Configuration des listes de contrôle d'accès dynamique par utilisateur dans ISE

Table des matières

Introduction

Ce document décrit la configuration d'une liste de contrôle d'accès dynamique (dACL) par utilisateur pour les utilisateurs présents dans un type de magasin d'identités.

Conditions préalables

Exigences

Cisco recommande que vous ayez connaissance de la configuration des stratégies sur Identity Services Engine (ISE).

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Identity Services Engine 3.0
- Microsoft Windows Active Directory 2016

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

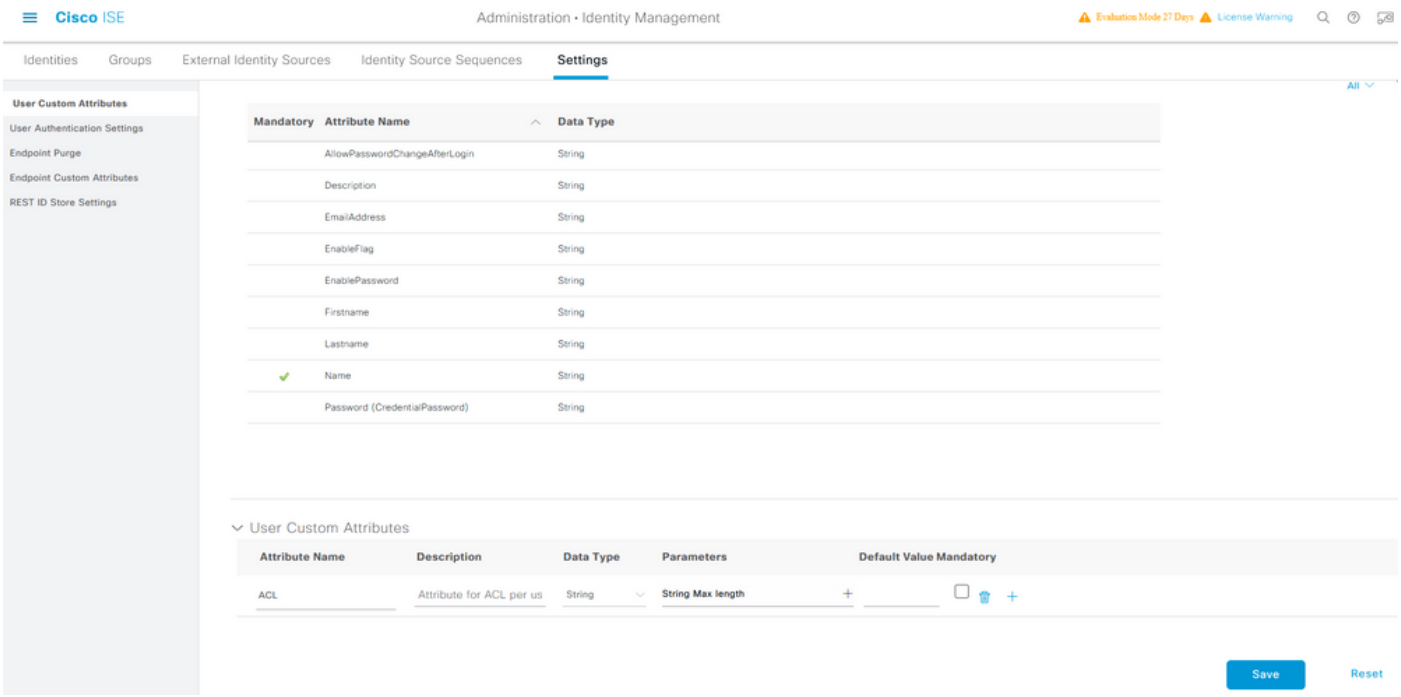
La configuration d'une liste de contrôle d'accès dynamique par utilisateur est destinée aux utilisateurs présents dans le magasin d'identité interne ISE ou dans un magasin d'identité externe.

Configurer

La dACL par utilisateur peut être configurée pour n'importe quel utilisateur du magasin interne qui utilise un attribut d'utilisateur personnalisé. Pour un utilisateur dans Active Directory (AD), n'importe quel attribut de type chaîne peut être utilisé pour obtenir le même résultat. Cette section fournit les informations requises pour configurer les attributs sur ISE et AD, ainsi que la configuration requise sur ISE pour que cette fonctionnalité fonctionne.

Configurer un nouvel attribut d'utilisateur personnalisé sur ISE

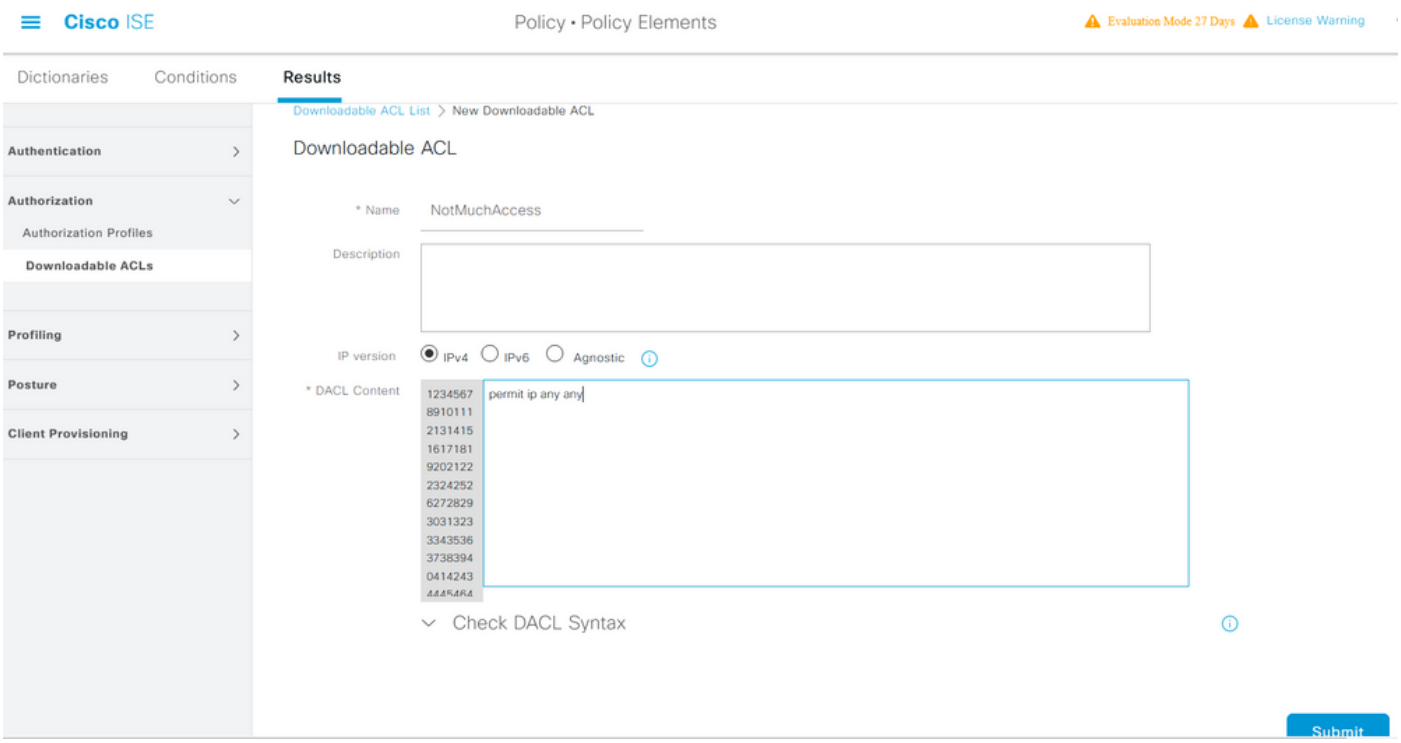
Accédez à Administration > Identity Management > Settings > User Custom Attributes. Cliquez sur le bouton +, comme illustré dans l'image, pour ajouter un nouvel attribut et enregistrer les modifications. Dans cet exemple, le nom de l'attribut personnalisé est ACL.



Configurer dACL

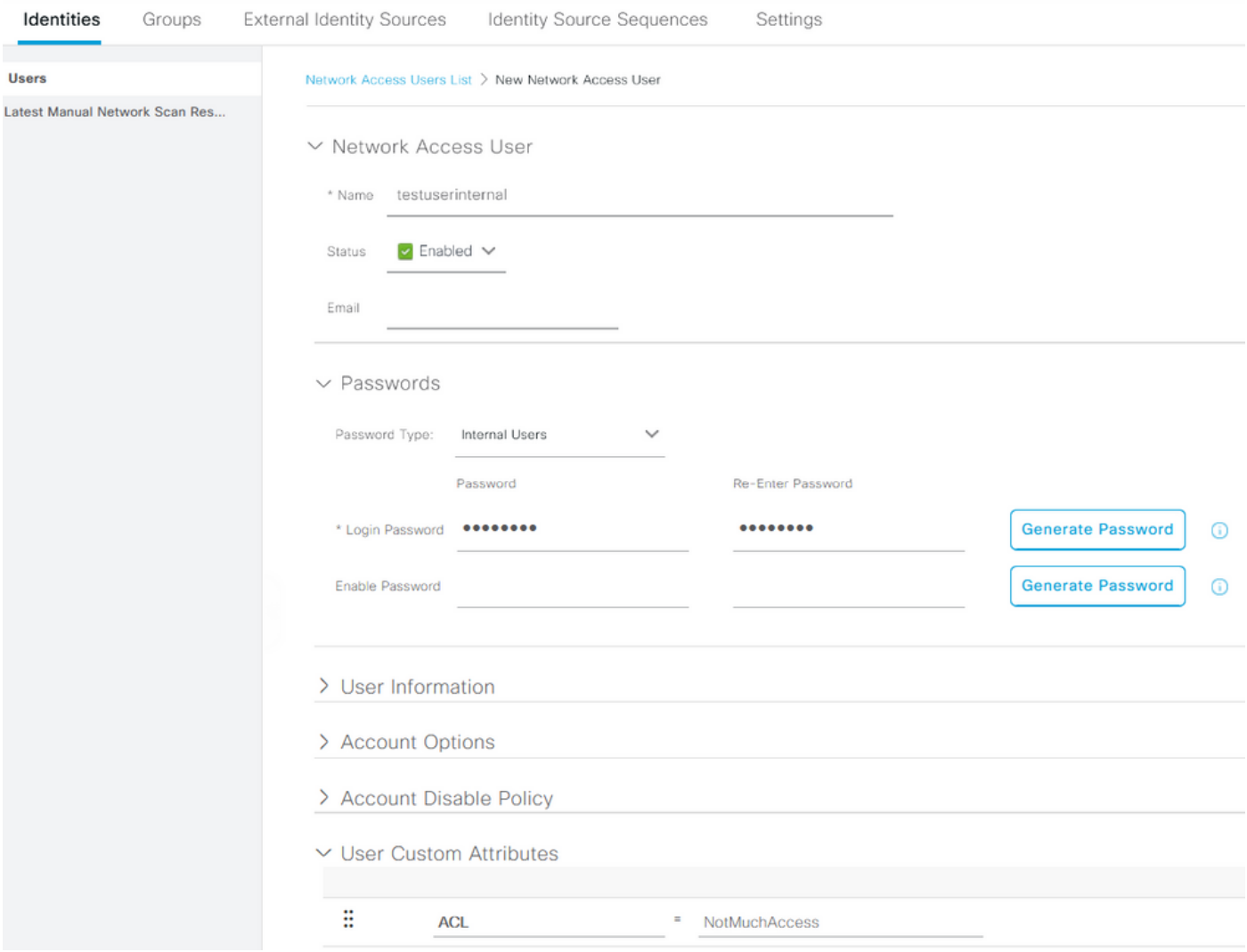
Afin de configurer les ACL téléchargeables, naviguez vers Policy > Policy Elements > Results > Authorization > Downloadable ACLs. Cliquez sur Add. Fournissez un nom et le contenu de la

dACL et enregistrez les modifications. Comme l'illustre l'image, le nom de la dACL est NotMuchAccess.



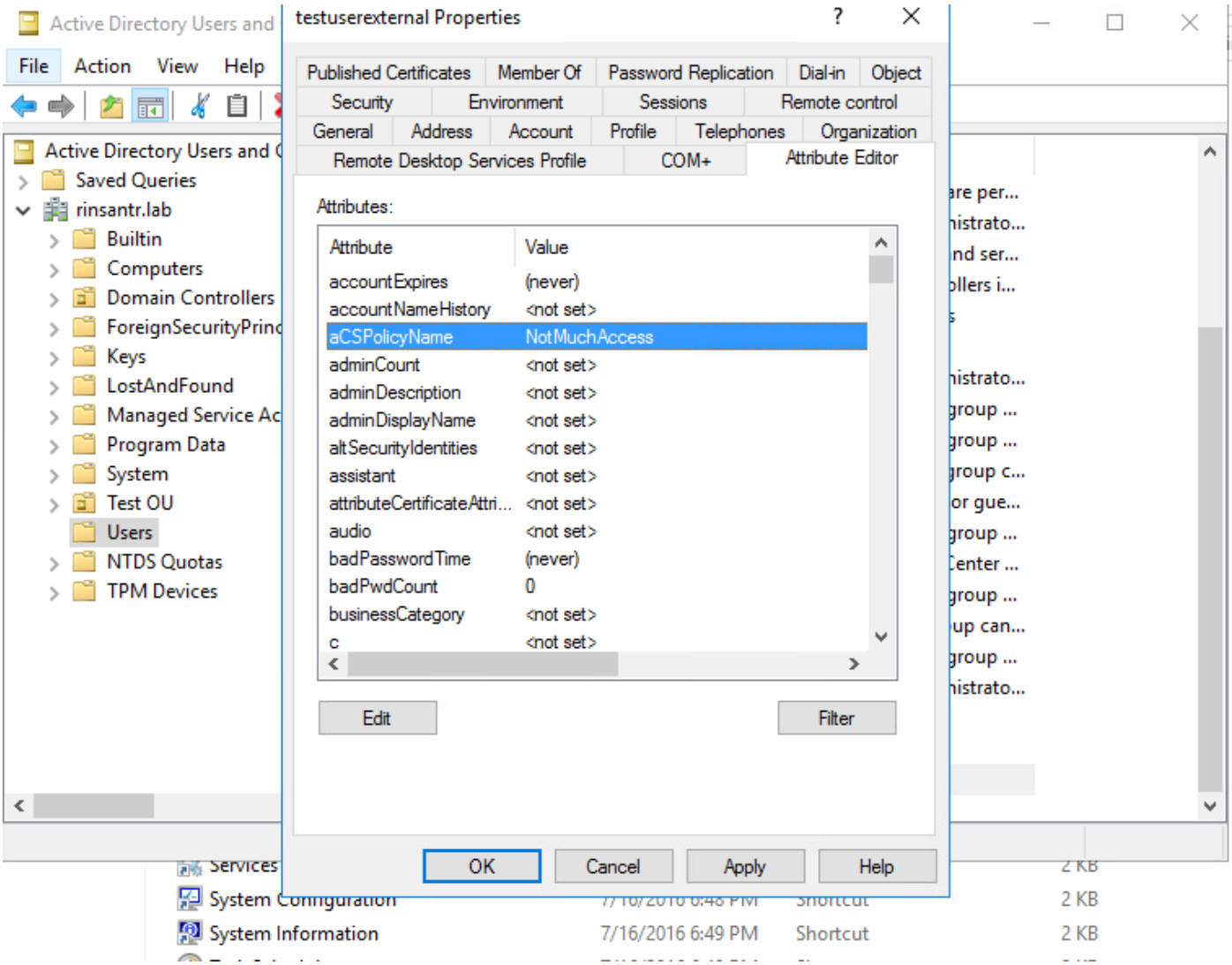
Configurer un compte utilisateur interne avec l'attribut personnalisé

Accédez à Administration > Identity Management > Identities > Users > Add. Créez un utilisateur et configurez la valeur d'attribut personnalisée avec le nom de la dACL que l'utilisateur doit obtenir lorsqu'il est autorisé. Dans cet exemple, le nom de la dACL est NotMuchAccess.



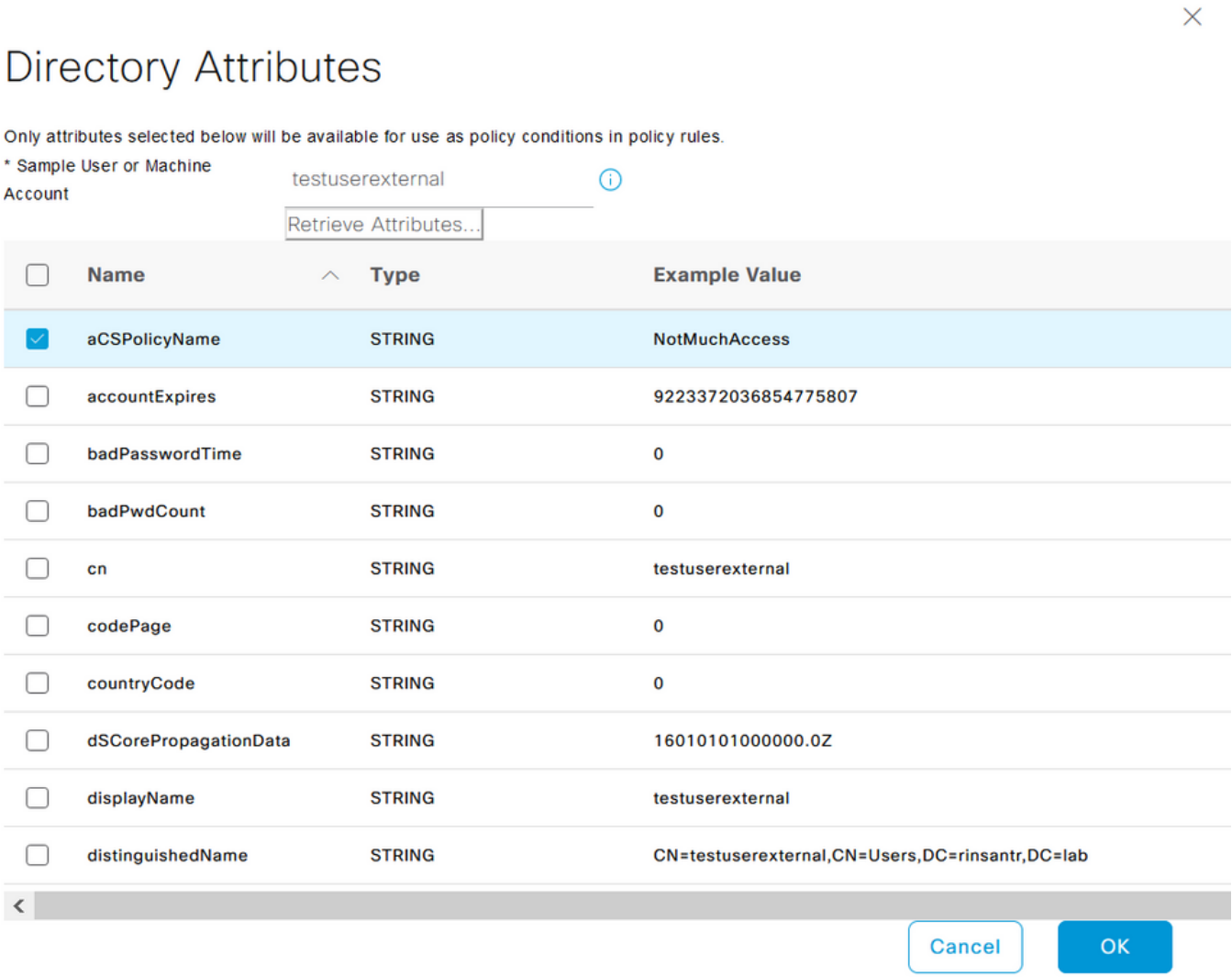
Configurer un compte d'utilisateur AD

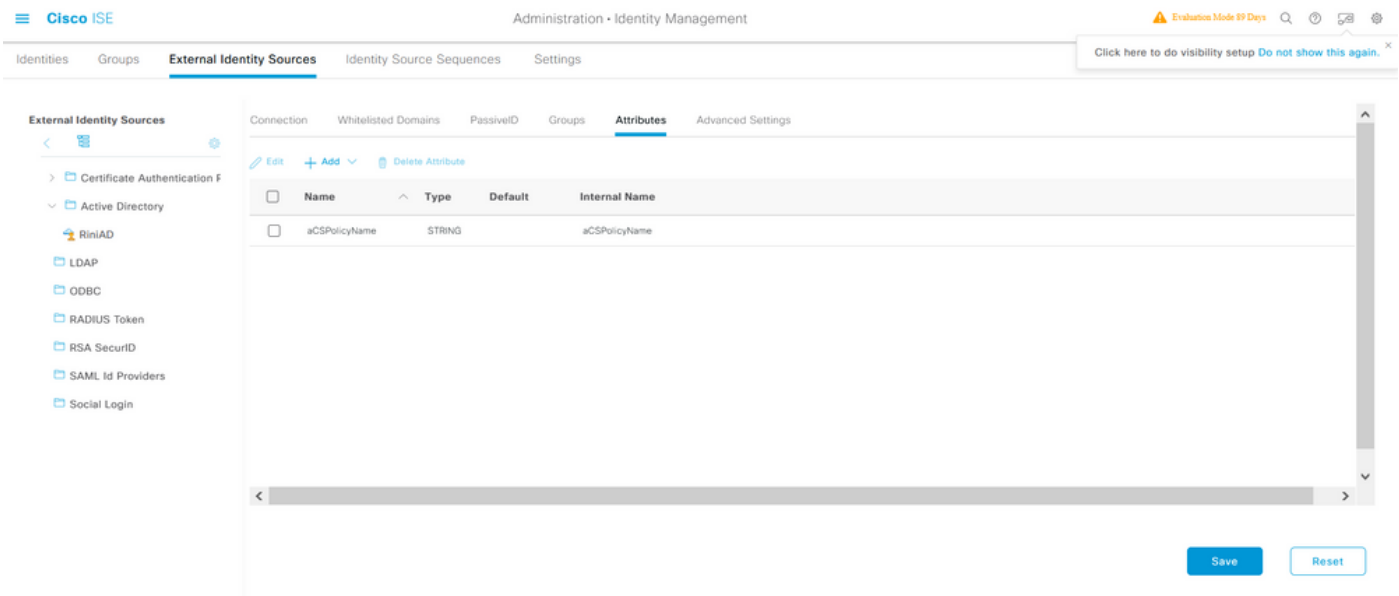
Dans Active Directory, accédez aux propriétés du compte d'utilisateur, puis à l'onglet Éditeur d'attributs. Comme l'illustre l'image, aCSPolicyName est l'attribut utilisé pour spécifier le nom de la liste de contrôle d'accès. Cependant, comme mentionné précédemment, tout attribut qui peut accepter une valeur de chaîne peut également être utilisé.



Importer l'attribut d'AD vers ISE

Pour utiliser l'attribut configuré sur AD, ISE doit l'importer. Pour importer l'attribut, accédez à Administration > Identity Management > External Identity Sources > Active Directory > [Point de connexion configuré] > onglet Attributes. Cliquez sur Add, puis sur Select Attributes From Directory. Fournissez le nom du compte d'utilisateur sur AD, puis cliquez sur Récupérer les attributs. Sélectionnez l'attribut configuré pour la dACL, cliquez sur OK, puis cliquez sur Save. Comme l'illustre l'image, aCSPolicyName est l'attribut.

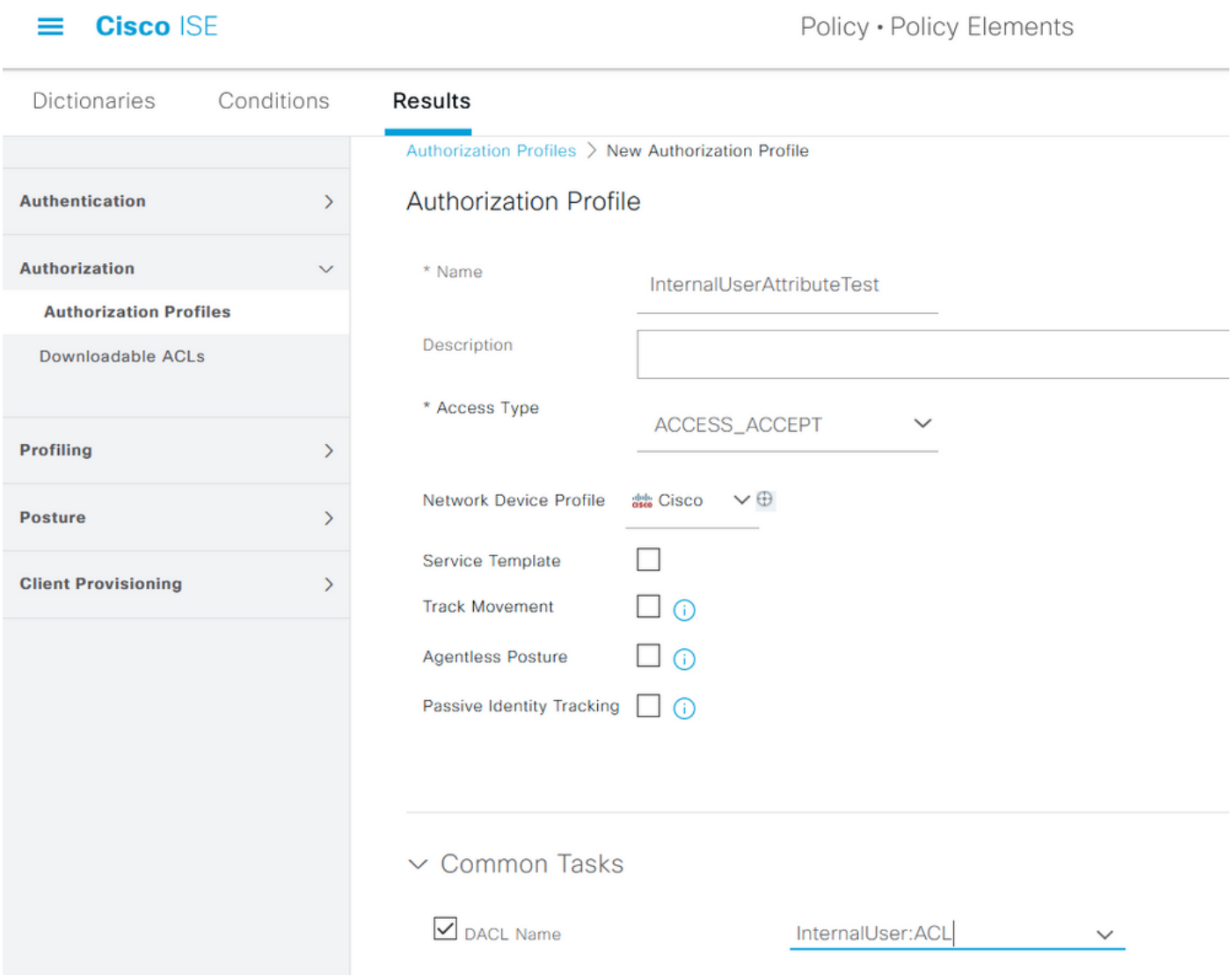




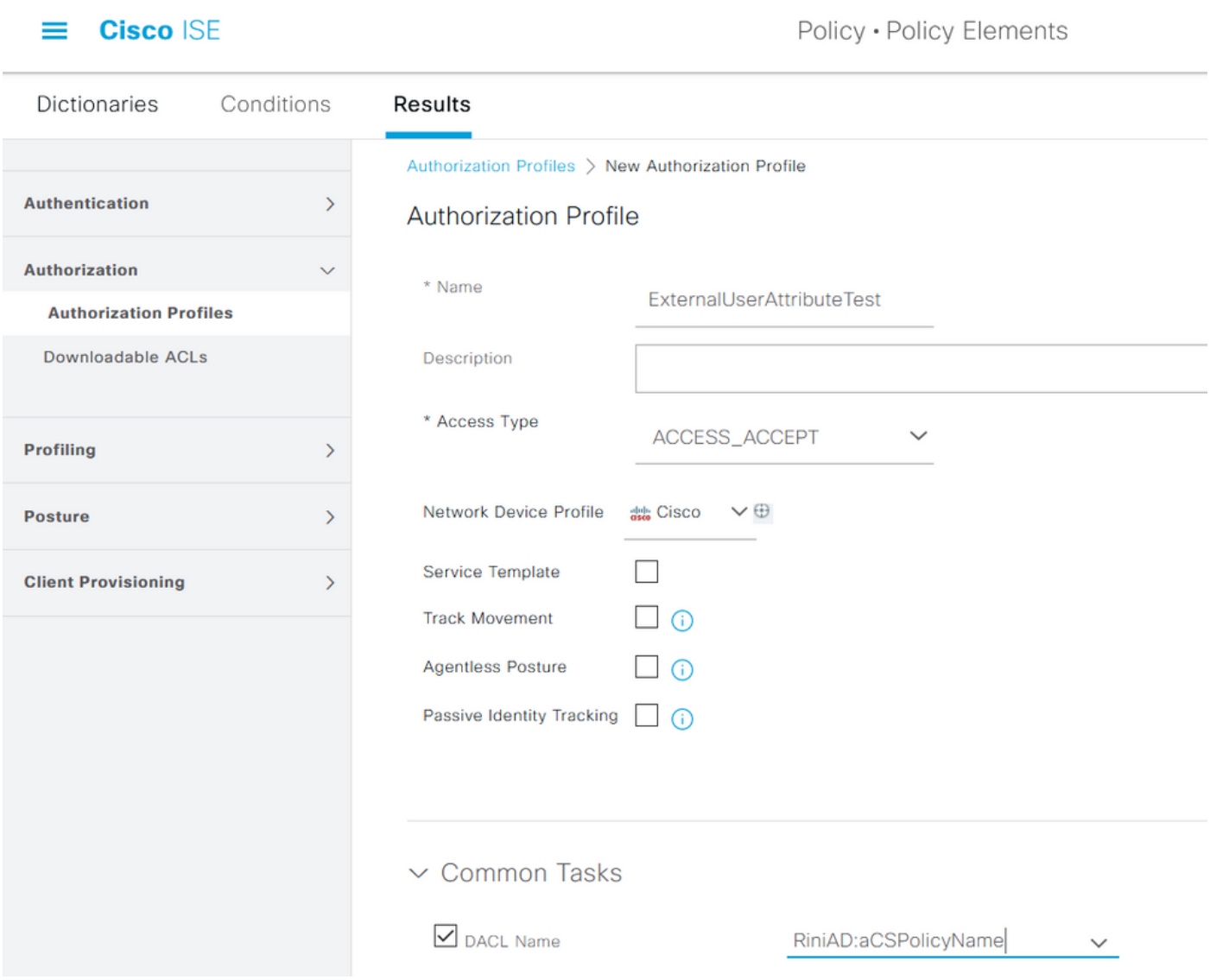
Configuration des profils d'autorisation pour les utilisateurs internes et externes

Afin de configurer les profils d'autorisation, accédez à Policy > Policy Elements > Results > Authorization > Authorization Profiles. Cliquez sur Add. Fournissez un nom et choisissez le nom de la dACL comme InternalUser:<nom de l'attribut personnalisé créé> pour l'utilisateur interne.

Comme l'illustre l'image, pour l'utilisateur interne, le profil InternalUserAttributeTest est configuré avec la dACL configurée comme InternalUser : ACL.

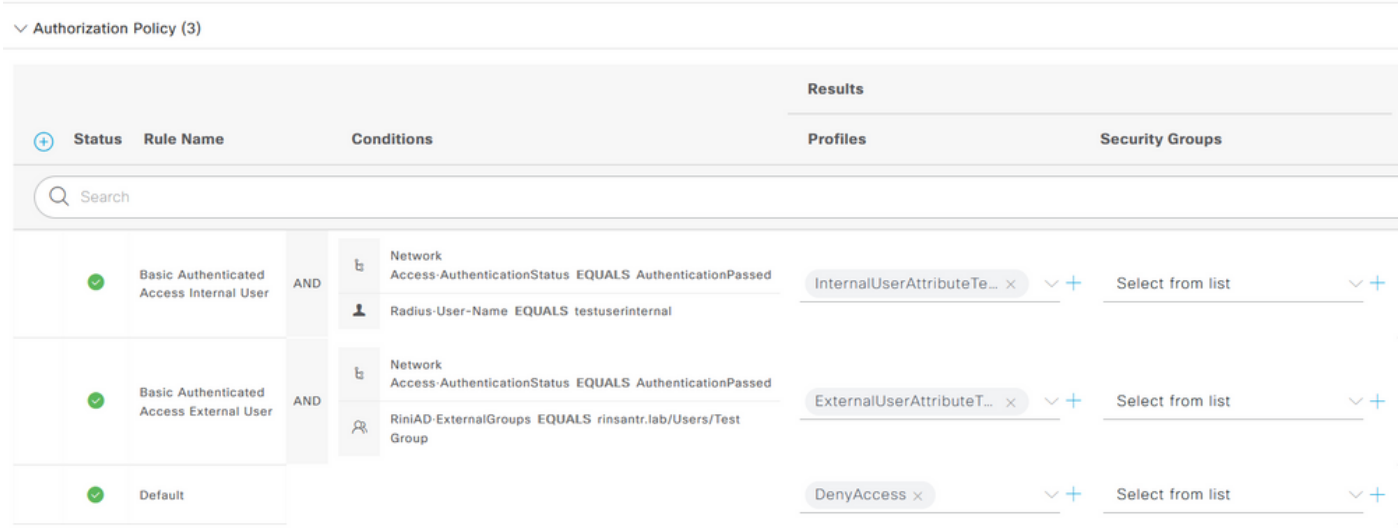


Pour l'utilisateur externe, utilisez <Join point name>:<attribute configured on AD> comme nom dACL. Dans cet exemple, le profil ExternalUserAttributeTest est configuré avec la dACL configurée comme RiniAD : aCSPolicyName où RiniAD est le nom du point de jonction.



Configurer les stratégies d'autorisation

Les stratégies d'autorisation peuvent être configurées dans Policy > Policy Sets en fonction des groupes dans lesquels l'utilisateur externe est présent sur AD et également en fonction du nom d'utilisateur dans le magasin d'identité interne ISE. Dans cet exemple, testuserexternal est un utilisateur présent dans le groupe rinsantr.lab/Users/Test Group et testuserinternal est un utilisateur présent dans le magasin d'identités interne ISE.

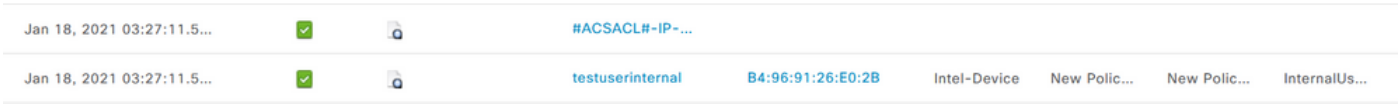


Vérifier

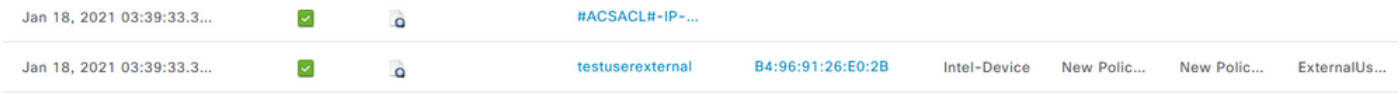
Utilisez cette section pour vérifier si la configuration fonctionne.

Vérifiez les journaux RADIUS en direct pour vérifier les authentifications des utilisateurs.

Utilisateur interne :



Utilisateur externe :



Cliquez sur l'icône en forme de loupe sur les authentifications d'utilisateurs réussies pour vérifier si les demandes correspondent aux stratégies correctes dans la section Vue d'ensemble des journaux en direct détaillés.

Utilisateur interne :

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

Utilisateur externe :

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

Consultez la section Autres attributs des journaux en direct détaillés pour vérifier si les attributs utilisateur ont été récupérés.

Utilisateur interne :

EnableFlag	Enabled
ACL	NotMuchAccess
RADIUS Username	testuserinternal

Utilisateur externe :

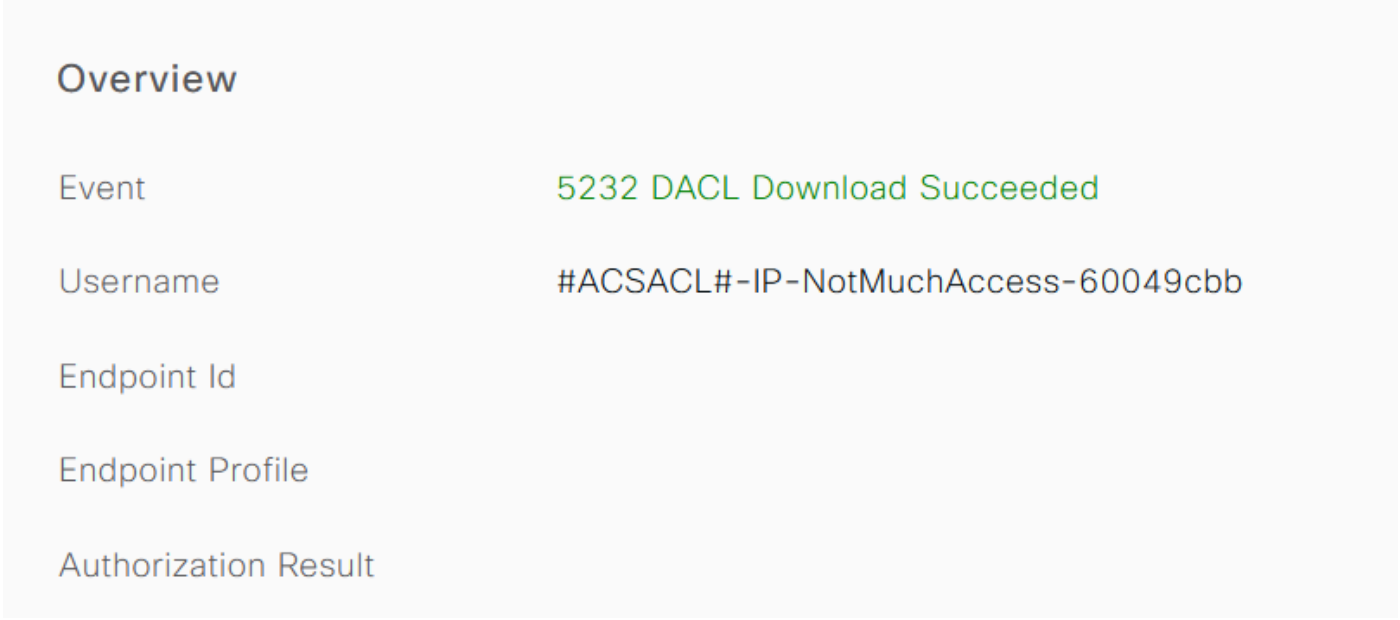
aCSPolicyName	NotMuchAccess
RADIUS Username	testuserexternal

Consultez la section Résultat des journaux en direct détaillés pour vérifier si l'attribut dACL est envoyé dans le cadre d'Access-Accept.

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

Vérifiez également les journaux RADIUS en direct pour vérifier si la dACL est téléchargée après l'authentification de l'utilisateur.

Cliquez sur l'icône en forme de loupe sur le journal de téléchargement de dACL réussi et vérifiez la section Overview pour confirmer le téléchargement de dACL.



Consultez la section Résultat de ce rapport détaillé pour vérifier le contenu de la dACL.

Dépannage

Il n’y a actuellement aucune information spécifique disponible pour dépanner cette configuration.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.