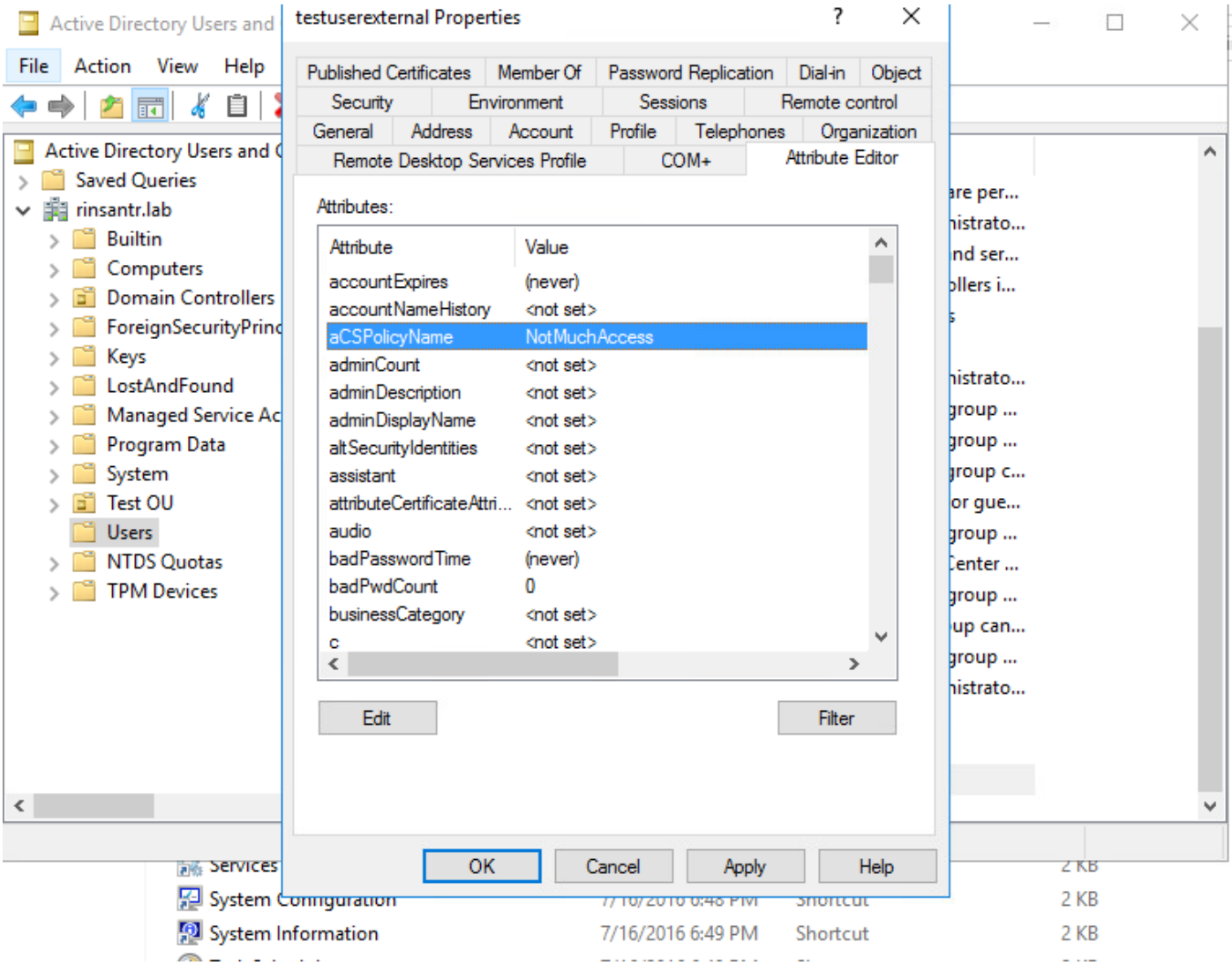
使用自定義屬性配置內部使用者帳戶

導航到Administration > Identity Management > Identities > Users > Add。建立使用者並使用使用者獲得授權時需要獲取的dACL名稱配置自定義屬性值。在本例中， dACL的名稱為NotMuchAccess。



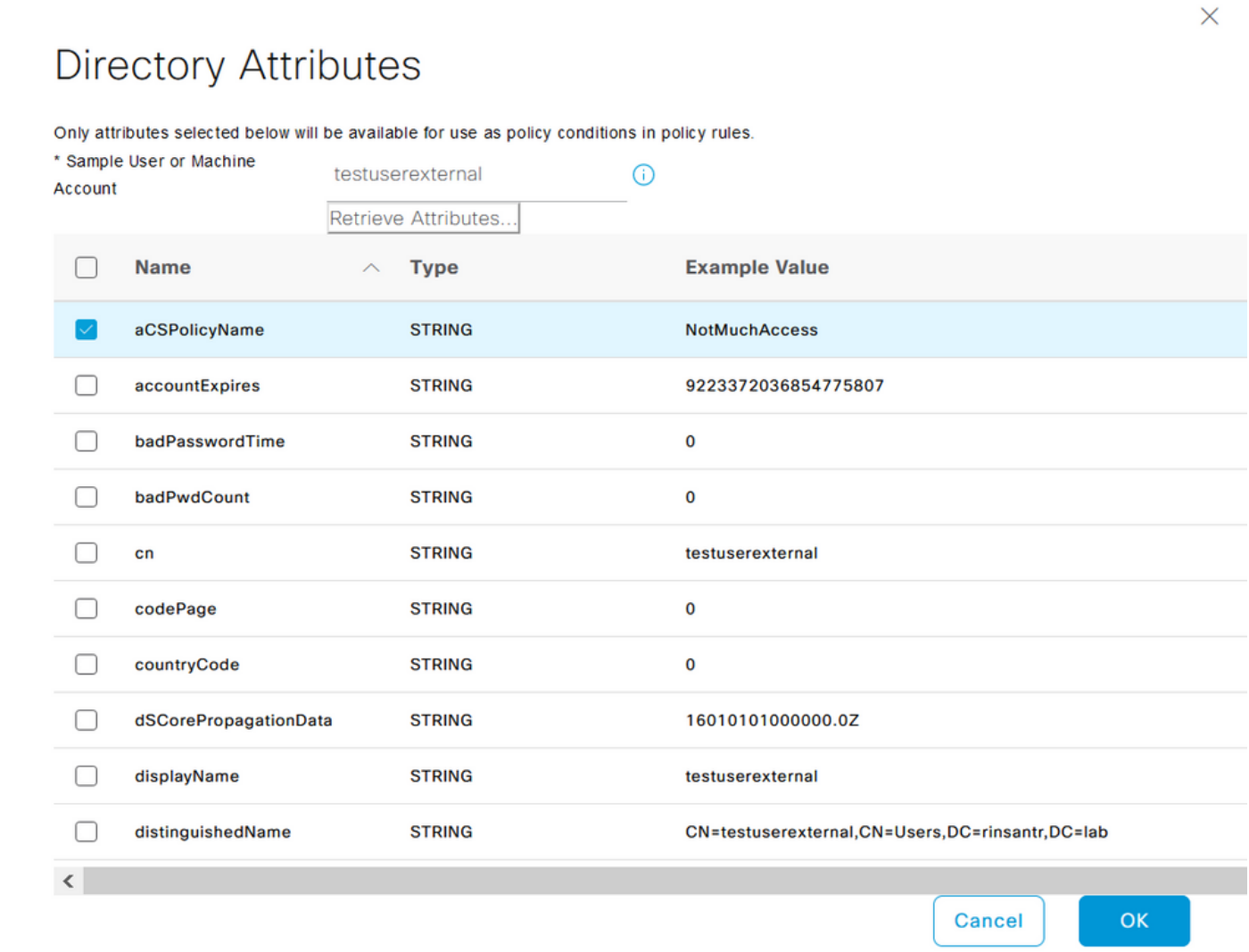
配置AD使用者帳戶

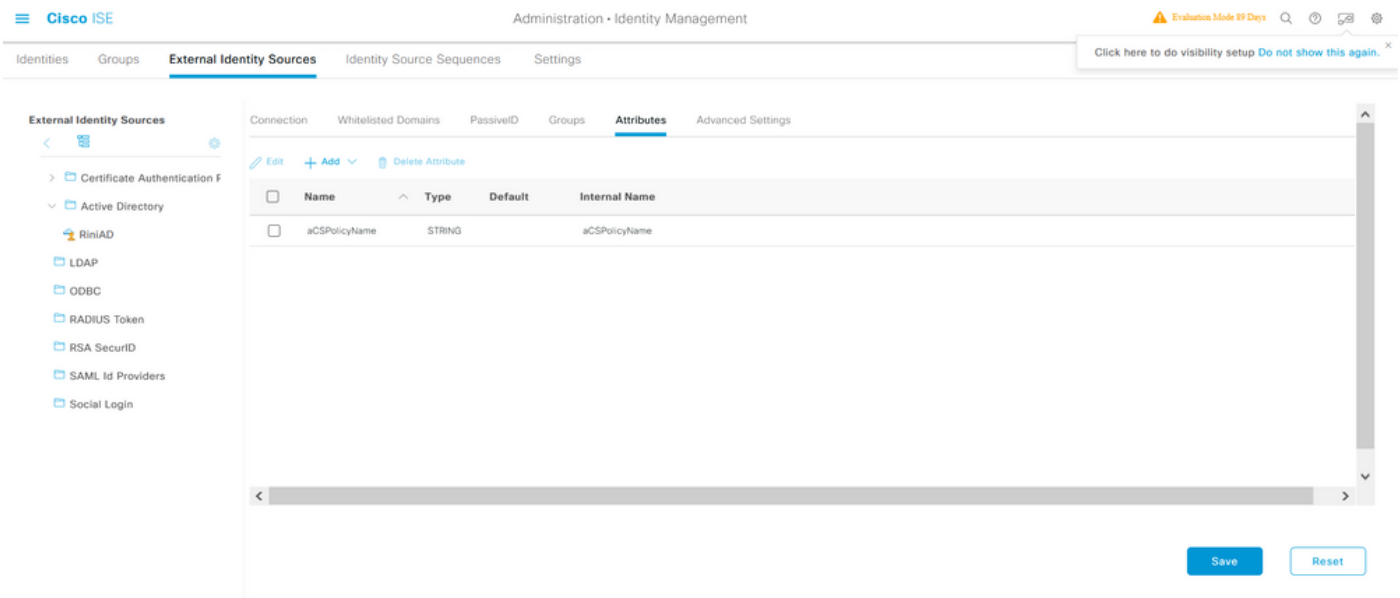
在Active Directory上，導航到使用者帳戶屬性，然後導航到屬性編輯器頁籤。如圖所示，aCSPolicyName是用於指定dACL名稱的屬性。但是，如前所述，也可以使用任何可以接受字串值的屬性。



將屬性從AD匯入ISE

要使用在AD上配置的屬性，ISE需要匯入該屬性。要匯入屬性，請導航到管理>身份管理>外部身份源> Active Directory > [配置的加入點] >屬性頁籤。按一下Add，然後按一下Select Attributes From Directory。 在AD上提供使用者帳戶名稱，然後按一下Retrieve Attributes。 選擇為dACL配置的屬性，按一下OK，然後按一下Save。如圖所示，aCSPolicyName是屬性。

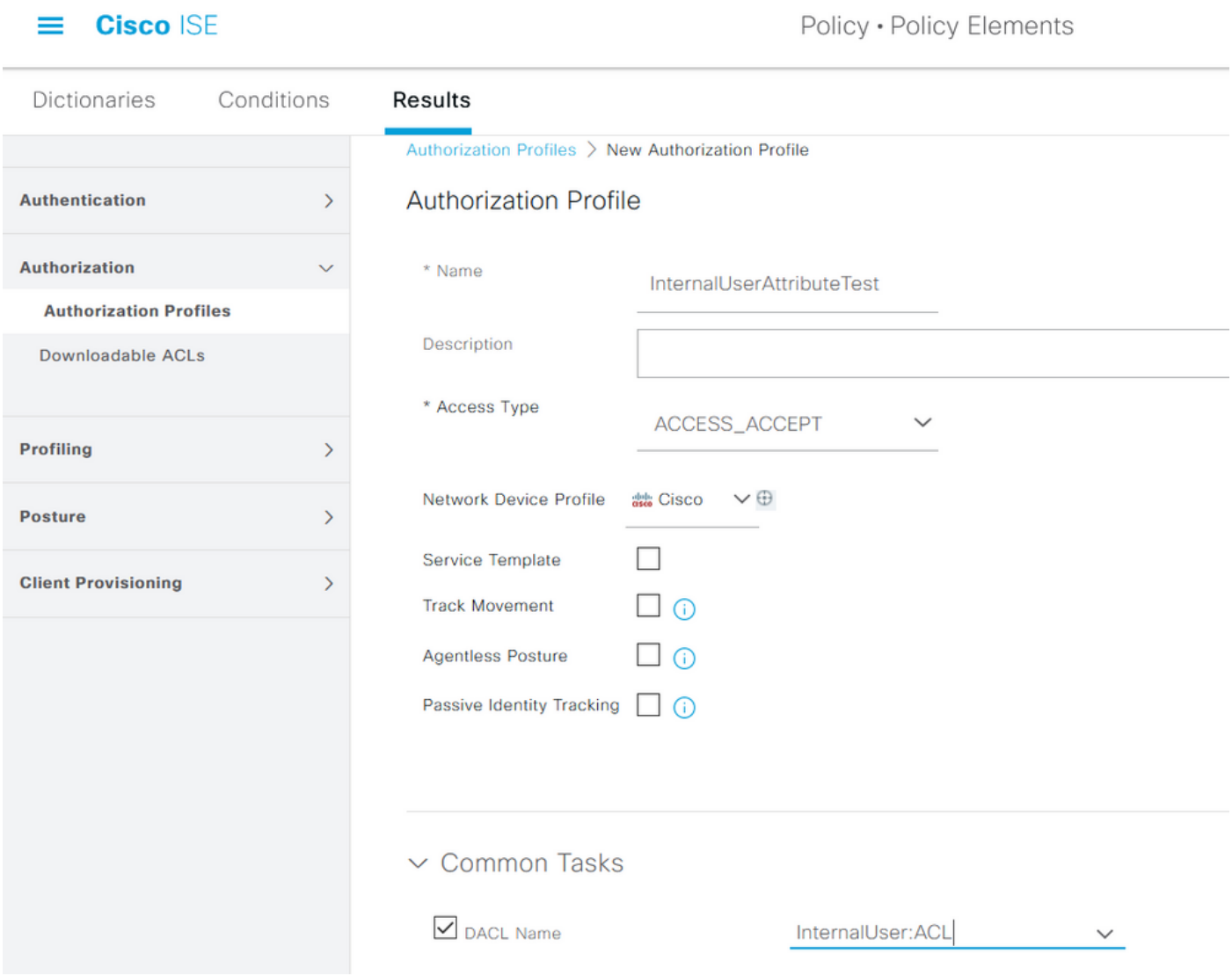




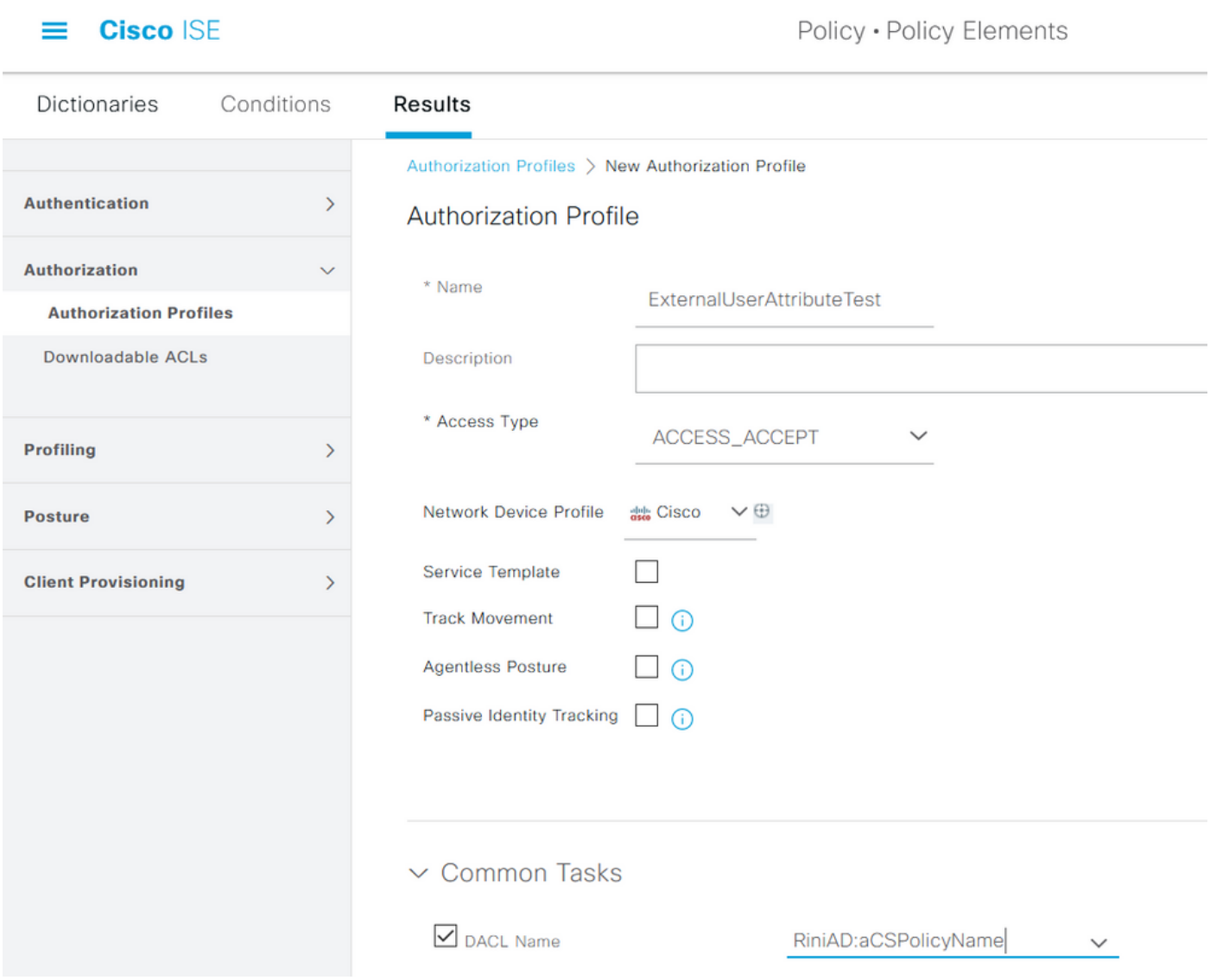
為內部和外部使用者配置授權配置檔案

要配置授權配置檔案，請導航到Policy > Policy Elements > Results > Authorization > Authorization Profiles。按一下「Add」。提供名稱，並為內部使用者選擇dACL名稱作為InternalUser:<name of custom attribute created>。如圖所示，對於內部使用者，配置檔案InternalUserAttributeTest已配置

有dACL，其配置為InternalUser:ACL。

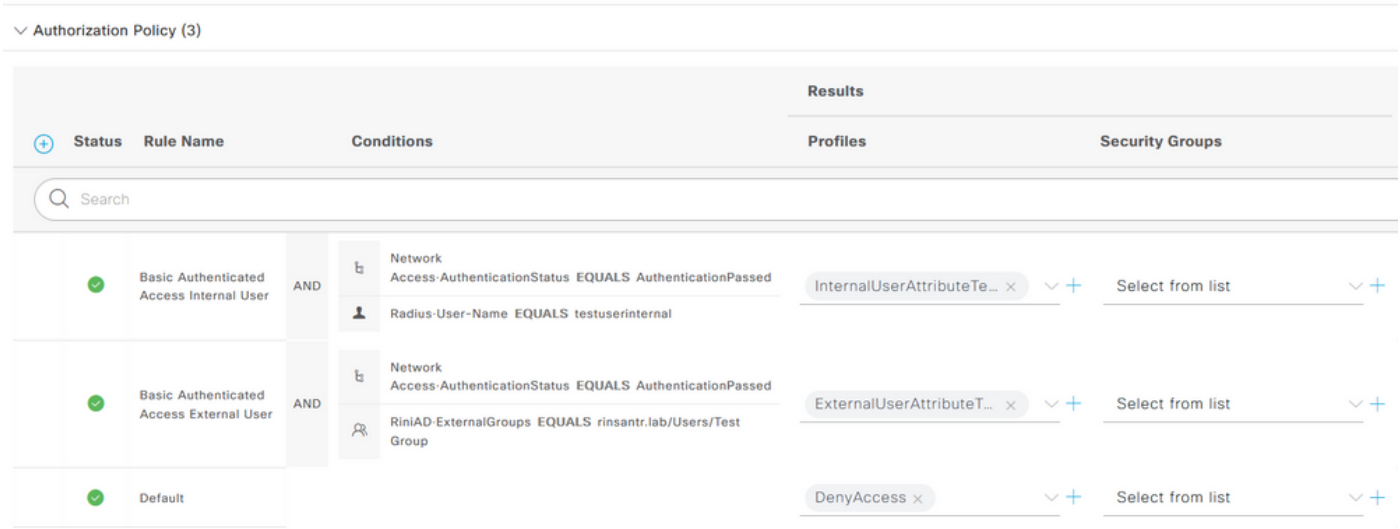


對於外部使用者，請使用<Join point name>:<attribute configured on AD>作為dACL名稱。在本示例中，使用配置為RiniAD:aCSPolicyName（其中RiniAD是連線點名稱）的dACL配置配置檔案ExternalUserAttributeTest。



配置授權策略

授權策略可以在Policy > Policy Sets中根據外部使用者在AD上存在的組以及ISE內部身份庫中的使用者名稱進行配置。在本示例中，testuserexternal是組rinsantr.lab/Users/Test Group中的使用者，而testuserinternal是ISE內部身份儲存庫中的使用者。

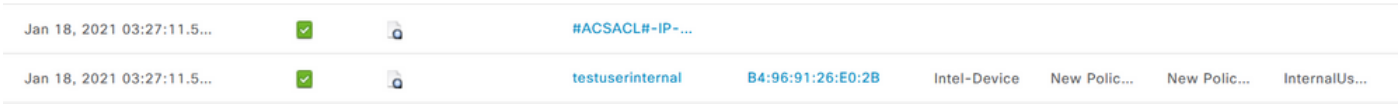


驗證

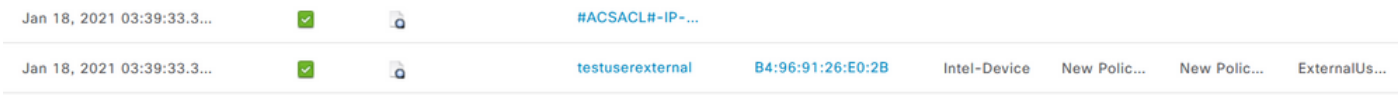
使用本節內容，驗證組態是否有效。

檢查RADIUS即時日誌以驗證使用者身份驗證。

內部使用者：

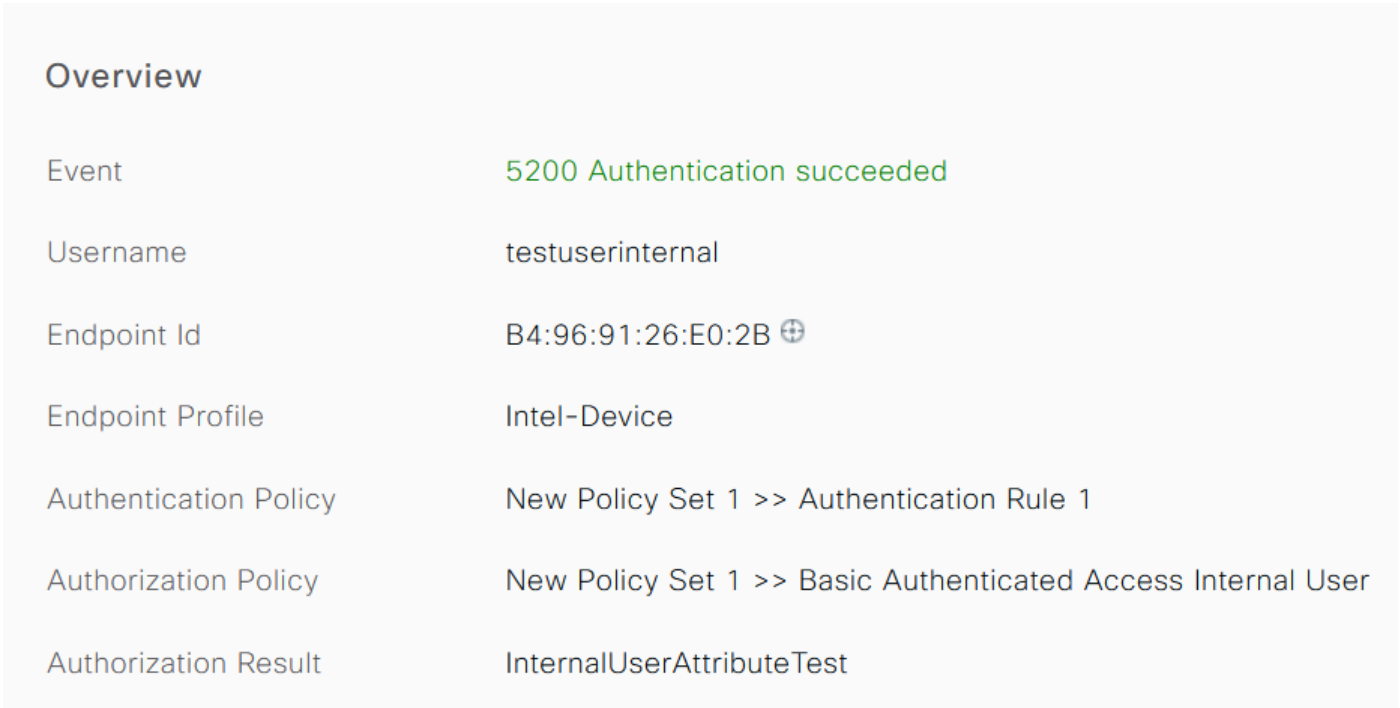


外部使用者：



在詳細即時日誌的「概述」部分中，按一下成功使用者身份驗證上的放大鏡圖示，驗證請求是否達到了正確的策略。

內部使用者：



外部使用者：

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

檢查詳細即時日誌的其他屬性部分，驗證是否已檢索到使用者屬性。

內部使用者：

EnableFlag	Enabled
ACL	NotMuchAccess
RADIUS Username	testuserinternal

外部使用者：

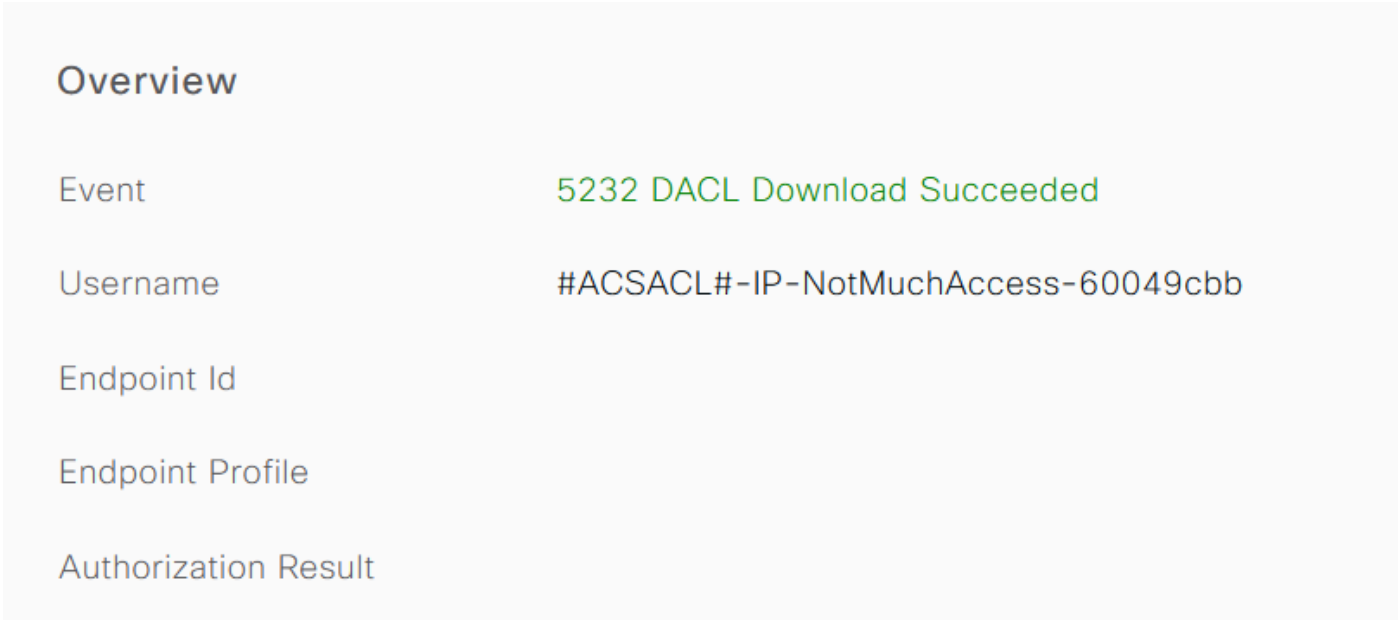
aCSPolicyName	NotMuchAccess
RADIUS Username	testuserexternal

檢查詳細即時日誌的結果部分，以驗證dACL屬性是否作為Access-Accept的一部分傳送。

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

此外，請檢查RADIUS即時日誌，以驗證在使用者驗證之後是否下載了dACL。

按一下成功的dACL下載日誌上的放大鏡圖示，並驗證「概述」部分以確認dACL下載。



檢查此詳細報告的結果部分以驗證dACL的內容。

疑難排解

目前尚無特定資訊可用於排解此組態的疑難問題。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。