Configura autenticazione a due fattori del computer per accesso supplicant

Sommario

Introduzione

In questo documento viene descritto come configurare l'autenticazione a due fattori con l'autenticazione computer e dot1x.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione di Cisco Identity Services Engine
- Configurazione di Cisco Catalyst
- IEEE802.1X

Componenti usati

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

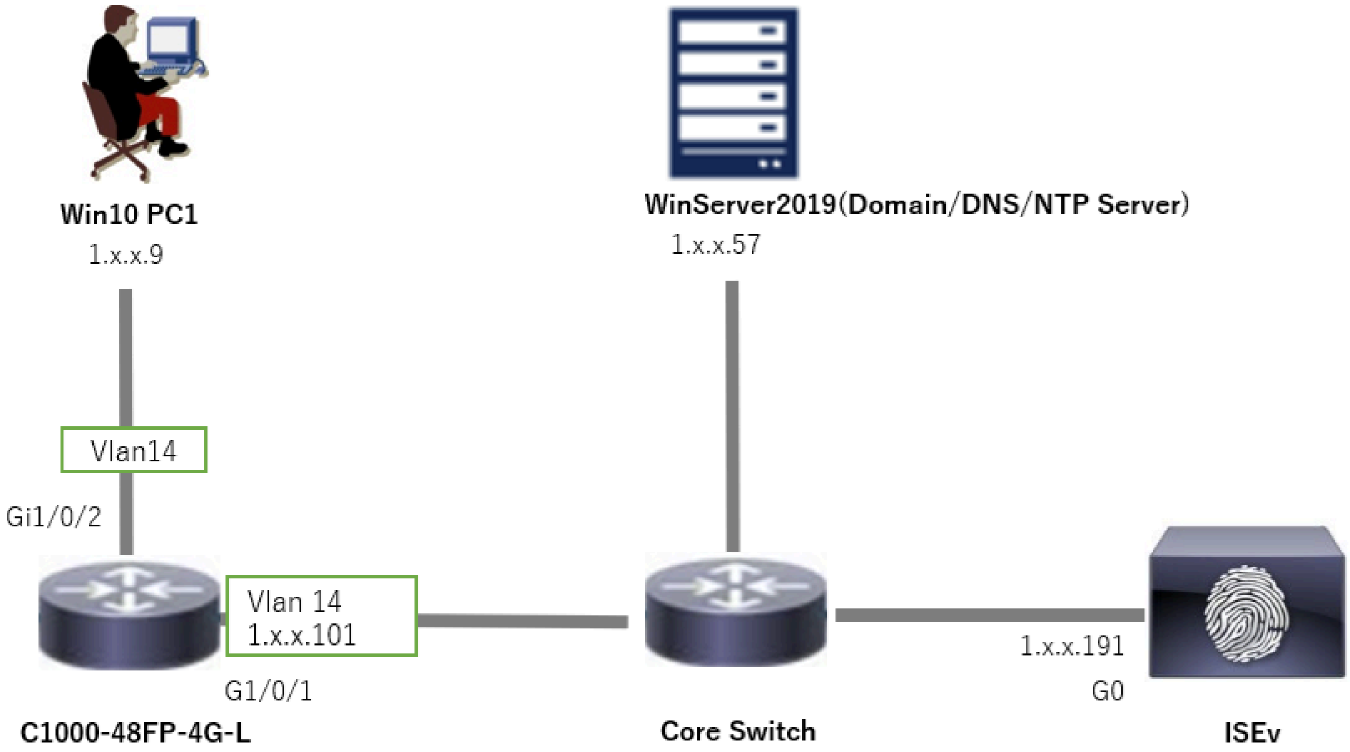
- Windows Server 2019

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esempio di rete

Nell'immagine è illustrata la topologia utilizzata per l'esempio del documento.

Il nome di dominio configurato in Windows Server 2019 è ad.rem-xxx.com, utilizzato come esempio in questo documento.



Esempio di rete

Premesse

L'autenticazione del computer è un processo di protezione che verifica l'identità di un dispositivo che richiede l'accesso a una rete o a un sistema. A differenza dell'autenticazione utente, che verifica l'identità di un utente in base a credenziali quali nome utente e password, l'autenticazione del computer è incentrata sulla convalida del dispositivo stesso. Questa operazione viene spesso eseguita utilizzando certificati digitali o chiavi di sicurezza univoche per il dispositivo.

Utilizzando l'autenticazione di computer e utenti insieme, un'organizzazione può garantire che solo i dispositivi e gli utenti autorizzati possano accedere alla propria rete, fornendo così un ambiente più sicuro. Questo metodo di autenticazione a due fattori è particolarmente utile per proteggere le informazioni sensibili e rispettare i severi standard normativi.

Configurazioni

Configurazione in C1000

Questa è la configurazione minima nella CLI di C1000.

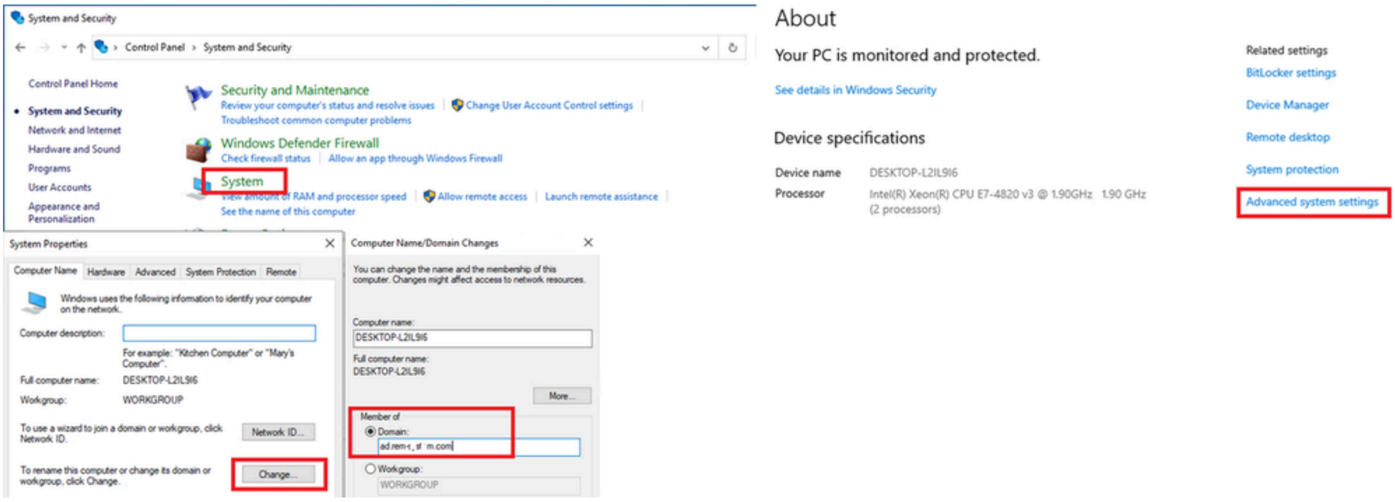
```
aaa new-model

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
```

Configurazione in un PC Windows

Passaggio 1. Aggiungi PC a dominio Active Directory

Passare a Pannello di controllo > Sistema e sicurezza, fare clic su Sistema e quindi su Impostazioni di sistema avanzate. Nella finestra Proprietà del sistema, fare clic su Cambia, selezionare Dominio e immettere il nome del dominio.



Your PC is monitored and protected.

Device specifications

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

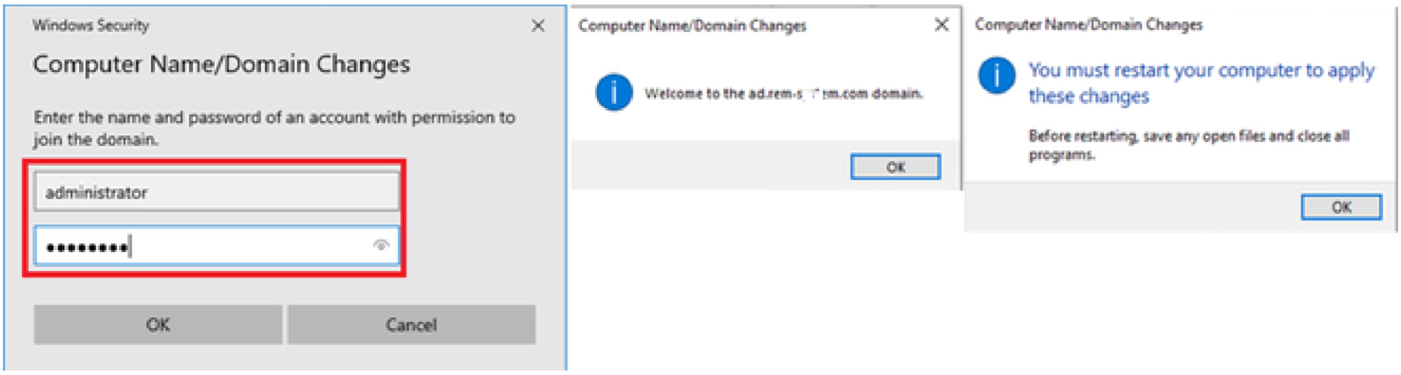
Member of

● Domain: ad.rem-t_s m.com

○ Workgroup: WORKGROUP

Aggiungi PC a dominio Active Directory

Nella finestra Protezione di Windows, immettere nome utente e password del server di dominio.



Windows Security

Computer Name/Domain Changes

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

administrator

•••••••••

OK | Cancel

Computer Name/Domain Changes

Welcome to the ad.rem-s rm.com domain.

OK

Computer Name/Domain Changes

You must restart your computer to apply these changes

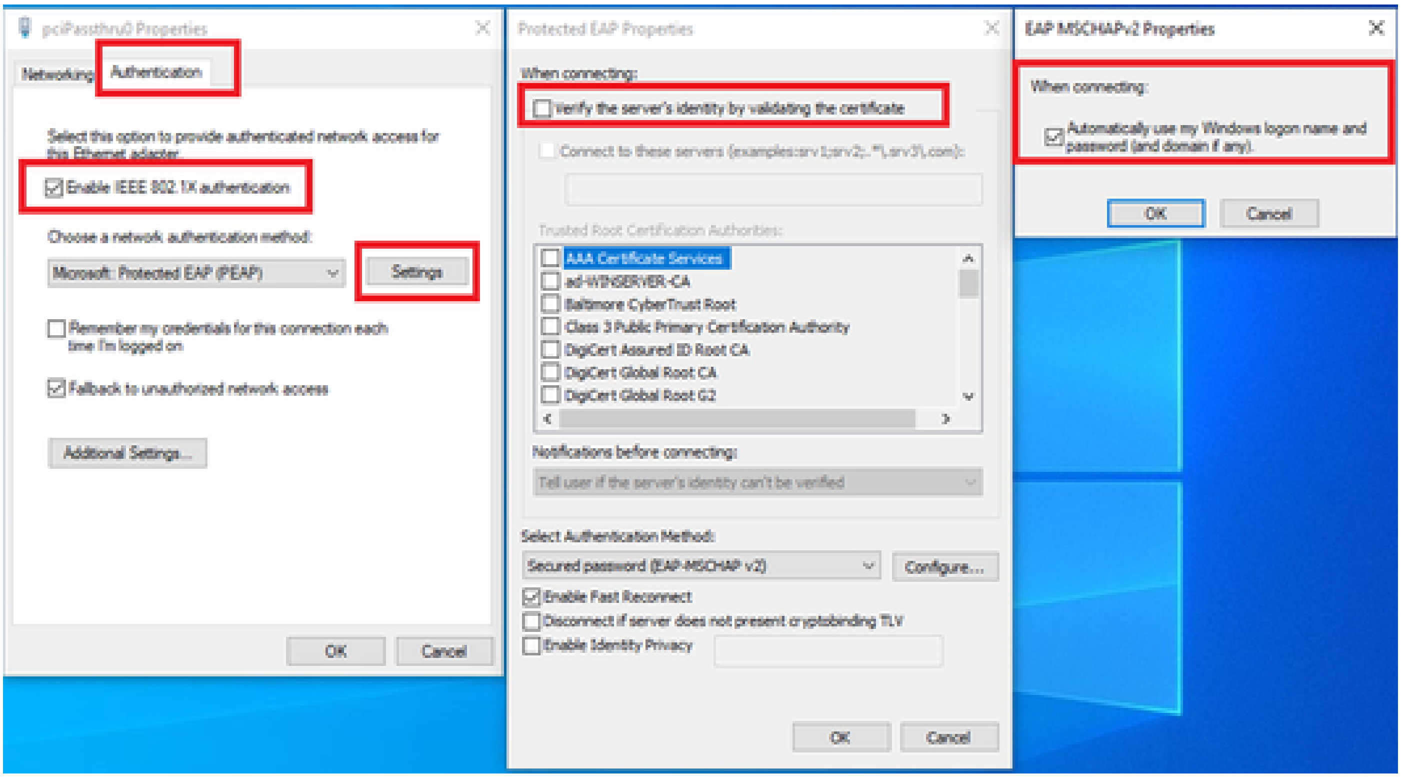
Before restarting, save any open files and close all programs.

OK

Immettere nome utente e password

Passaggio 2. Configura autenticazione utente

Passare a Autenticazione, selezionare Abilita autenticazione IEEE 802.1X. Fare clic su Impostazioni nella finestra Proprietà PEAP, deselezionare Verifica l'identità del server convalidando il certificato e fare clic su Configura. Nella finestra EAP MSCHAPv2 Properties, selezionare Automatically use my Windows logon name and password (and domain if any) (Usa automaticamente nome di accesso e password di Windows (e dominio se presente) per utilizzare il nome utente immesso durante l'accesso al computer Windows per l'autenticazione utente.



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

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) | Configure...

☑ Enable Fast Reconnect

☐ Disconnect if server does not present cryptobinding TLV

☐ Enable Identity Privacy

OK | Cancel

EAP MSCHAPv2 Properties

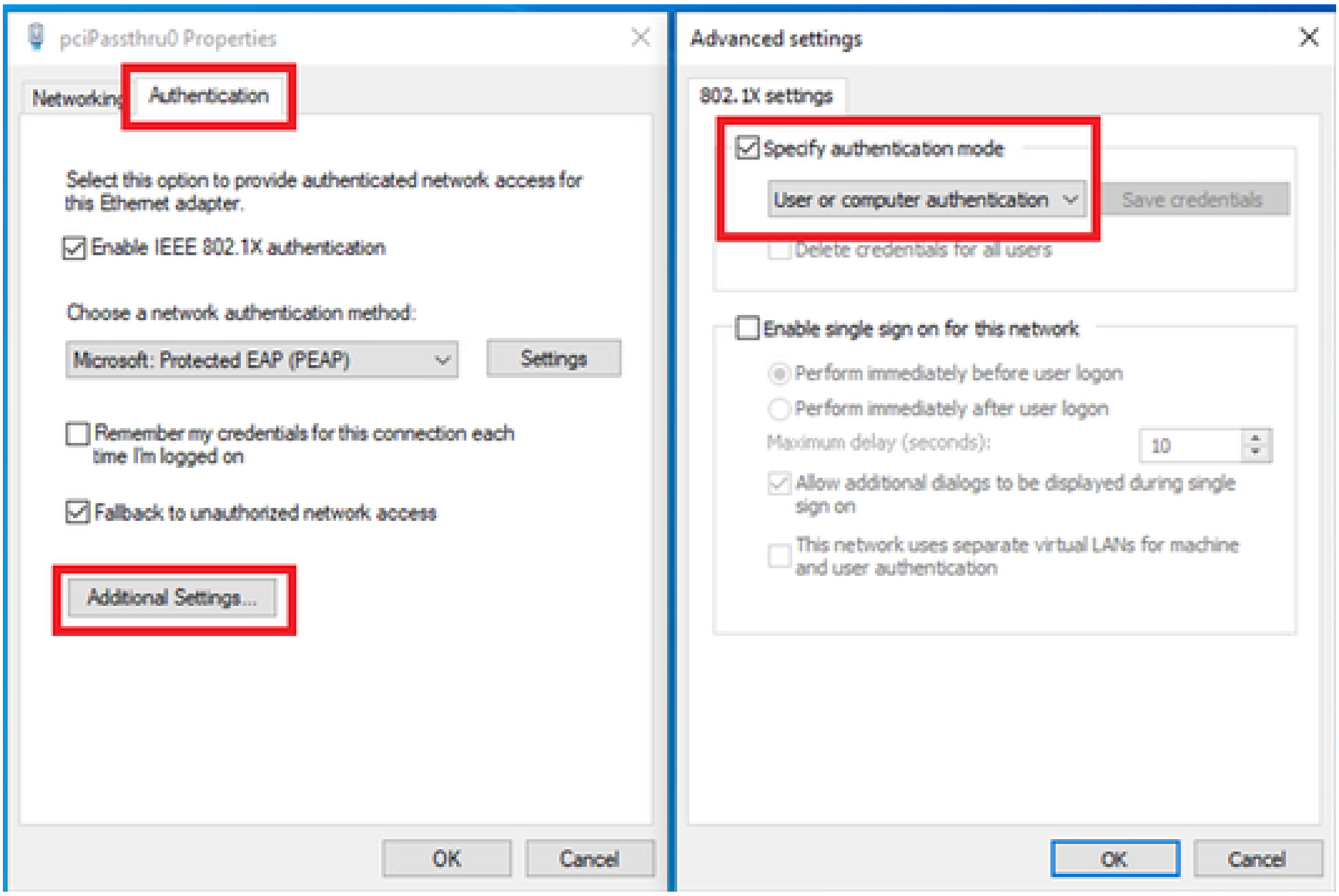
When connecting:

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

OK Cancel

Abilita autenticazione utente

Passare a Autenticazione, selezionare Impostazioni aggiuntive. Selezionare Autenticazione utente o computer dall'elenco a discesa.



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

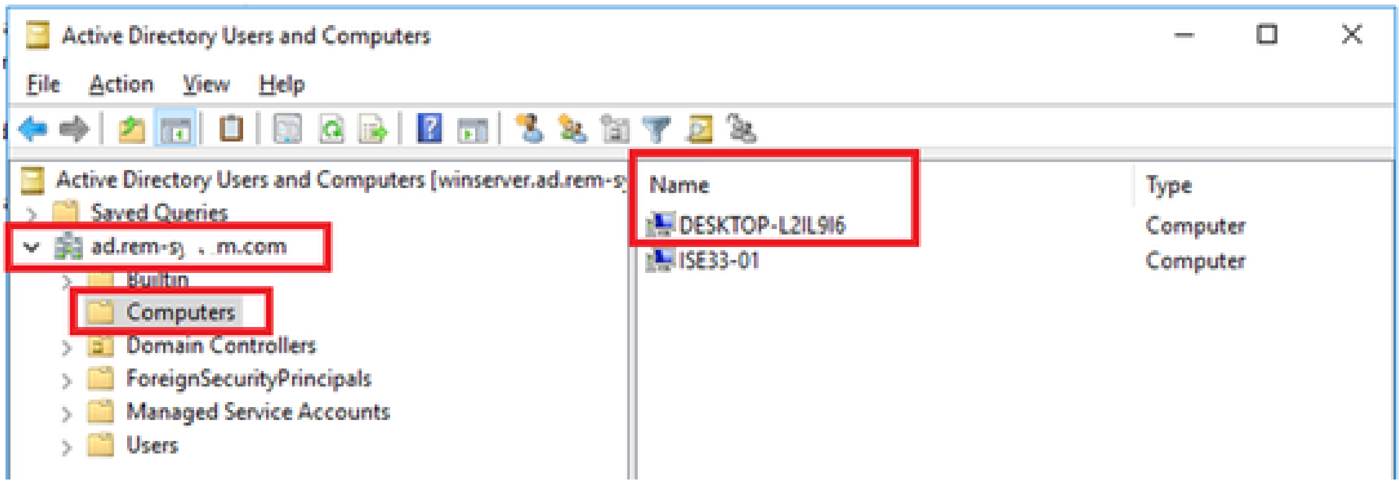
OK | Cancel

Specifica modalità di autenticazione

Configurazione in Windows Server

Passaggio 1. Conferma computer del dominio

Passare a Utenti e computer di Active Directory, quindi fare clic su Computer. Confermare che Win10 PC1 sia elencato nel dominio.



Active Directory Users and Computers

Active Directory Users and Computers [winserver.ad.rem-sy

Saved Queries

ad.rem-sy . m.com

Builtin

Computers

Domain Controllers

ForeignSecurityPrincipals

Managed Service Accounts

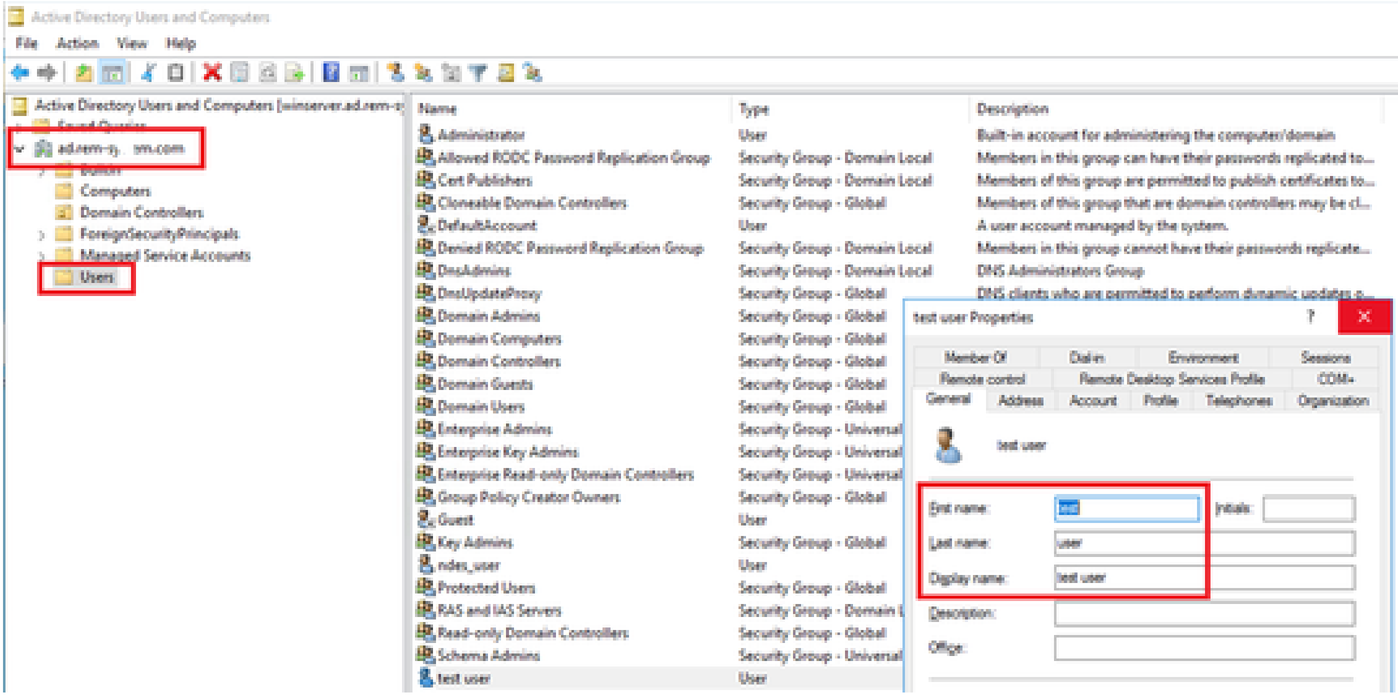
Users

Name	Type
DESKTOP-L2IL9I6	Computer
ISE33-01	Computer

Conferma computer del dominio

Passaggio 2. Aggiungi utente di dominio

Passare a Utenti e computer di Active Directory, quindi fare clic su Utenti. Aggiungere testuser come utente di dominio.



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	

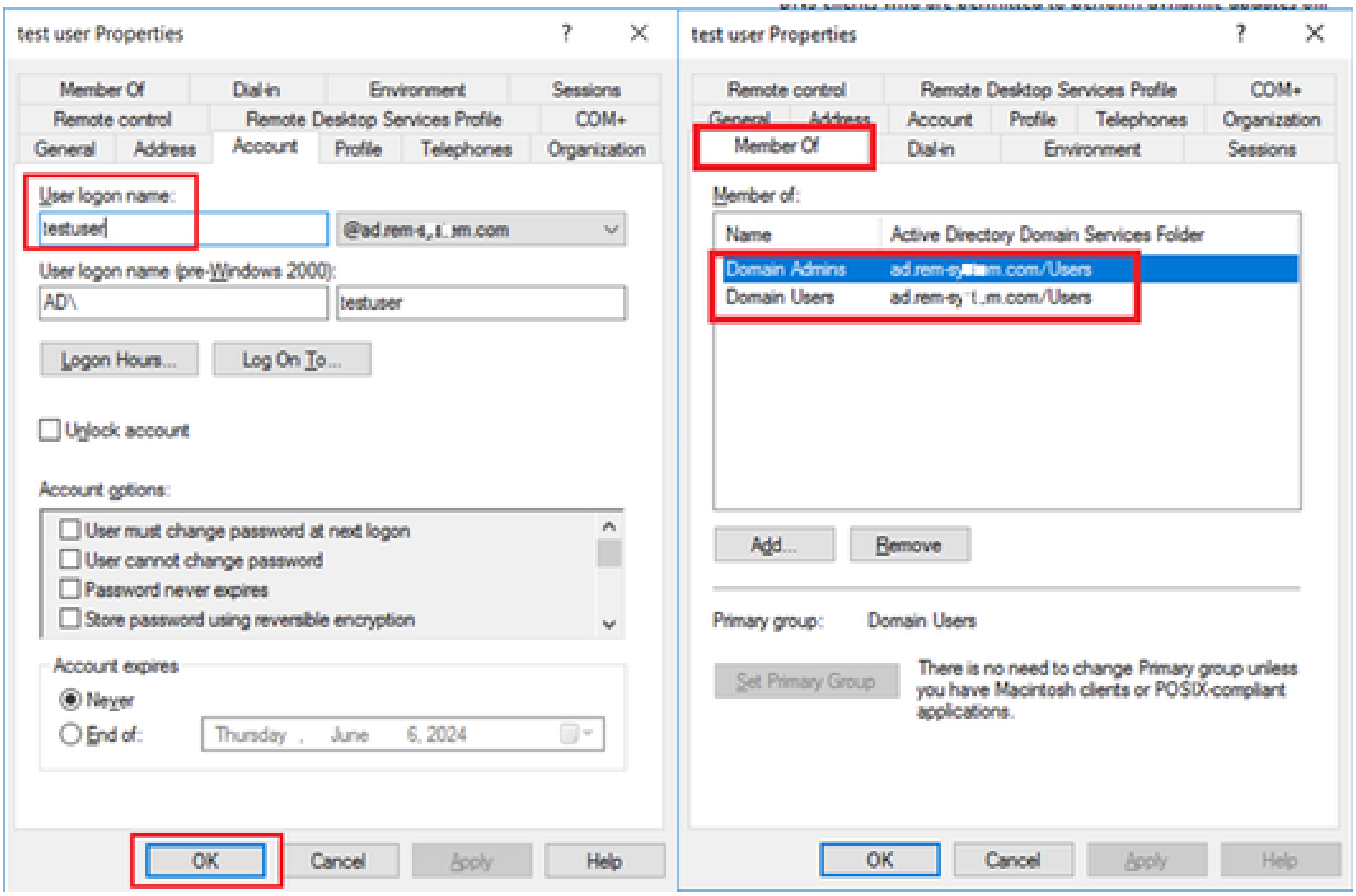
test user Properties

test user

First name: test
Initials:
Last name: user
Display name: test user
Description:
Office:

Aggiungi utente di dominio

Aggiungere l'utente del dominio al membro di Domain Admins e Domain Users.



test user Properties

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

test user Properties

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

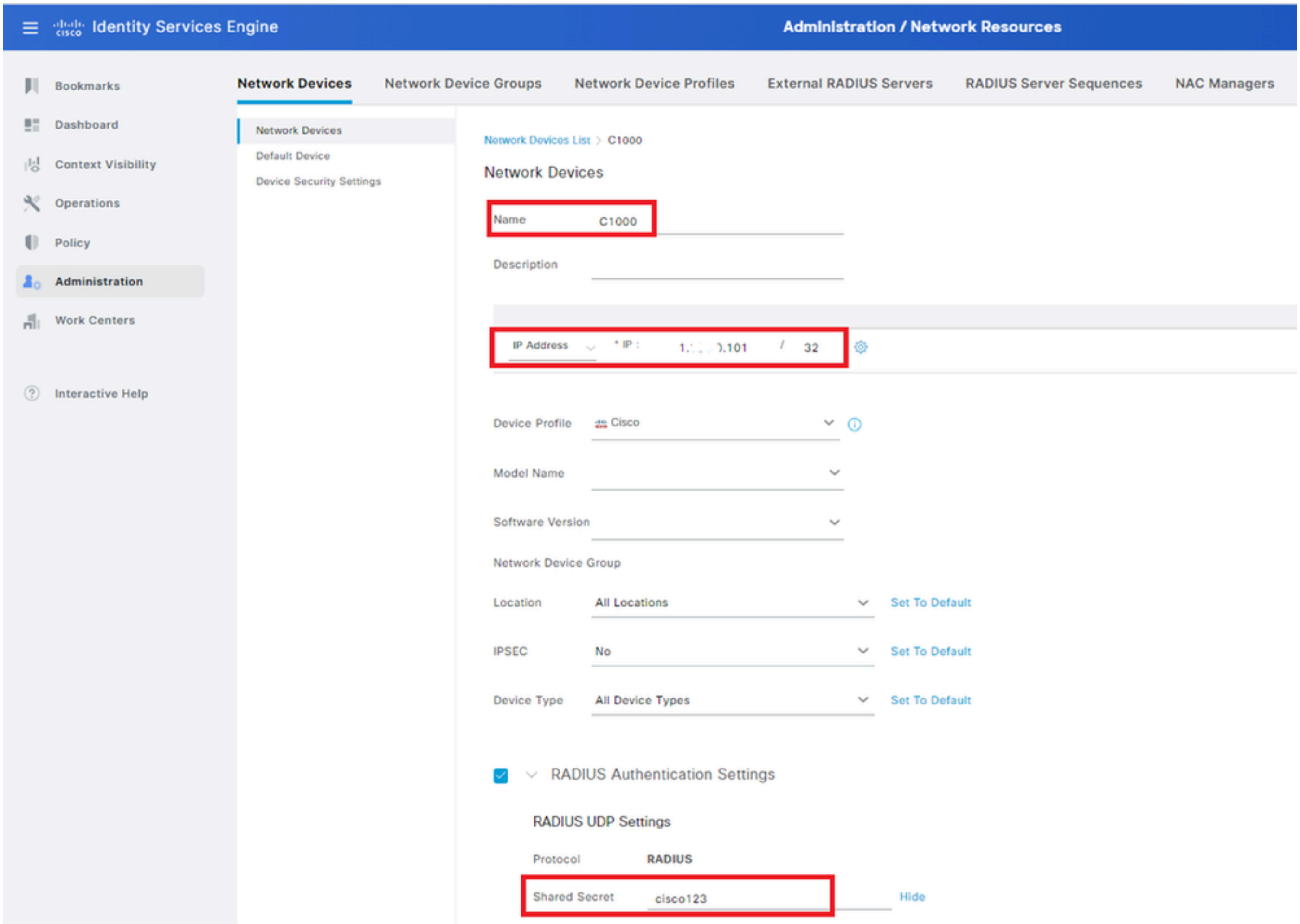
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

Domain Admins e Domain Users

Configurazione in ISE

Passaggio 1. Aggiungi dispositivo

Passare a Amministrazione > Dispositivi di rete, fare clic su Aggiungi pulsante per aggiungere un dispositivo C1000.



Name C1000

Description

IP Address * IP : 1.).101 / 32

Device Profile Cisco

Model Name

Software Version

Network Device Group

Location All Locations

IPSEC No

Device Type All Device Types

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

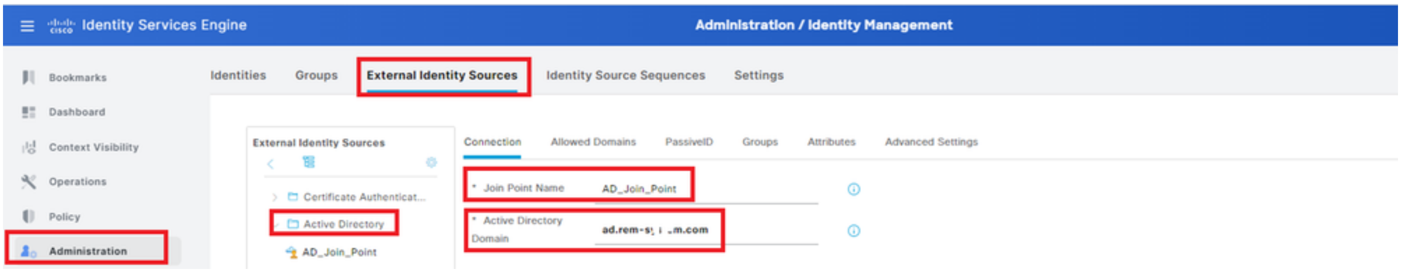
Shared Secret cisco123

Aggiungi dispositivo

Passaggio 2. Aggiungi Active Directory

Selezionare Amministrazione > Origini identità esterne > Active Directory, fare clic sulla scheda Connessione, quindi aggiungere Active Directory a ISE.

- Nome punto di join: AD_Join_Point
- Dominio Active Directory: ad.rem-xxx.com

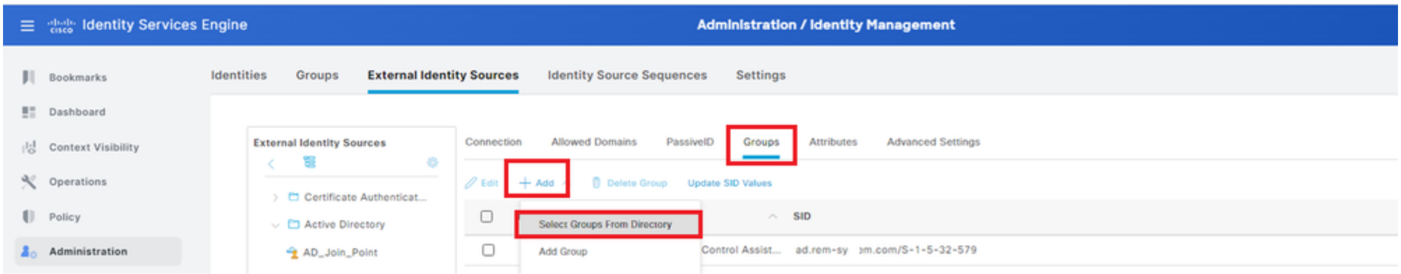


* Join Point Name AD_Join_Point

* Active Directory Domain ad.rem-s ı .m.com

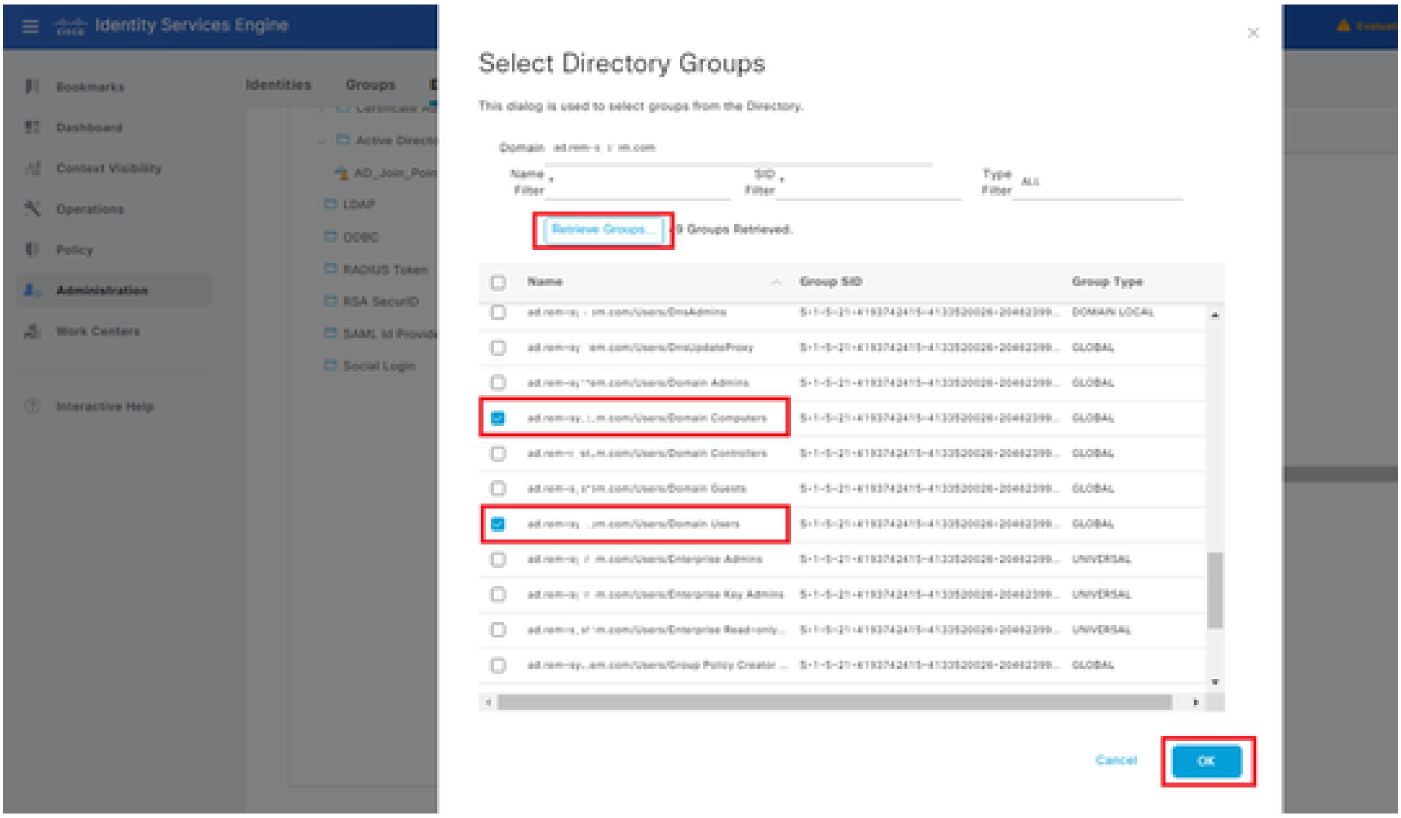
Aggiungi Active Directory

Passare alla scheda Gruppi, quindi selezionare Seleziona gruppi dalla directory dall'elenco a discesa.



Seleziona gruppi dalla directory

Fare clic su Recupera gruppi dall'elenco a discesa. Selezionare ad.rem-xxx.com/Users/Domain Computer e ad.rem-xxx.com/Users/Domain Utenti e fare clic su OK.



This dialog is used to select groups from the Directory.

Domain ad.rem-s m.com

Name Filter

SID Filter

Type Filter ALL

59 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-sy m.com/Users/Domain Controllers	S-1-5-21-4193742415-4133520026-20462399...	GLOBAL
☐	ad.rem-sy 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-sy 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

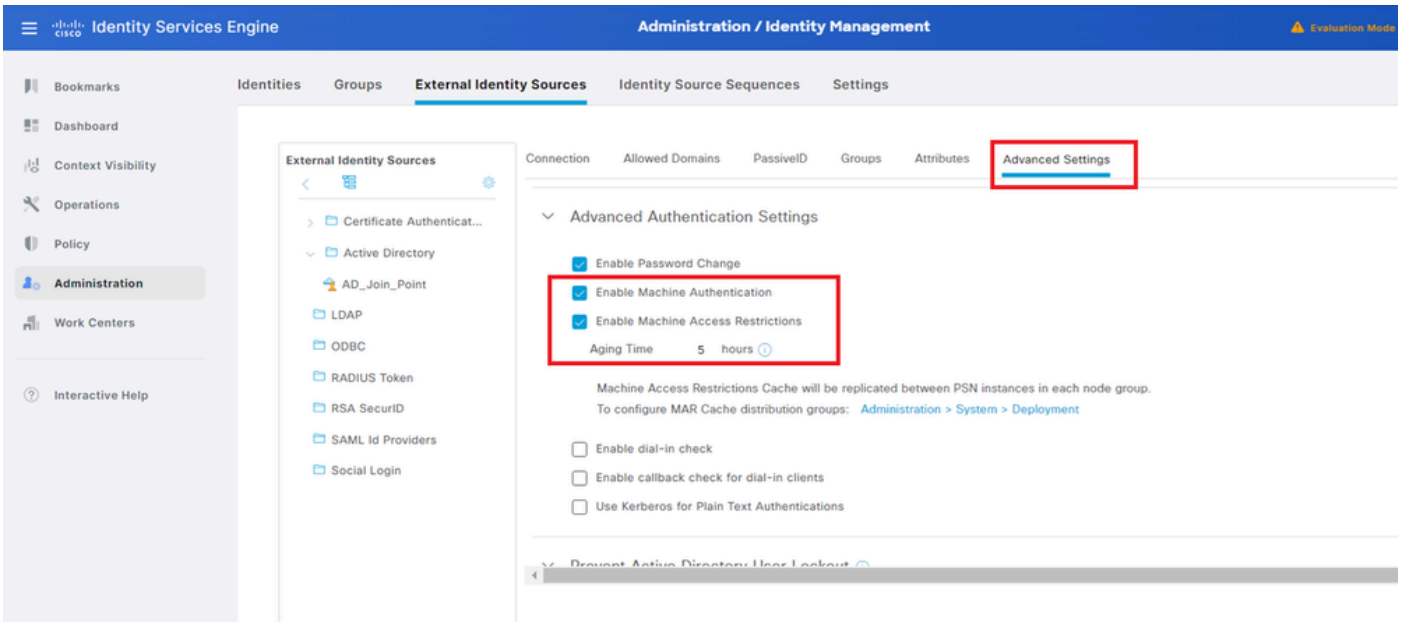
Aggiungi computer e utenti del dominio

Passaggio 3. Conferma impostazione autenticazione computer

Passare alla scheda Advanced Settings (Impostazioni avanzate) e confermare l'impostazione dell'autenticazione del computer.

- Abilita autenticazione computer: per abilitare l'autenticazione del computer
- Abilita restrizione accesso computer: per combinare l'autenticazione di utenti e computer prima dell'autorizzazione

Nota: l'intervallo valido per il periodo di aging è compreso tra 1 e 8760.



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

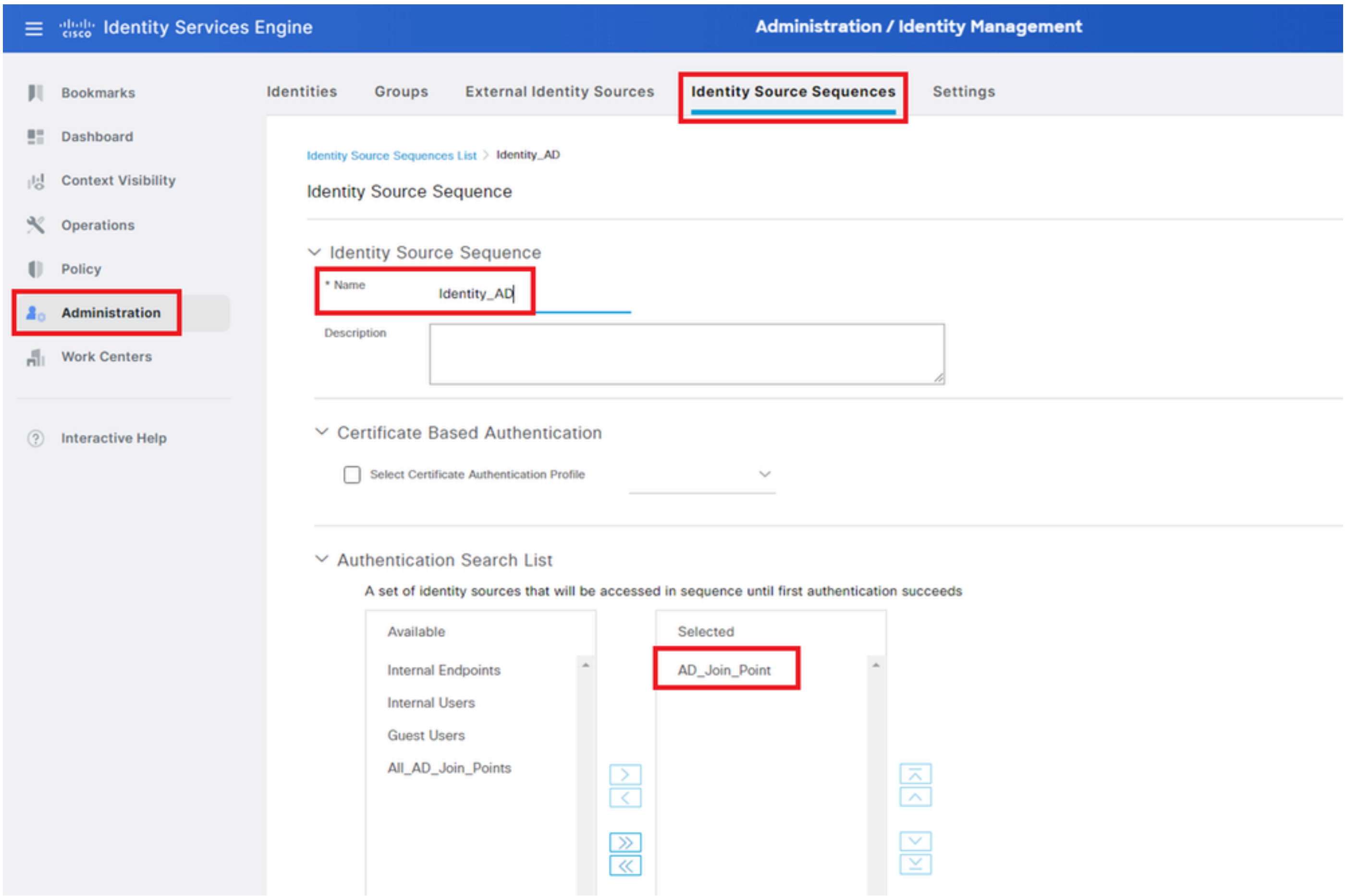
☐ Use Kerberos for Plain Text Authentications

Impostazione di autenticazione computer

Passaggio 4. Aggiungi sequenze origine identità

Passare a Amministrazione > Sequenze origine identità, quindi aggiungere una sequenza.

- Nome: Identity_AD
- Elenco di ricerca autenticazione: AD_Join_Point



Name: Identity_AD

☐ Select Certificate Authentication Profile

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

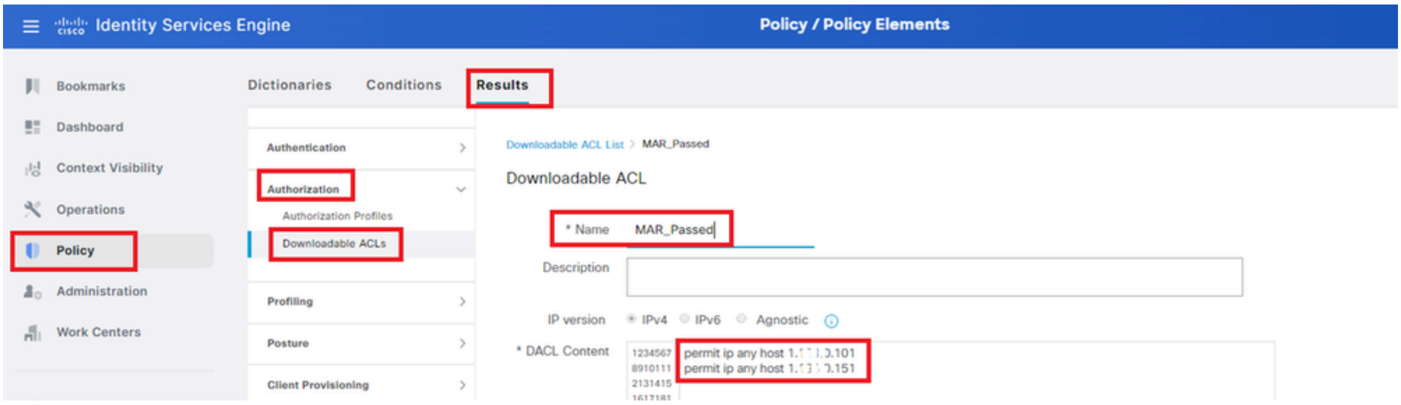
Selected: AD_Join_Point

Aggiungi sequenze origine identità

Passaggio 5. Aggiungi DACL e profilo di autorizzazione

Selezionare Policy > Results > Authorization > Downloadable ACLs (Policy > Risultati > Autorizzazione > ACL scaricabili), quindi aggiungere un DACL.

- Nome: MAR_Passed
- Contenuto DACL: permette ip su qualsiasi host 1.x.x.101 e permette ip su qualsiasi host 1.x.x.105



Downloadable ACL List > MAR_Passed

Downloadable ACL

* Name MAR_Passed

Description

IP version ● IPv4 ○ IPv6 ○ Agnostic

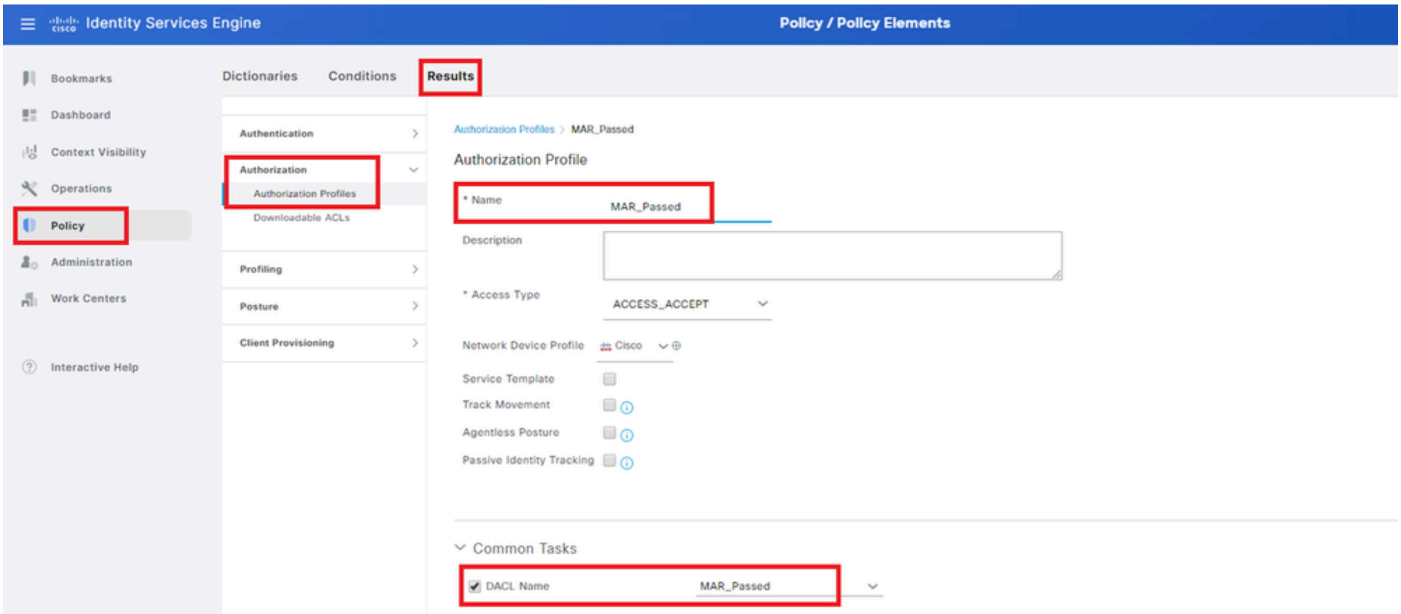
* DACL Content

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

Aggiungi DACL

Passare a Criterio > Risultati > Autorizzazione > Profili di autorizzazione, quindi aggiungere un profilo di autorizzazione.

- Nome: MAR_Passed
- Nome DACL: 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

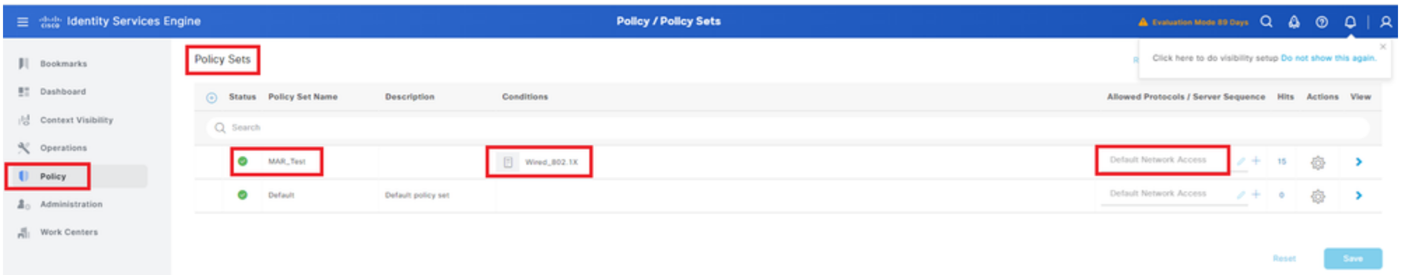
☑ DACL Name MAR_Passed

Aggiungi profilo di autorizzazione

Passaggio 6. Aggiungi set di criteri

Passare a Criterio > Set di criteri, fare clic su + per aggiungere un set di criteri.

- Nome set di criteri: MAR_Test
- Condizioni: Wired_802.1X
- Protocolli consentiti/sequenza server: accesso alla rete predefinito



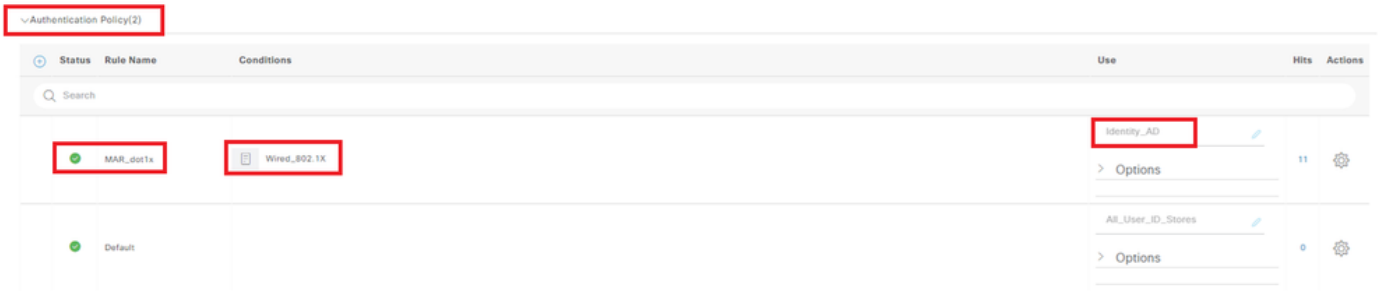
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	MAR_Test		Wired_802.1X	Default Network Access	15	⚙	>
●	Default	Default policy set		Default Network Access	0	⚙	>

Aggiungi set di criteri

Passaggio 7. Aggiungi criterio di autenticazione

Passare a Set di criteri, quindi fare clic su MAR_Test per aggiungere un criterio di autenticazione.

- Nome regola: MAR_dot1x
- Condizioni: Wired_802.1X
- Uso: 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	⚙

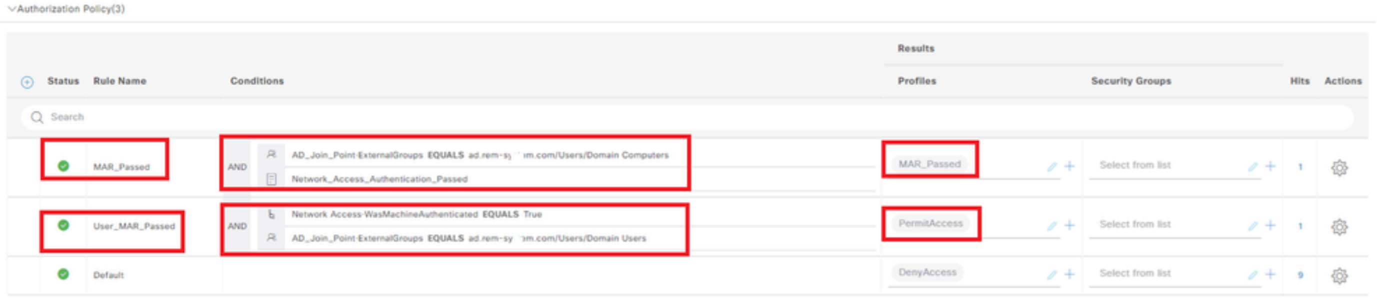
Aggiungi criterio di autenticazione

Passaggio 8. Aggiungi criterio di autorizzazione

Passare a Set di criteri, quindi fare clic su MAR_Test per aggiungere un criterio di autorizzazione.

- Nome regola: MAR_Passed
- Condizioni: AD_Join_Point·ExternalGroups EQUALS ad.rem-xxx.com/Users/Domain Computer E Network_Access_Authentication_Passed
- Risultati: MAR_Passed

- Nome regola: User_MAR_Passed
- Condizioni: Accesso alla rete·WasMachineAuthenticated EQUALS True AND AD_Join_Point·ExternalGroups EQUALS ad.rem-xxx.com/Users/Domain Users
- Risultati: 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	⚙

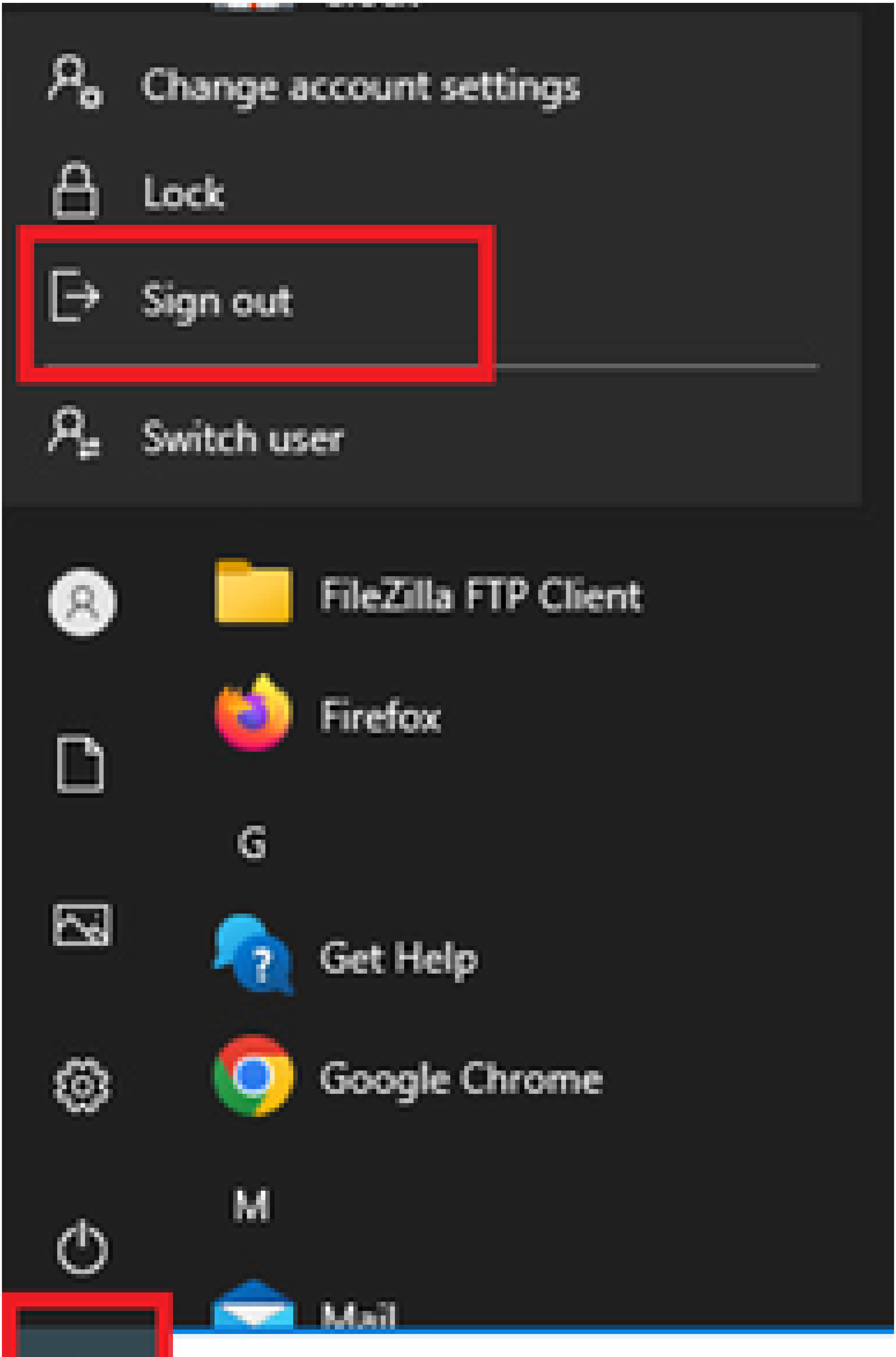
Aggiungi criterio di autorizzazione

Verifica

Motivo 1. Autenticazione computer e autenticazione utente

Passaggio 1. Esci da Windows PC

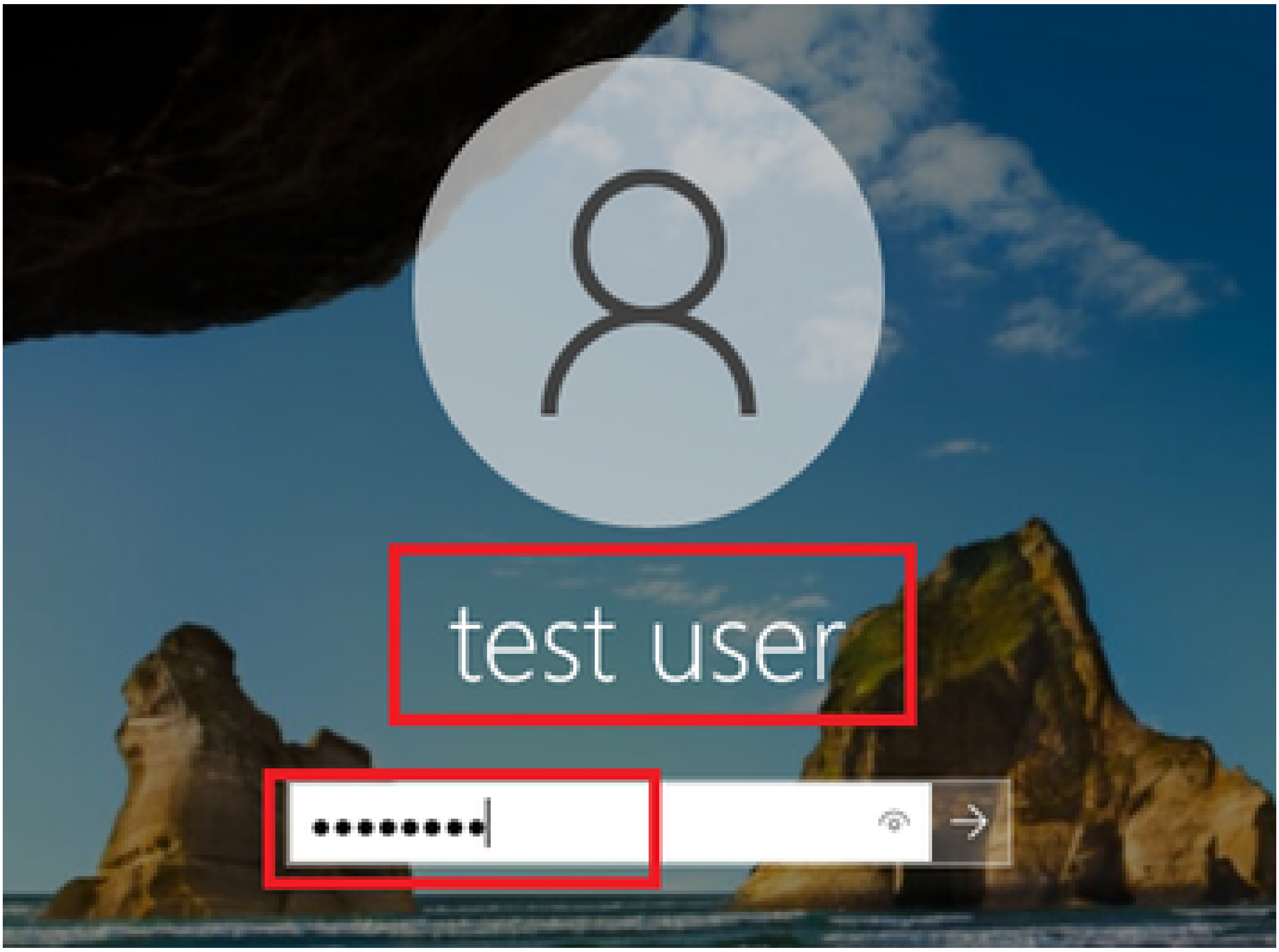
Fare clic sul pulsante Disconnetti da Win10 PC1 per attivare l'autenticazione del computer.


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
```

Passaggio 3. Accedi a PC Windows

Accedere a Win10 PC1, immettere nome utente e password per attivare l'autenticazione utente.



test user

••••••••

Accedi a PC Windows

Passaggio 4. Conferma sessione di autenticazione

Eseguire il comandoshow authentication sessions interface GigabitEthernet1/0/2 details per confermare la sessione di autenticazione utente in 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:
```

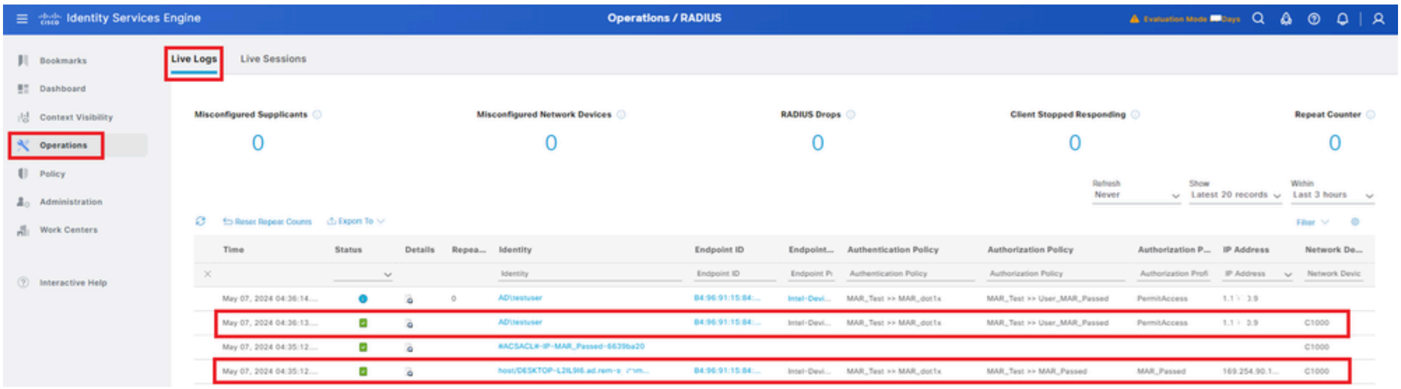
```
AD\testuser
```

```
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
```

Passaggio 5. Conferma registro dinamico Radius

Selezionare **Operations** > **RADIUS** > **Live Logs** nell'interfaccia utente di ISE, quindi confermare il log attivo per l'autenticazione del computer e dell'utente.



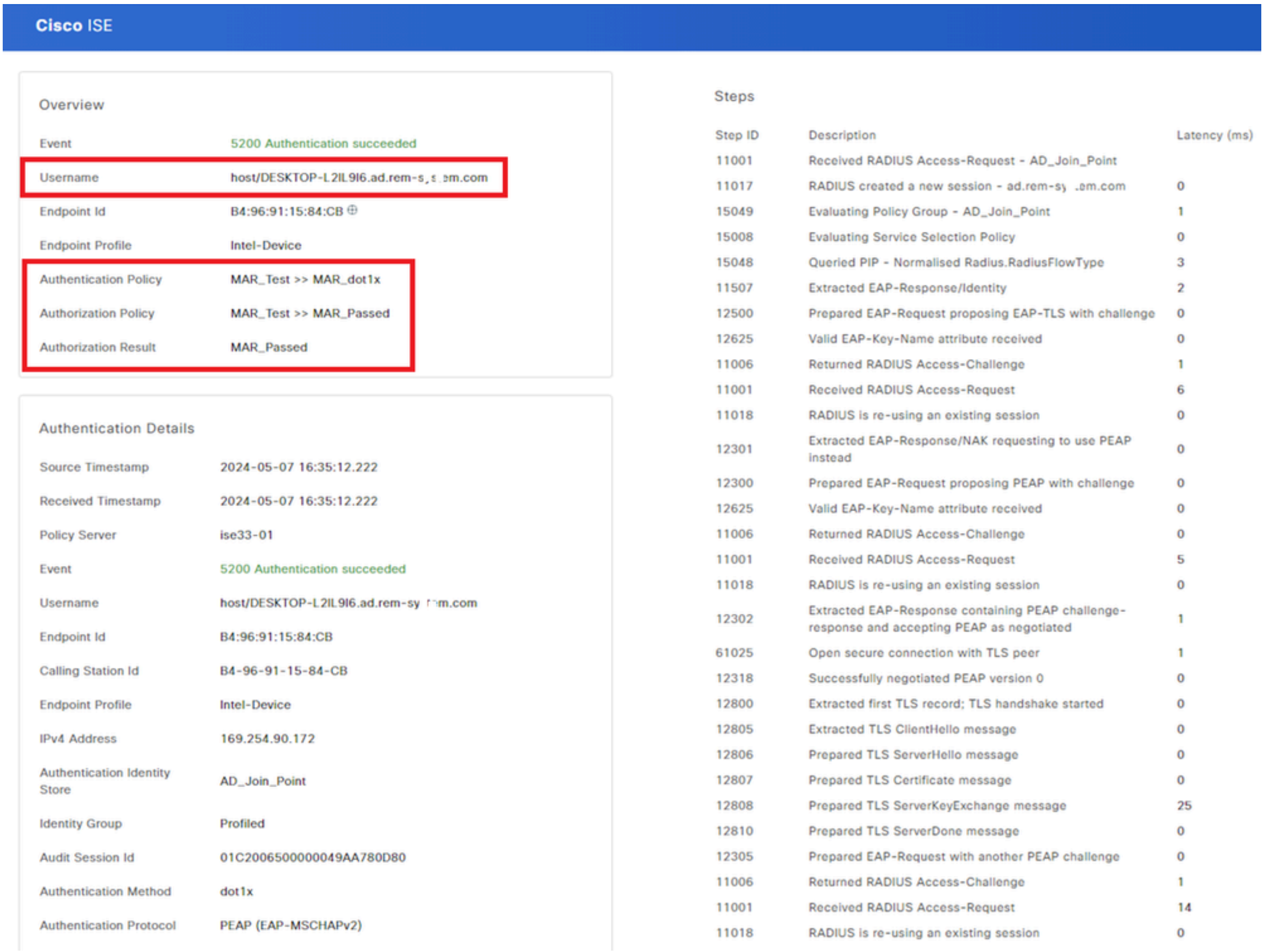
Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	0	0	0

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 [illegible] 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 [illegible] 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[illegible]m...	B4:96:91:15:84:...	Intel-Devi...	MAR_Test >> MAR_dot1x	MAR_Test >> MAR_Passed	MAR_Passed	169.254.90.1...	C1000

Registro Radius Live

Confermare il registro dettagliato dell'autenticazione del computer.



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

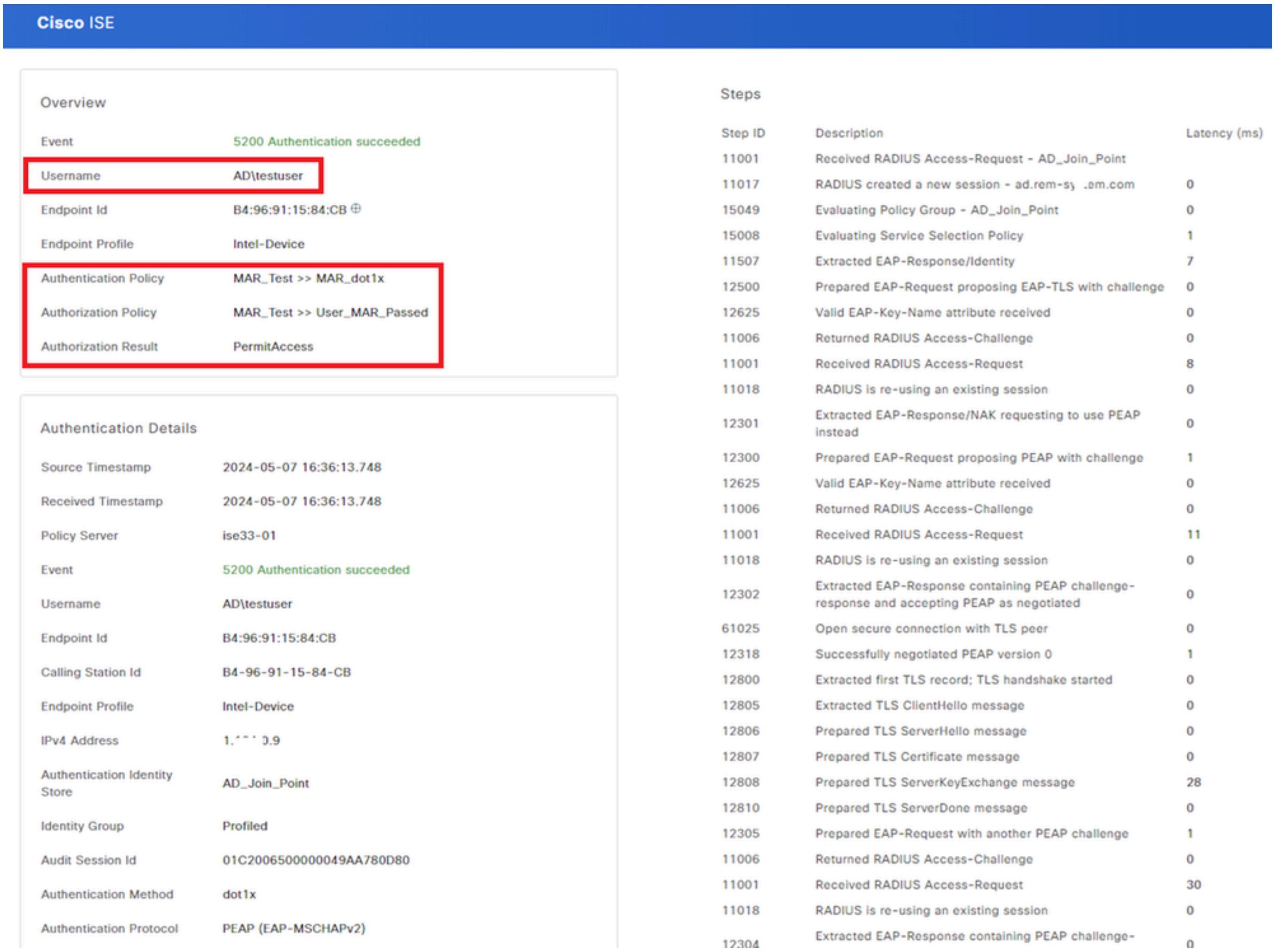
Source Timestamp	2024-05-07 16:35:12.222
Received Timestamp	2024-05-07 16:35:12.222
Policy Server	ise33-01
Event	5200 Authentication succeeded
Username	host/DESKTOP-L2IL9I6.ad.rem-sy m.com
Endpoint Id	B4:96:91:15:84:CB
Calling Station Id	B4-96-91-15-84-CB
Endpoint Profile	Intel-Device
IPv4 Address	169.254.90.172
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

Dettagli di autenticazione computer

Confermare il log dettagliato dell'autenticazione utente.



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

Dettagli di autenticazione utente

Motivo 2. Solo autenticazione utente

Passaggio 1. Disabilitare e abilitare la scheda NIC del PC Windows

Per attivare l'autenticazione dell'utente, disabilitare e abilitare la scheda NIC di Win10 PC1.

Passaggio 2. Conferma sessione di autenticazione

Eseguire il comandoshow authentication sessions interface GigabitEthernet1/0/2 details per confermare la sessione di autenticazione utente in C1000.

<#root>

Switch#

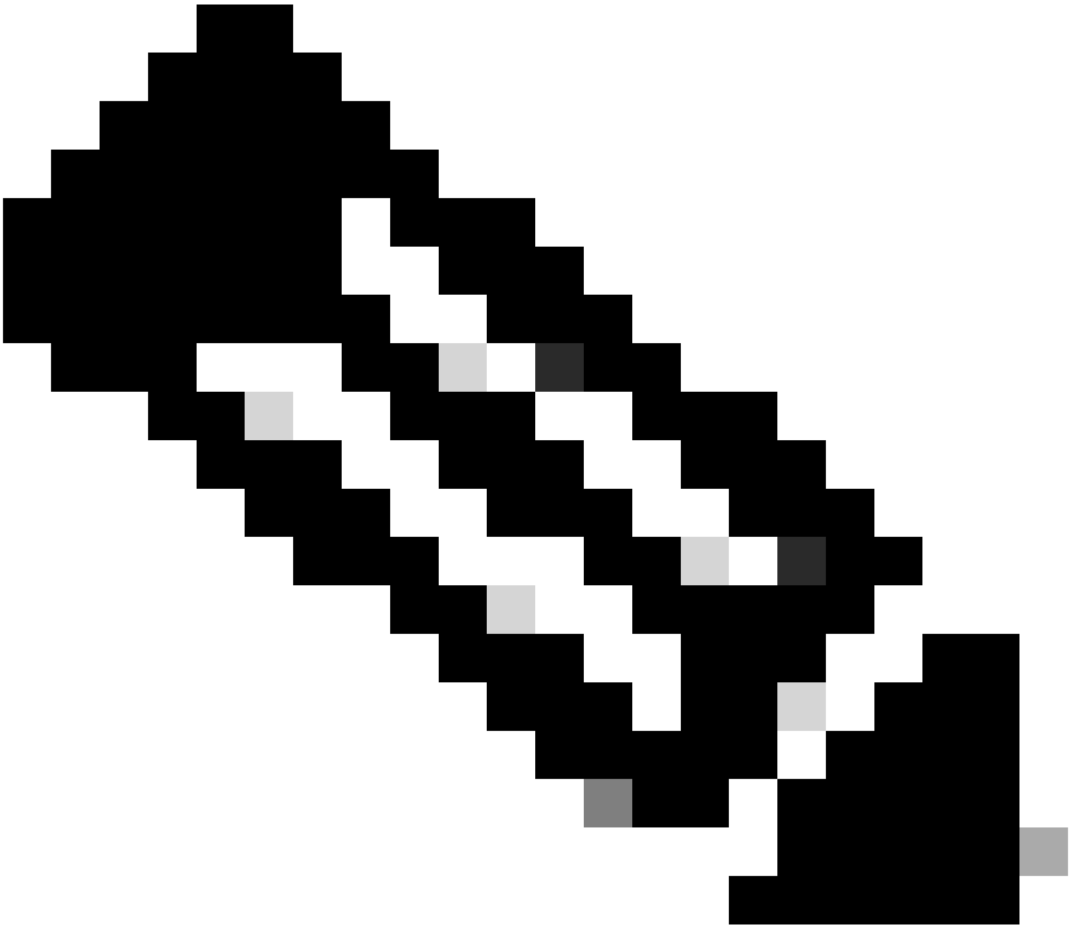
`show authentication sessions interface GigabitEthernet1/0/2 details`

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

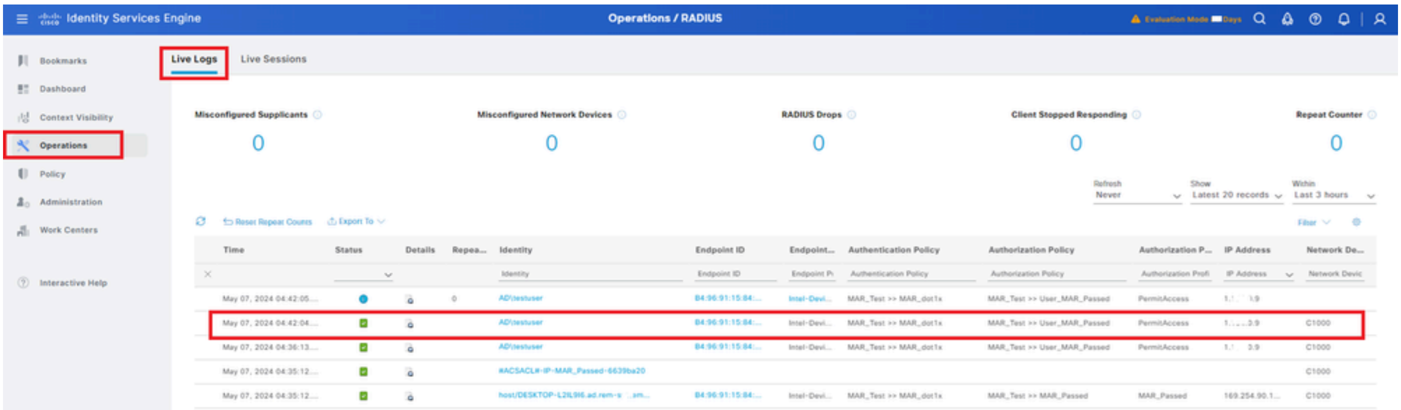
```
User-Name: AD\testuser
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 419s
Common Session ID: 01C2006500000049AA780D80
Acct Session ID: 0x0000003D
Handle: 0x66000016
Current Policy: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

Passaggio 3. Conferma registro dinamico Radius

Selezionare **Operations > RADIUS > Live Logs** in ISE GUI, quindi confermare il log attivo per l'autenticazione dell'utente.



Nota: poiché la cache MAR è memorizzata in ISE, è necessaria solo l'autenticazione utente.



Misconfigured Supplicants 0

Misconfigured Network Devices 0

RADIUS Drops 0

Client Stopped Responding 0

Repeat Counter 0

Refresh: Never

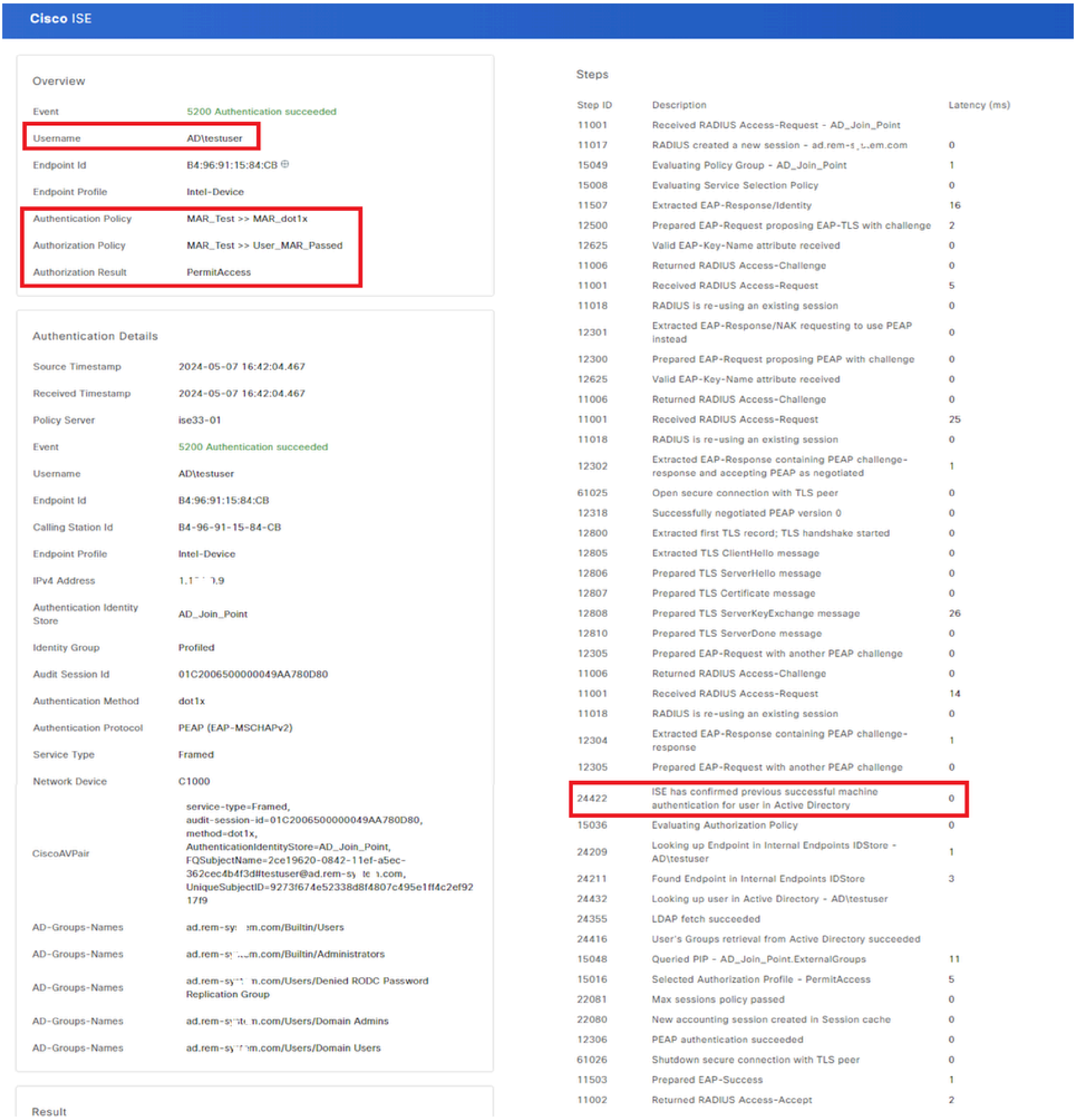
Show: Latest 20 records

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 Pr	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 .sm...	B4:96:91:15:84:...	Intel-Devi...	MAR_Test >> MAR_dot1x	MAR_Test >> MAR_Passed	MAR_Passed	169.254.90.1...	C1000

Registro Radius Live

Confermare il log dettagliato dell'autenticazione utente.



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[redacted].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[redacted].com,
	UniqueSubjectID=9273f674e52338d8f4807c495e1ff4c2ef9217f9

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

Dettagli di autenticazione utente

Risoluzione dei problemi

Questi log di debug (prrt-server.log) aiutano a confermare il comportamento dettagliato dell'autenticazione in ISE.

- configurazione runtime

- registrazione in fase di esecuzione

- runtime-AAA

Questo è un esempio del log di debug per il **modello 1. Autenticazione computer e autenticazione utente** nel documento.

<#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
```

Informazioni correlate

[Vantaggi e svantaggi delle restrizioni di accesso al computer]