サプリカントアクセスのためのマシンの二要素認証の設定

内容

はじめに

このドキュメントでは、マシン認証とdot1x認証を使用した2要素認証を設定するために必要な手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Identity Services Engineの設定
- Cisco Catalyst設定
- IEEE802.1X

使用するコンポーネント

- Identity Services Engine仮想3.3パッチ1
- C1000-48FP-4G-L 15.2(7)E9

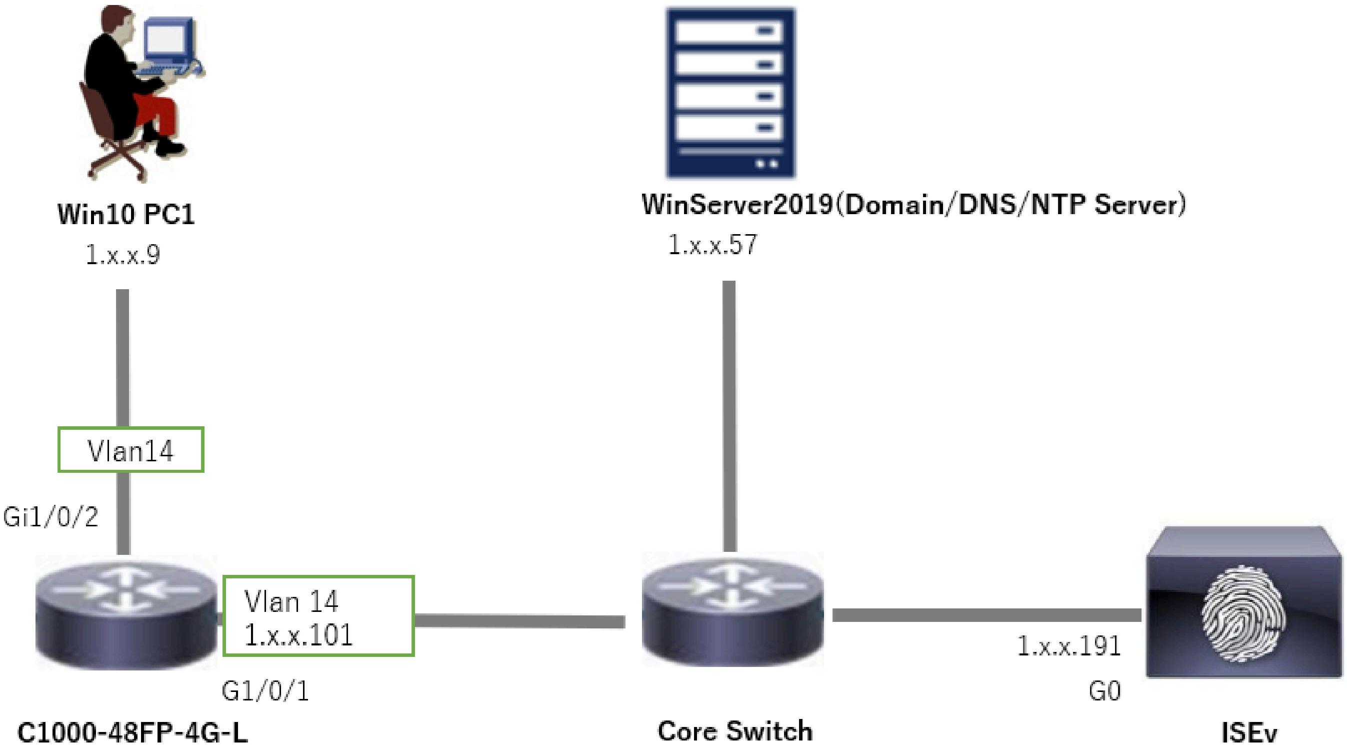
- Windows Server 2019

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

ネットワーク図

次の図は、このドキュメントの例で使用するトポロジを示しています。

Windows Server 2019で設定されるドメイン名は、このドキュメントの例で使用するad.rem-xxx.comです。



ネットワーク図

背景説明

マシン認証は、ネットワークまたはシステムへのアクセスを求めるデバイスのIDを確認するセキュリティプロセスです。ユーザ名やパスワードなどのクレデンシャルに基づいて個人のアイデンティティを検証するユーザ認証とは異なり、マシン認証ではデバイス自体の検証に重点が置かれます。これは多くの場合、デバイスに固有のデジタル証明書またはセキュリティキーを使用して行われます。

マシン認証とユーザ認証を組み合わせて使用することで、許可されたデバイスとユーザだけがネットワークにアクセスできるようにすることができ、より安全な環境を実現できます。この2要素認証方式は、機密情報を保護し、厳格な規制基準を遵守するために特に役立ちます。

コンフィギュレーション

C1000での設定

これは、C1000 CLIでの最小限の設定です。

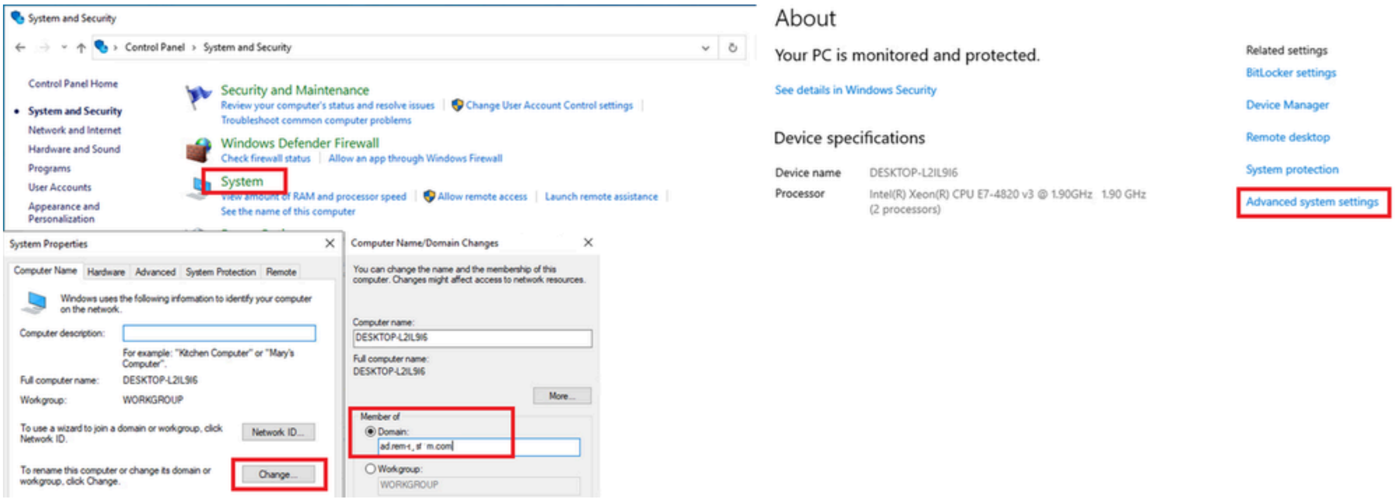
```
aaa new-model

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
```

Windows PCでの設定

ステップ 1：PCをADドメインに追加

Control Panel > System and Securityの順に移動し、Systemをクリックしてから、Advanced system settingsをクリックします。System PropertiesウィンドウでChangeをクリックし、Domainを選択してドメイン名を入力します。



Your PC is monitored and protected.

Device name DESKTOP-L2IL9I6

Processor Intel(R) Xeon(R) CPU E7-4820 v3 @ 1.90GHz 1.90 GHz (2 processors)

Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: DESKTOP-L2IL9I6

Workgroup: WORKGROUP

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: DESKTOP-L2IL9I6

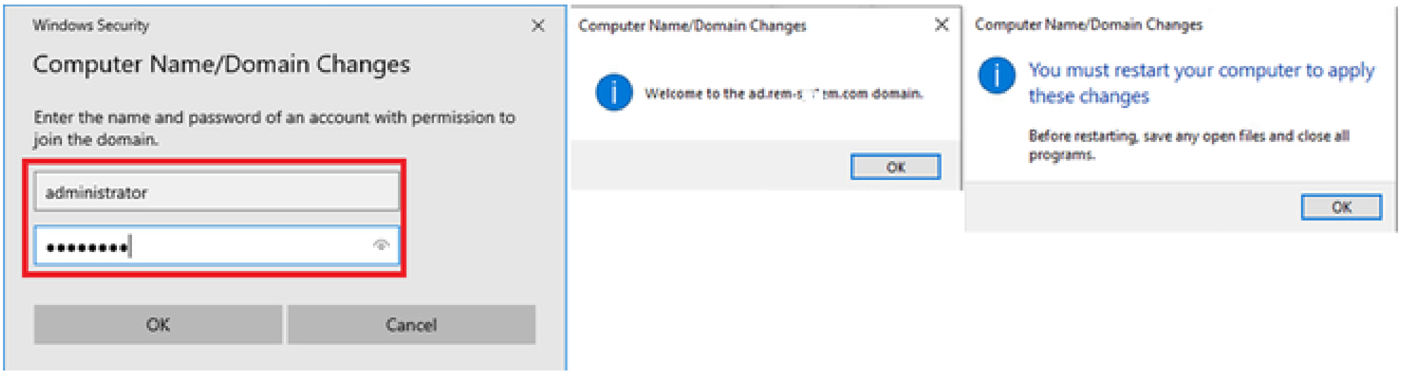
Full computer name: DESKTOP-L2IL9I6

● Domain: ad.rem-ı, st m.com

○ Workgroup: WORKGROUP

PCをADドメインに追加

Windowsのセキュリティウィンドウで、ドメインサーバのユーザ名とパスワードを入力します。



Windows Security

Computer Name/Domain Changes

Enter the name and password of an account with permission to join the domain.

administrator

•••••••••

Computer Name/Domain Changes

Welcome to the ad.rem-s[illegible]m.com domain.

Computer Name/Domain Changes

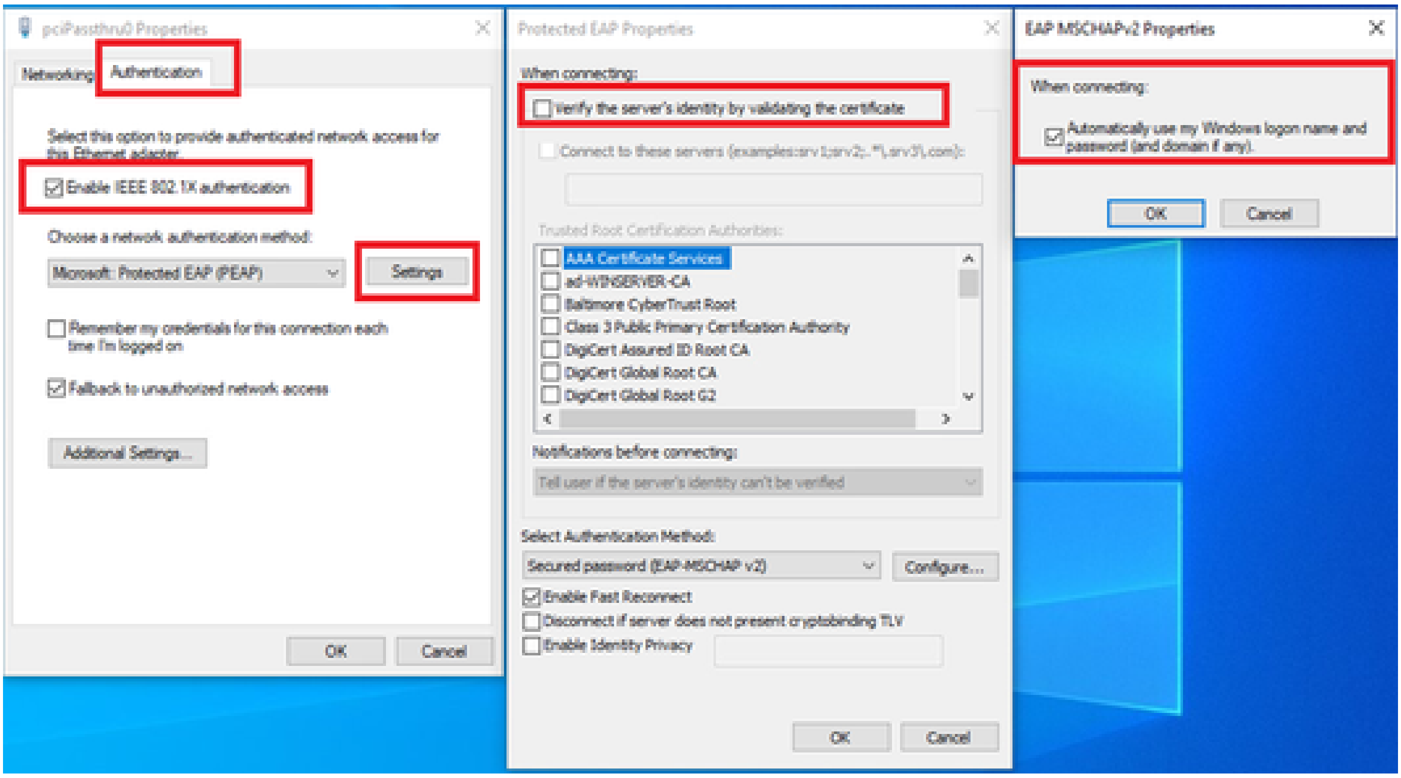
You must restart your computer to apply these changes

Before restarting, save any open files and close all programs.

ユーザ名とパスワードの入力

ステップ２：ユーザ認証の設定

Authenticationに移動し、Enable IEEE 802.1X authenticationにチェックマークを付けます。 Protected EAP PropertiesウィンドウでSettingsをクリックし、Verify the server's identity by validating the certificateのチェックマークを外して、Configureをクリックします。EAP MSCHAPv2 Propertiesウィンドウで、Automatically use my Windows logon name and password (and domain if any)にチェックマークを付けて、Windowsマシンのログイン時に入力したユーザ名をユーザ認証に使用します。



pciPassthru0 Properties

Select this option to provide authenticated network access for this Ethernet adapter.

☑ Enable IEEE 802.1X authentication

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

□ Remember my credentials for this connection each time I'm logged on

☑ Fallback to unauthorized network access

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
□ ad-WINSERVER-CA
□ Baltimore CyberTrust Root
□ Class 3 Public Primary Certification Authority
□ DigiCert Assured ID Root CA
□ DigiCert Global Root CA
□ DigiCert Global Root G2

Notifications before connecting:

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

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

☑ Enable Fast Reconnect

□ Disconnect if server does not present cryptobinding TLV

□ Enable Identity Privacy

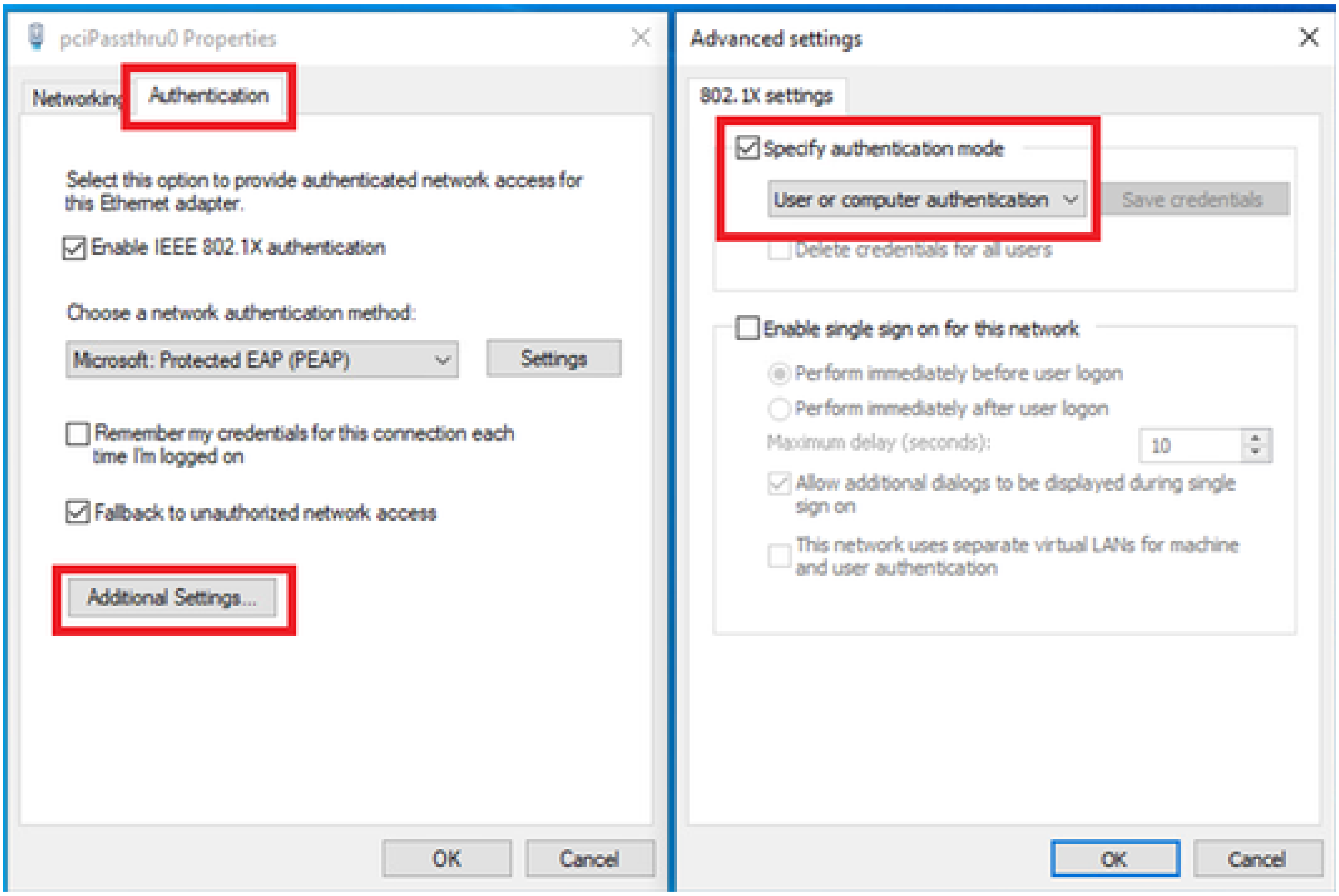
EAP MSCHAPv2 Properties

When connecting:

☑ Automatically use my Windows logon name and password (and domain if any).

ユーザ認証の有効化

Authenticationに移動し、Additional Settingsにチェックマークを入れます。ドロップダウンリストからユーザまたはコンピュータの認証を選択します。



pciPassthru0 Properties

Networking | Authentication

Select this option to provide authenticated network access for this Ethernet adapter.

☑ Enable IEEE 802.1X authentication

Choose a network authentication method:

Microsoft: Protected EAP (PEAP) | Settings

☐ Remember my credentials for this connection each time I'm logged on

☑ Fallback to unauthorized network access

Additional Settings...

OK | Cancel

Advanced settings

802.1X settings

☑ Specify authentication mode

User or computer authentication | Save credentials

☐ Delete credentials for all users

☐ Enable single sign on for this network

● Perform immediately before user logon

○ Perform immediately after user logon

Maximum delay (seconds): 10

☑ Allow additional dialogs to be displayed during single sign on

☐ This network uses separate virtual LANs for machine and user authentication

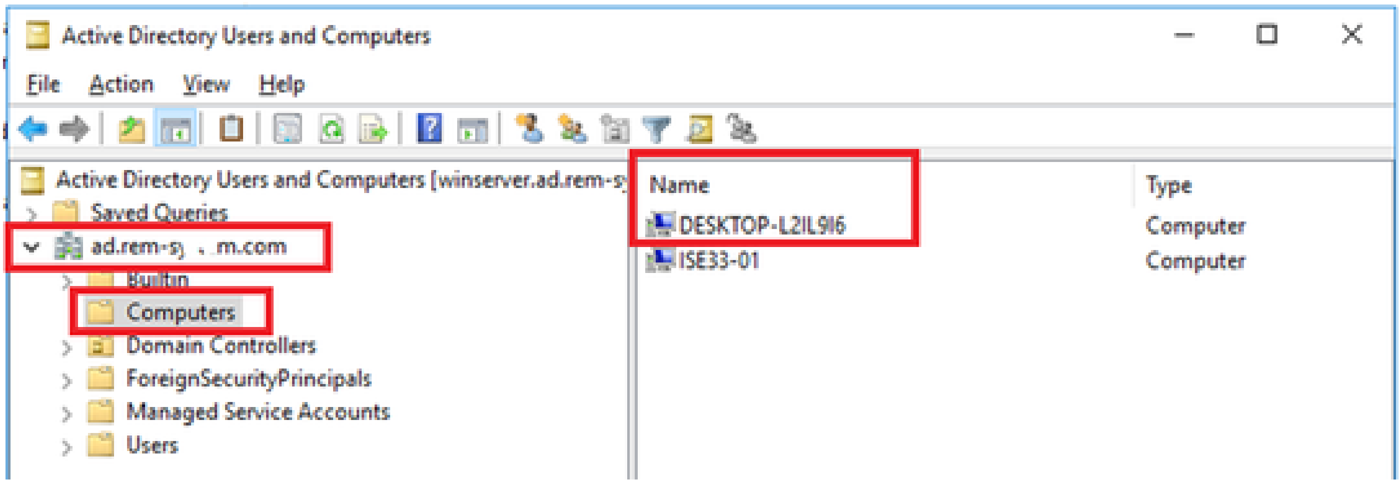
OK | Cancel

認証モードの指定

Windows Serverでの設定

ステップ１：ドメインコンピューターの確認

Active Directory Users and Computersに移動し、Computersをクリックします。Win10 PC1がドメインにリストされていることを確認します。



Active Directory Users and Computers

File Action View Help

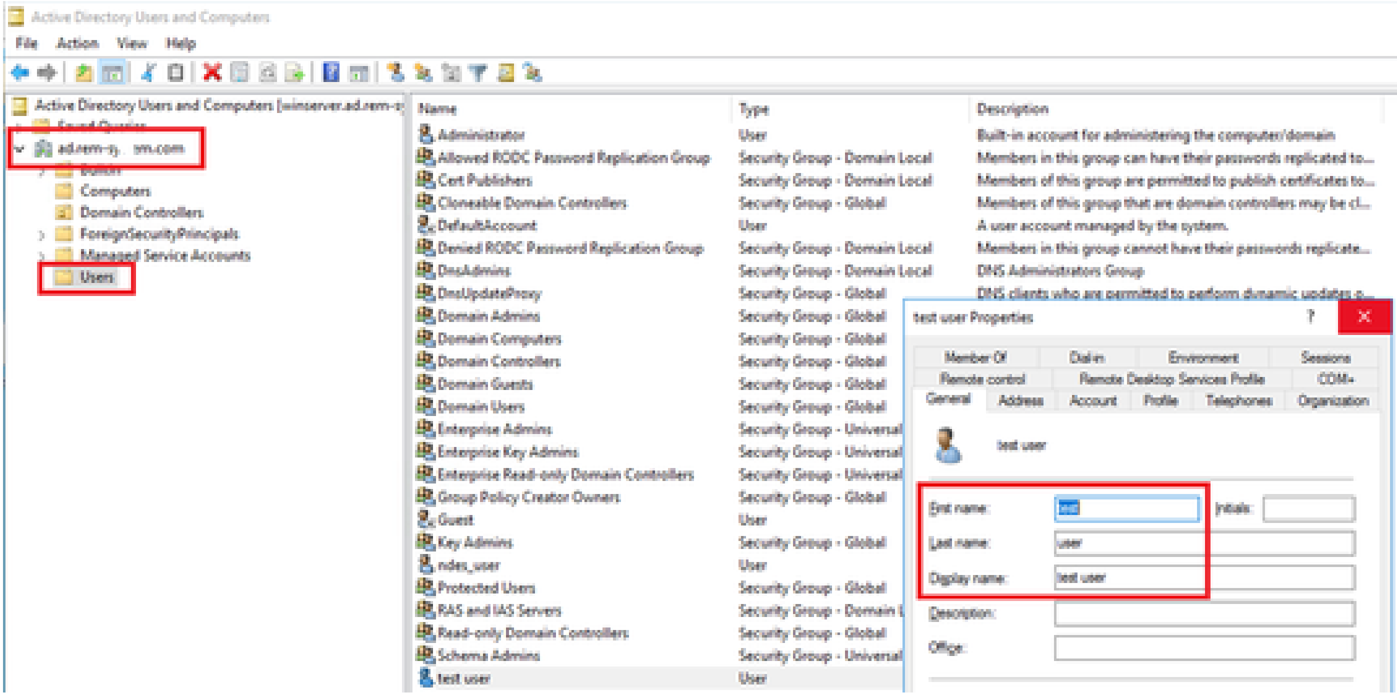
- Active Directory Users and Computers [winserver.ad.rem-sy
  - Saved Queries
  - ad.rem-s) . m.com
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Managed Service Accounts
    - Users

Name	Type
DESKTOP-L2IL9I6	Computer
ISE33-01	Computer

ドメインコンピュータの確認

ステップ２：ドメインユーザの追加

Active Directory Users and Computersに移動し、Usersをクリックします。testuserをドメインユーザとして追加します。



Name	Type	Description
Administrator	User	Built-in account for administering the computer/domain
Allowed RODC Password Replication Group	Security Group - Domain Local	Members in this group can have their passwords replicated to...
Cert Publishers	Security Group - Domain Local	Members of this group are permitted to publish certificates to...
Cloneable Domain Controllers	Security Group - Global	Members of this group that are domain controllers may be cl...
DefaultAccount	User	A user account managed by the system.
Denied RODC Password Replication Group	Security Group - Domain Local	Members in this group cannot have their passwords replicate...
DnsAdmins	Security Group - Domain Local	DNS Administrators Group
DnsUpdateProxy	Security Group - Global	DNS clients who are permitted to perform dynamic updates o...
Domain Admins	Security Group - Global	
Domain Computers	Security Group - Global	
Domain Controllers	Security Group - Global	
Domain Guests	Security Group - Global	
Domain Users	Security Group - Global	
Enterprise Admins	Security Group - Universal	
Enterprise Key Admins	Security Group - Universal	
Enterprise Read-only Domain Controllers	Security Group - Universal	
Group Policy Creator Owners	Security Group - Global	
Guest	User	
Key Admins	Security Group - Global	
ndes_user	User	
Protected Users	Security Group - Global	
RAS and IAS Servers	Security Group - Domain L	
Read-only Domain Controllers	Security Group - Global	
Schema Admins	Security Group - Universal	
test user	User	

test user

First name: test

Initials:

Last name: user

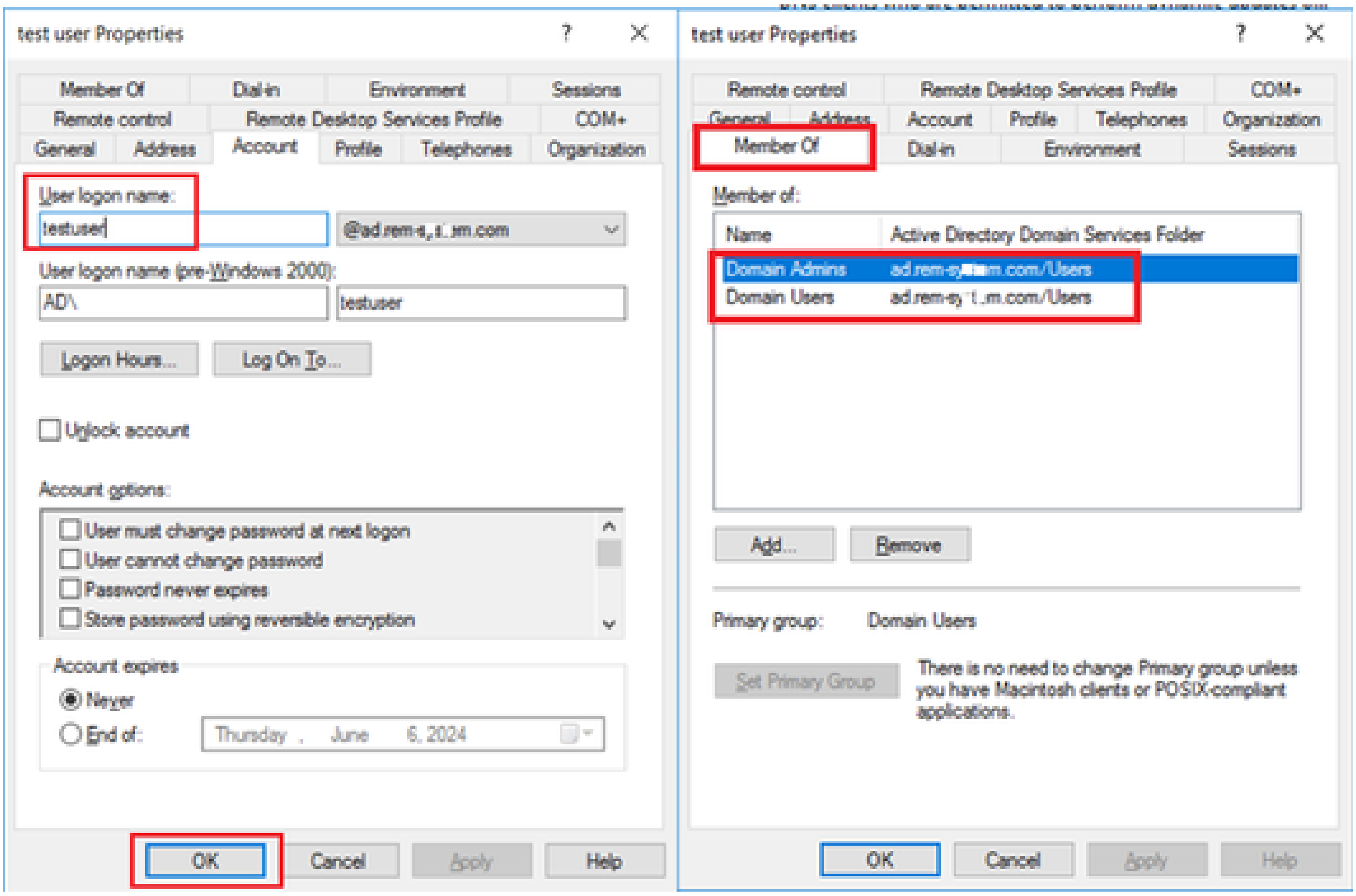
Display name: test user

Description:

Office:

ドメインユーザの追加

Domain AdminsとDomain Usersのメンバにドメインユーザを追加します。



User logon name: testuser @ad.rem-s[redacted]m.com

User logon name (pre-Windows 2000): AD\ testuser

□ Unlock account

Account options:

□ User must change password at next logon
□ User cannot change password
□ Password never expires
□ Store password using reversible encryption

Account expires

● Never

○ End of: Thursday , June 6, 2024

Member of:

Name	Active Directory Domain Services Folder
Domain Admins	ad.rem-sy[redacted]m.com/Users
Domain Users	ad.rem-sy[redacted]m.com/Users

Primary group: Domain Users

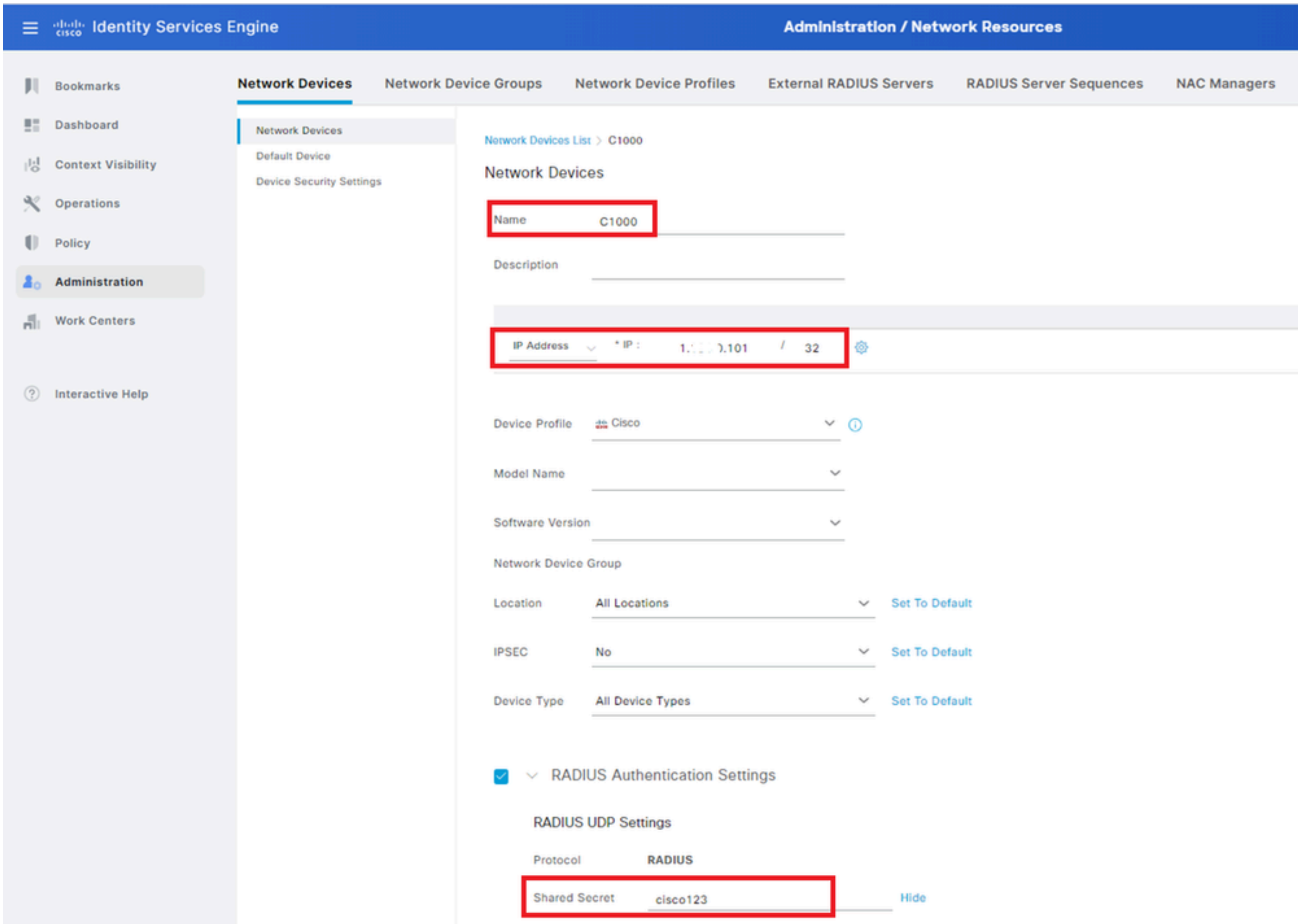
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

ドメイン管理者とドメインユーザー

ISEでの設定

ステップ 1：デバイスの追加

Administration > Network Devicesの順に移動し、AddボタンをクリックしてC1000デバイスを追加します。



Network Devices

Name: C1000

Description:

IP Address * IP : 1.[redacted].101 / 32

Device Profile: Cisco

Model Name:

Software Version:

Network Device Group

Location: All Locations — Set To Default

IPSEC: No — Set To Default

Device Type: All Device Types — Set To Default

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

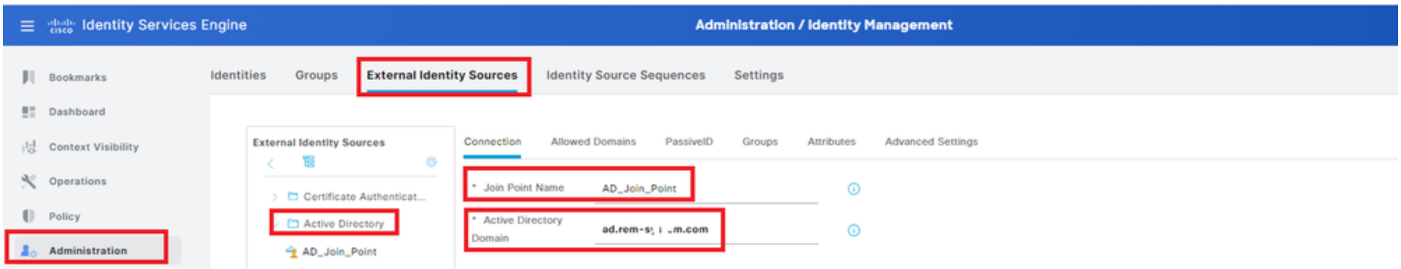
Shared Secret: cisco123 — Hide

デバイスの追加

ステップ 2：Active Directoryの追加

Administration > External Identity Sources > Active Directoryの順に移動し、Connectionタブをクリックして、Active DirectoryをISEに追加します。

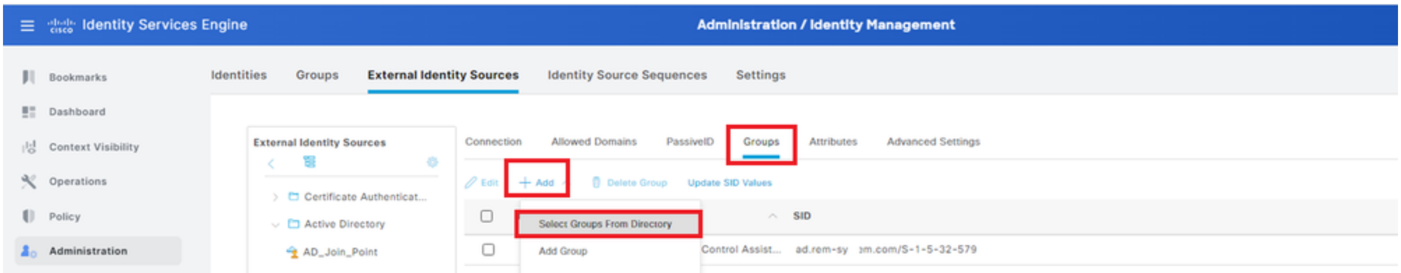
- [結合ポイント名]: AD_Join_Point
- Active Directoryドメイン：ad.rem-xxx.com



* Join Point Name: AD_Join_Point

* Active Directory Domain: ad.rem-s[redacted]m.com

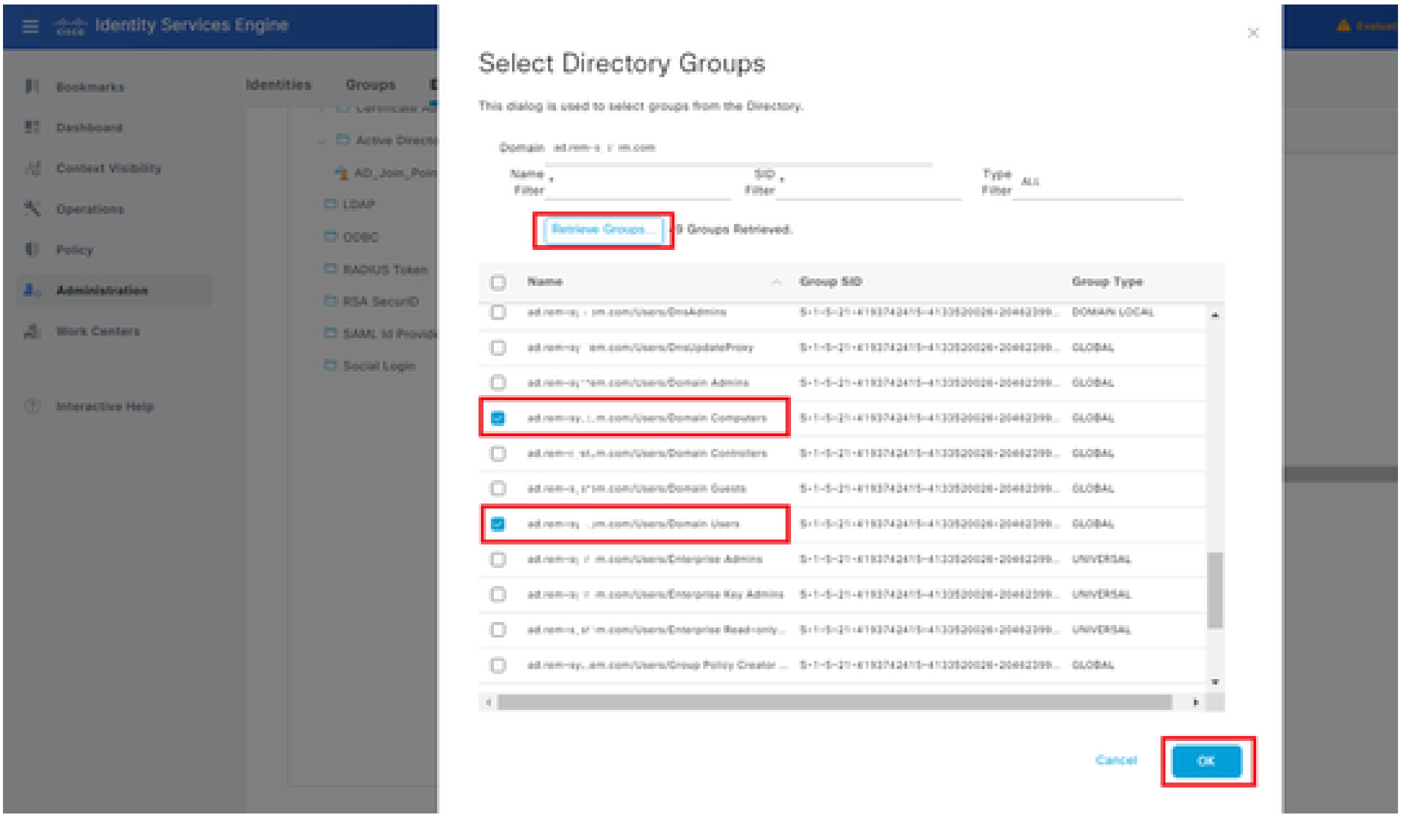
Groupsタブに移動し、ドロップダウンリストからSelect Groups From Directoryを選択します。



Control Assist... ad.rem-sy m.com/S-1-5-32-579

ディレクトリからグループを選択

Retrieve Groups fromドロップダウンリストをクリックします。ad.rem-xxx.com/Users/Domain Computersとad.rem-xxx.com/Users/Domain Usersにチェックマークを入れて、OKをクリックします。



This dialog is used to select groups from the Directory.

Domain ad.rem-s m.com

Name Filter *
SID Filter *
Type Filter ALL

9 Groups Retrieved.

☐	Name	Group SID	Group Type
☐	ad.rem-sy m.com/Users/DnsAdmins	S-1-5-21-4193742415-4133520026-20462399...	DOMAIN LOCAL
☐	ad.rem-sy m.com/Users/DnsUpdateProxy	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
☐	ad.rem-sy m.com/Users/Domain Admins	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
☑	ad.rem-sy m.com/Users/Domain Computers	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
☐	ad.rem-s m.com/Users/Domain Controllers	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
☐	ad.rem-s m.com/Users/Domain Guests	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
☑	ad.rem-sy m.com/Users/Domain Users	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
☐	ad.rem-sy m.com/Users/Enterprise Admins	S-1-5-21-4193742415-4133520026-20462399...	UNIVERSAL
☐	ad.rem-sy m.com/Users/Enterprise Key Admins	S-1-5-21-4193742415-4133520026-20462399...	UNIVERSAL
☐	ad.rem-s m.com/Users/Enterprise Read-only...	S-1-5-21-4193742415-4133520026-20462399...	UNIVERSAL
☐	ad.rem-sy m.com/Users/Group Policy Creator ...	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL

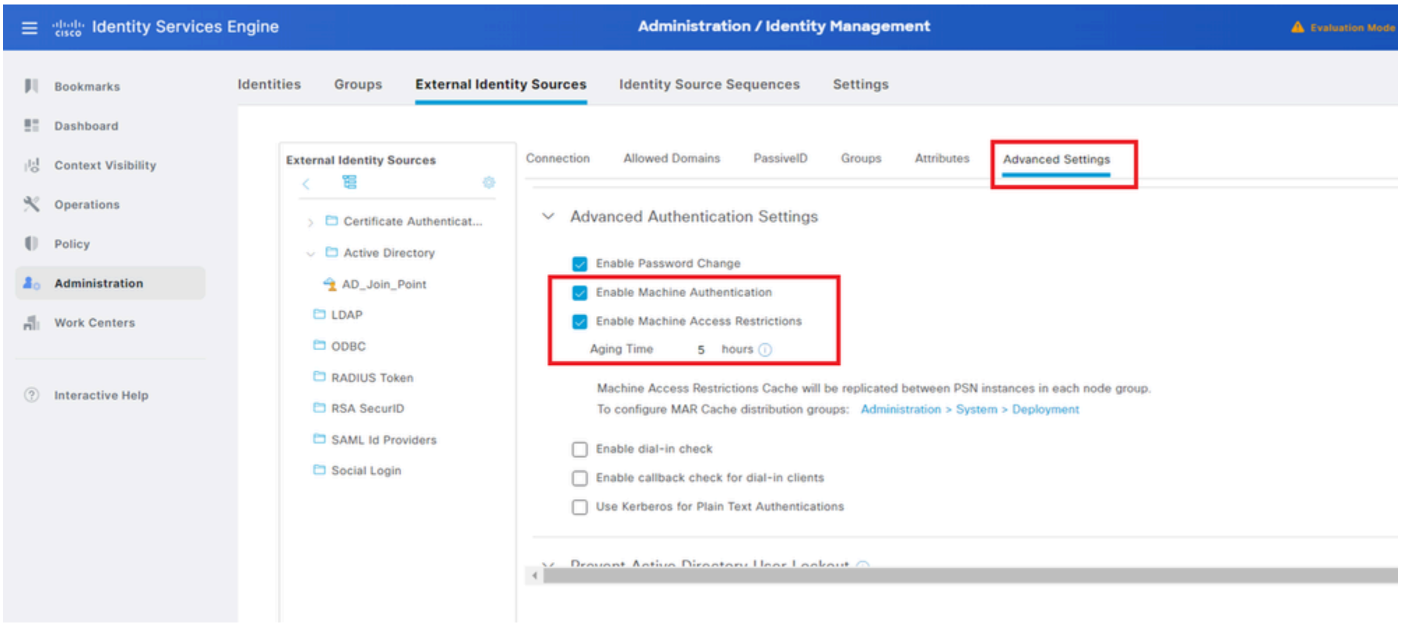
ドメインコンピューターとユーザーの追加

ステップ 3：マシン認証設定の確認

Advanced Settingsタブに移動し、マシン認証の設定を確認します。

- マシン認証の有効化：マシン認証を有効にします。
- マシンアクセス制限の有効化：認証の前にユーザ認証とマシン認証を組み合わせます。

注：エージングタイムの有効範囲は1 ～ 8760です。



Advanced Authentication Settings

☑ Enable Password Change

☑ Enable Machine Authentication

☑ Enable Machine Access Restrictions

Aging Time 5 hours

Machine Access Restrictions Cache will be replicated between PSN instances in each node group.
To configure MAR Cache distribution groups: Administration > System > Deployment

☐ Enable dial-in check

☐ Enable callback check for dial-in clients

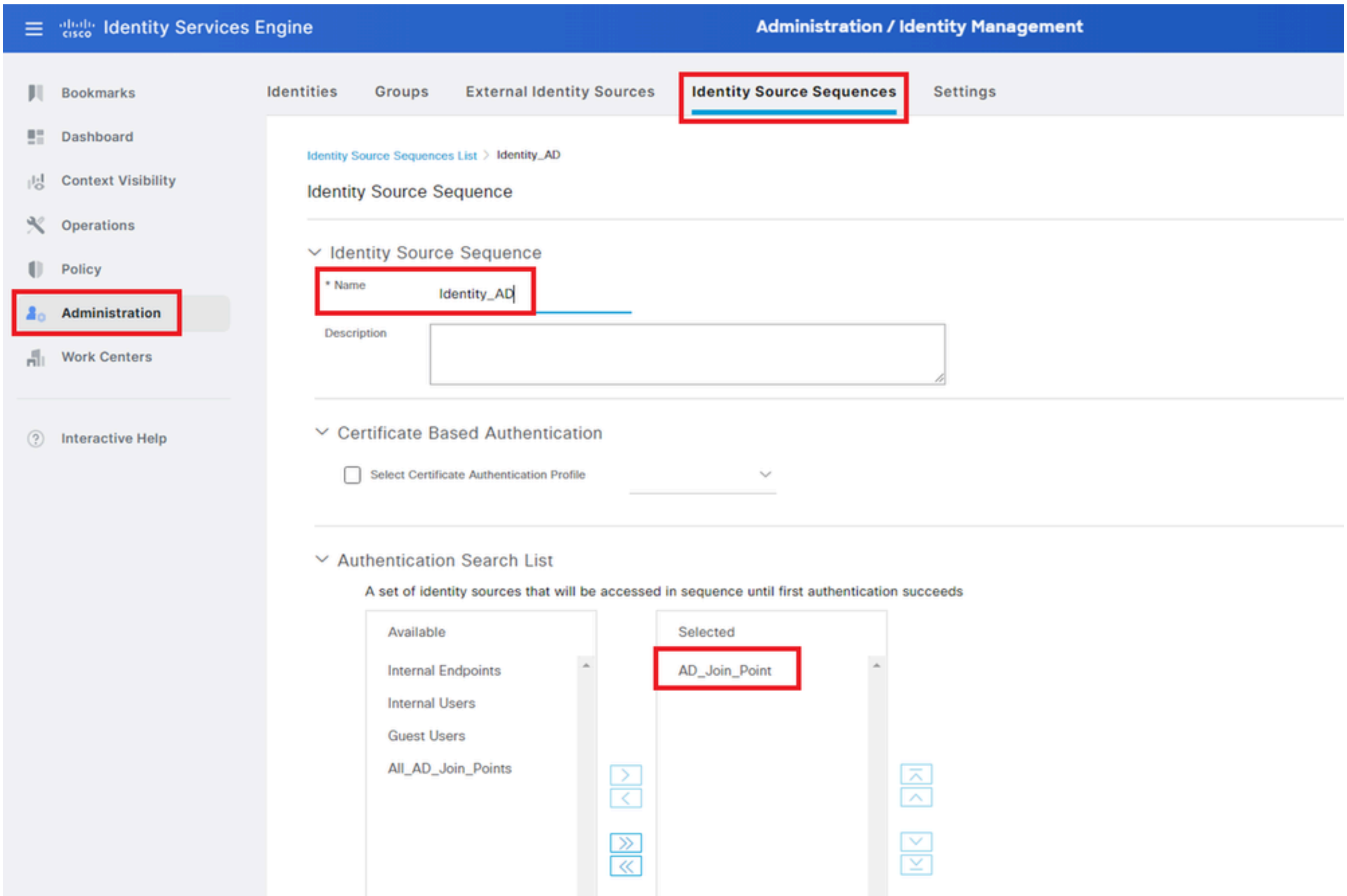
☐ Use Kerberos for Plain Text Authentications

Prevent Active Directory User Lockout

ステップ４：アイデンティティソースシーケンスの追加

Administration > Identity Source Sequencesの順に移動し、Identity Source Sequenceを追加します。

- 名前：Identity_AD
- 認証検索リスト：AD_Join_Point



* Name Identity_AD

Description

□ Select Certificate Authentication Profile

A set of identity sources that will be accessed in sequence until first authentication succeeds

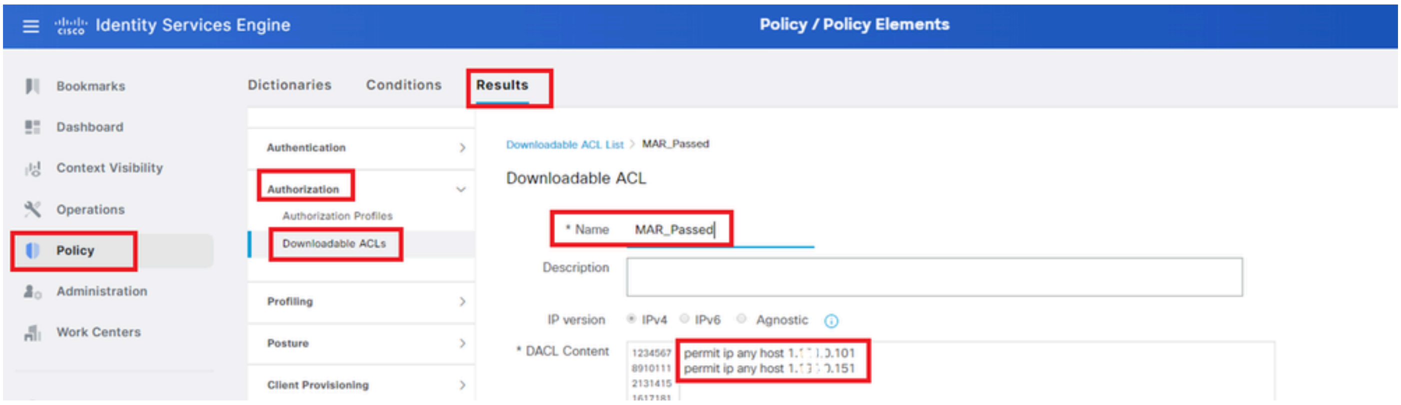
AD_Join_Point

アイデンティティソースシーケンスの追加

ステップ５：DACLと許可プロファイルの追加

Policy > Results > Authorization > Downloadable ACLsの順に移動し、DACLを追加します。

- 名前：MAR_Passed
- DACLコンテンツ：permit ip any host 1.x.x.101およびpermit ip any host 1.x.x.105



Downloadable ACL List > MAR_Passed

Downloadable ACL

* Name MAR_Passed

Description

IP version ● IPv4 ○ IPv6 ○ Agnostic

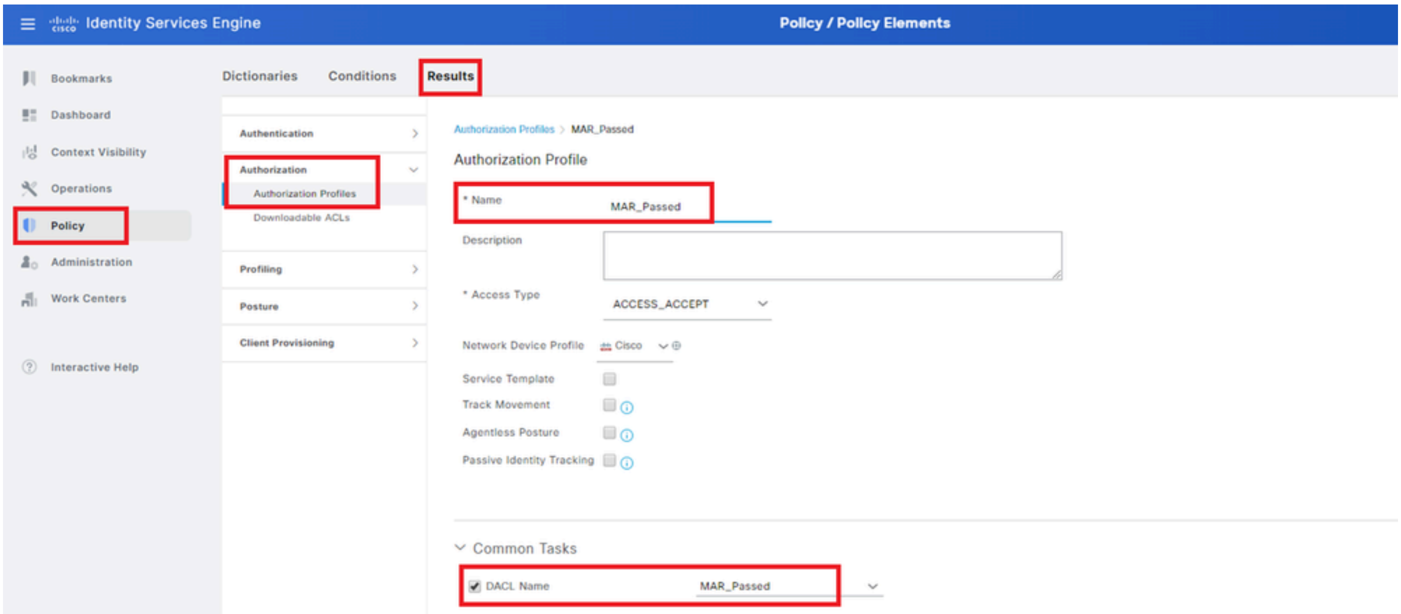
* DACL Content

```
permit ip any host 1.[redacted]0.101
permit ip any host 1.[redacted]0.151
```

DACLの追加

Policy > Results > Authorization > Authorization Profilesの順に移動し、認可プロファイルを追加します。

- 名前：MAR_Passed
- DACL名：MAR_Passed



Authorization Profiles > MAR_Passed

Authorization Profile

* Name MAR_Passed

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template □

Track Movement □

Agentless Posture □

Passive Identity Tracking □

Common Tasks

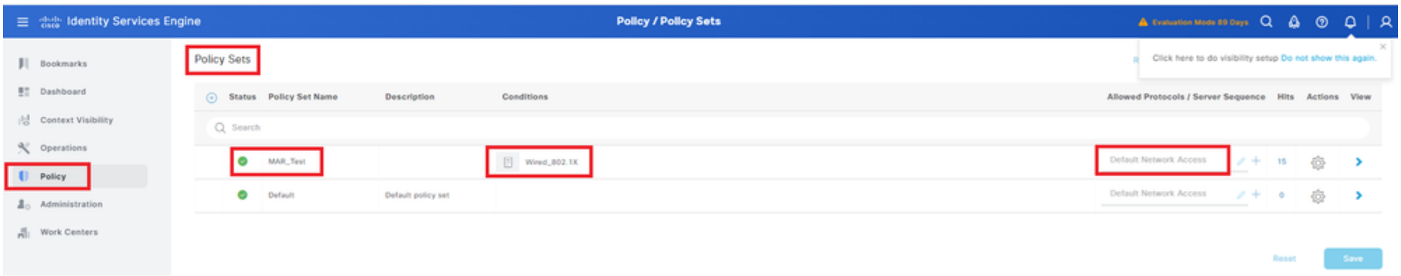
☑ DACL Name MAR_Passed

許可プロファイルの追加

手順 6：ポリシーセットの追加

Policy > Policy Setsの順に移動し、+ をクリックしてポリシーセットを追加します。

- ポリシーセット名：MAR_Test
- 条件：Wired_802.1X
- 許可されるプロトコル/サーバシーケンス：デフォルトのネットワークアクセス



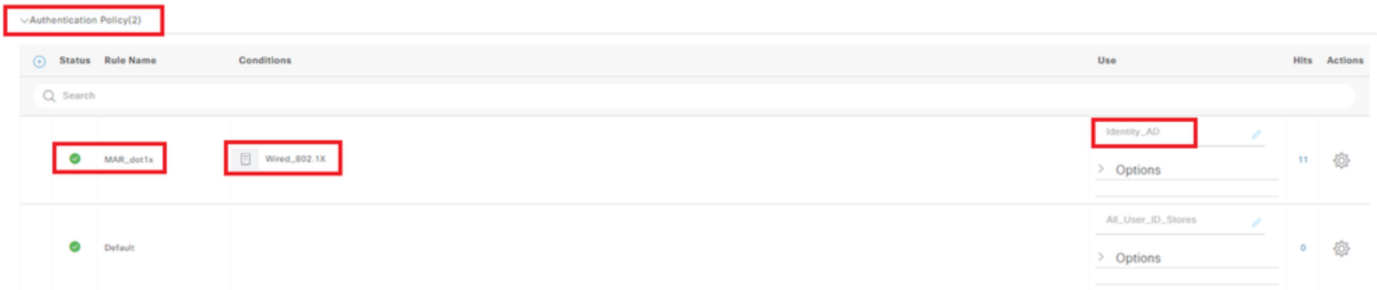
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	MAR_Test		Wired_802.1X	Default Network Access	15	⚙	>
●	Default	Default policy set		Default Network Access	0	⚙	>

ポリシーセットの追加

手順 7：認証ポリシーの追加

Policy Setsに移動し、MAR_Testをクリックして認証ポリシーを追加します。

- ルール名：MAR_dot1x
- 条件：Wired_802.1X
- 使用：Identity_AD



Status	Rule Name	Conditions	Use	Hits	Actions
●	MAR_dot1x	Wired_802.1X	Identity_AD Options	11	⚙
●	Default		All_User_ID_Stores Options	0	⚙

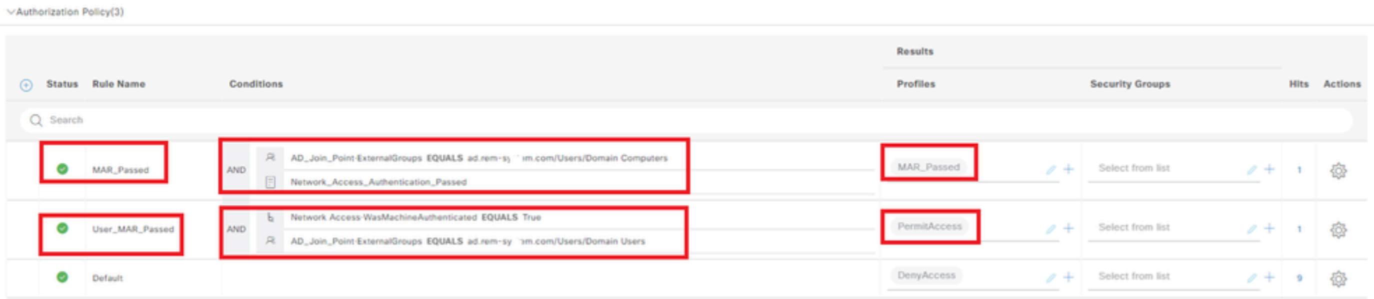
認証ポリシーの追加

ステップ 8：許可ポリシーの追加

Policy Setsに移動し、MAR_Testをクリックして認可ポリシーを追加します。

- ルール名： MAR_Passed
- 条件：AD_Join_Point· ExternalGroups EQUALS ad.rem-xxx.com/Users/Domain Computers およびNetwork_Access_Authentication_Passed
- 結果：MAR_Passed

- ルール名： User_MAR_Passed
- 条件：ネットワークアクセス· WasMachineAuthenticated EQUALS True AND AD_Join_Point· ExternalGroups EQUALS ad.rem-xxx.com/Users/Domain Users
- 結果：PermitAccess



			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
●	MAR_Passed	AND AD_Join_Point·ExternalGroups EQUALS ad.rem-sy ·m.com/Users/Domain Computers Network_Access_Authentication_Passed	MAR_Passed	Select from list	1	⚙
●	User_MAR_Passed	AND Network Access·WasMachineAuthenticated EQUALS True AD_Join_Point·ExternalGroups EQUALS ad.rem-sy ·m.com/Users/Domain Users	PermitAccess	Select from list	1	⚙
●	Default		DenyAccess	Select from list	9	⚙

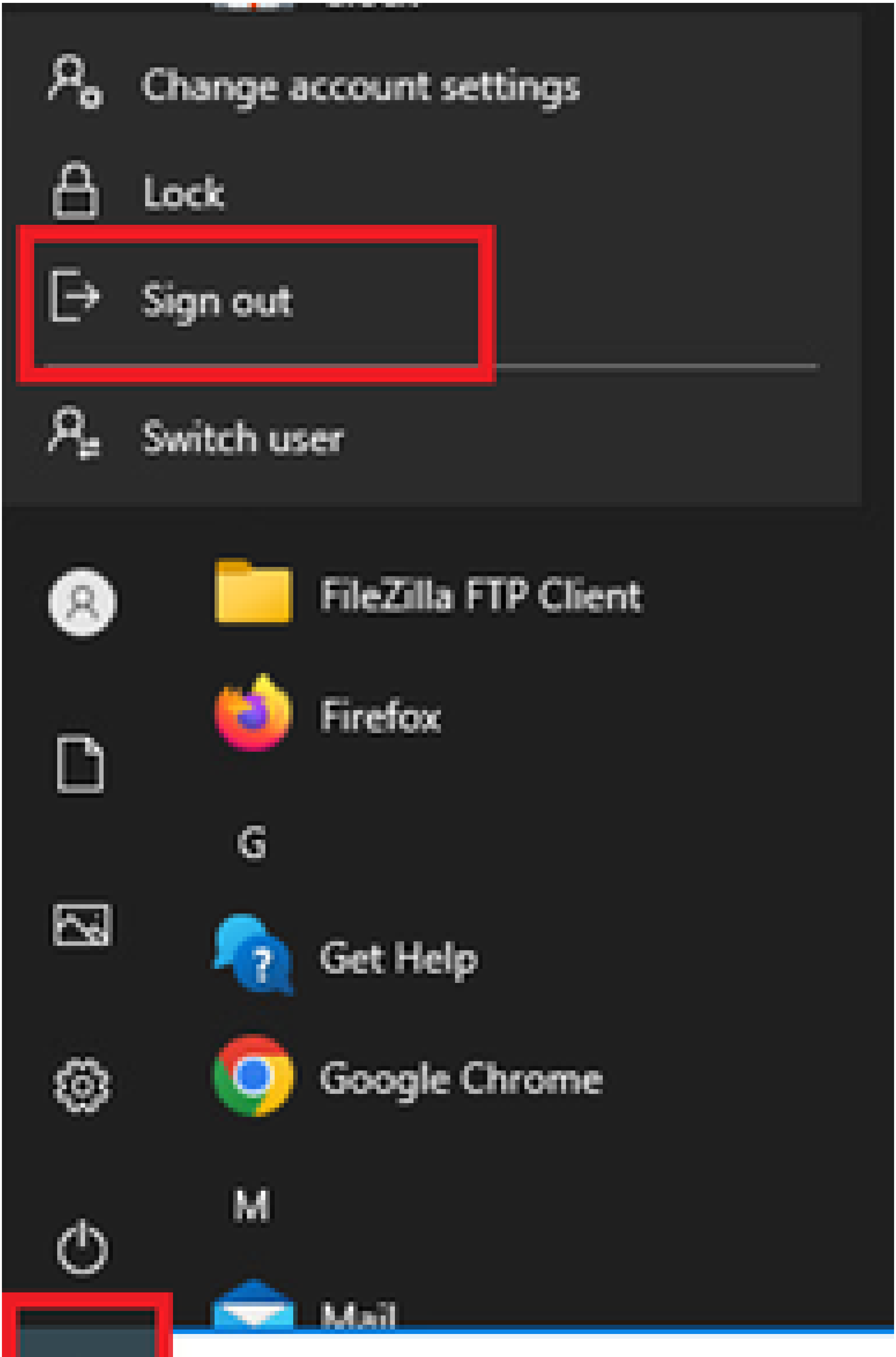
許可ポリシーの追加

確認

パターン1マシン認証とユーザ認証

ステップ１：Windows PCからのサインアウト

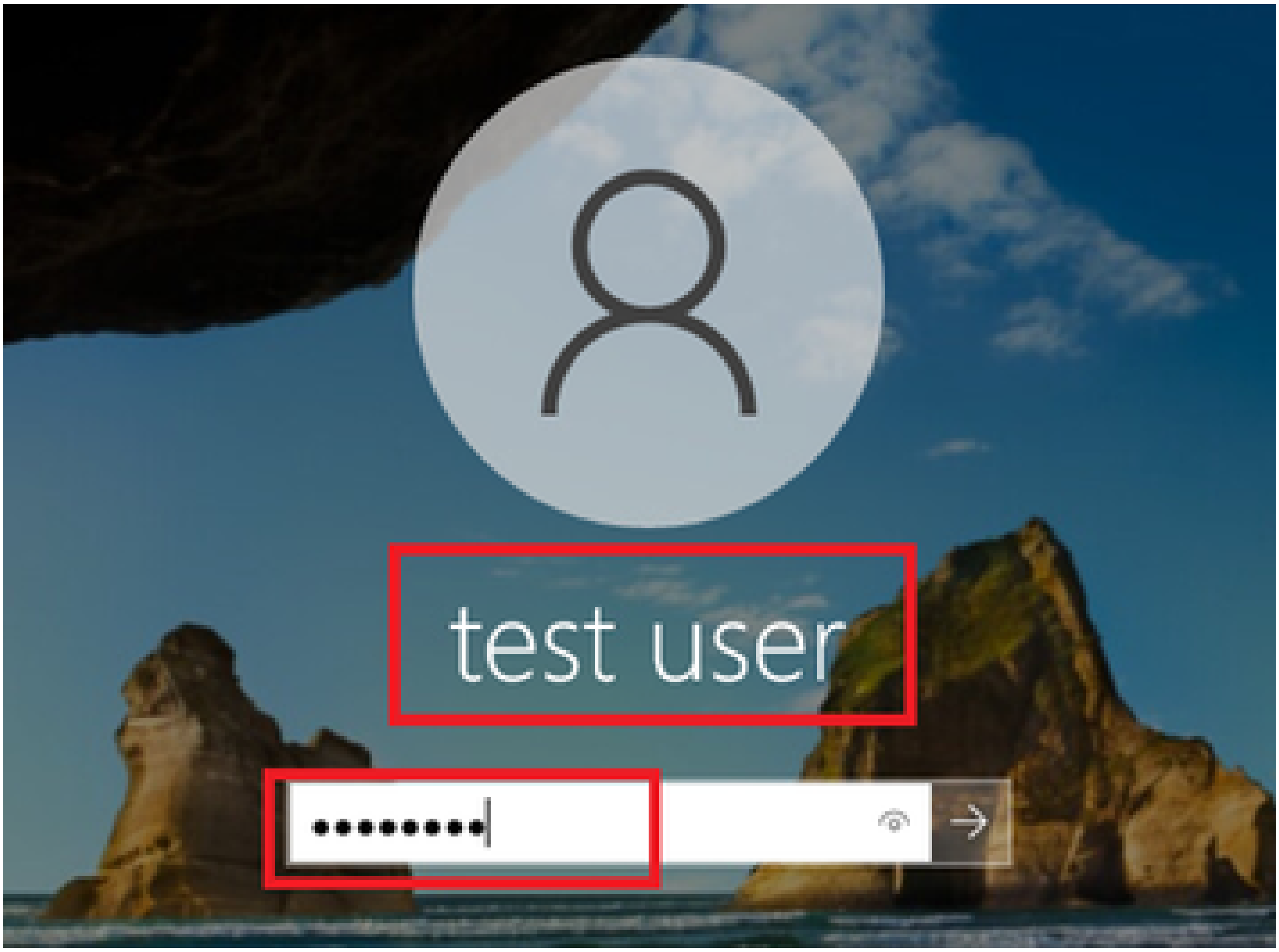
Win10 PC1からSign outボタンをクリックして、マシン認証をトリガーします。


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

```
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
```

ステップ 3：Windows PCへのログイン

Win10 PC1にログインし、ユーザ認証をトリガーするためのユーザ名とパスワードを入力します。



*Windows PC*へのログイン

ステップ 4：認証セッションの確認

show authentication sessions interface GigabitEthernet1/0/2 detailsコマンドを実行して、C1000でのユーザ認証セッションを確認します。

<#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:
```

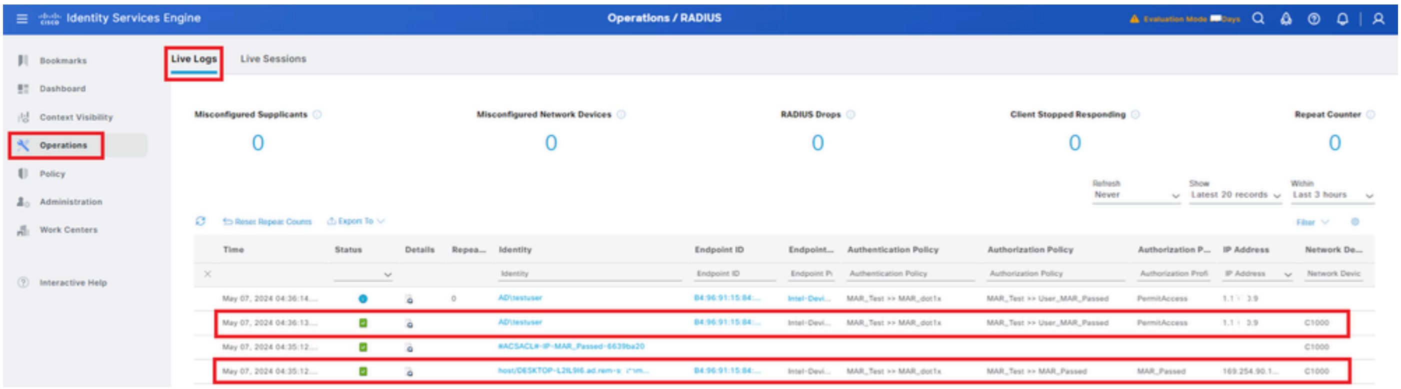
`AD\testuser`

```
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
```

ステップ５：Radiusライブログの確認

ISE GUIで、**Operations** > **RADIUS** > **Live Logs**の順に移動し、マシン認証とユーザ認証のライブログを確認します。



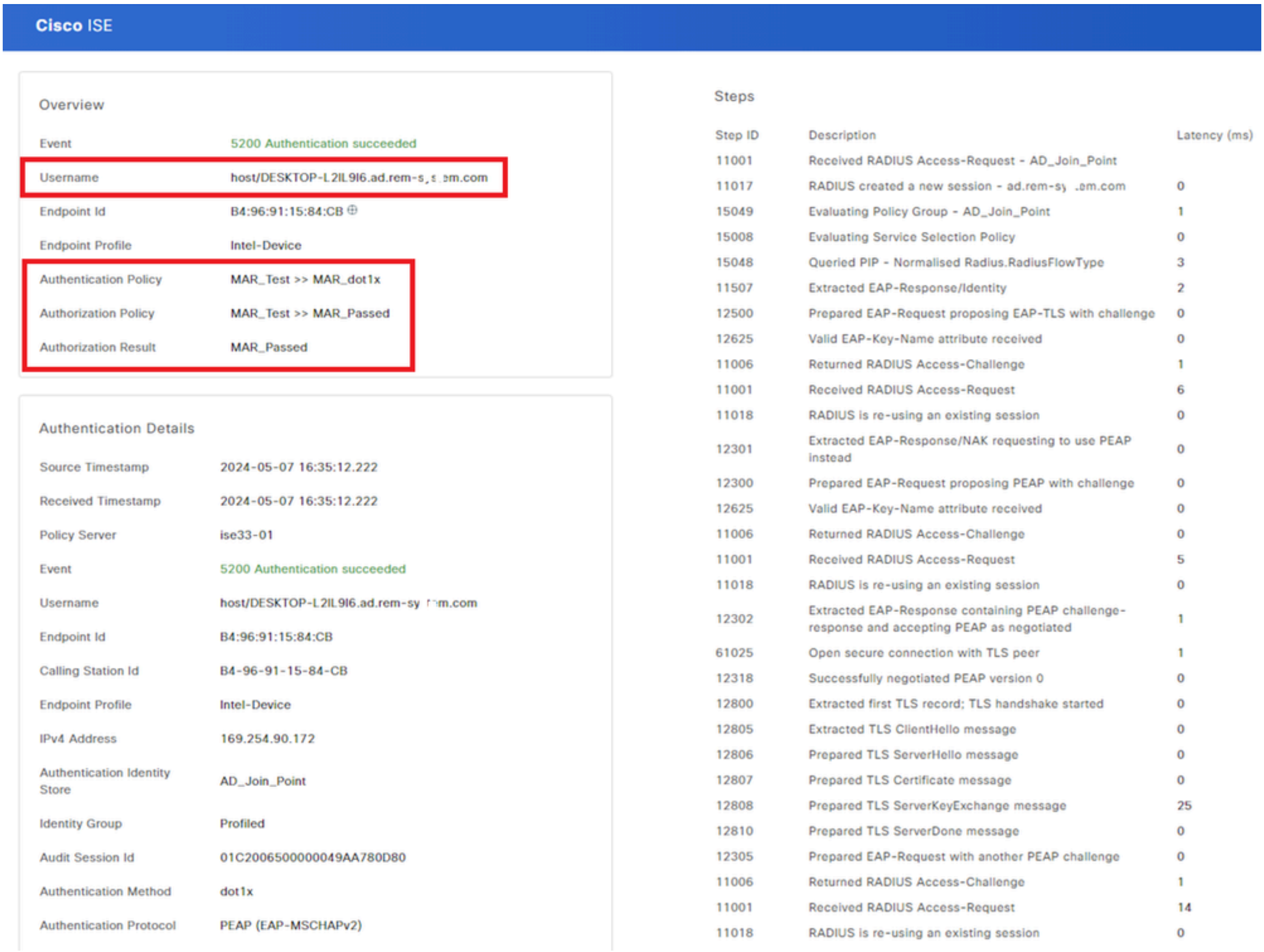
Misconfigured Supplicants: 0
Misconfigured Network Devices: 0
RADIUS Drops: 0
Client Stopped Responding: 0
Repeat Counter: 0

Refresh: Never
Show: Latest 20 records
Within: Last 3 hours

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication Policy	Authorization Policy	Authorization P...	IP Address	Network De...
May 07, 2024 04:36:14....	●	🔍	0	AD\testuser	B4:96:91:15:84:...	Intel-Devi...	MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed	PermitAccess	1.1 [redacted] 3.9	
May 07, 2024 04:36:13....	✓	🔍		AD\testuser	B4:96:91:15:84:...	Intel-Devi...	MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed	PermitAccess	1.1 [redacted] 3.9	C1000
May 07, 2024 04:35:12....	✓	🔍		#ACSACL#-IP-MAR_Passed-6639ba20							C1000
May 07, 2024 04:35:12....	✓	🔍		host/DESKTOP-L2IL9I6.ad.rem-s [redacted] m...	B4:96:91:15:84:...	Intel-Devi...	MAR_Test >> MAR_dot1x	MAR_Test >> MAR_Passed	MAR_Passed	169.254.90.1...	C1000

Radiusライブログ

マシン認証の詳細なライブログを確認します。



Cisco ISE

Overview

Event	5200 Authentication succeeded
Username	host/DESKTOP-L2IL9I6.ad.rem-s, s em.com
Endpoint Id	B4:96:91:15:84:CB ⊕
Endpoint Profile	Intel-Device
Authentication Policy	MAR_Test >> MAR_dot1x
Authorization Policy	MAR_Test >> MAR_Passed
Authorization Result	MAR_Passed

Authentication Details

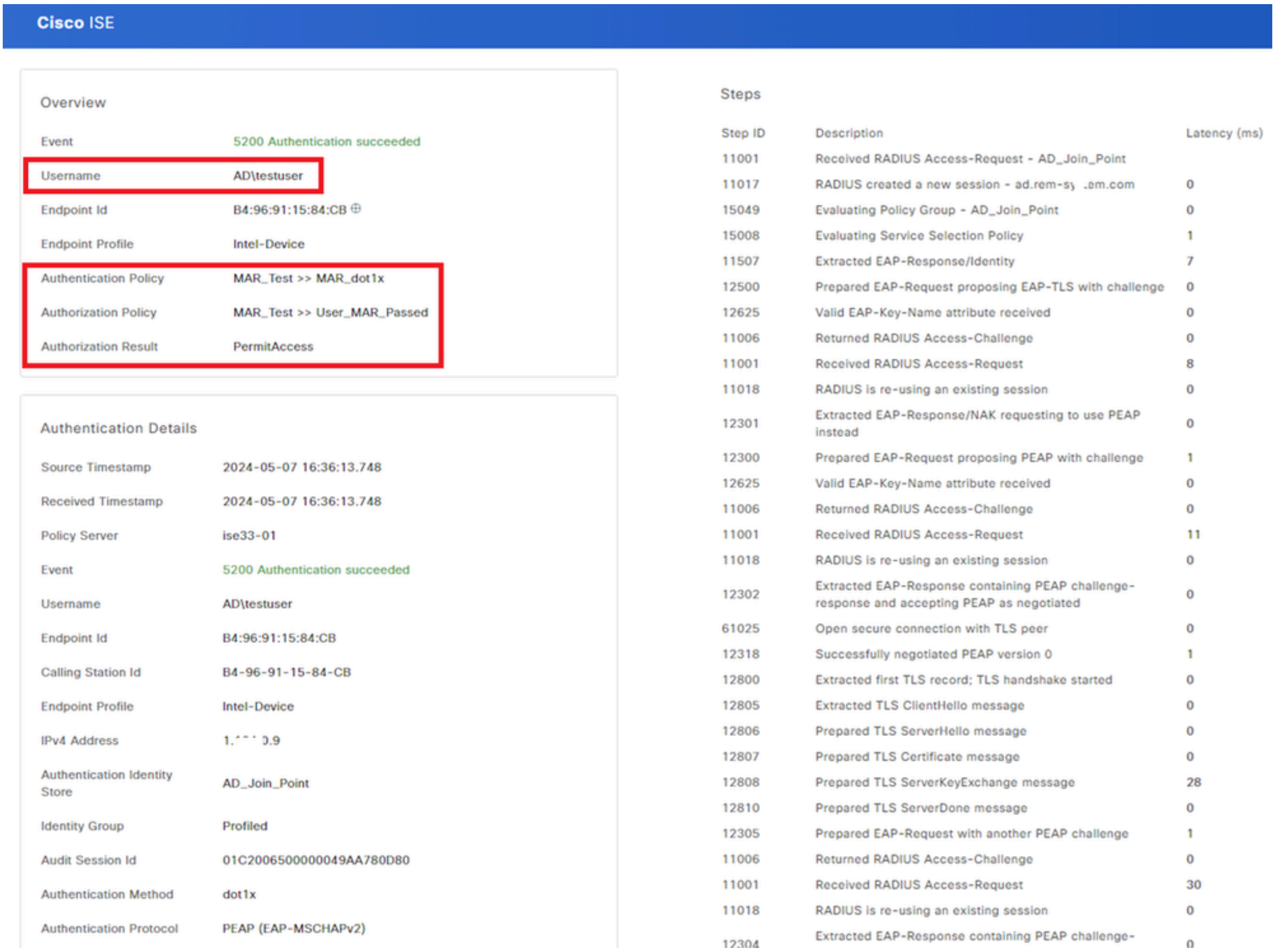
Source Timestamp	2024-05-07 16:35:12.222
Received Timestamp	2024-05-07 16:35:12.222
Policy Server	ise33-01
Event	5200 Authentication succeeded
Username	host/DESKTOP-L2IL9I6.ad.rem-sy m.com
Endpoint Id	B4:96:91:15:84:CB
Calling Station Id	B4-96-91-15-84-CB
Endpoint Profile	Intel-Device
IPv4 Address	169.254.90.172
Authentication Identity Store	AD_Join_Point
Identity Group	Profiled
Audit Session Id	01C2006500000049AA780D80
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)

Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request - AD_Join_Point	
11017	RADIUS created a new session - ad.rem-sy .em.com	0
15049	Evaluating Policy Group - AD_Join_Point	1
15008	Evaluating Service Selection Policy	0
15048	Queried PIP - Normalised Radius.RadiusFlowType	3
11507	Extracted EAP-Response/Identity	2
12500	Prepared EAP-Request proposing EAP-TLS with challenge	0
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	1
11001	Received RADIUS Access-Request	6
11018	RADIUS is re-using an existing session	0
12301	Extracted EAP-Response/NAK requesting to use PEAP instead	0
12300	Prepared EAP-Request proposing PEAP with challenge	0
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	5
11018	RADIUS is re-using an existing session	0
12302	Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated	1
61025	Open secure connection with TLS peer	1
12318	Successfully negotiated PEAP version 0	0
12800	Extracted first TLS record; TLS handshake started	0
12805	Extracted TLS ClientHello message	0
12806	Prepared TLS ServerHello message	0
12807	Prepared TLS Certificate message	0
12808	Prepared TLS ServerKeyExchange message	25
12810	Prepared TLS ServerDone message	0
12305	Prepared EAP-Request with another PEAP challenge	0
11006	Returned RADIUS Access-Challenge	1
11001	Received RADIUS Access-Request	14
11018	RADIUS is re-using an existing session	0

マシン認証の詳細

ユーザ認証の詳細なライブログを確認します。



Cisco ISE

Overview

Event	5200 Authentication succeeded
Username	AD\testuser
Endpoint Id	B4:96:91:15:84:CB
Endpoint Profile	Intel-Device
Authentication Policy	MAR_Test >> MAR_dot1x
Authorization Policy	MAR_Test >> User_MAR_Passed
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2024-05-07 16:36:13.748
Received Timestamp	2024-05-07 16:36:13.748
Policy Server	ise33-01
Event	5200 Authentication succeeded
Username	AD\testuser
Endpoint Id	B4:96:91:15:84:CB
Calling Station Id	B4-96-91-15-84-CB
Endpoint Profile	Intel-Device
IPv4 Address	1.[redacted]0.9
Authentication Identity Store	AD_Join_Point
Identity Group	Profiled
Audit Session Id	01C2006500000049AA780D80
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)

Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request - AD_Join_Point	
11017	RADIUS created a new session - ad.rem-sy[redacted].em.com	0
15049	Evaluating Policy Group - AD_Join_Point	0
15008	Evaluating Service Selection Policy	1
11507	Extracted EAP-Response/Identity	7
12500	Prepared EAP-Request proposing EAP-TLS with challenge	0
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	8
11018	RADIUS is re-using an existing session	0
12301	Extracted EAP-Response/NAK requesting to use PEAP instead	0
12300	Prepared EAP-Request proposing PEAP with challenge	1
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	11
11018	RADIUS is re-using an existing session	0
12302	Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated	0
61025	Open secure connection with TLS peer	0
12318	Successfully negotiated PEAP version 0	1
12800	Extracted first TLS record; TLS handshake started	0
12805	Extracted TLS ClientHello message	0
12806	Prepared TLS ServerHello message	0
12807	Prepared TLS Certificate message	0
12808	Prepared TLS ServerKeyExchange message	28
12810	Prepared TLS ServerDone message	0
12305	Prepared EAP-Request with another PEAP challenge	1
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	30
11018	RADIUS is re-using an existing session	0
12304	Extracted EAP-Response containing PEAP challenge-	0

ユーザ認証の詳細

パターン2ユーザ認証のみ

ステップ１：Windows PCのNICを無効および有効にする

ユーザ認証をトリガーするには、Win10 PC1のNICを無効および有効にします。

ステップ２：認証セッションの確認

show authentication sessions interface GigabitEthernet1/0/2 detailsコマンドを実行して、C1000でのユーザ認証セッションを確認します。

<#root>

Switch#

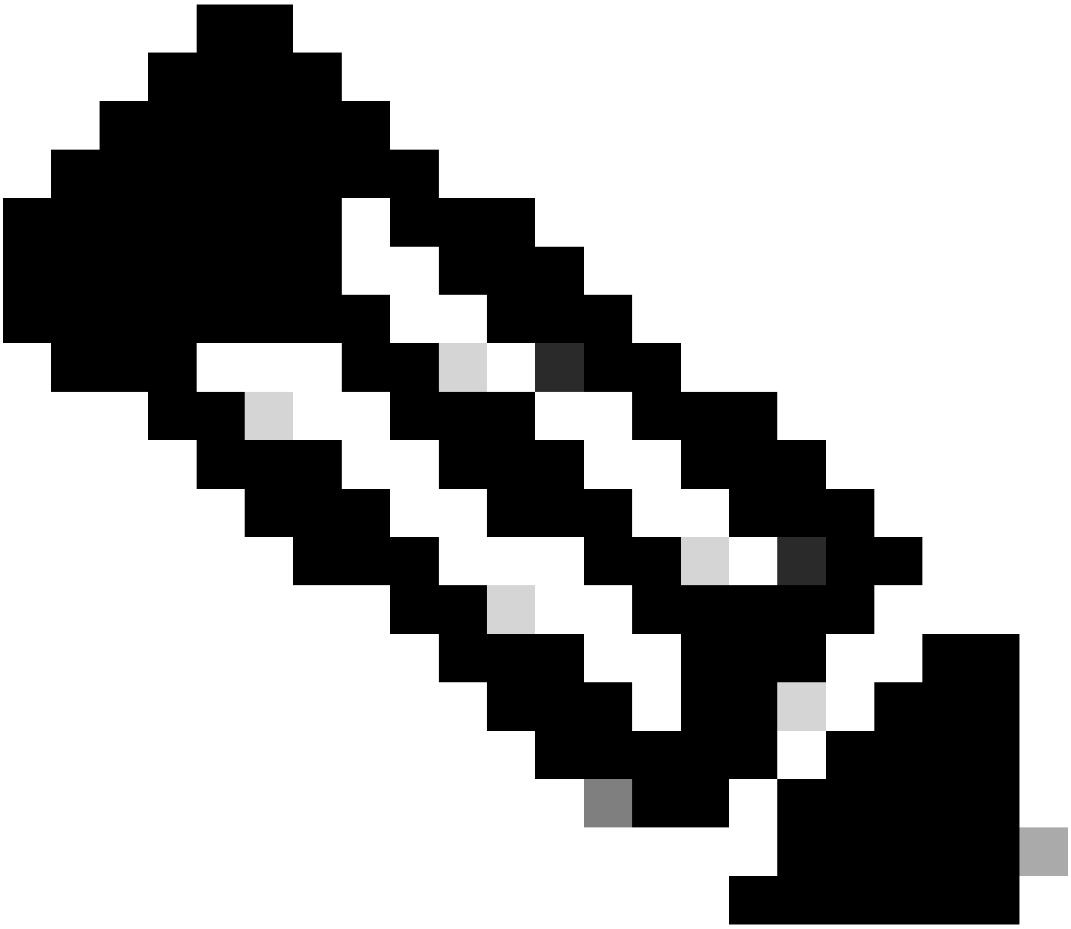
show authentication sessions interface GigabitEthernet1/0/2 details

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

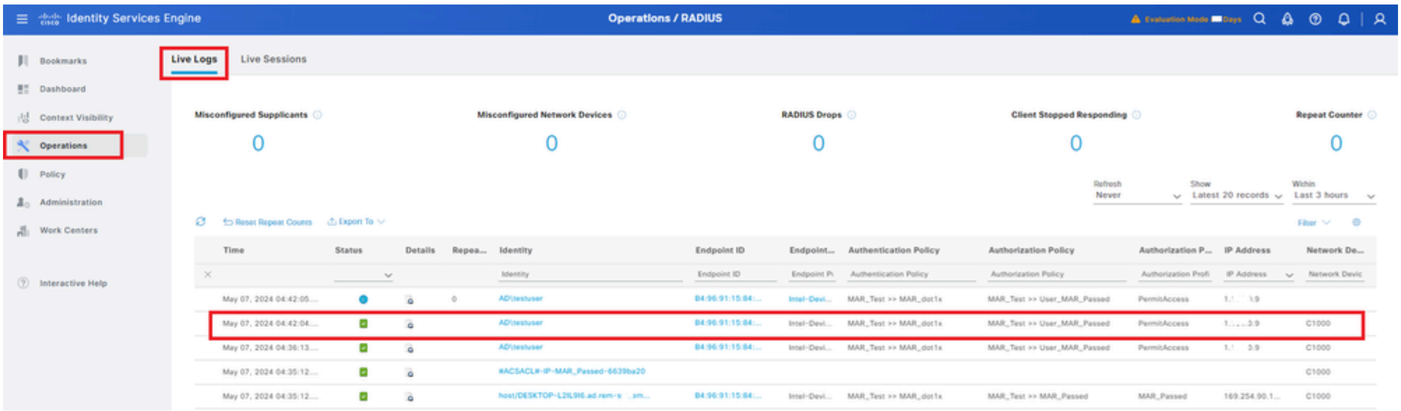
```
User-Name: AD\testuser
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 419s
Common Session ID: 01C2006500000049AA780D80
Acct Session ID: 0x0000003D
Handle: 0x66000016
Current Policy: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

ステップ 3：Radiusライブログの確認

ISE GUIで、**Operations** > **RADIUS** > **Live Logs**の順に移動し、ユーザ認証のライブログを確認します。



注:MARキャッシュはISEに保存されるため、必要なのはユーザ認証だけです。



Misconfigured Supplicants 0

Misconfigured Network Devices 0

RADIUS Drops 0

Client Stopped Responding 0

Repeat Counter 0

Refresh: Never

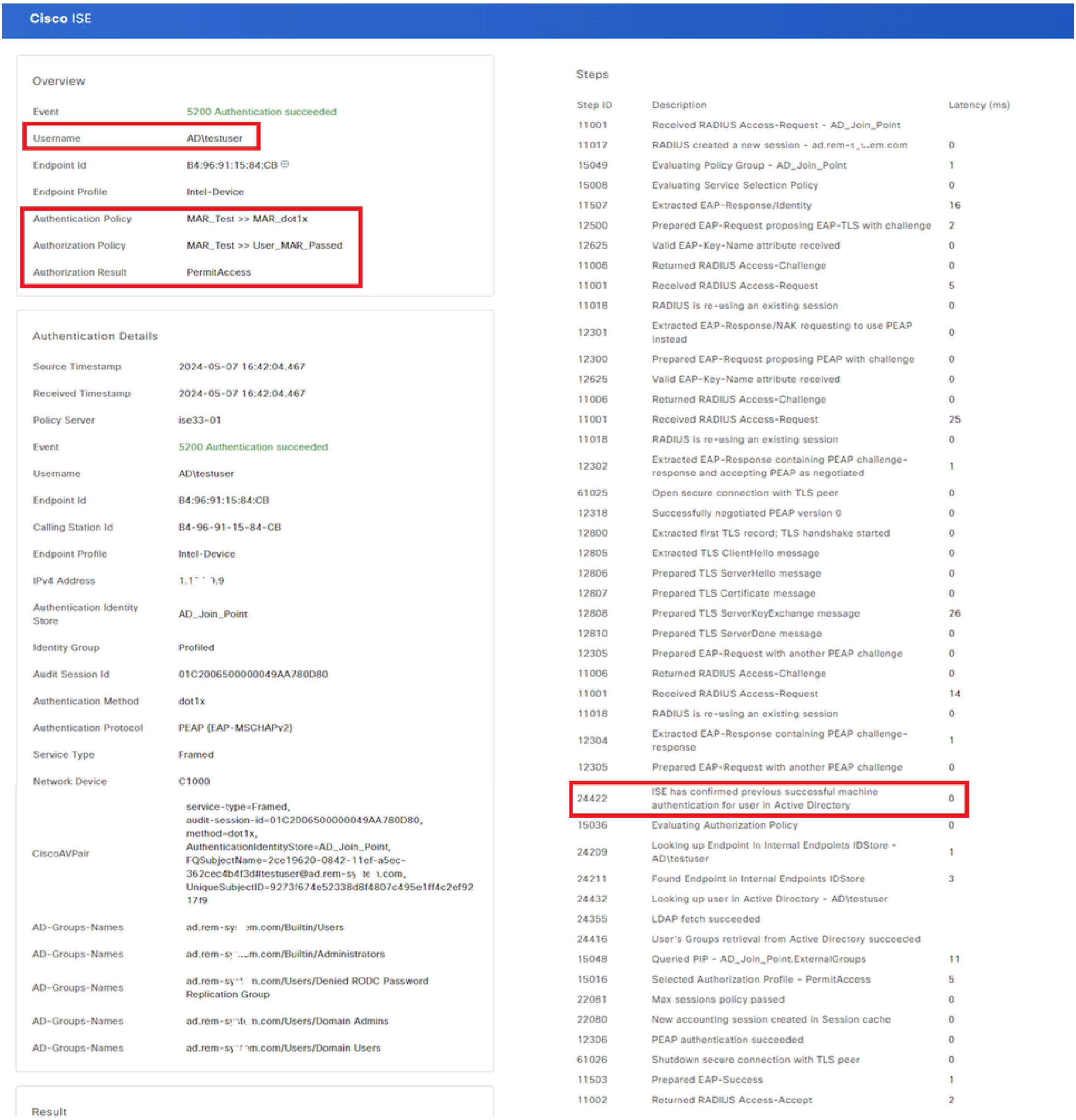
Show: Latest 20 records

Within: Last 3 hours

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication Policy	Authorization Policy	Authorization P...	IP Address	Network De...
				Identity	Endpoint ID	Endpoint P	Authentication Policy	Authorization Policy	Authorization Profi	IP Address	Network Devic
May 07, 2024 04:42:05....	●		0	AD\testuser	B4:96:91:15:84:...	Intel-Devi...	MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed	PermitAccess	1.1. 1.9	
May 07, 2024 04:42:04....	✓			AD\testuser	B4:96:91:15:84:...	Intel-Devi...	MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed	PermitAccess	1. .3.9	C1000
May 07, 2024 04:36:13....	✓			AD\testuser	B4:96:91:15:84:...	Intel-Devi...	MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed	PermitAccess	1.1 3.9	C1000
May 07, 2024 04:35:12....	✓			#ACSACL#-IP-MAR_Passed-6639ba20							C1000
May 07, 2024 04:35:12....	✓			host/DESKTOP-L2IL9I6.ad.rem-s .am...	B4:96:91:15:84:...	Intel-Devi...	MAR_Test >> MAR_dot1x	MAR_Test >> MAR_Passed	MAR_Passed	169.254.90.1...	C1000

*Radius*ライブログ

ユーザ認証の詳細なライブログを確認します。



Cisco ISE

Overview

Event	5200 Authentication succeeded
Username	AD\testuser
Endpoint Id	B4:96:91:15:84:CB ⊕
Endpoint Profile	Intel-Device
Authentication Policy	MAR_Test >> MAR_dot1x
Authorization Policy	MAR_Test >> User_MAR_Passed
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2024-05-07 16:42:04.467
Received Timestamp	2024-05-07 16:42:04.467
Policy Server	ise33-01
Event	5200 Authentication succeeded
Username	AD\testuser
Endpoint Id	B4:96:91:15:84:CB
Calling Station Id	B4-96-91-15-84-CB
Endpoint Profile	Intel-Device
IPv4 Address	1.1⁻ ˈ).9
Authentication Identity Store	AD_Join_Point
Identity Group	Profiled
Audit Session Id	01C2006500000049AA780D80
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	C1000

CiscoAVPair	service-type=Framed,
	audit-session-id=01C2006500000049AA780D80,
	method=dot1x,
	AuthenticationIdentityStore=AD_Join_Point,
	FQSubjectName=2ce19620-0842-11ef-a5ec-362cec4b4f3d#testuser@ad.rem-sy te 1.com,
	UniqueSubjectID=9273f674e52338d8f4807c495e1ff4c2ef9217f9

AD-Groups-Names	ad.rem-sy: :m.com/Builtin/Users
AD-Groups-Names	ad.rem-s ..m.com/Builtin/Administrators
AD-Groups-Names	ad.rem-sy n.com/Users/Denied RODC Password Replication Group
AD-Groups-Names	ad.rem-syste n.com/Users/Domain Admins
AD-Groups-Names	ad.rem-sy m.com/Users/Domain Users

Result

Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request - AD_Join_Point	
11017	RADIUS created a new session - ad.rem-s ..em.com	0
15049	Evaluating Policy Group - AD_Join_Point	1
15008	Evaluating Service Selection Policy	0
11507	Extracted EAP-Response/Identity	16
12500	Prepared EAP-Request proposing EAP-TLS with challenge	2
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	5
11018	RADIUS is re-using an existing session	0
12301	Extracted EAP-Response/NAK requesting to use PEAP instead	0
12300	Prepared EAP-Request proposing PEAP with challenge	0
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	25
11018	RADIUS is re-using an existing session	0
12302	Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated	1
61025	Open secure connection with TLS peer	0
12318	Successfully negotiated PEAP version 0	0
12800	Extracted first TLS record; TLS handshake started	0
12805	Extracted TLS ClientHello message	0
12806	Prepared TLS ServerHello message	0
12807	Prepared TLS Certificate message	0
12808	Prepared TLS ServerKeyExchange message	26
12810	Prepared TLS ServerDone message	0
12305	Prepared EAP-Request with another PEAP challenge	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	14
11018	RADIUS is re-using an existing session	0
12304	Extracted EAP-Response containing PEAP challenge-response	1
12305	Prepared EAP-Request with another PEAP challenge	0
24422	ISE has confirmed previous successful machine authentication for user in Active Directory	0
15036	Evaluating Authorization Policy	0
24209	Looking up Endpoint in Internal Endpoints IDStore - AD\testuser	1
24211	Found Endpoint in Internal Endpoints IDStore	3
24432	Looking up user in Active Directory - AD\testuser	
24355	LDAP fetch succeeded	
24416	User's Groups retrieval from Active Directory succeeded	
15048	Queried PIP - AD_Join_Point.ExternalGroups	11
15016	Selected Authorization Profile - PermitAccess	5
22081	Max sessions policy passed	0
22080	New accounting session created in Session cache	0
12306	PEAP authentication succeeded	0
61026	Shutdown secure connection with TLS peer	0
11503	Prepared EAP-Success	1
11002	Returned RADIUS Access-Accept	2

ユーザ認証の詳細

トラブルシュート

次のデバッグログ(prrt-server.log)は、ISEでの認証の詳細な動作を確認するのに役立ちます。

- ランタイム設定

- ランタイムロギング
- ランタイムAAA

次に、パターン1のデバッググログの例を示します。このドキュメントの「マシン認証とユーザ認証」。

<#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
```

関連情報

マシン アクセス制限の長所と短所

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。