Configurer l'authentification à deux facteurs de la machine pour l'accès demandeur

Table des matières

Introduction

Ce document décrit les étapes requises pour configurer l'authentification à deux facteurs avec l'authentification machine et dot1x.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de Cisco Identity Services Engine
- Configuration de Cisco Catalyst
- IEEE802.1X

Composants utilisés

- Correctif 1 d'Identity Services Engine Virtual 3.3
- C1000-48FP-4G-L 15.2(7)E9

- Windows Server 2019

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.

Diagramme du réseau

Cette image présente la topologie utilisée pour l'exemple de ce document.

Le nom de domaine configuré sur Windows Server 2019 est ad.rem-xxx.com, qui est utilisé comme exemple dans ce document.

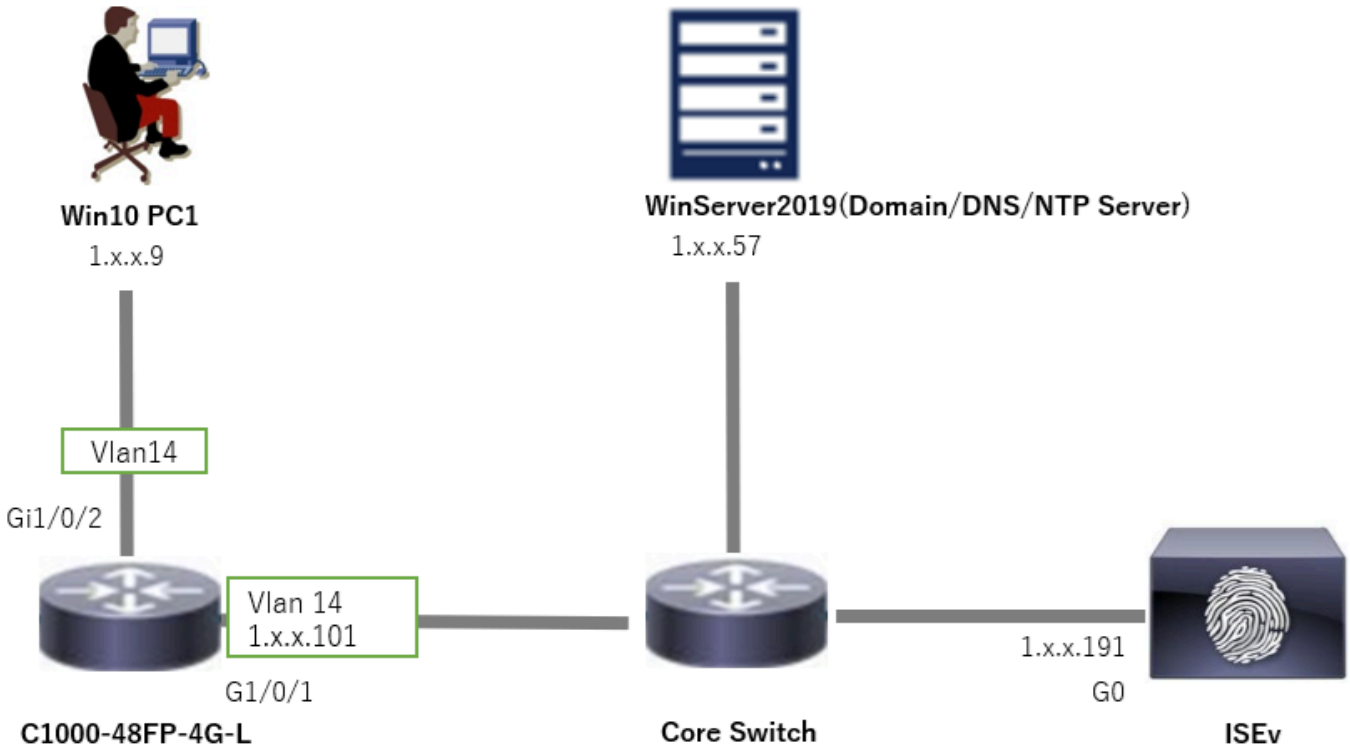


Diagramme du réseau

Informations générales

L'authentification de machine est un processus de sécurité qui vérifie l'identité d'un périphérique cherchant à accéder à un réseau ou à un système. Contrairement à l'authentification des utilisateurs, qui vérifie l'identité d'une personne en se basant sur des informations d'identification telles qu'un nom d'utilisateur et un mot de passe, l'authentification des ordinateurs se concentre sur la validation du périphérique lui-même. Cette opération est souvent effectuée à l'aide de certificats numériques ou de clés de sécurité uniques au périphérique.

En utilisant conjointement l'authentification des machines et des utilisateurs, une entreprise peut s'assurer que seuls les périphériques et les utilisateurs autorisés peuvent accéder à son réseau, offrant ainsi un environnement plus sécurisé. Cette méthode d'authentification à deux facteurs est particulièrement utile pour protéger les informations sensibles et respecter des normes réglementaires strictes.

Configurations

Configuration dans C1000

Il s’agit de la configuration minimale de l’interface de ligne de commande C1000.

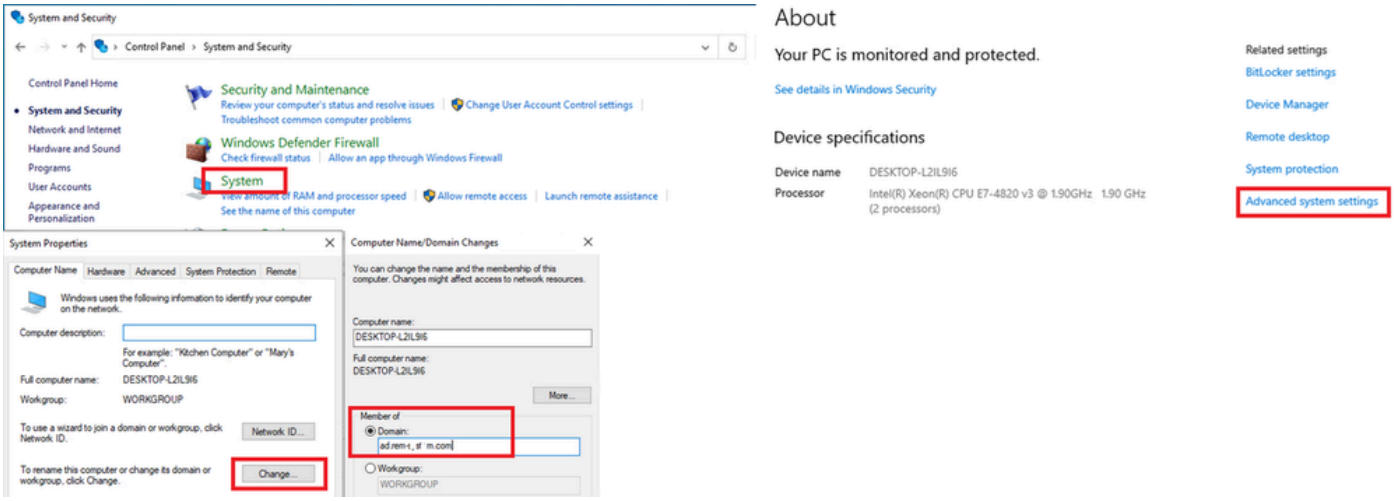
```
aaa new-model

radius server ISE33
address ipv4 1.x.x.191
```

```
key cisco123

aaa group server radius AAASERVER
server name ISE33

aaa authentication dot1x default group AAASERVER
aaa authorization network default group AAASERVER
aaa accounting dot1x default start-stop group AAASERVER
dot1x system-auth-control

interface Vlan14
ip address 1.x.x.101 255.0.0.0

interface GigabitEthernet1/0/1
switchport access vlan 14
switchport mode access

interface GigabitEthernet1/0/2
switchport access vlan 14
switchport mode access
authentication host-mode multi-auth
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
```

Configuration dans le PC Windows

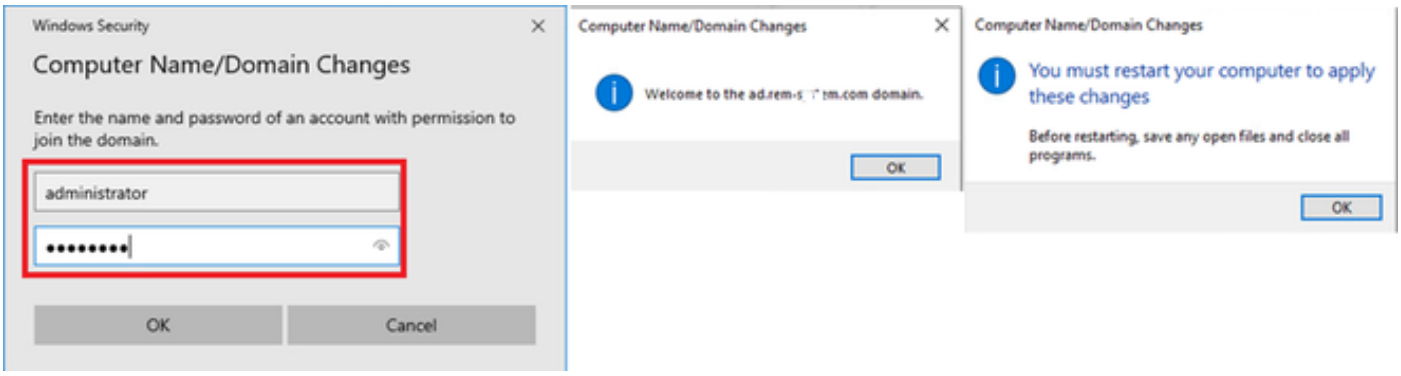
Étape 1. Ajouter un PC au domaine AD

Accédez à Panneau de configuration > Système et sécurité, cliquez sur Système, puis cliquez sur Paramètres système avancés. Dans la fenêtre Propriétés système, cliquez sur Modifier, sélectionnez Domaine et entrez le nom de domaine.



Ajouter un PC au domaine AD

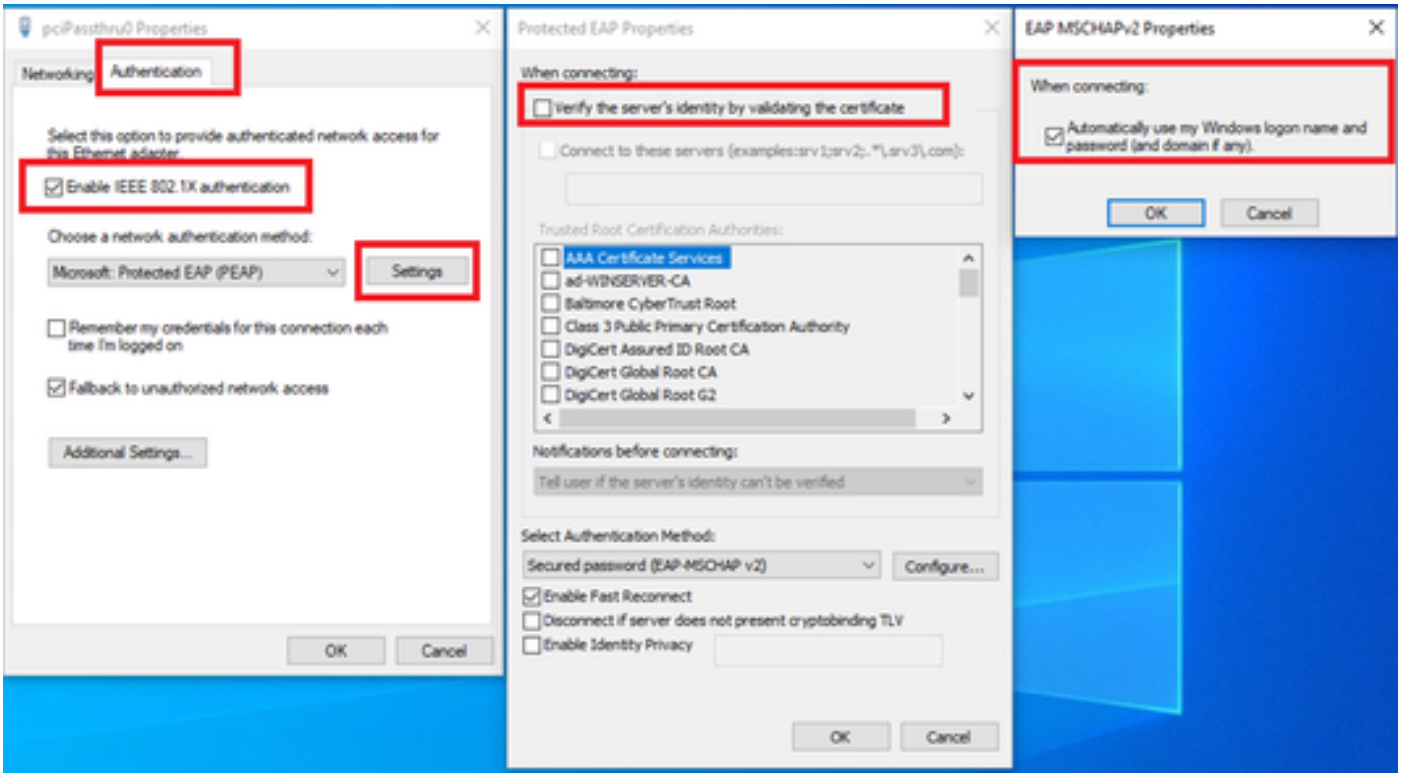
Dans la fenêtre Sécurité Windows, entrez le nom d'utilisateur et le mot de passe du serveur de domaine.



Nom d'utilisateur et mot de passe

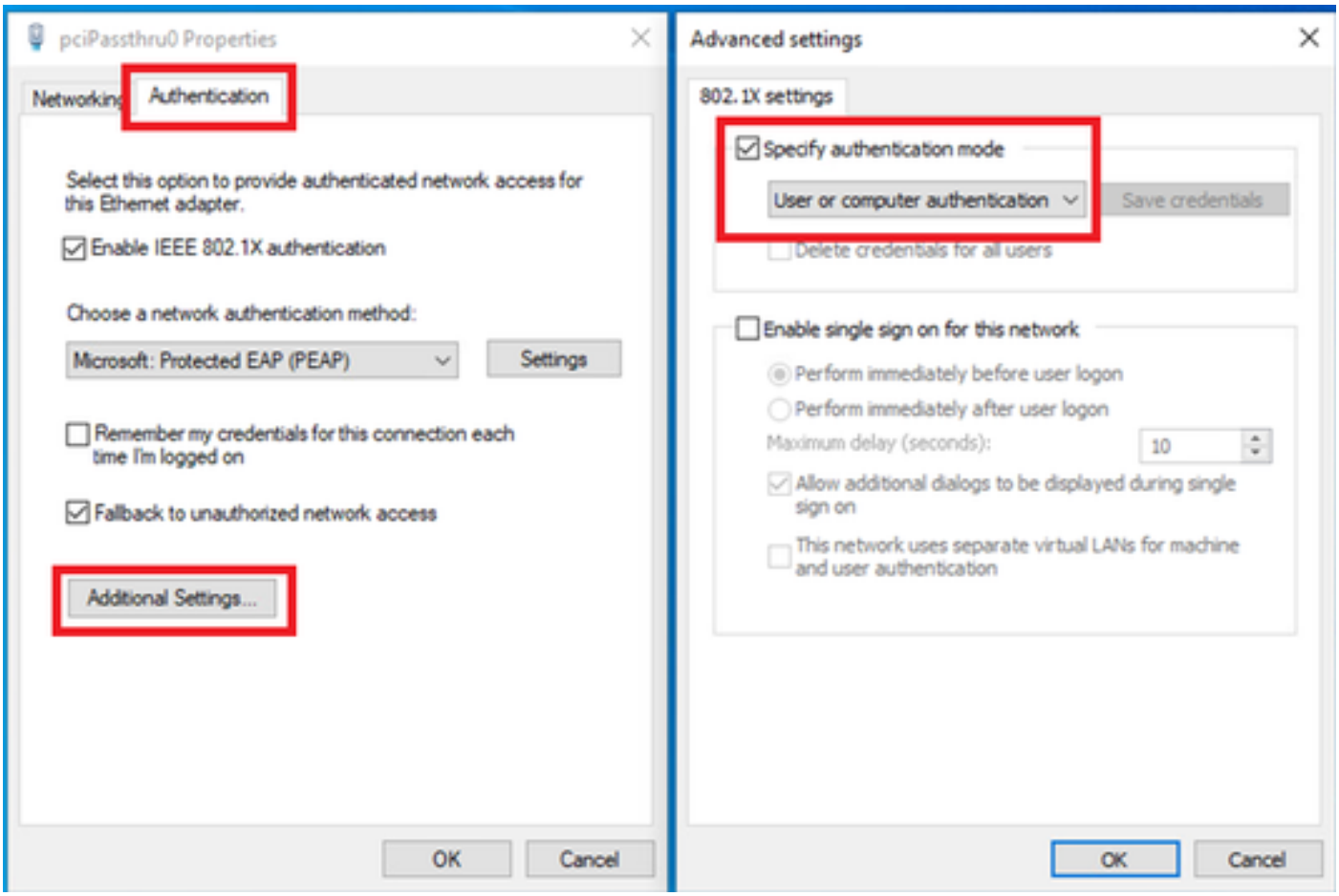
Étape 2. Configurer l'authentification utilisateur

Accédez à Authentication, cochez Enable IEEE 802.1X authentication. Cliquez sur Settings dans la fenêtre Protected EAP Properties, décochez Verify the server's identity by validating the certificate, puis cliquez sur Configure. Dans la fenêtre Propriétés de EAP MSCHAPv2, cochez Utiliser automatiquement mon nom d'ouverture de session Windows et mon mot de passe (et le domaine s'il y a lieu) pour utiliser le nom d'utilisateur saisi lors de la connexion de l'ordinateur Windows pour l'authentification de l'utilisateur.



Activer l'authentification utilisateur

Accédez à Authentication, cochez Additional Settings. Sélectionnez Authentification utilisateur ou ordinateur dans la liste déroulante.

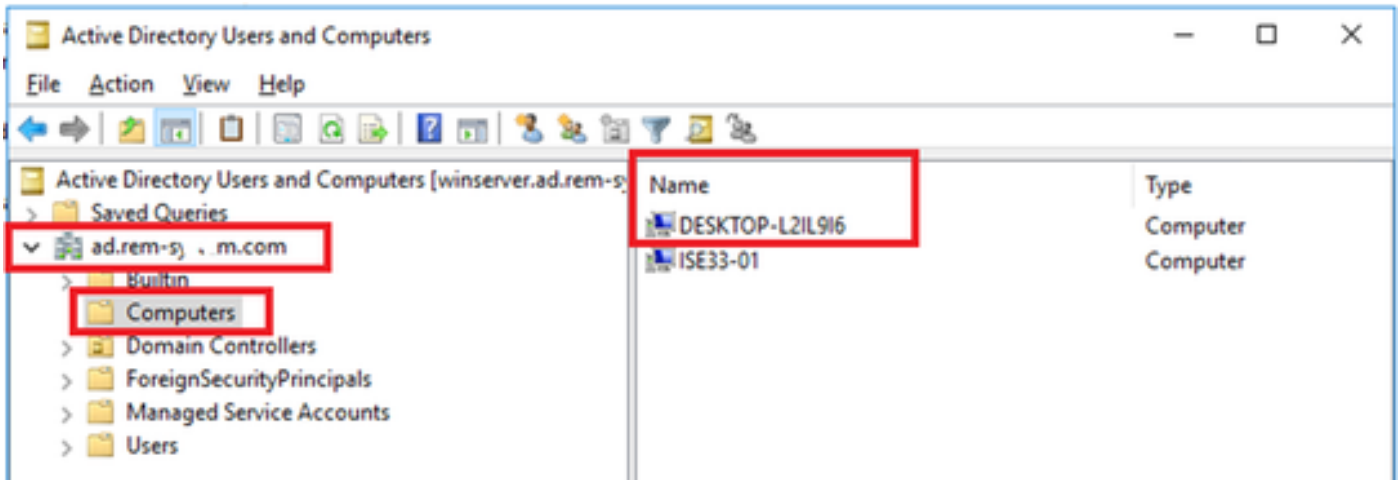


Spécifier le mode d'authentification

Configuration dans Windows Server

Étape 1. Confirmer les ordinateurs du domaine

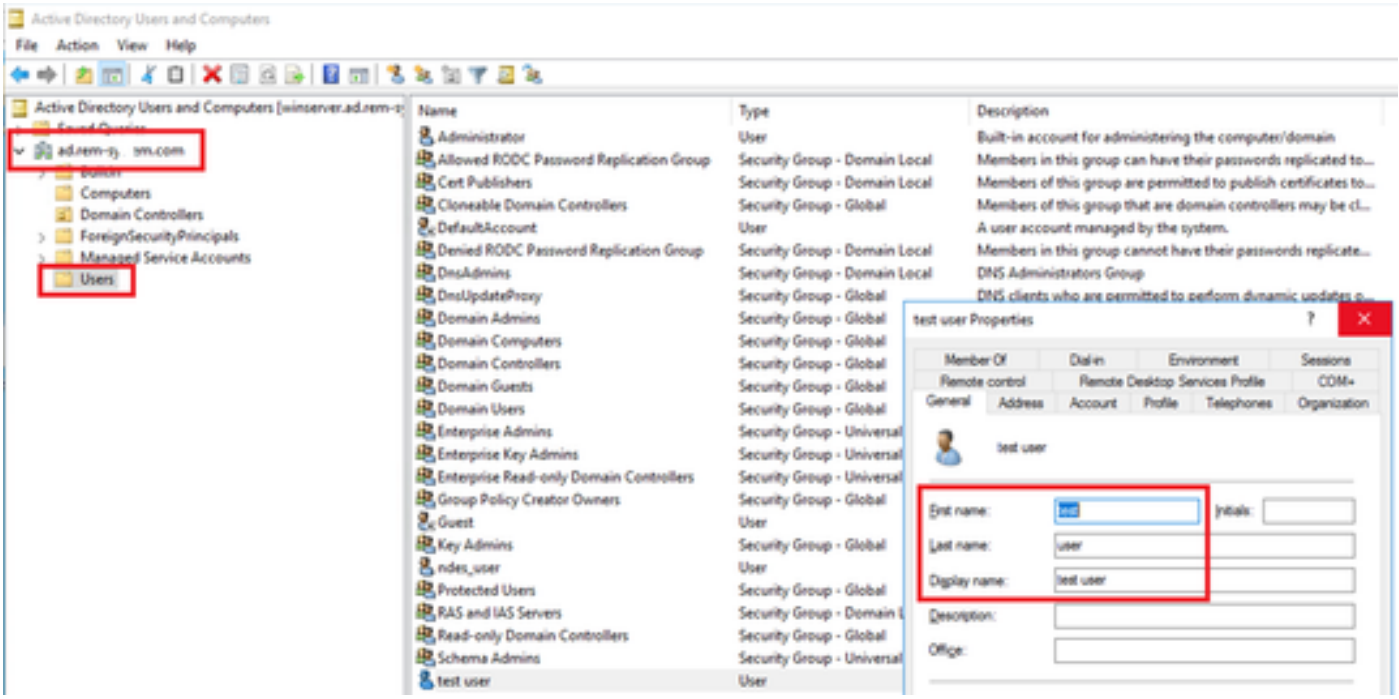
Accédez à Utilisateurs et ordinateurs Active Directory, cliquez sur Ordinateurs. Vérifiez que Win10 PC1 est répertorié dans le domaine.



Confirmer l'ordinateur du domaine

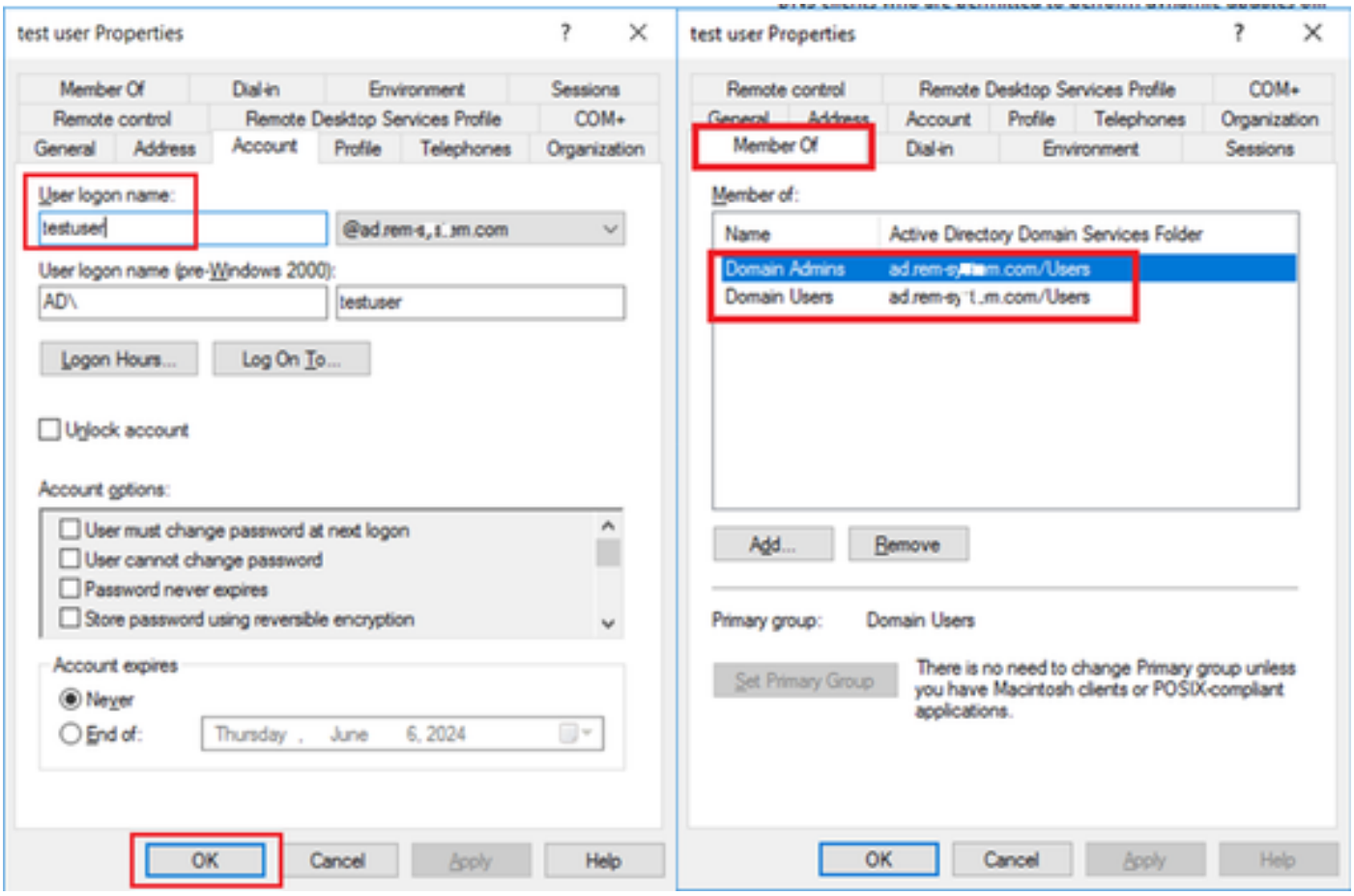
Étape 2. Ajouter un utilisateur de domaine

Accédez à Utilisateurs et ordinateurs Active Directory, cliquez sur Utilisateurs. Ajoutez testuser en tant qu'utilisateur de domaine.



Ajouter un utilisateur de domaine

Ajoutez l'utilisateur du domaine aux membres Admins du domaine et Utilisateurs du domaine.

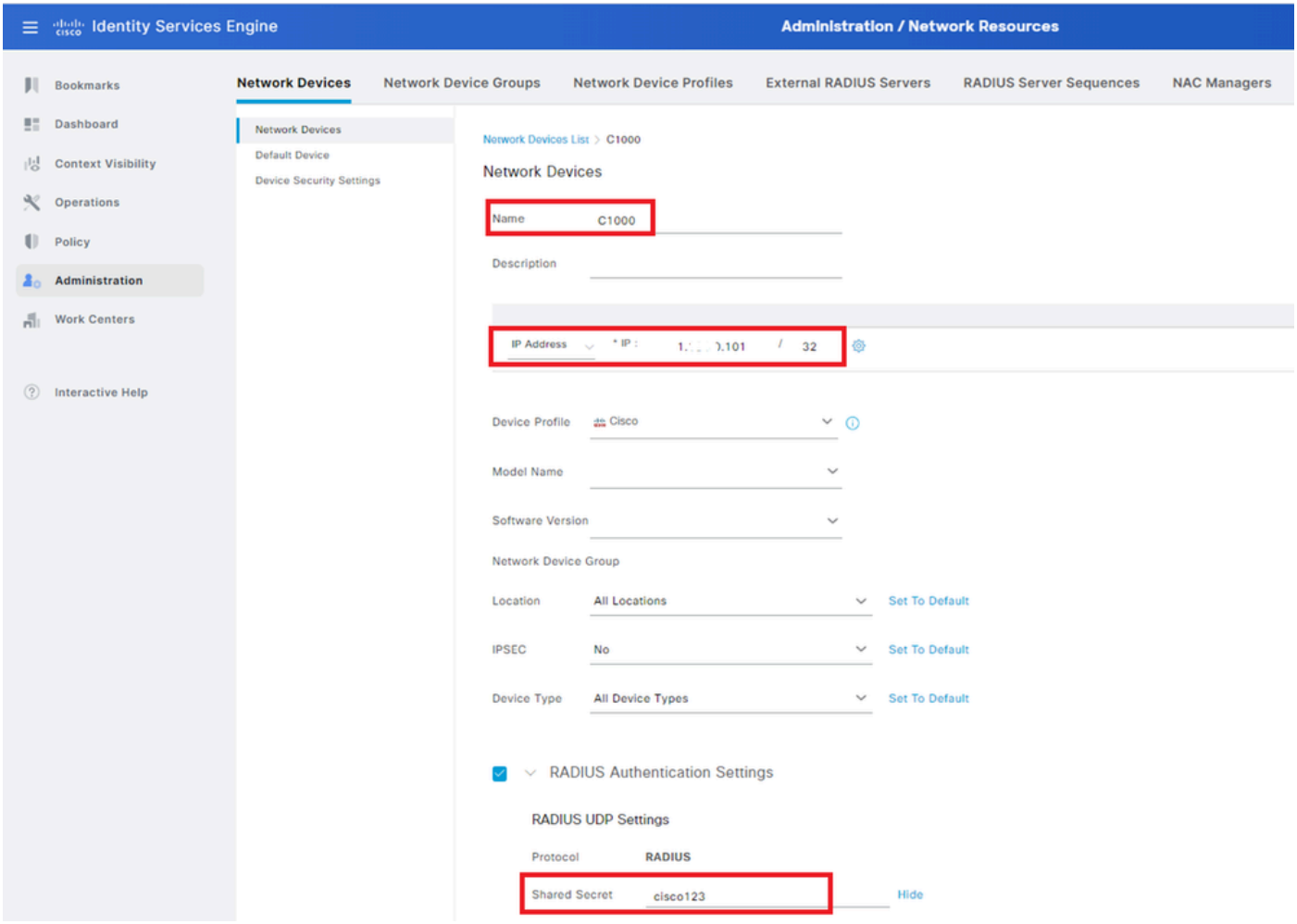


Administrateurs de domaine et utilisateurs de domaine

Configuration dans ISE

Étape 1. Ajouter un périphérique

Accédez à Administration > Network Devices, cliquez sur Add button to add C1000 device.

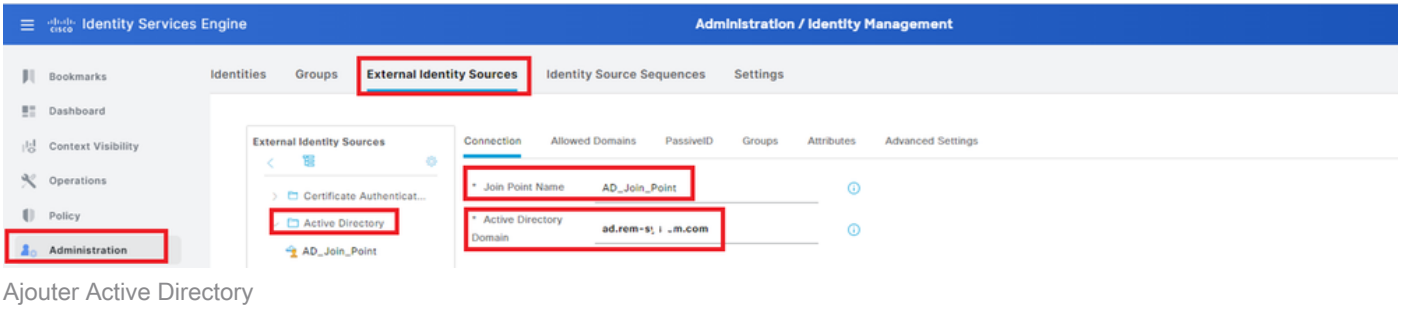


Ajouter un périphérique

Étape 2. Ajouter Active Directory

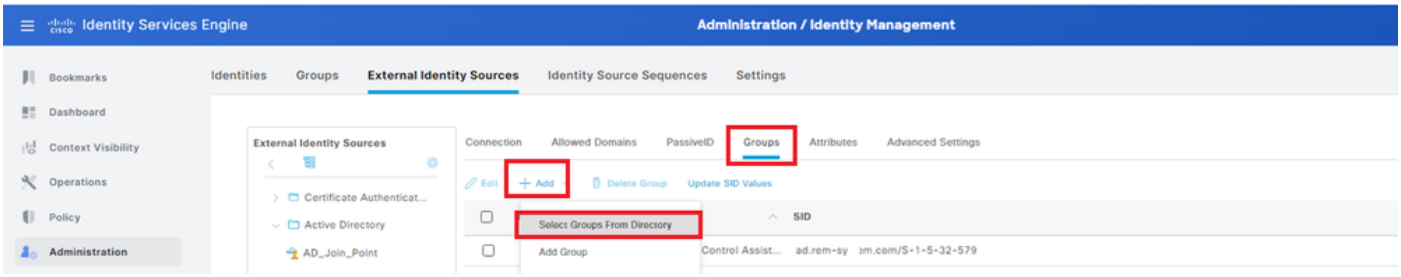
Accédez à Administration > External Identity Sources > Active Directory, cliquez sur l'onglet Connection, ajoutez Active Directory à ISE.

- Nom du point de jointure : AD_Join_Point
- Domaine Active Directory : ad.rem-xxx.com



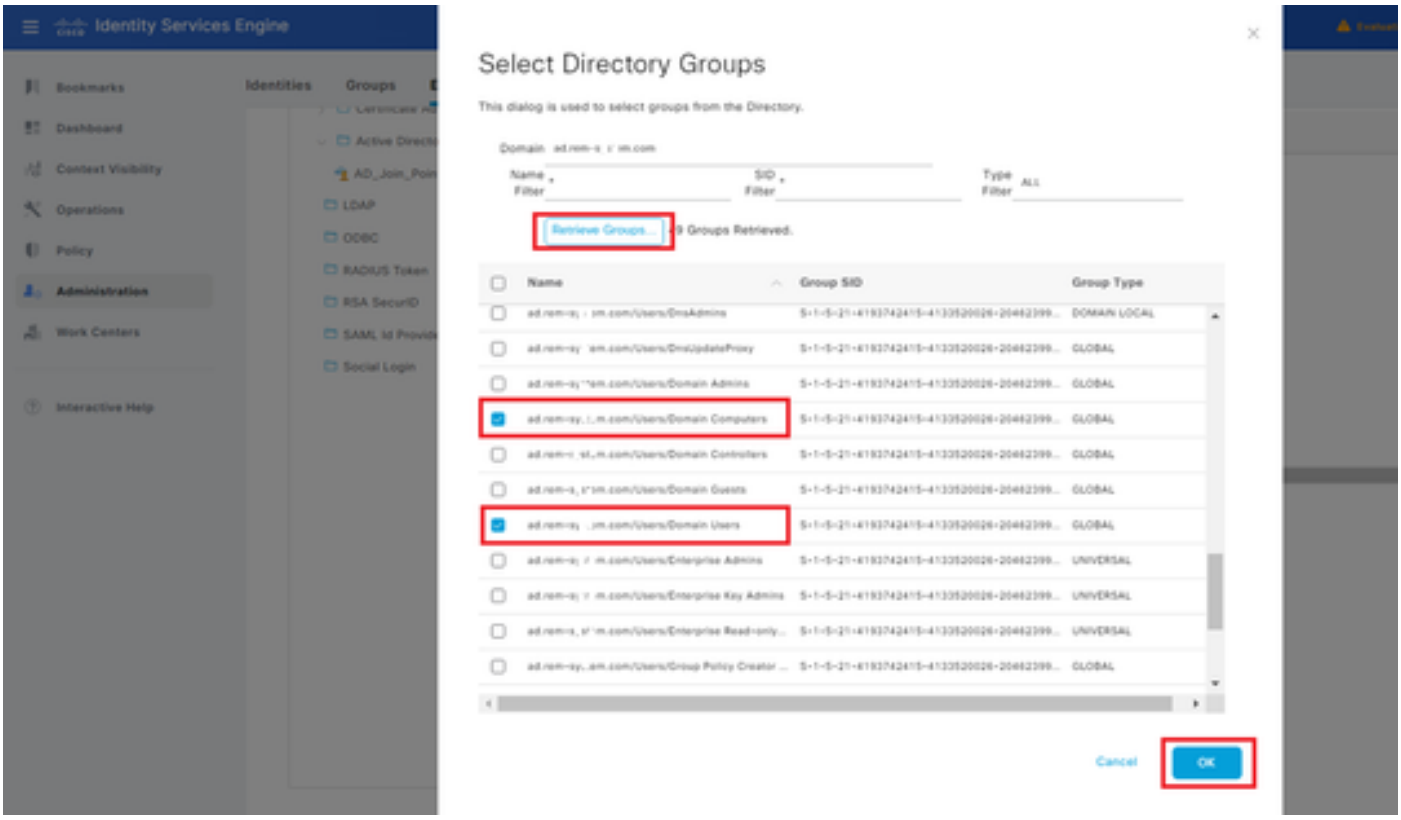
Ajouter Active Directory

Accédez à l'onglet Groups, sélectionnez Select Groups From Directory dans la liste déroulante.



Sélectionner des groupes dans le répertoire

Cliquez sur Récupérer des groupes dans la liste déroulante. Cochez ad.rem-xxx.com/Users/Domain Computers et ad.rem-xxx.com/Users/Domain Users et cliquez sur OK.

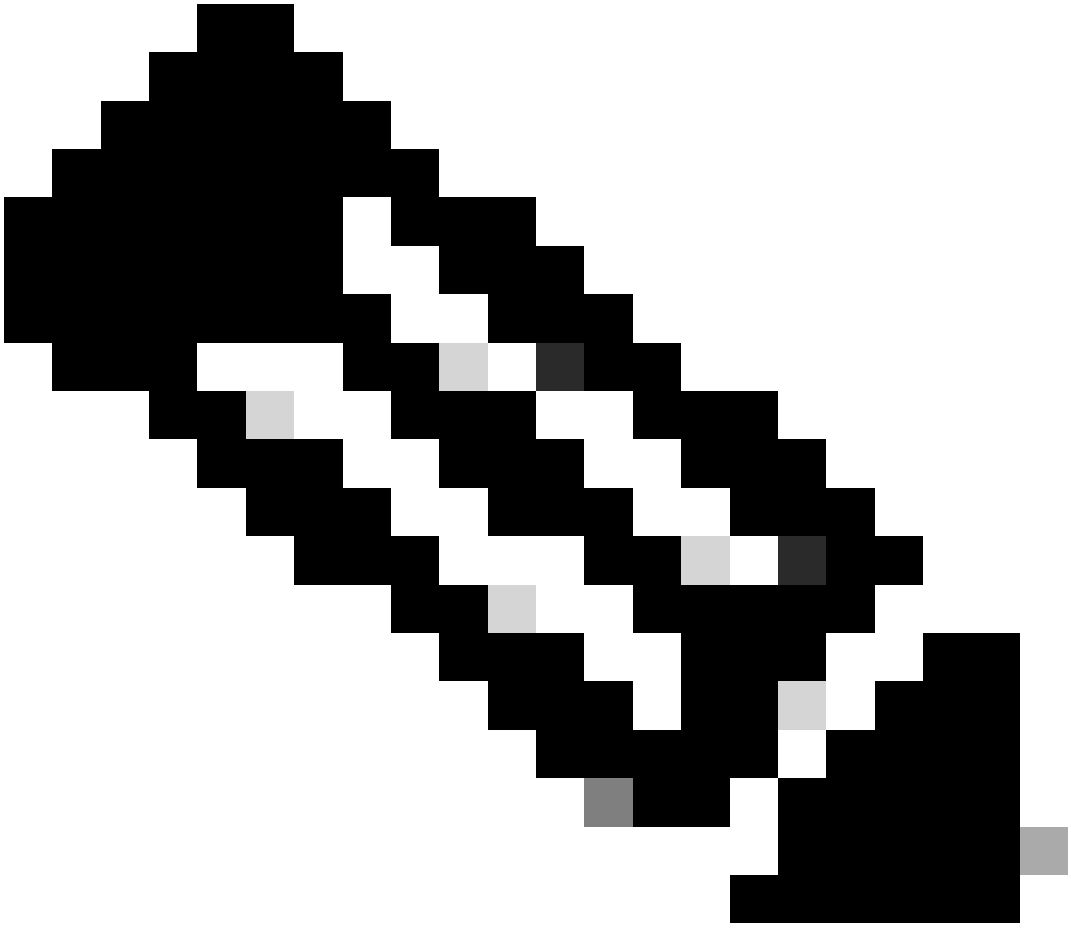


Ajouter des ordinateurs et des utilisateurs de domaine

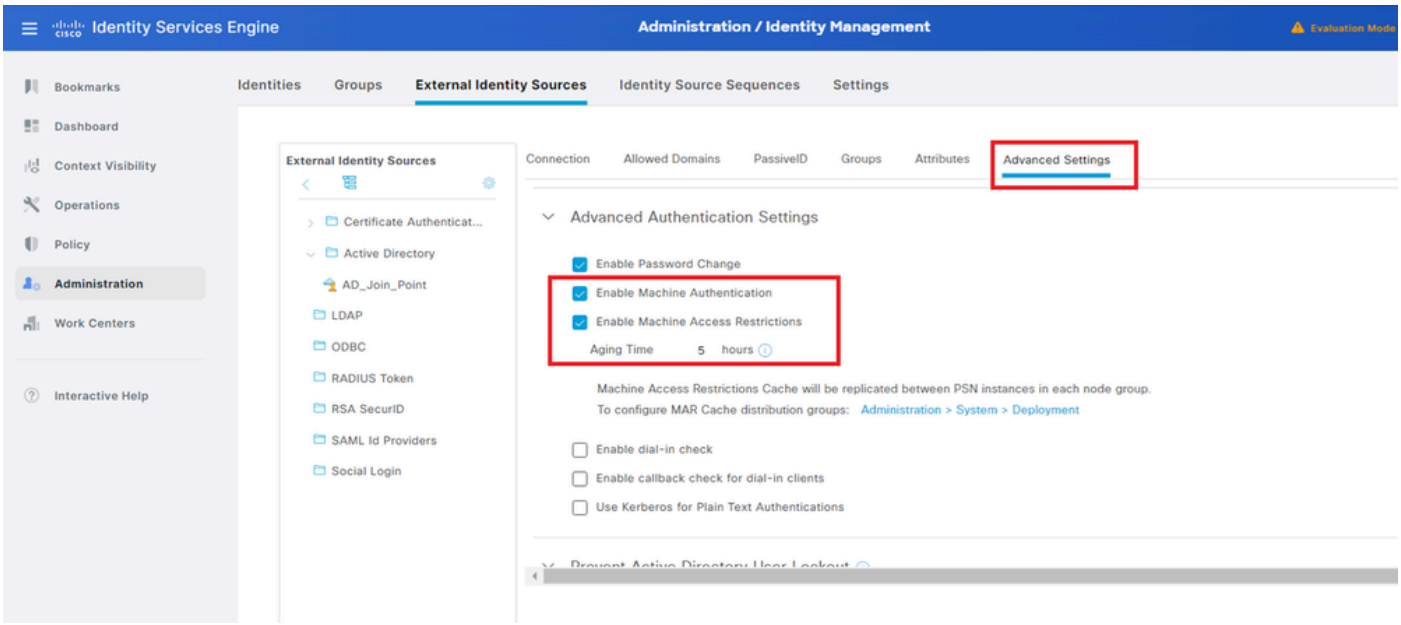
Étape 3. Confirmer le paramètre d'authentification ordinateur

Accédez à l'onglet Advanced Settings, confirmez le paramètre de l'authentification de l'ordinateur.

- Enable Machine Authentication : pour activer l'authentification de l'ordinateur
- Enable Machine Access Restriction : pour combiner l'authentification des utilisateurs et des ordinateurs avant l'autorisation



Remarque : la plage de temps de vieillissement valide est comprise entre 1 et 8 760.

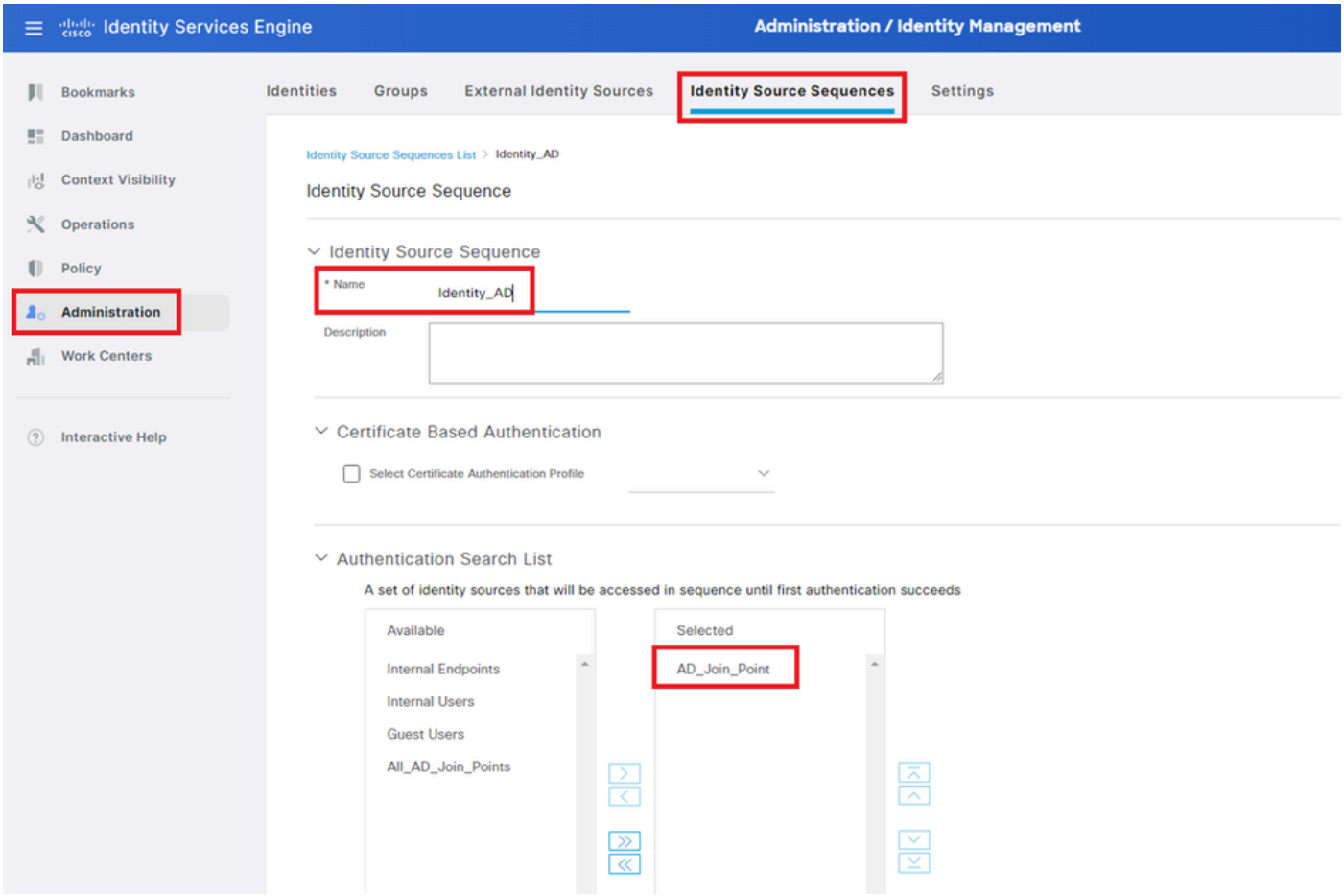


Paramètre d'authentification machine

Étape 4. Ajouter des séquences source d'identité

Accédez à Administration > Identity Source Sequences, ajoutez une Identity Source Sequence.

- Nom : Identity_AD
- Liste de recherche d'authentification : AD_Join_Point

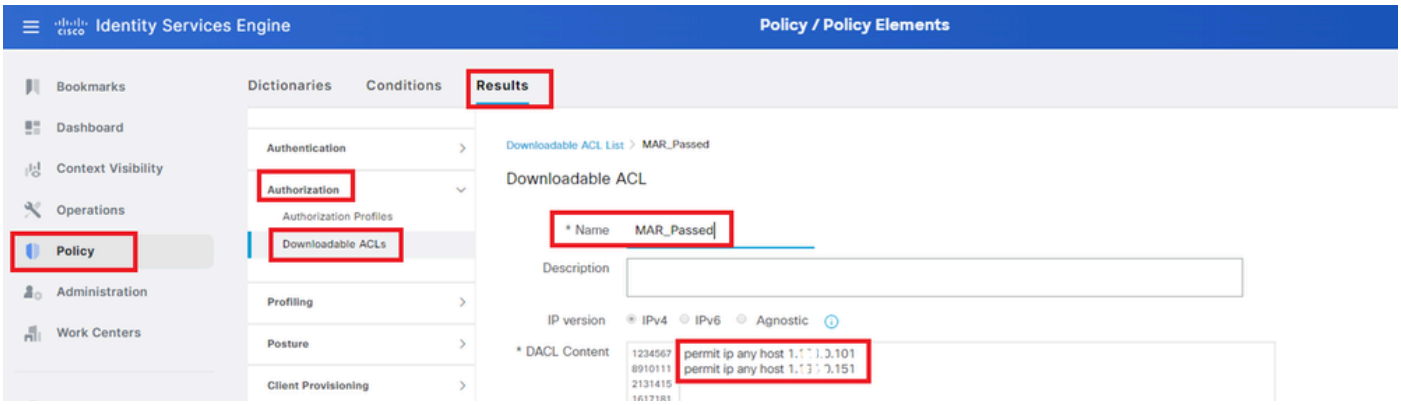


Ajouter des séquences source d'identité

Étape 5. Ajouter une DACL et un profil d'autorisation

Accédez à Policy > Results > Authorization > Downloadable ACLs, ajoutez une DACL.

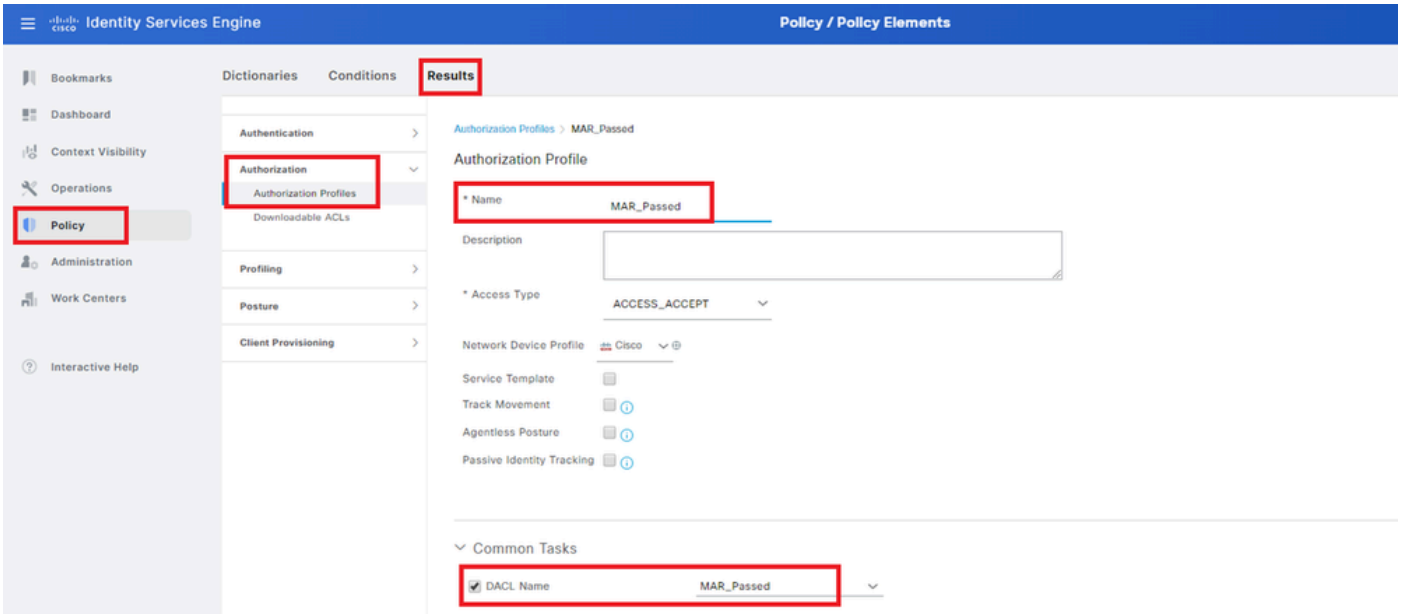
- Nom : MAR_Passed
- Contenu DACL : permit ip any host 1.x.x.101 et permit ip any host 1.x.x.105



Ajouter une DACL

Accédez à Policy > Results > Authorization > Authorization Profiles, ajoutez un profil d'autorisation.

- Nom : MAR_Passed
- Nom DACL : MAR_Passed

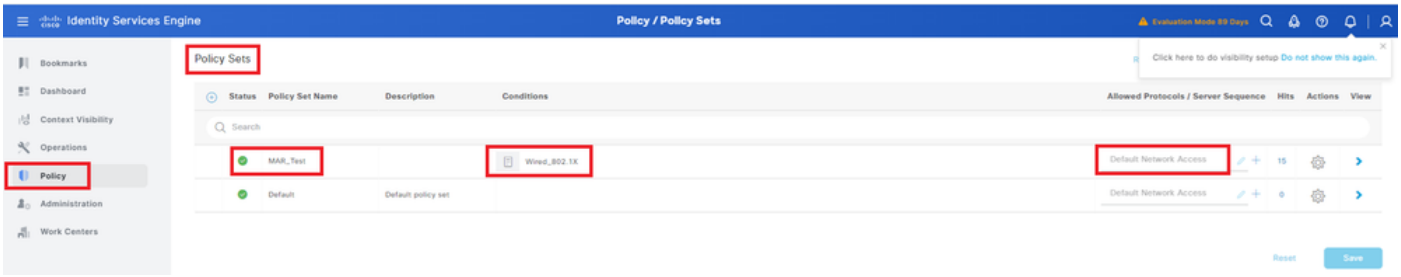


Ajouter un profil d'autorisation

Étape 6. Ajouter un jeu de stratégies

Accédez à Policy > Policy Sets, cliquez sur + pour ajouter un jeu de stratégies.

- Nom du jeu de stratégies : MAR_Test
- Conditions : Wired_802.1X
- Protocoles autorisés / Séquence de serveurs : Accès réseau par défaut

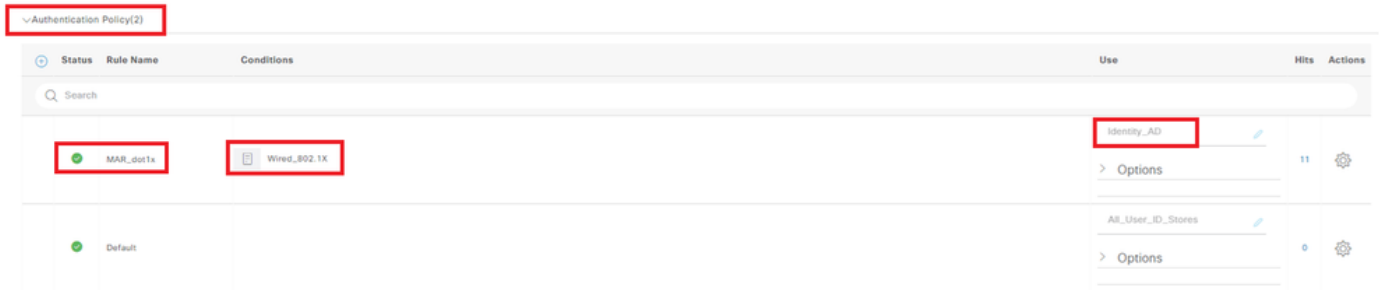


Ajouter un jeu de stratégies

Étape 7. Ajouter une stratégie d'authentification

Accédez à Jeux de stratégies, cliquez sur MAR_Test pour ajouter une stratégie d'authentification.

- Nom de la règle : MAR_dot1x
- Conditions : Wired_802.1X
- Utiliser : Identity_AD



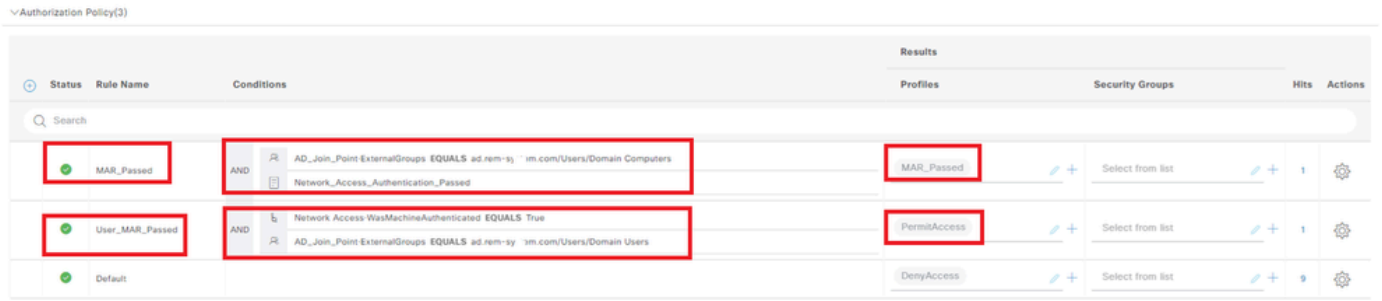
Ajouter une stratégie d'authentification

Étape 8. Ajouter une stratégie d'autorisation

Accédez à Jeux de stratégies, cliquez sur MAR_Test pour ajouter une stratégie d'autorisation.

- Nom de la règle : MAR_Passed
- Conditions : AD_Join_Point·ExternalGroups ÉGALE ad.rem-xxx.com/Users/Domain Ordinateurs ET Network_Access_Authentication_Passed
- Résultats : MAR_Passed

- Nom de la règle : User_MAR_Passed
- Conditions : Accès réseau·WasMachineAuthenticated EQUALS True ET AD_Join_Point·ExternalGroups EQUALS ad.rem-xxx.com/Users/Domain Utilisateurs
- Résultats : PermitAccess



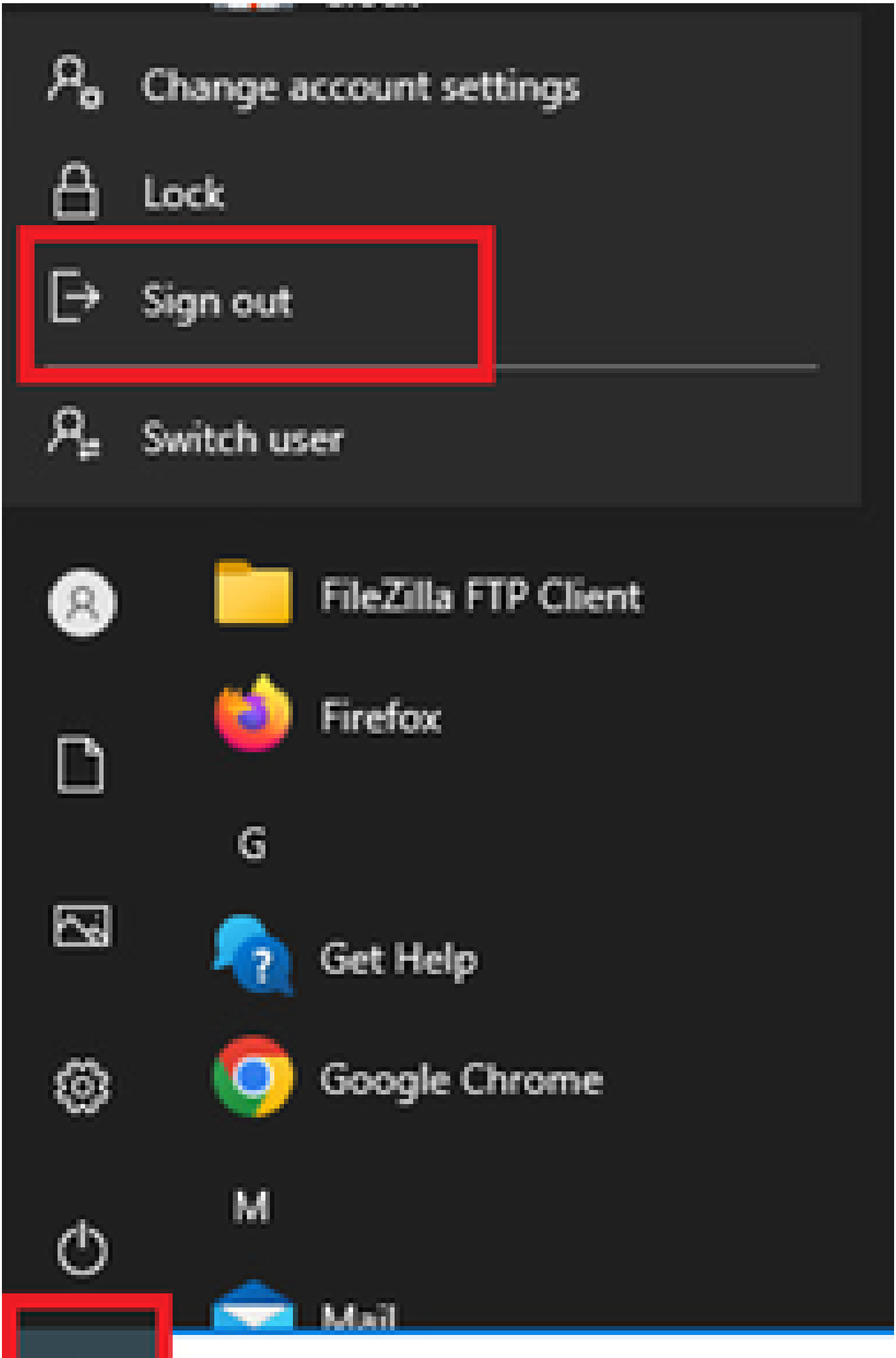
Ajouter une stratégie d'autorisation

Vérifier

Modèle 1. Authentification des ordinateurs et des utilisateurs

Étape 1. Se déconnecter d'un PC Windows

Cliquez sur le bouton Déconnexion de Win10 PC1 pour déclencher l'authentification de l'ordinateur.


Change account settings
Lock
Sign out
Switch user
FileZilla FTP Client
Firefox
G
Get Help
Google Chrome
M
Mail

show authentication sessions interface GigabitEthernet1/0/2 details la commande pour confirmer la session d'authentification de la machine dans C1000.

<#root>

Switch#

show authentication sessions interface GigabitEthernet1/0/2 details

Interface: GigabitEthernet1/0/2
MAC Address: b496.9115.84cb
IPv6 Address: Unknown
IPv4 Address: 1.x.x.9
User-Name:

host/DESKTOP-L2IL9I6.ad.rem-xxx.com

Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 5s
Common Session ID: 01C2006500000049AA780D80
Acct Session ID: 0x0000003C
Handle: 0x66000016
Current Policy: POLICY_Gi1/0/2

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

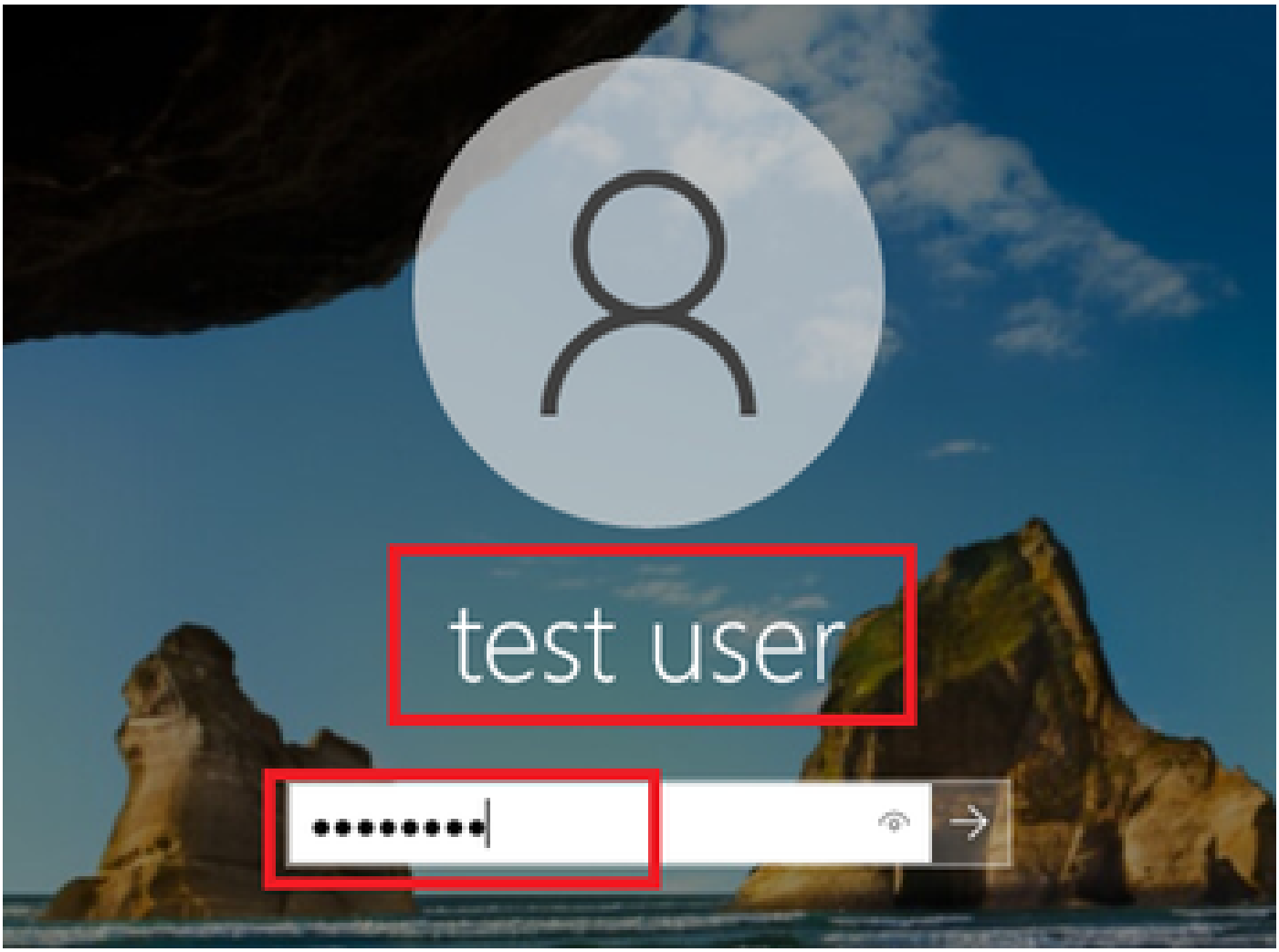
Server Policies:
ACS ACL: xACSACLx-IP-MAR_Passed-6639ba20

Method status list:
Method State

dot1x Authc Success

Étape 3. Connexion au PC Windows

Connectez-vous à Win10 PC1, entrez le nom d'utilisateur et le mot de passe pour déclencher l'authentification utilisateur.



Connexion au PC Windows

Étape 4. Confirmer la session d'authentification

Exécutez show authentication sessions interface GigabitEthernet1/0/2 details la commande pour confirmer la session d'authentification utilisateur dans C1000.

<#root>

Switch#

show authentication sessions interface GigabitEthernet1/0/2 details

```
Interface: GigabitEthernet1/0/2
MAC Address: b496.9115.84cb
IPv6 Address: Unknown
IPv4 Address: 1.x.x.9
User-Name:
```

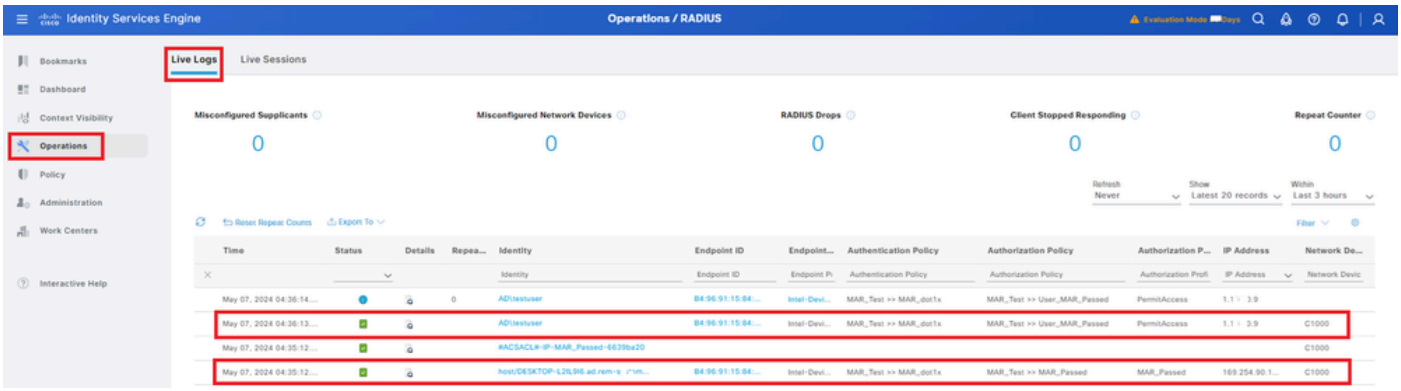
AD\testuser

```
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
```

```
Session timeout: N/A
Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 85s
Common Session ID: 01C2006500000049AA780D80
Acct Session ID: 0x0000003D
Handle: 0x66000016
Current Policy: POLICY_Gi1/0/2

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:


Method status list:
Method State

dot1x Authc Success
```

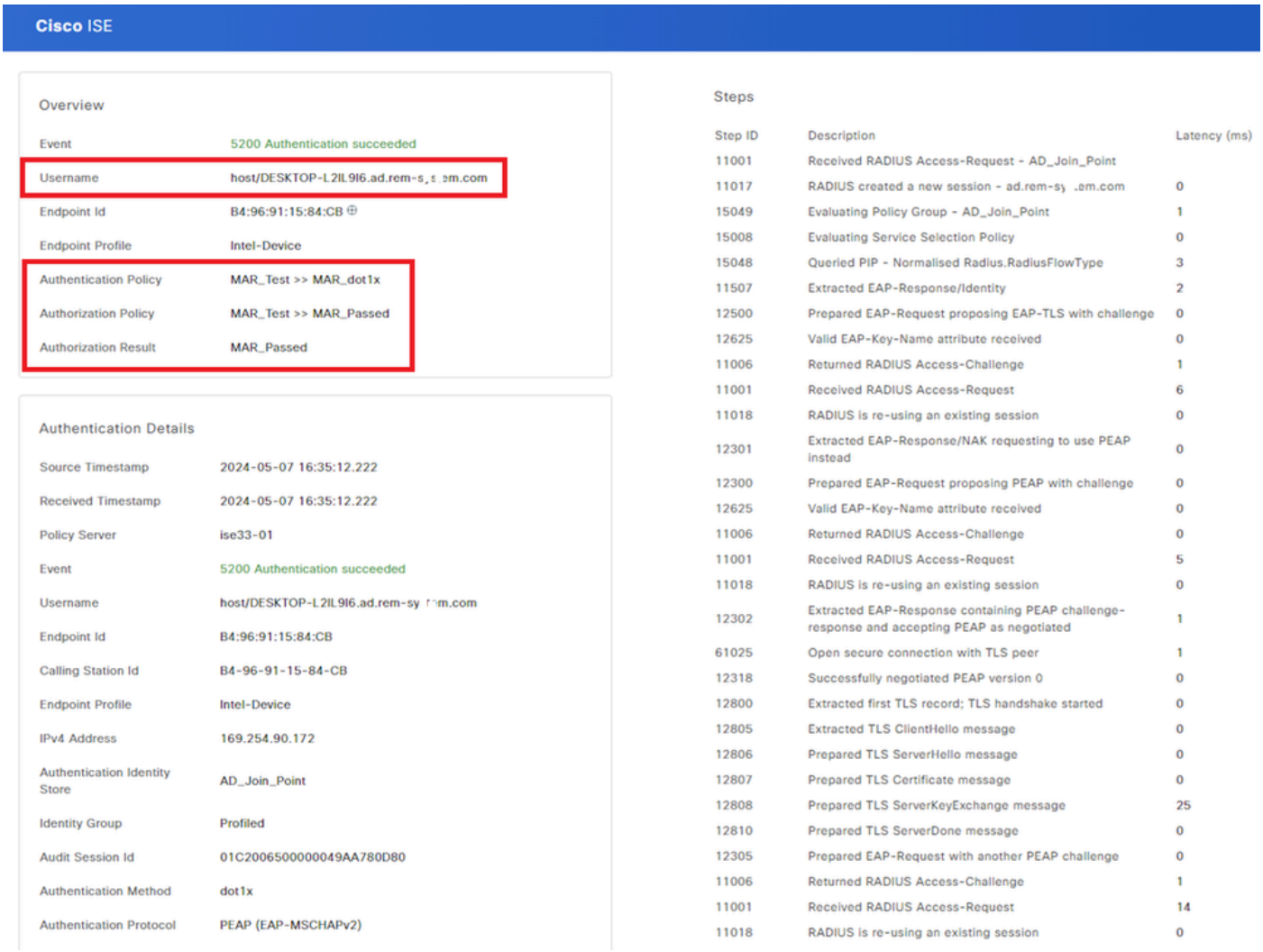
Étape 5. Confirmer le journal Radius en direct

Accédez à **Operations > RADIUS > Live Logs** dans l'interface utilisateur graphique ISE, confirmez le journal en direct pour l'authentification de la machine et l'authentification de l'utilisateur.



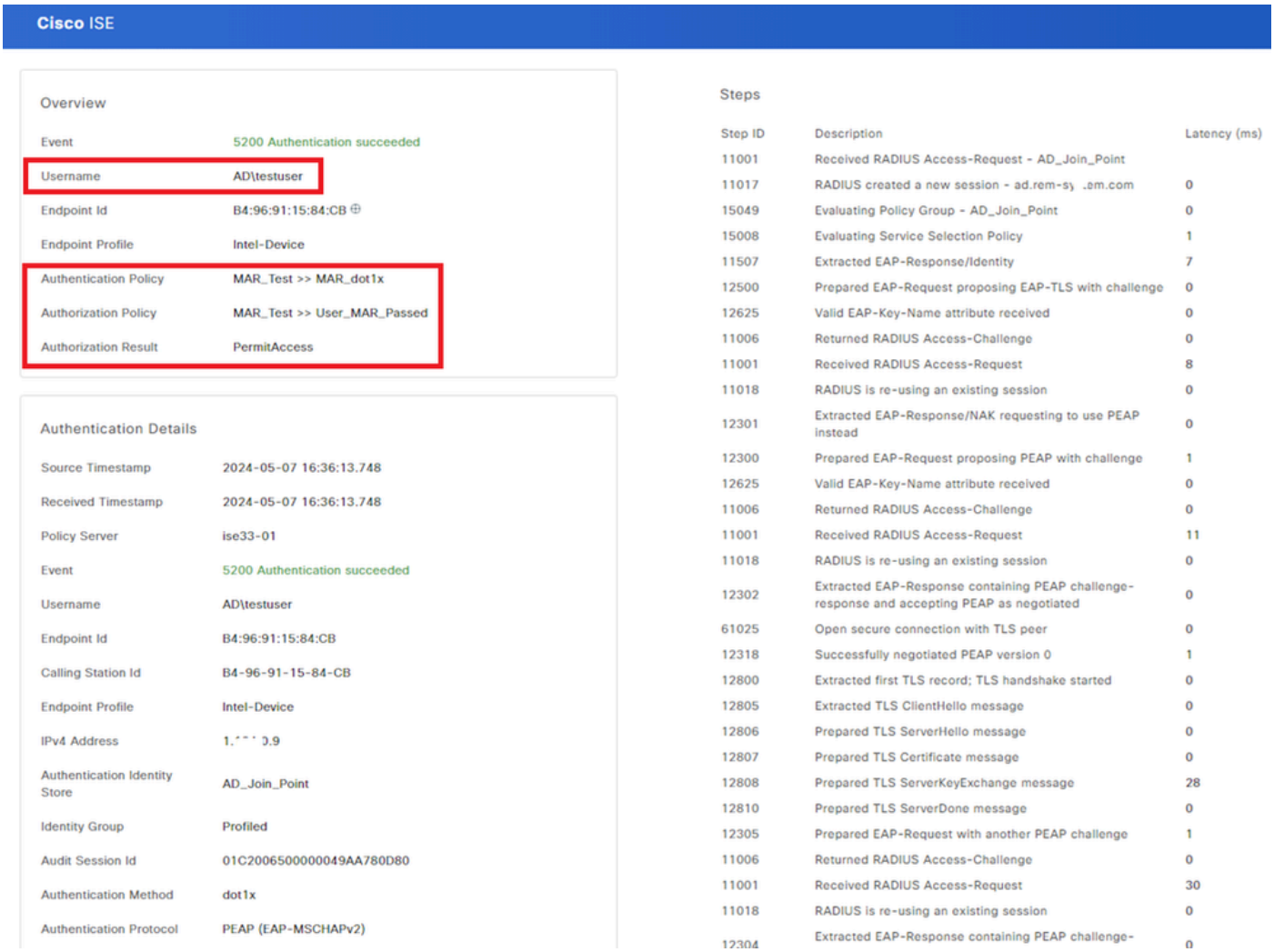
Journal Radius Live

Confirmez le journal en direct détaillé de l'authentification de la machine.



Détail de l'authentification machine

Confirmez le journal en direct détaillé de l'authentification utilisateur.



Détail de l'authentification utilisateur

Modèle 2. Authentification utilisateur uniquement

Étape 1. Désactiver et activer la carte réseau du PC Windows

Afin de déclencher l'authentification de l'utilisateur, désactivez et activez la carte réseau de Win10 PC1.

Étape 2. Confirmer la session d'authentification

Exécutez show authentication sessions interface GigabitEthernet1/0/2 details la commande pour confirmer la session d'authentification utilisateur dans C1000.

<#root>

Switch#

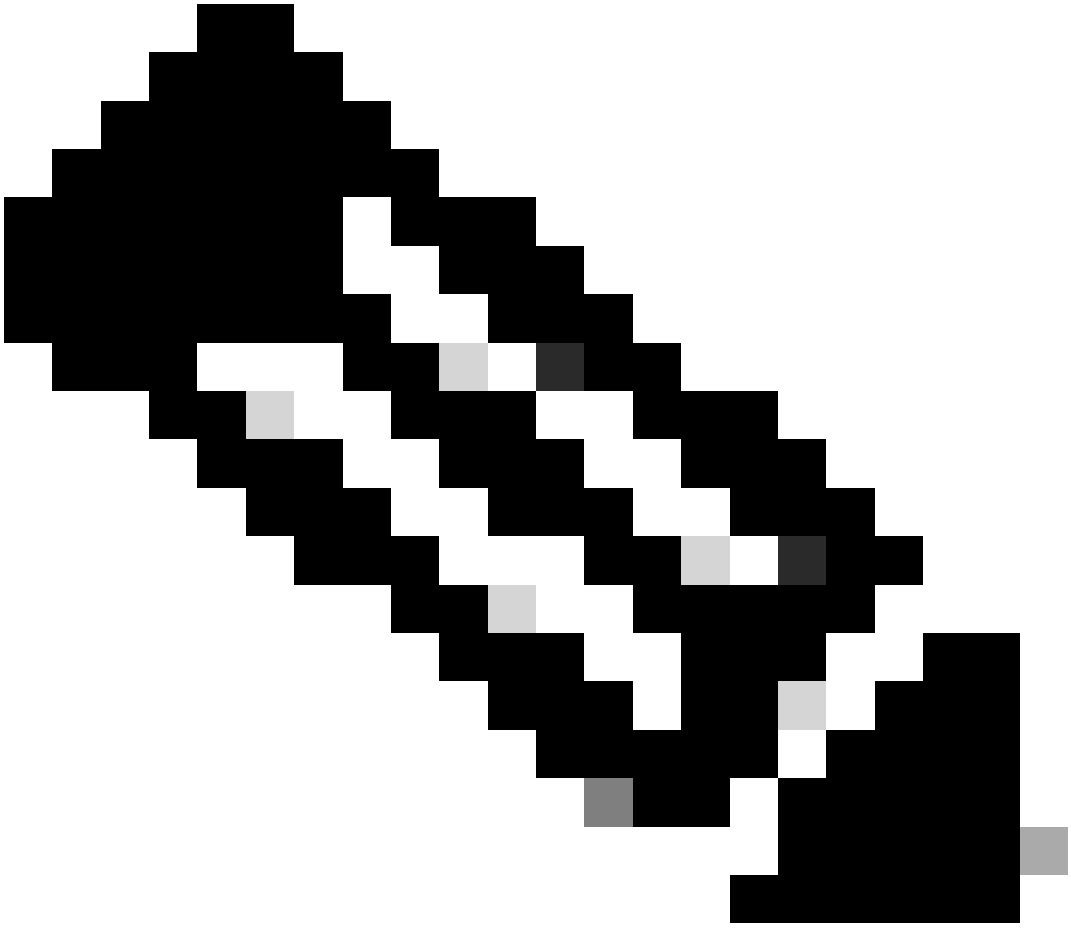
show authentication sessions interface GigabitEthernet1/0/2 details

```
Interface: GigabitEthernet1/0/2
MAC Address: b496.9115.84cb
IPv6 Address: Unknown
IPv4 Address: 1.x.x.9
```

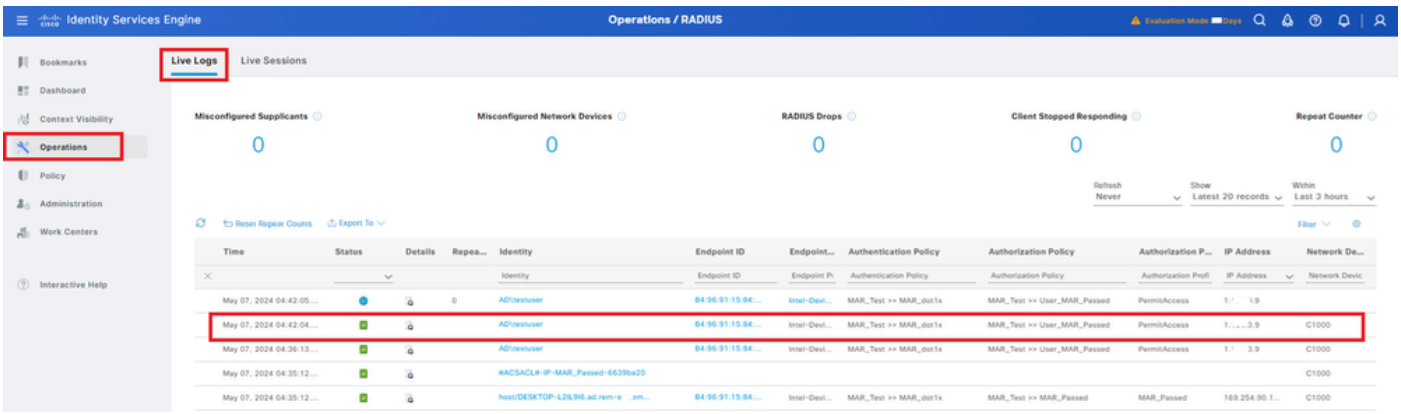
```
User-Name: AD\testuser
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 419s
Common Session ID: 01C2006500000049AA780D80
Acct Session ID: 0x0000003D
Handle: 0x66000016
Current Policy: POLICY_Gi1/0/2

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:


Method status list:
Method State

dot1x Authc Success
```

Étape 3. Confirmer le journal Radius en direct

Accédez à **Operations > RADIUS > Live Logs** dans l'interface utilisateur graphique ISE, confirmez le journal en direct pour l'authentification de l'utilisateur.

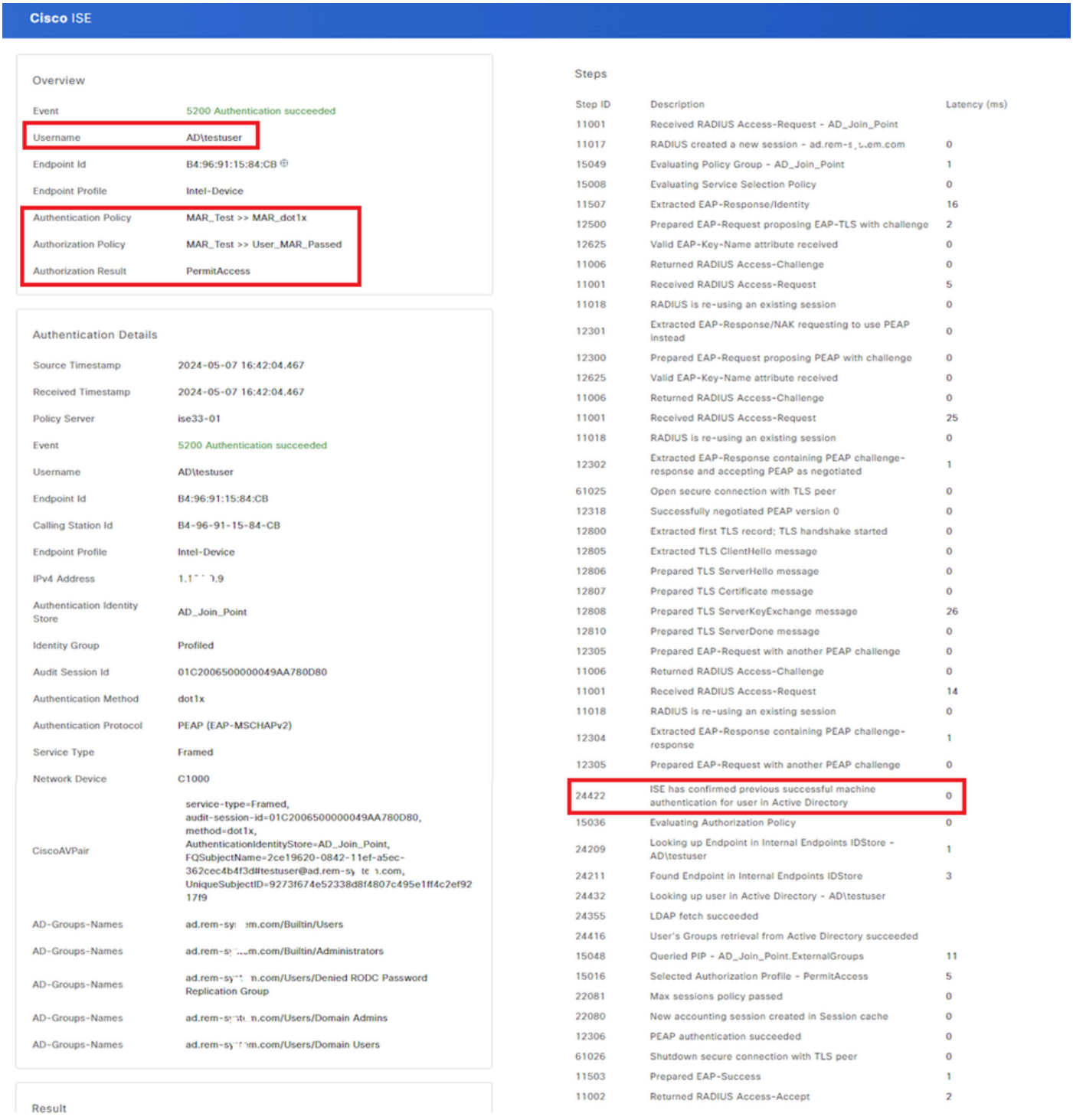


Remarque : le cache MAR étant stocké dans ISE, seule l'authentification des utilisateurs est nécessaire.



Journal Radius Live

Confirmez le journal en direct détaillé de l'authentification utilisateur.



Détail de l'authentification utilisateur

Dépannage

Ces journaux de débogage (prrt-server.log) vous aident à confirmer le comportement détaillé de l'authentification dans ISE.

- runtime-config

- journalisation de l'exécution

- runtime-AAA

Ceci est un exemple du journal de débogage pour le **modèle 1. Authentification de l'ordinateur et authentification de l'utilisateur** dans ce document.

<#root>

// machine authentication
MAR,2024-05-08 16:54:50,582,DEBUG,0x7fb2fd3db700,cntx=0000034313,sesn=ise33-01/504417979/41,CPMSessionID=01C2006500000049AA780D8

user=host/DESKTOP-L2IL9I6.ad.rem-xxx.com

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::checkInsertConditions:

subject=machine

, calling-station-id=B4-96-91-15-84-CB, HostName=DESKTOP-L2IL9I6$@ad.rem-xxx.com,MARCache.cpp:105

// insert MAR cache
MAR,2024-05-08 16:54:50,582,DEBUG,0x7fb2fd3db700,cntx=0000034313,sesn=ise33-01/504417979/41,CPMSessionI

user=host/DESKTOP-L2IL9I6.ad.rem-xxx.com

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,

Inserting new entry to cache

CallingStationId=B4-96-91-15-84-CB, HostName=DESKTOP-L2IL9I6$@ad.rem-xxx.com, IDStore=AD_Join_Point an
MAR,2024-05-08 16:54:50,582,DEBUG,0x7fb2fd3db700,cntx=0000034313,sesn=ise33-01/504417979/41,CPMSessionI

user=host/DESKTOP-L2IL9I6.ad.rem-xxx.com

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::onInsertRequest: event not locall

// user authentication
MAR,2024-05-08 16:55:11,120,DEBUG,0x7fb2fdde0700,cntx=0000034409,sesn=ise33-01/504417979/45,CPMSessionI

user=AD\testuser

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::onQueryRequest:

machine authentication confirmed locally

,MARCache.cpp:222
MAR,2024-05-08 16:55:11,130,DEBUG,0x7fb2fe5e4700,cntx=0000034409,sesn=ise33-01/504417979/45,CPMSessionI

user=AD\testuser

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::onMachineQueryResponse:

machine DESKTOP-L2IL9I6$@ad.rem-xxx.com valid in AD

,MARCache.cpp:316

Informations connexes

Restrictions d'accès aux machines Avantages et inconvénients

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.