

# ACL téléchargeable dans les commutateurs Catalyst 1300

## Objectif

L'objectif de cet article est de démontrer le fonctionnement de la liste de contrôle d'accès (DACL) téléchargeable sur les commutateurs Cisco Catalyst 1300 avec Cisco Identity Service Engine (ISE).

## Périphériques pertinents | Version logicielle

- Gamme Catalyst 1300 |4.1.6.54

## Introduction

Les listes de contrôle d'accès dynamiques sont des listes attribuées à un port de commutateur en fonction d'une stratégie ou de critères tels que l'appartenance à un groupe de comptes d'utilisateurs, l'heure, etc. Il peut s'agir de listes de contrôle d'accès locales spécifiées par filter-ID ou de listes de contrôle d'accès téléchargeables (DACL).

Les listes de contrôle d'accès téléchargeables sont des listes dynamiques créées et téléchargées à partir du serveur Cisco ISE. Ils appliquent dynamiquement des règles de contrôle d'accès basées sur l'identité des utilisateurs et le type de périphérique. La liste de contrôle d'accès dynamique a l'avantage de vous permettre d'avoir un référentiel central pour les listes de contrôle d'accès. Vous n'avez donc pas besoin de les créer manuellement sur chaque commutateur. Lorsqu'un utilisateur se connecte à un commutateur, il n'a qu'à s'authentifier et le commutateur télécharge les listes de contrôle d'accès applicables à partir du serveur Cisco ISE.

## Exemples d'utilisation de listes de contrôle téléchargeables

- 1 Différents utilisateurs recevront différentes listes de contrôle d'accès lorsqu'ils se connectent à un commutateur (utilisateurs ISE locaux).
- 2 Les utilisateurs disposant d'une connectivité réseau limitée peuvent se connecter à un portail Web central pour un accès complet au réseau (authentification Web centrale).
- 3 Avancé : utilisation du contournement d'authentification MAC (MAB) pour permettre la communication avec Windows Active Directory (AD) et certains services associés lors de la connexion de votre serveur ISE à AD et de la surveillance de l'authentification des utilisateurs. Avant l'ouverture de session Windows AD, le réseau autorise uniquement l'accès à des ressources très limitées, mais l'authentification AD télécharge différentes listes de contrôle d'accès basées sur des groupes Windows et

autorise un accès réseau complet.

4 Avancé : les utilisateurs reçoivent différentes listes de contrôle d'accès en fonction du jour de la semaine, de l'heure ou d'un autre facteur en raison des stratégies sur le serveur ISE.

Dans cet article, le premier cas d'utilisation sera traité en détail.

## Table des matières

- [Configuration du client RADIUS](#)
- [Configuration de l'authentification 802.1x](#)
- [Configuration du serveur Cisco ISE pour ACL téléchargeable](#)
- [Configurations client](#)
- [Vérification DACL](#)

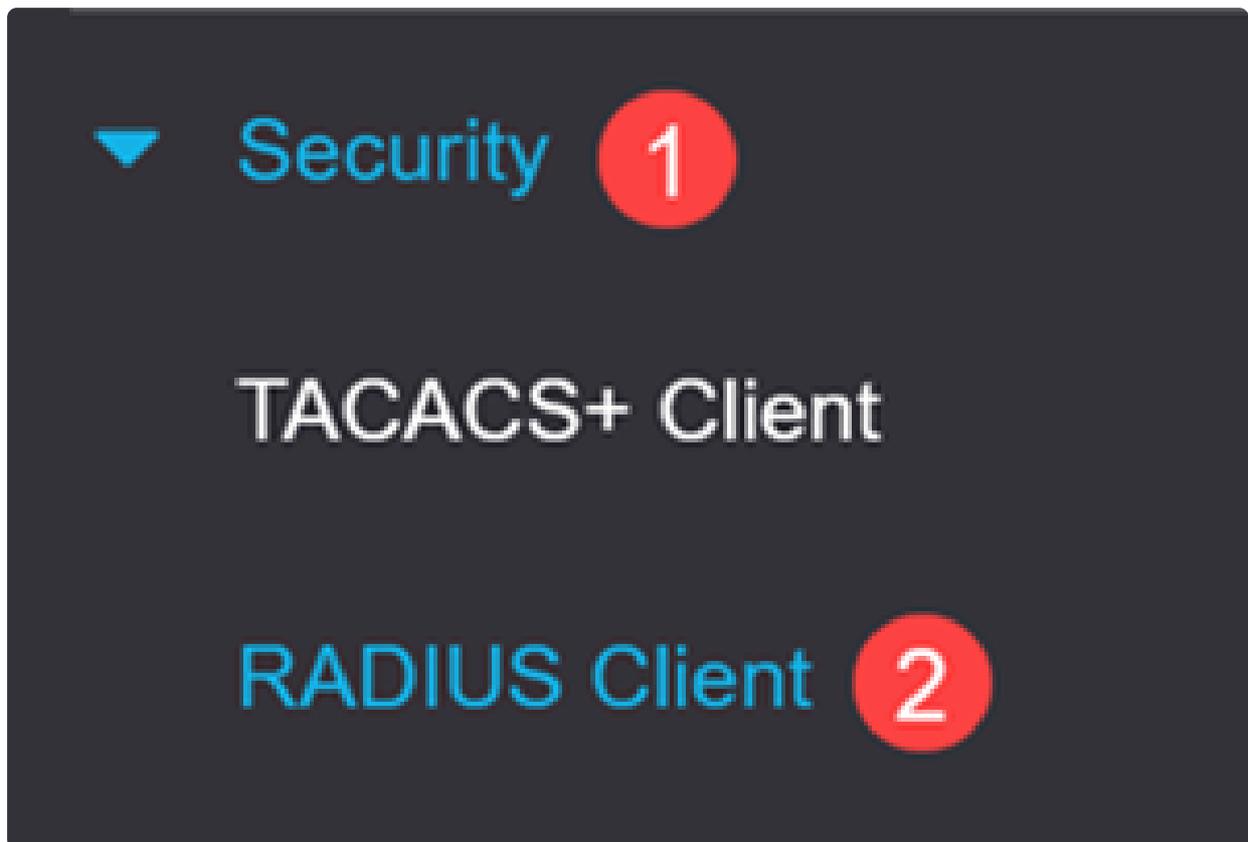
### Conditions préalables

- Assurez-vous que votre commutateur Catalyst 1300 est mis à niveau vers la dernière version du micrologiciel (la version du micrologiciel du commutateur doit être 4.1.6 ou supérieure).
- Attribuez une adresse IP statique au commutateur à des fins de gestion.

## Configuration du client RADIUS

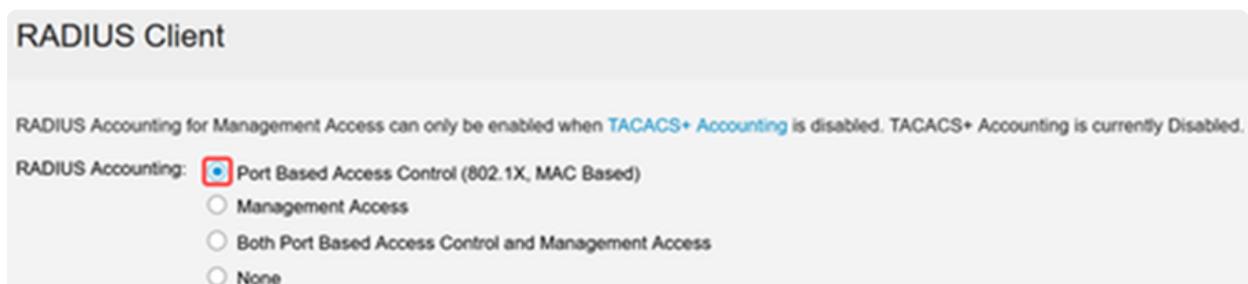
### Étape 1

Connectez-vous au commutateur Catalyst 1300 et accédez au menu Security > RADIUS Client.



## Étape 2

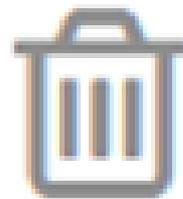
Pour RADIUS Accounting, sélectionnez l'option Port Based Access Control.



## Étape 3

Sous RADIUS Table, cliquez sur l'icône plus pour ajouter le serveur Cisco ISE.

# RADIUS Table



## Étape 4

Entrez les détails du serveur Cisco ISE et cliquez sur Apply.

**Add RADIUS Server** x

Server Definition:  By IP address  By name

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface:

Server IP Address/Name:

Priority:  (Range: 0 - 65535)

Key String:  Use Default  
 User Defined (Encrypted)   
 User Defined (Plaintext)  (0-128 characters used)

Timeout for Reply:  Use Default  
 User Defined  sec (Range: 1 - 30, Default: 3)

Authentication Port:  (Range: 0 - 65535, Default: 1812)

Retries:  Use Default  
 User Defined  (Range: 1 - 15, Default: 3)

Dead Time:  Use Default  
 User Defined  min (Range: 0 - 2000, Default: 0)

Usage Type:  Login  
 802.1x  
 All

Note:

Le type d'utilisation doit être sélectionné comme 802.1x.

## Configuration de l'authentification 802.1x

### Étape 1

Accédez au menu Security > 802.1X Authentication > Properties.

▼ Security 1

TACACS+ Client

RADIUS Client

▶ RADIUS Server

Login Settings

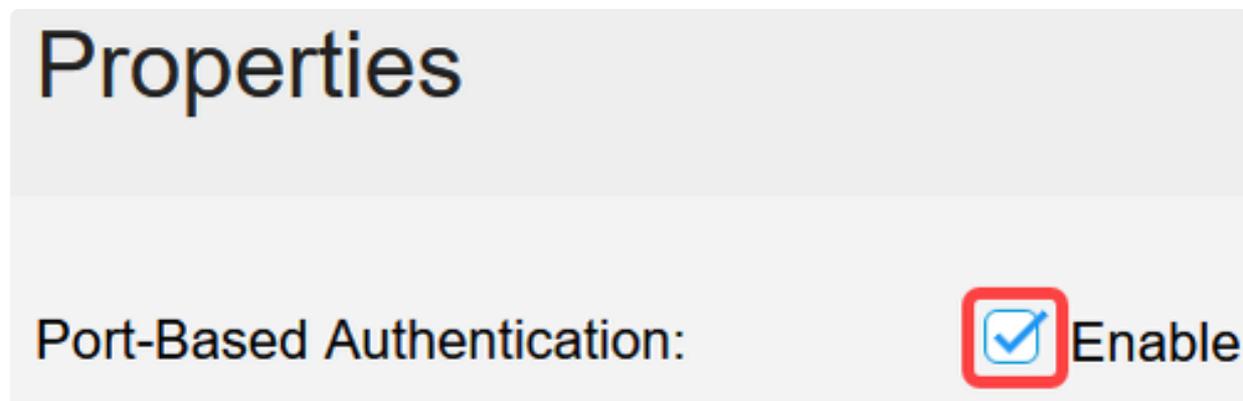
Login Protection Status

▶ Mgmt Access Method

Management Access

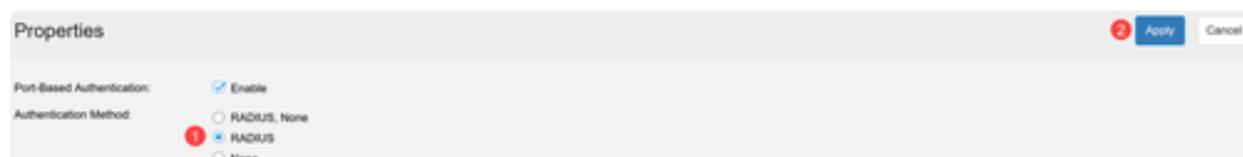
## Étape 2

Cochez cette case pour activer l'authentification basée sur les ports.



## Étape 3

Sous Authentication Method, sélectionnez RADIUS et cliquez sur Apply.



## Étape 4

Accédez au menu Security > 802.1X Authentication > Port Authentication.  
Sélectionnez le port auquel votre ordinateur portable est connecté et cliquez sur l'icône edit (Modifier). Dans cet exemple, GE8 est sélectionné.

## Port Authentication



Filter: *Interface Type* equals to Port of Unit 1 ▾ **Go**

	Entry No.	Port	Current Port Control	Administrative Port Control	RADIUS VLAN Assignment
<input type="radio"/>	1	GE1	Authorized	Force Authorized	Disabled
<input type="radio"/>	2	GE2		Force Authorized	Disabled
<input type="radio"/>	3	GE3		Force Authorized	Disabled
<input type="radio"/>	4	GE4		Force Authorized	Disabled
<input type="radio"/>	5	GE5		Force Authorized	Disabled
<input type="radio"/>	6	GE6		Auto	Disabled
<input checked="" type="radio"/>	7	GE7		Force Authorized	Disabled
<input checked="" type="radio"/>	8	GE8	Authorized	Auto	Disabled
<input type="radio"/>	9	GE9	Authorized	Force Authorized	Disabled

### Étape 5

Sélectionnez Administrative Port Control comme Auto et activez l'authentification basée sur 802.1x. Cliquez sur Apply.

## Edit Port Authentication

Interface: Unit  Port

Current Port Control: Authorized

Administrative Port Control:  Force Unauthorized  Auto  Force Authorized

RADIUS VLAN Assignment:  Disable  Reject  Static

Guest VLAN:  Enable

Open Access:  Enable

802.1x Based Authentication:  Enable

MAC Based Authentication:  Enable

Web Based Authentication:  Enable

Periodic Reauthentication:  Enable

3

Apply

## Configuration du serveur Cisco ISE pour ACL téléchargeable

### Note:

La configuration ISE sort du cadre de l'assistance Cisco Business. Reportez-vous au [guide d'administration ISE](#) pour plus d'informations.

Les configurations présentées dans cet article sont un exemple de liste de contrôle d'accès téléchargeable à utiliser avec le commutateur de la gamme Cisco Catalyst 1300.

### Étape 1

Connectez-vous à votre serveur Cisco ISE et accédez à Administration > Network Resources > Network Devices et ajoutez le périphérique de commutateur Catalyst.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration interface. The breadcrumb navigation path is: Home > Context Visibility > Operations > Pol <sup>1</sup> > Administration > System > Identity Management > Network Resources <sup>2</sup> > Network Devices <sup>3</sup>. The 'Network Resources' and 'Network Devices' menus are highlighted with red boxes. Below the navigation, the 'Network Devices' page is displayed, showing a list of devices and a toolbar with an 'Add' button highlighted by a red box and a red circle <sup>4</sup>.

## Étape 2

Pour créer des groupes d'identité utilisateur, accédez à l'onglet Groupes et ajoutez les groupes d'identité utilisateur.

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The navigation menu at the top includes 'Home', 'Context Visibility', 'Operations', 'Policy', and 'Administration'. Under 'Administration', the path 'System > Identity Management > Identities > Groups' is highlighted. The 'Groups' tab is selected, and the 'Add' button is circled in red with a red circle containing the number 2. The main content area displays 'User Identity Groups' with a table of existing groups:

Name	Description
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL
<input type="checkbox"/> Employee	Default Em
<input type="checkbox"/> Filter-ID	Filter-ID
<input type="checkbox"/> GROUP_ACCOUNTS (default)	Default GR
<input type="checkbox"/> GuestType_Contractor (default)	Identity gr

## Étape 3

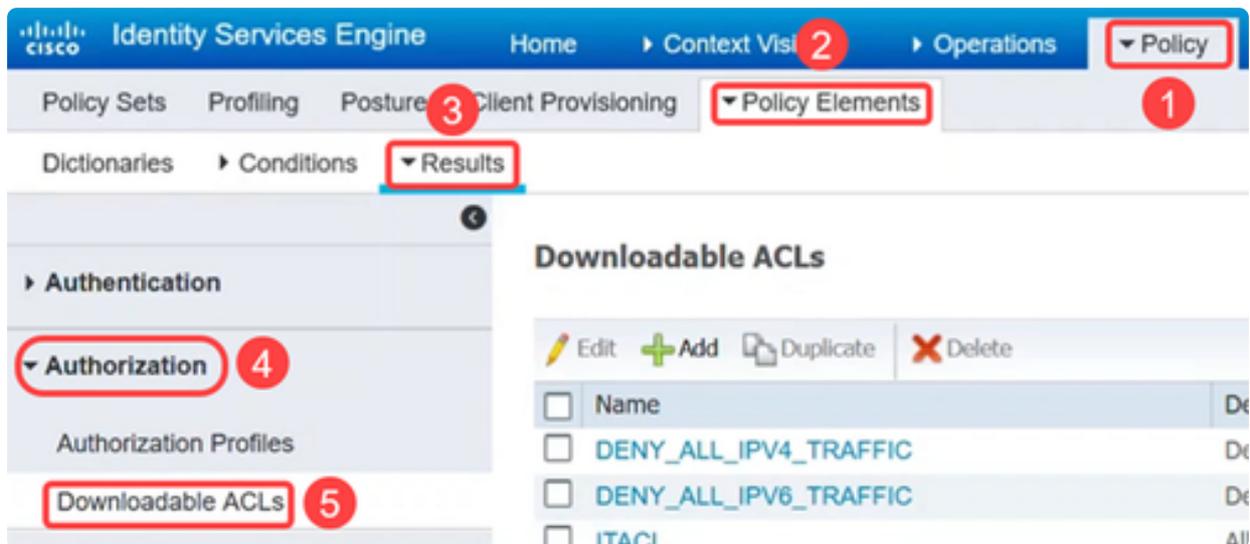
Accédez au menu Administration > Identity Management > Identities pour définir les utilisateurs et les mapper aux groupes.

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The navigation menu at the top includes 'Home', 'Context Visibility', 'Operations', 'Policy', and 'Administration'. Under 'Administration', the path 'System > Identity Management > Identities' is highlighted. The 'Identities' tab is selected, and the 'Add' button is circled in red with a red circle containing the number 4. The main content area displays 'Network Access Users' with a table of existing users:

Status	Name	Description	First
<input checked="" type="checkbox"/> Enabled	user1		

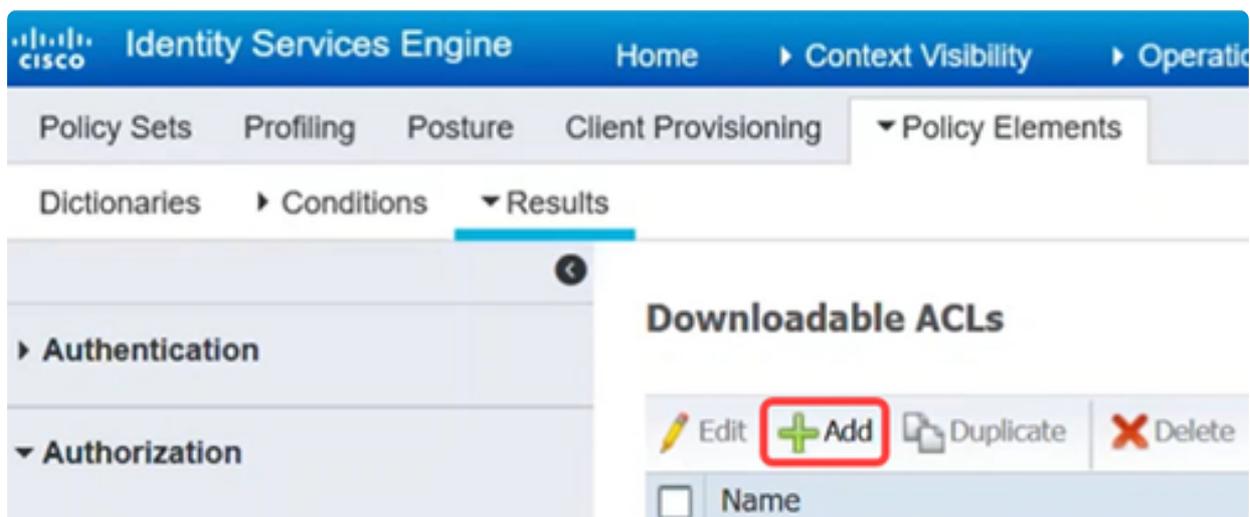
## Étape 4

Accédez au menu Politique > Eléments de politique > Résultats. Sous Authorization, cliquez sur Downloadable ACLs.



## Étape 5

Cliquez sur l'icône Add pour créer la liste de contrôle d'accès téléchargeable.



## Étape 6

Configurez le nom, la description, sélectionnez la version IP et entrez les entrées de contrôle d'accès (ACE) qui constitueront la liste de contrôle d'accès téléchargeable dans le champ DACL Content. Cliquez sur Save.

## Downloadable ACL List > ITACL

### Downloadable ACL

\* Name

Description

IP version  IPv4  IPv6  Agnostic 

\* DACL Content

```
1234567 permit ip any any  
8910111  
2131415  
1617181  
9202122  
2324252  
6272829  
3031323  
3343536
```



▶ Check DACL Syntax

Save

Reset

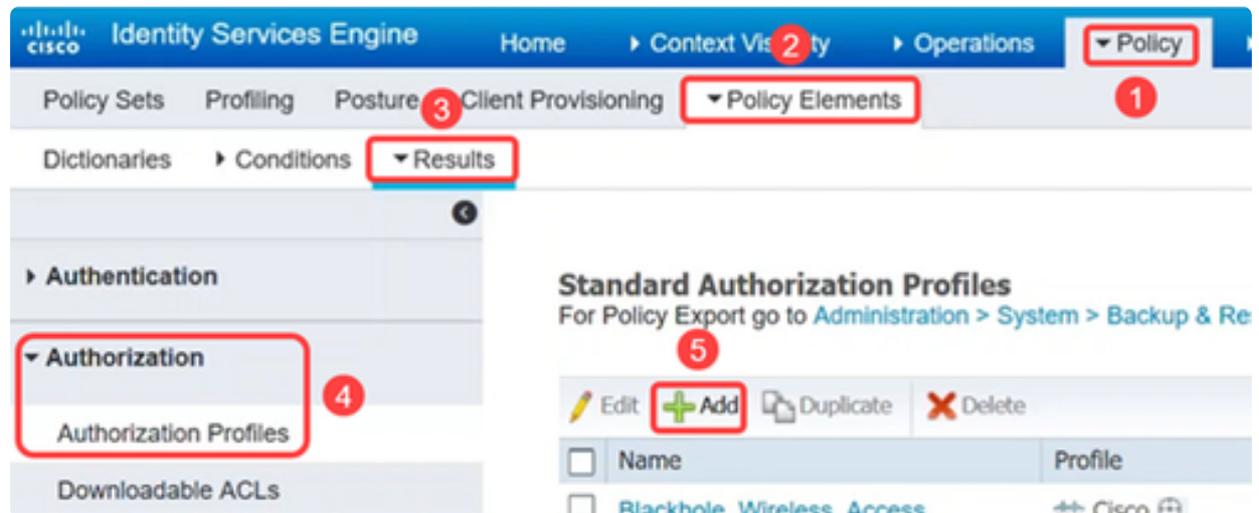
#### Note:

Seules les listes de contrôle d'accès IP sont prises en charge et la source doit être ANY. Pour les listes de contrôle d'accès sur ISE, seul IPv4 est désormais pris en charge. Si une liste de contrôle d'accès est entrée avec une autre source, alors que la syntaxe peut être correcte en ce qui concerne ISE, elle échouera lorsqu'elle sera appliquée au commutateur.

## Étape 7

Créez des profils d'autorisation qui seront utilisés pour associer logiquement votre liste de contrôle d'accès et d'autres stratégies à l'intérieur des ensembles de stratégies ISE.

Pour ce faire, accédez à Policy > Policy Elements > Results > Authorization > Authorization Profiles et cliquez sur Add.



## Étape 8

Dans la page Authorization Profile, configurez les éléments suivants :

- Nom
- Description
- Type d'accès - doit être défini sur ACCESS\_ACCEPT. Si la valeur est ACCESS\_REJECT, l'authentification est rejetée.
- Profil de périphérique réseau - il doit être sélectionné comme Cisco.
- Passif Identity Tracking - peut nécessiter d'être activé pour certains scénarios d'authentification. Elle est requise pour les scénarios EasyConnect\_PassiveID liés à Active Directory.
- Tâches courantes - Cette section propose de nombreuses options. Pour cet exemple, DACL Name est configuré.

Cliquez sur Save.

## Authorization Profile

* Name	<input type="text" value="IT_Auth"/>
Description	<input type="text"/>
* Access Type	<input type="text" value="ACCESS_ACCEPT"/>
Network Device Profile	<input type="text" value="Cisco"/>  <input type="text" value="Cisco"/> 
Service Template	<input type="checkbox"/>
Track Movement	<input type="checkbox"/> 
Passive Identity Tracking	<input checked="" type="checkbox"/> 

### ▼ Common Tasks

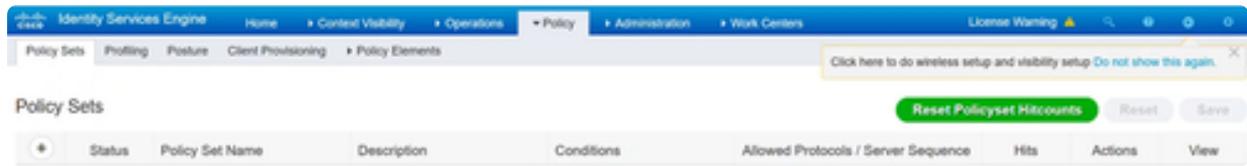
#### Étape 9

Pour configurer des ensembles de stratégies qui sont des regroupements logiques de stratégies d'authentification et d'autorisation, cliquez sur le menu Stratégie > Jeux de stratégies.

Vous pouvez afficher les éléments suivants lorsque vous consultez une liste d'ensembles de stratégies :

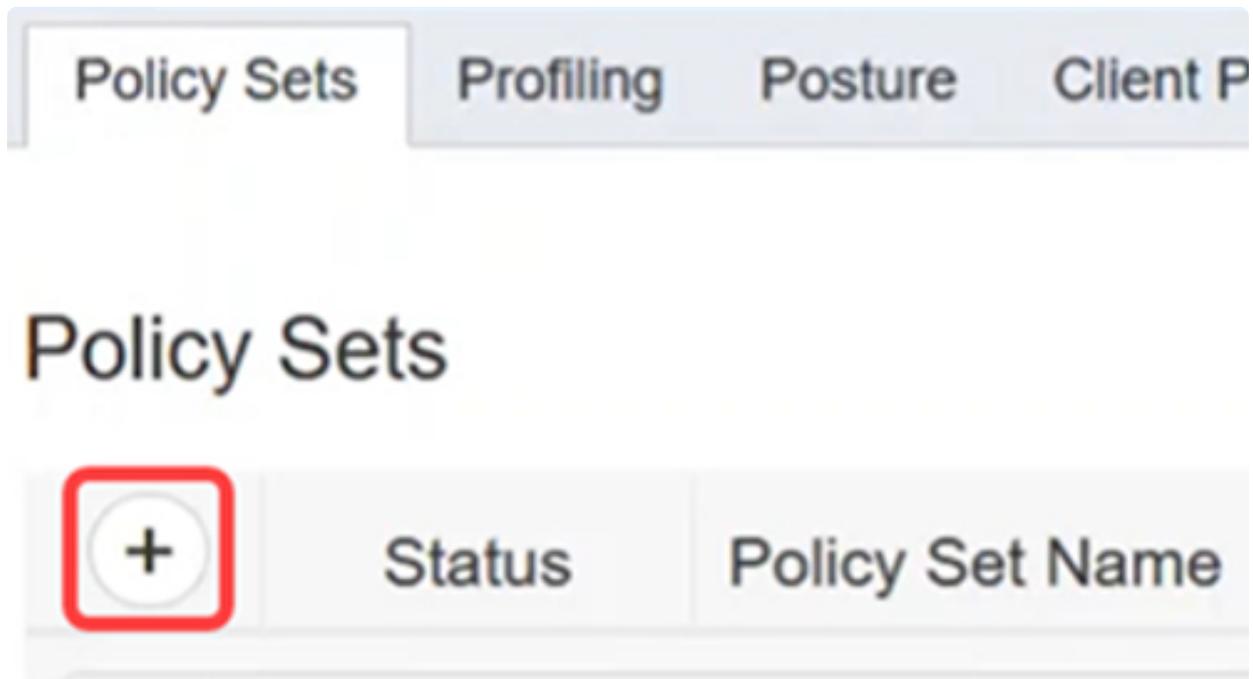
- État - Une coche verte indique activé, un cercle blanc vide indique désactivé et une icône en forme d'oeil indique une configuration de moniteur uniquement.
- Nom et description du jeu de stratégies explicites
- Conditions - Définit l'application du jeu de stratégies.
- Protocoles autorisés/Séquence de serveur - définit des contrôles plus avancés.
- Hits : indique le nombre de fois où le jeu de stratégies a été utilisé.

- Actions : vous permet de modifier l'ordre dans lequel les jeux de stratégies peuvent être appliqués, de copier un jeu de stratégies existant ou de supprimer un jeu de stratégies existant.
- Afficher - vous permet de modifier les détails de l'ensemble de stratégies.



## Étape 10

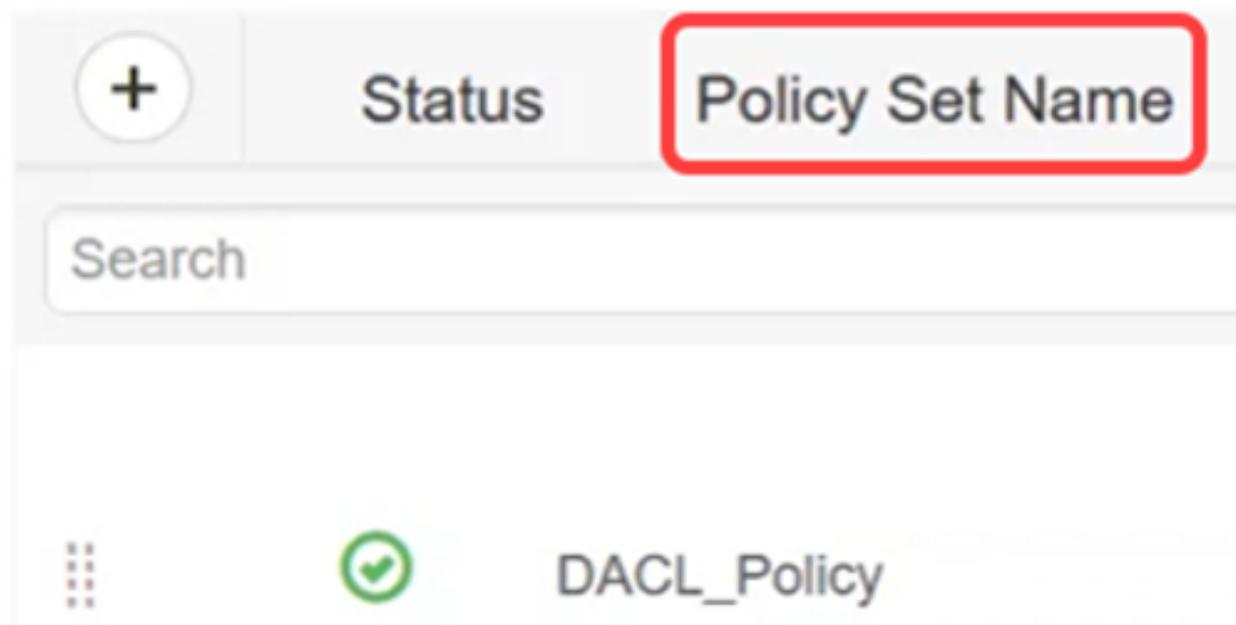
Pour créer un jeu de stratégies, cliquez sur le bouton add (ajouter).



## Étape 11

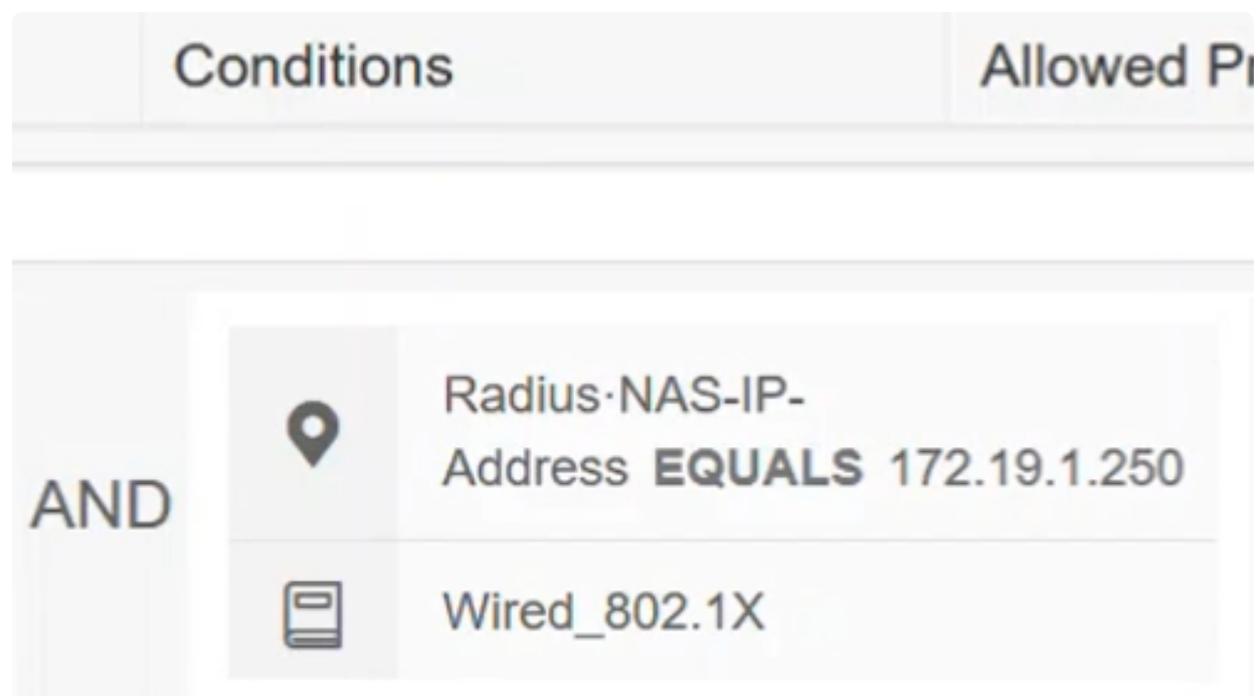
Définissez un nom de jeu de stratégies.

# Policy Sets



## Étape 12

Sous Conditions, cliquez sur le bouton Ajouter. Cela ouvre le Studio Conditions où vous pouvez définir où ce profil d'authentification sera utilisé. Dans cet exemple, il a été appliqué à l'adresse IP Radius-NAS-IP (le commutateur) qui est 172.19.1.250 et le trafic filaire 802.1x.



## Étape 13

Configurez les protocoles autorisés sur l'accès réseau par défaut et cliquez sur Enregistrer.



## Étape 14

Sous View, cliquez sur l'icône en forme de flèche pour configurer les stratégies d'authentification et d'autorisation en fonction de la configuration et des exigences de votre réseau. Vous pouvez également choisir les paramètres par défaut. Dans cet exemple, cliquez sur Stratégie d'autorisation.

Actions	View

42



### Étape 15

Cliquez sur l'icône plus pour ajouter une stratégie.

- Authentication Policy
- Authorization Policy - Local Exceptions
- Authorization Policy - Global Exceptions
- Authorization Policy

Étape 16

Saisissez le nom de la règle.

	Status	Rule Name
<input type="text" value="Search"/>		



SalesUser\_Policy

Étape 17

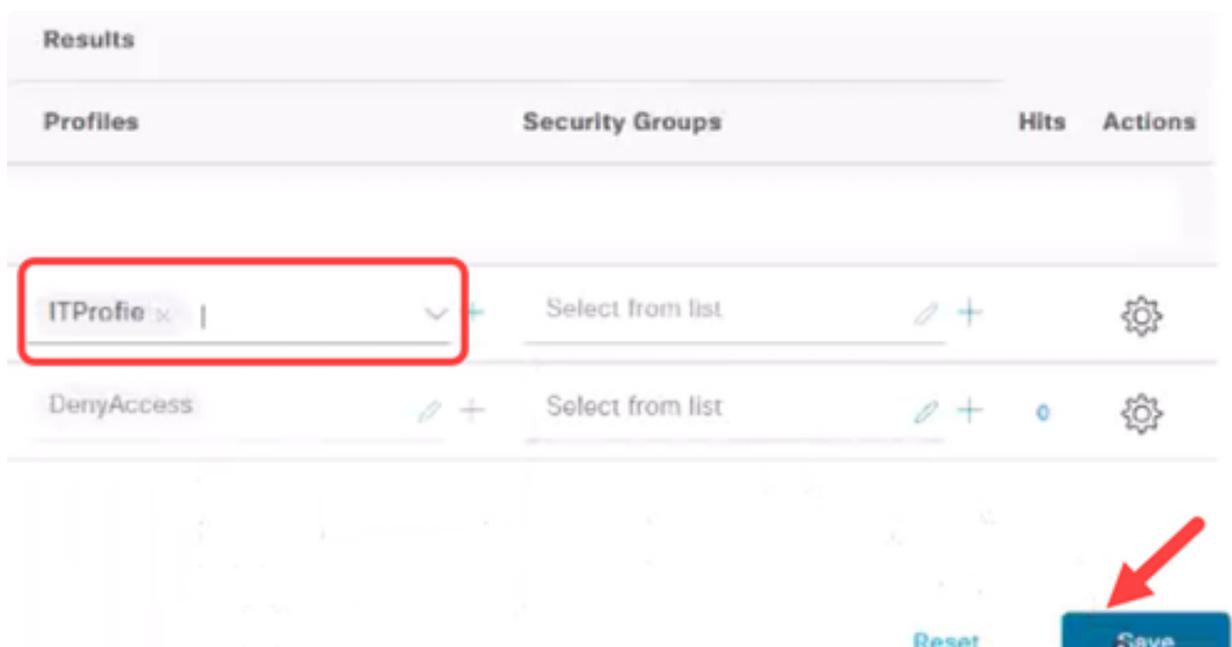
Sous Conditions, cliquez sur l'icône plus et sélectionnez le groupe d'identité. Cliquez

sur Utiliser.



## Étape 18

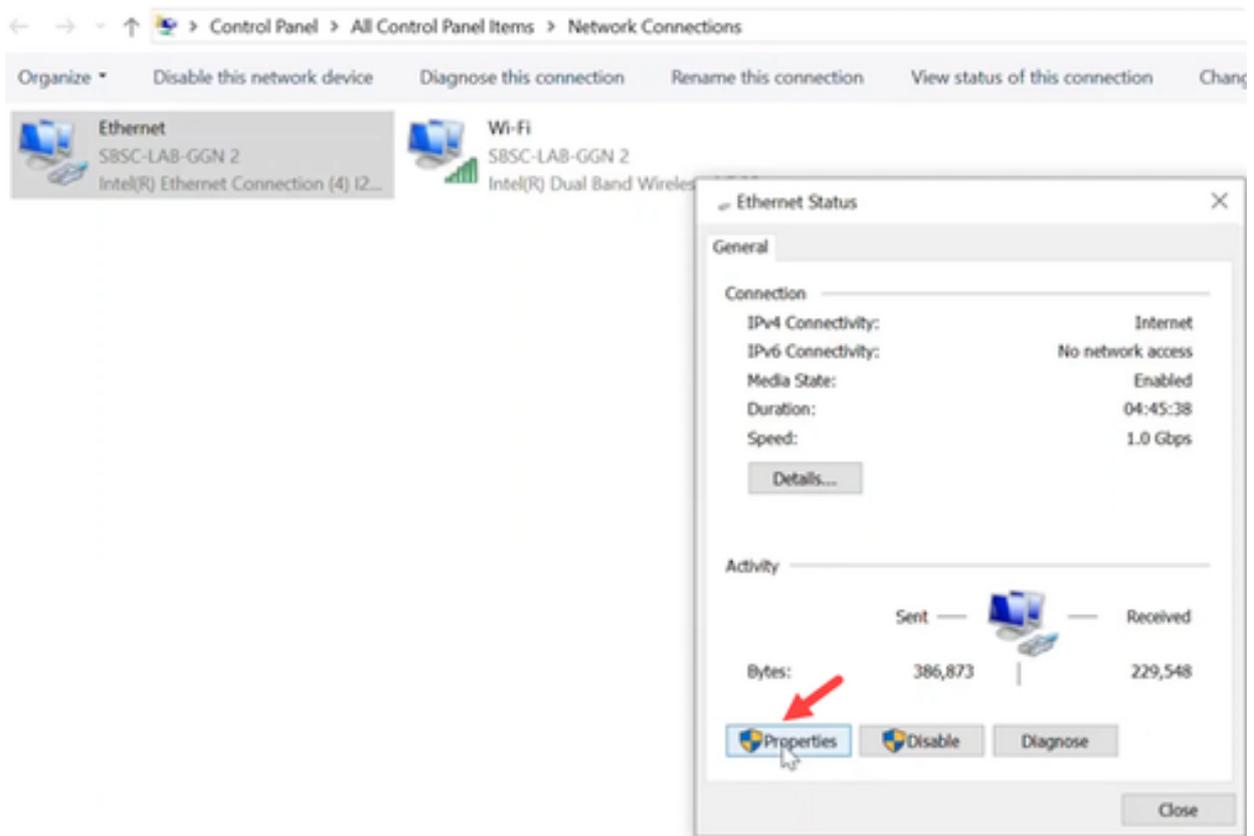
Appliquez le profil requis et cliquez sur Enregistrer.



## Configurations client

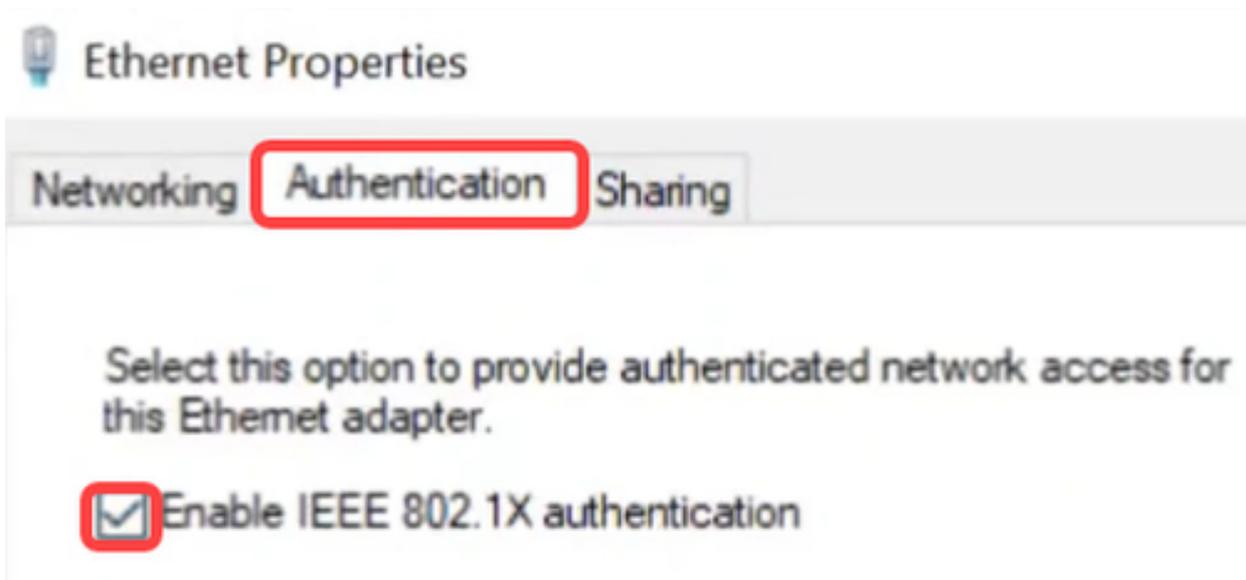
### Étape 1

Sur l'ordinateur portable client, accédez à Connexions réseau > Ethernet et cliquez sur Propriétés.



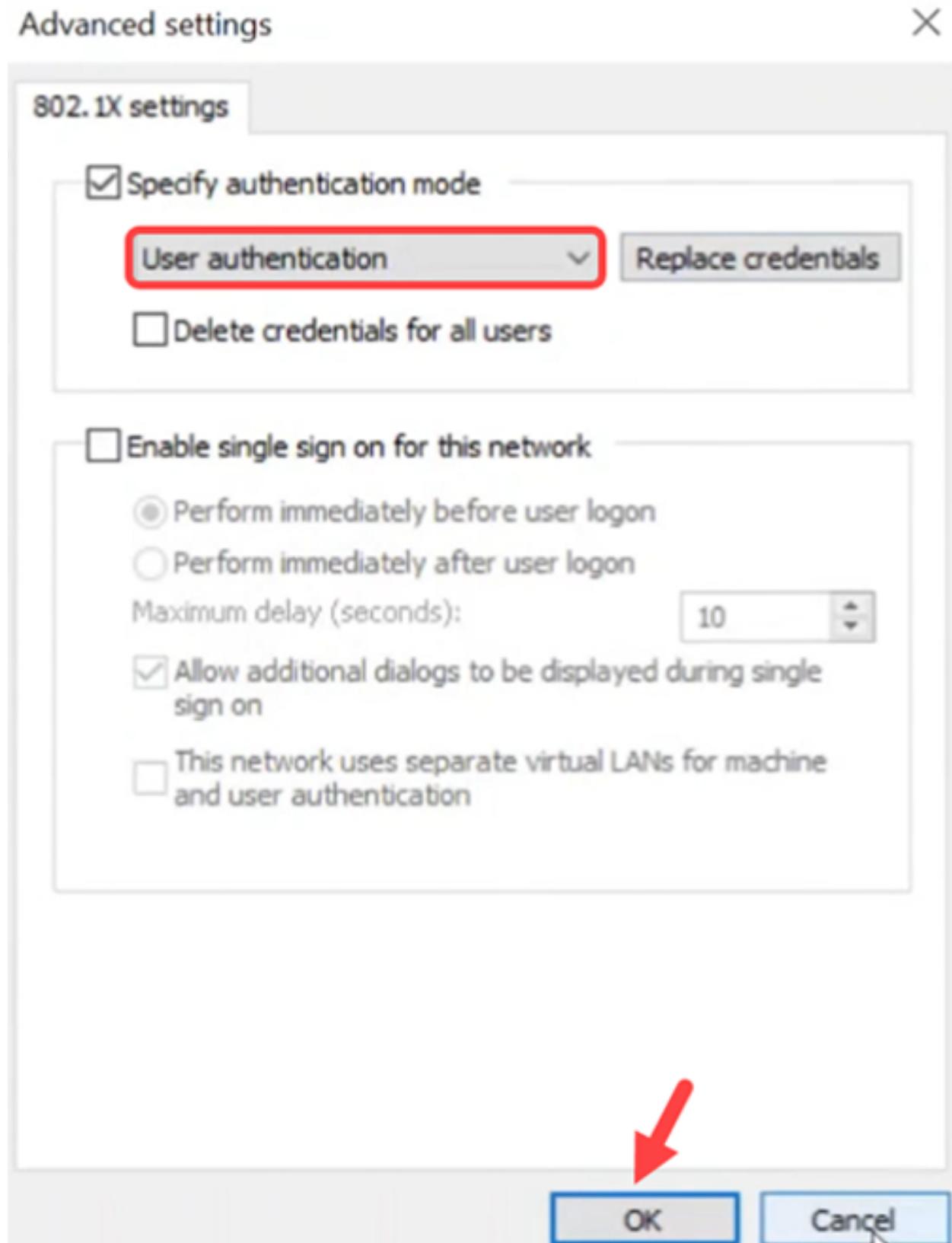
## Étape 2

Cliquez sur l'onglet Authentication et vérifiez que l'authentification 802.1X est activée.



## Étape 3

Sous Additional Settings, sélectionnez User authentication comme mode d'authentification. Cliquez sur Save Credentials, puis sur OK.



#### Étape 4

Cliquez sur Settings et assurez-vous que la case en regard de Verify the server's identity by validating the certificate est décochée. Click OK.

## Protected EAP Properties



When connecting:

Verify the server's identity by validating the certificate

Connect to these servers (examples: srv1;srv2;. \*\.srv3\.com):

Trusted Root Certification Authorities:

- AAA Certificate Services
- Baltimore CyberTrust Root
- Certum Trusted Network CA
- Class 3 Public Primary Certification Authority
- COMODO RSA Certification Authority
- DESKTOP-N0NBRSQ
- DigiCert Assured ID Root CA

Notifications before connecting:

Tell user if the server's identity can't be verified

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

Configure...

Enable Fast Reconnect

Disconnect if server does not present cryptobinding TLV

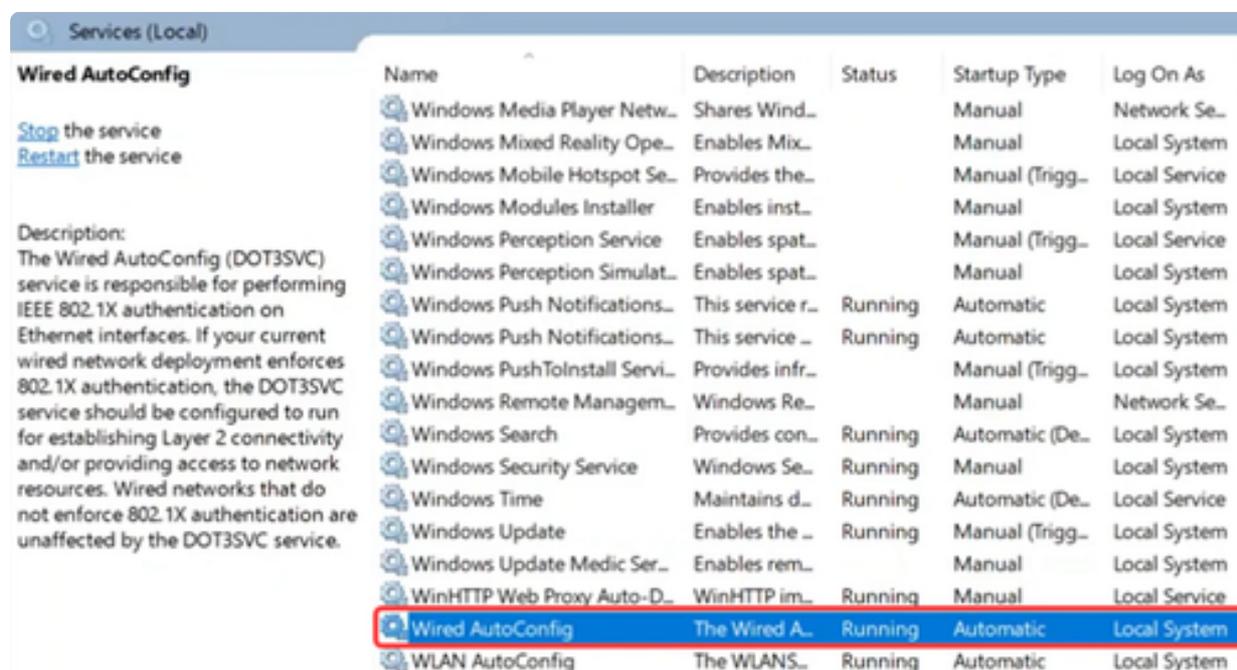
Enable Identity Privacy

OK

Cancel

## Étape 5

Sous Services, activez les paramètres Wired AutoConfig.



## Vérification DACL

Une fois l'utilisateur authentifié, vous pouvez vérifier la liste de contrôle d'accès téléchargeable.

## Étape 1

Connectez-vous au commutateur Catalyst 1300 et accédez au menu Access Control > IPv4-Based ACL.



Access Control

1

MAC-Based ACL

MAC-Based ACE

IPv4-Based ACL

2

Étape 2

La table des ACL basées sur IPv4 affiche la liste de contrôle d'accès téléchargée.

# IPv4-Based ACL

## IPv4-Based ACL Table



ACL Name

Originators



redirect\_acl

Static



filter\_id\_acl

Static



xACSACLx-IP-ITACL-67a...

Dynamic



Auth-Default-ACL

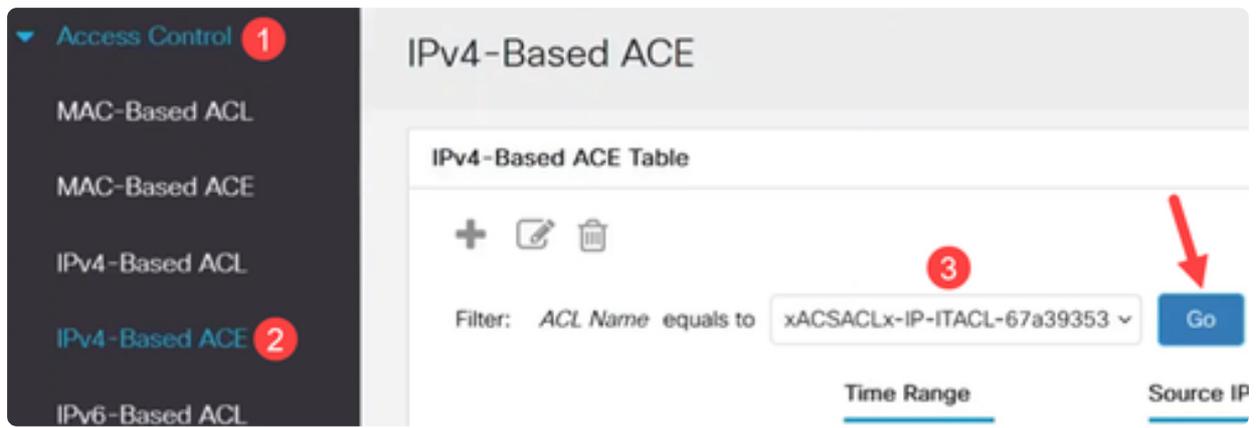
System

### Note:

Impossible de modifier les listes de contrôle d'accès téléchargeables.

### Étape 3

Une autre méthode de vérification consiste à accéder à l'ACE IPv4, à sélectionner la liste de contrôle d'accès téléchargeable dans le menu déroulant Nom de la liste de contrôle d'accès, puis à cliquer sur Exécuter. Les règles configurées dans ISE s'affichent.



#### Étape 4

Accédez au menu Security > 802.1 Authentication > Authenticated Hosts. Vous pouvez vérifier les utilisateurs qui sont authentifiés. Cliquez sur Authenticated Sessions pour afficher plus de détails.

## ▼ 802.1X Authentication

Properties

Port Authentication

Host and Session  
Authentication

Supplicant Credentials

**Authenticated Hosts**

### Étape 5

À partir de l'interface de ligne de commande, exécutez la commande `show ip access-lists interface` suivie de l'ID d'interface.

Dans cet exemple, les listes de contrôle d'accès et les ACE appliquées à Gigabit Ethernet 3 sont visibles.

```

switch4a7d55#show ip access-lists interface gel/0/3
ip access-list extended xACSACLx-IP-SalesACL-6760399d
  deny ip any host 192.168.251.10 ace-priority 1
  permit ip any any ace-priority 2
ip access-list extended Auth-Default-ACL
  permit udp any any any domain ace-priority 20
  permit tcp any any any domain ace-priority 40
  permit udp any bootps any any ace-priority 60
  permit udp any any any bootpc ace-priority 80
  permit udp any bootpc any any ace-priority 100
  deny ip any any ace-priority 120

```

## Étape 6

Vous pouvez également afficher les paramètres relatifs à la connexion ISE et aux téléchargements de listes de contrôle d'accès à l'aide de la commande

show dot1x sessions interface <ID> detailed. Vous pouvez afficher l'état, l'état d'authentification 802.1x et les listes de contrôle d'accès téléchargées.

```

switch4a7d55#show dot1x sessions interface gel/0/3 detailed

Interface: gil/0/3
MAC Address: e4: :31
IPv4 Address: 192.168.251.11
User-Name: user5
Status: Authorized
Oper host mode: multi-host
Session timeout: N/A
Session Uptime: 196 sec
Common Session ID: 14FBA8C00500032222C35D9E
Acct Session ID: 0x05000322
Server Policies:
  ACS ACL: xACSACLx-IP-SalesACL-6760399d

Method status list:
  Method      State
  802.1x      Authentication success

```

## Conclusion

Et voilà ! Allez ! Vous savez maintenant comment les listes de contrôle d'accès téléchargeables fonctionnent sur les commutateurs Cisco Catalyst 1300 avec Cisco ISE.

Pour plus d'informations, consultez le [Guide d'administration de Catalyst 1300](#) et la [page de support de la gamme Cisco Catalyst 1300](#).

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.