Konfigurieren der Zwei-Faktor-Authentifizierung für den Supplicant-Zugriff

Inhalt

Einleitung

In diesem Dokument werden die erforderlichen Schritte zur Konfiguration der Zwei-Faktor-Authentifizierung mit Computer- und Punkt1x-Authentifizierung beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Konfiguration der Cisco Identity Services Engine
- Konfiguration des Cisco Catalyst
- IEEE 802.1X

Verwendete Komponenten

- Identity Services Engine Virtual 3.3 Patch 1
- C1000-48FP-4G-L 15,2(7)E9

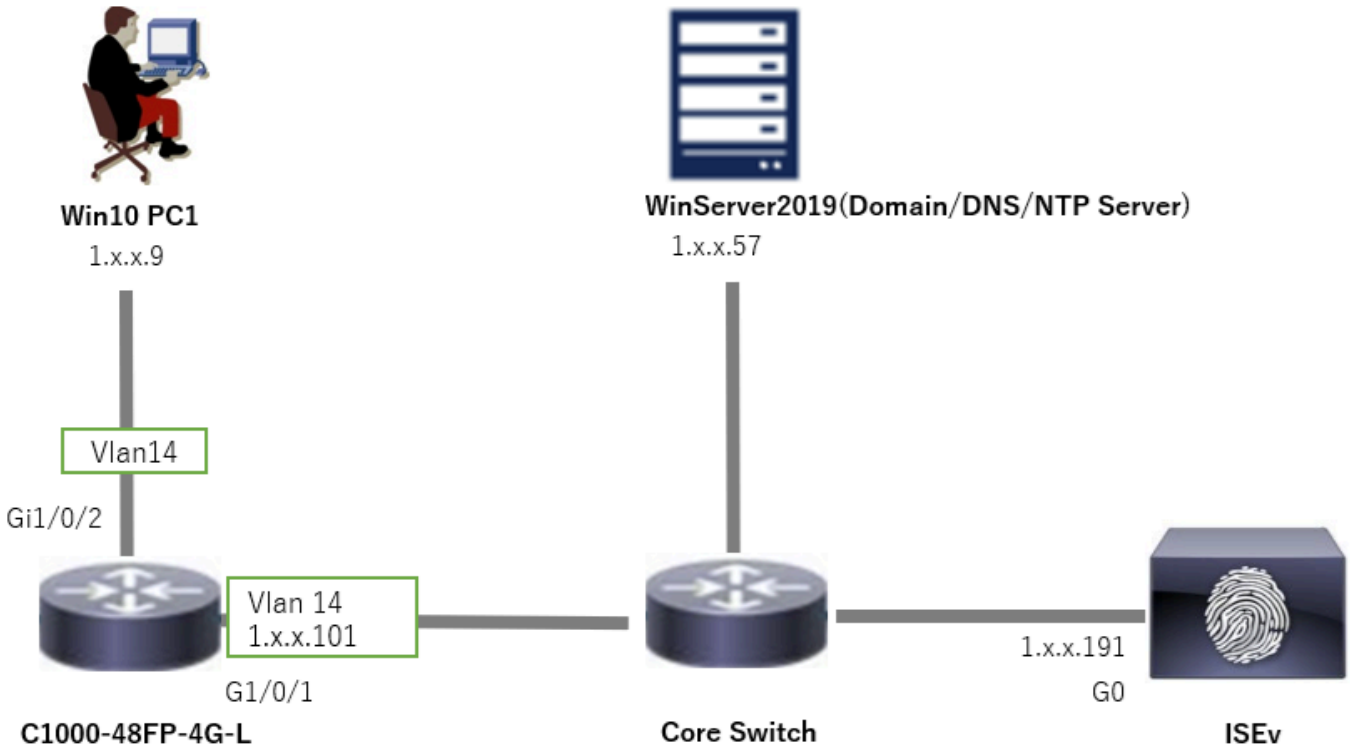
- Windows Server 2019

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Netzwerkdiagramm

Dieses Bild zeigt die Topologie, die für das Beispiel dieses Dokuments verwendet wird.

Der unter Windows Server 2019 konfigurierte Domänenname ist ad.rem-xxx.com. Dies wird in diesem Dokument als Beispiel verwendet.



Netzwerkdiagramm

Hintergrundinformationen

Die Systemauthentifizierung ist ein Sicherheitsprozess, der die Identität eines Geräts überprüft, das Zugriff auf ein Netzwerk oder System benötigt. Im Gegensatz zur Benutzerauthentifizierung, bei der die Identität einer Person anhand von Anmeldeinformationen wie Benutzername und Kennwort überprüft wird, konzentriert sich die Computerauthentifizierung auf die Validierung des Geräts selbst. Dies geschieht häufig mithilfe digitaler Zertifikate oder Sicherheitsschlüssel, die für das Gerät einzigartig sind.

Durch die kombinierte Verwendung von Computer- und Benutzerauthentifizierung kann ein Unternehmen sicherstellen, dass nur autorisierte Geräte und Benutzer auf sein Netzwerk zugreifen können, wodurch eine sicherere Umgebung geschaffen wird. Diese Zwei-Faktor-Authentifizierungsmethode ist besonders nützlich, um vertrauliche Informationen zu schützen und strenge gesetzliche Vorschriften einzuhalten.

Konfigurationen

Konfiguration in C1000

Dies ist die minimale Konfiguration in C1000 CLI.

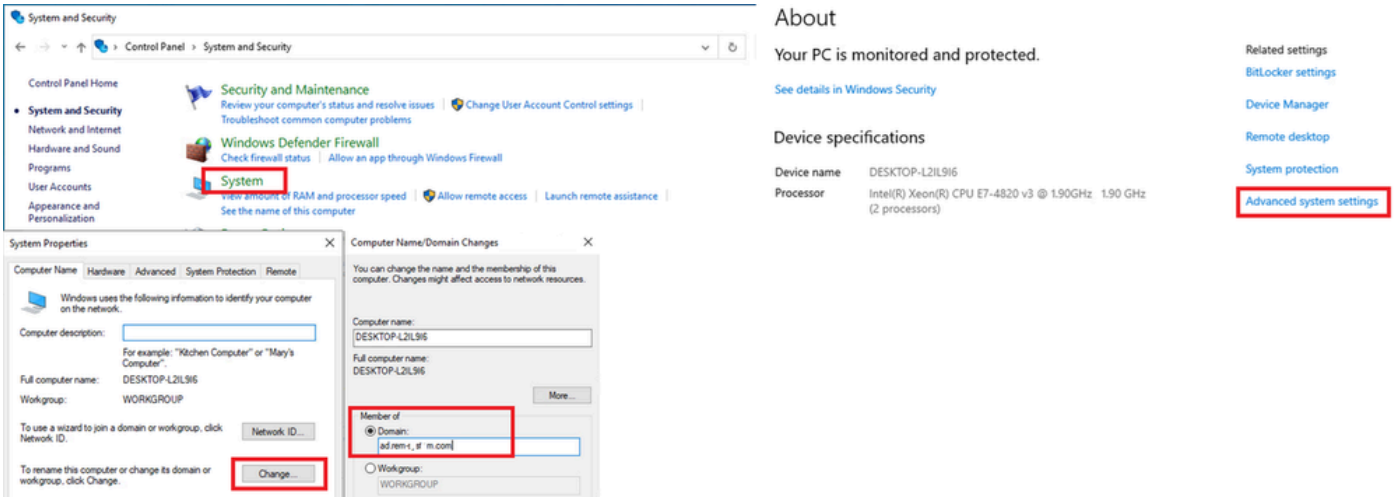
```
aaa new-model

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
```

Konfiguration auf Windows-PCs

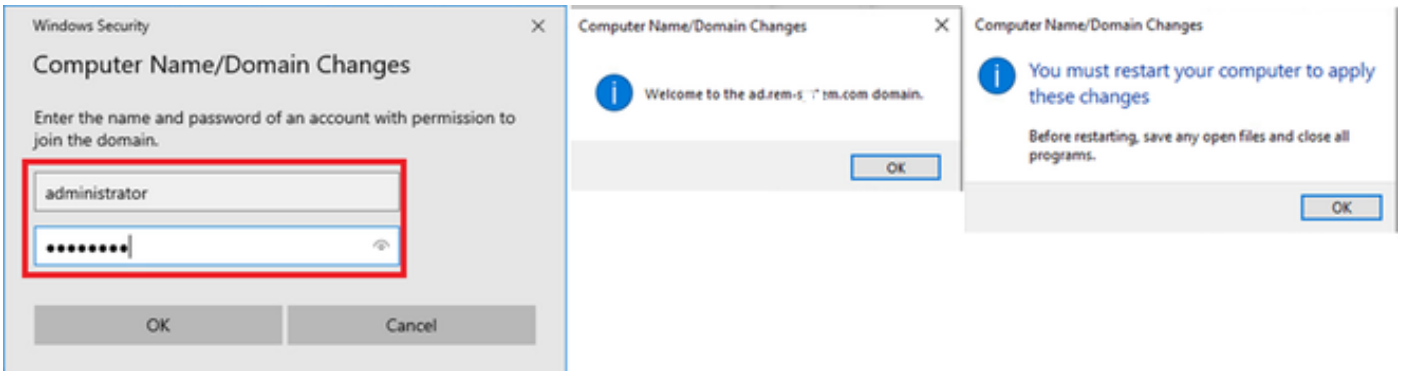
Schritt 1: PC zur AD-Domäne hinzufügen

Navigieren Sie zu Systemsteuerung > System und Sicherheit, klicken Sie auf System, und klicken Sie dann auf Erweiterte Systemeinstellungen. Klicken Sie im Fenster Systemeigenschaften auf Ändern, wählen Sie Domäne aus, und geben Sie den Domänennamen ein.



PC zur AD-Domäne hinzufügen

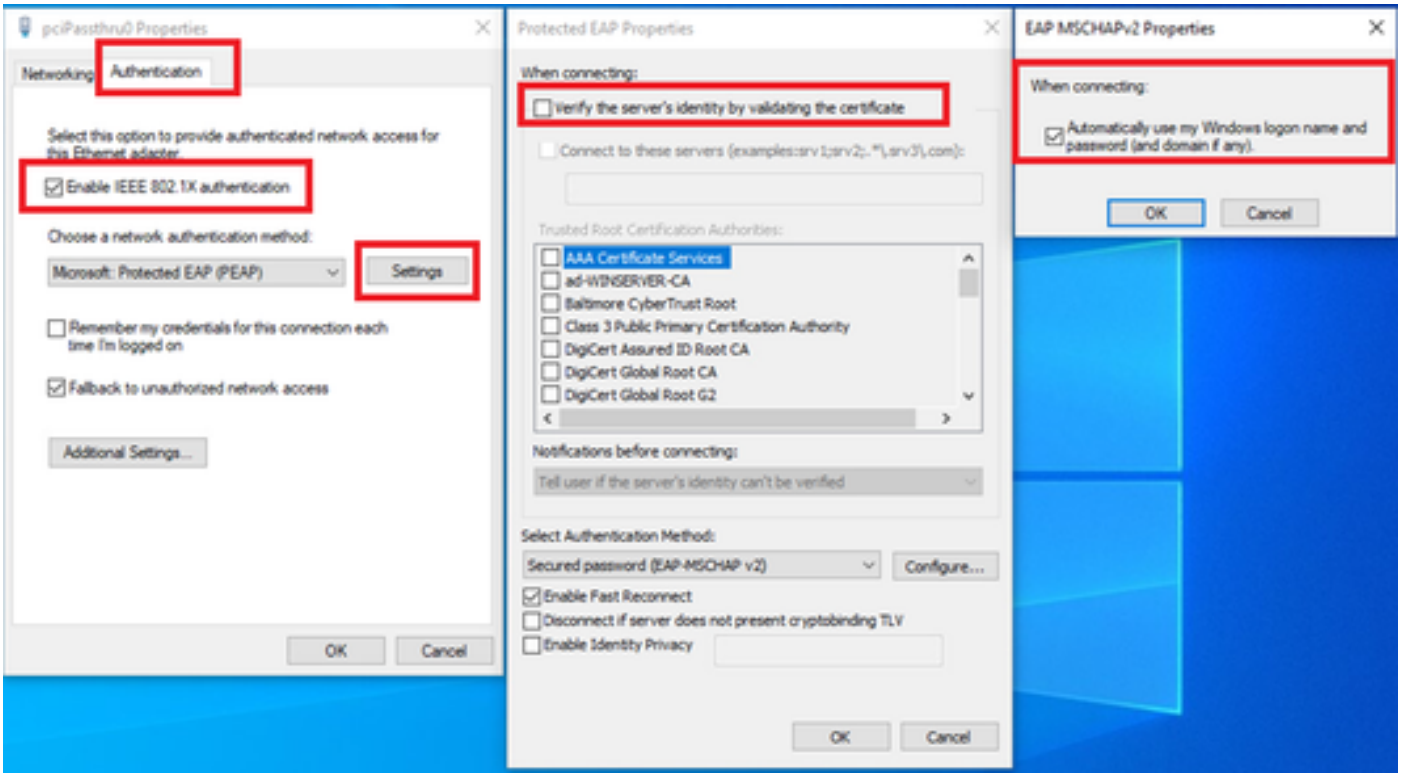
Geben Sie im Fenster Windows-Sicherheit den Benutzernamen und das Kennwort des Domänenservers ein.



Benutzername und Kennwort eingeben

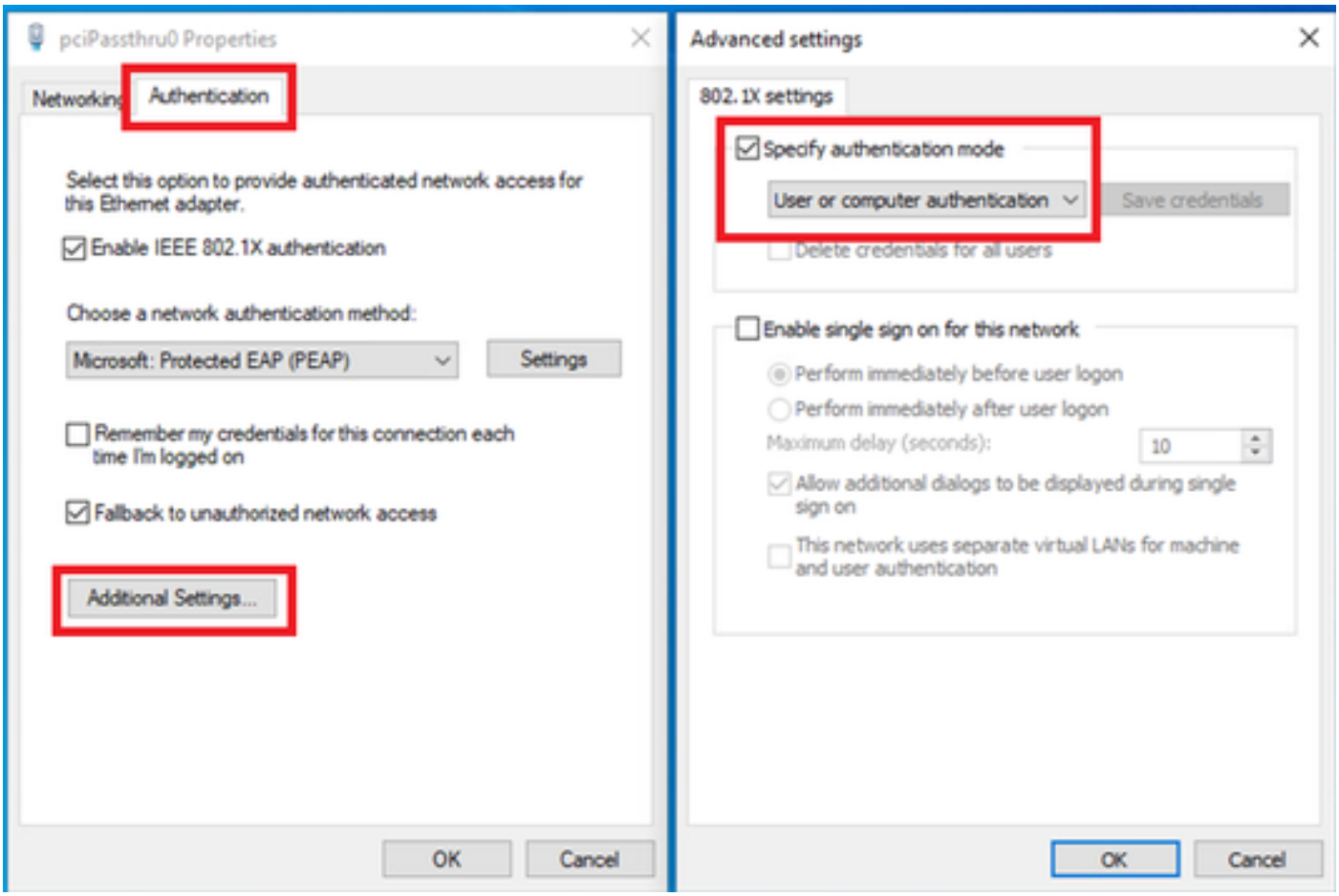
Schritt 2: Benutzerauthentifizierung konfigurieren

Navigieren Sie zu Authentication (Authentifizierung), und aktivieren Sie das Kontrollkästchen Enable IEEE 802.1X authentication. Klicken Sie im Fenster Protected EAP Properties auf Settings (Einstellungen), deaktivieren Sie Verify the server's identity by validating the certificate, und klicken Sie dann auf Configure. Aktivieren Sie im Fenster Eigenschaften von EAP MSCHAPv2 die Option Windows-Anmeldename und -Kennwort (und ggf. Domäne) automatisch verwenden, um den bei der Windows-Computeranmeldung eingegebenen Benutzernamen für die Benutzerauthentifizierung zu verwenden.



Benutzerauthentifizierung aktivieren

Navigieren Sie zu Authentifizierung, und aktivieren Sie Zusätzliche Einstellungen. Wählen Sie Benutzer- oder Computerauthentifizierung aus der Dropdown-Liste aus.

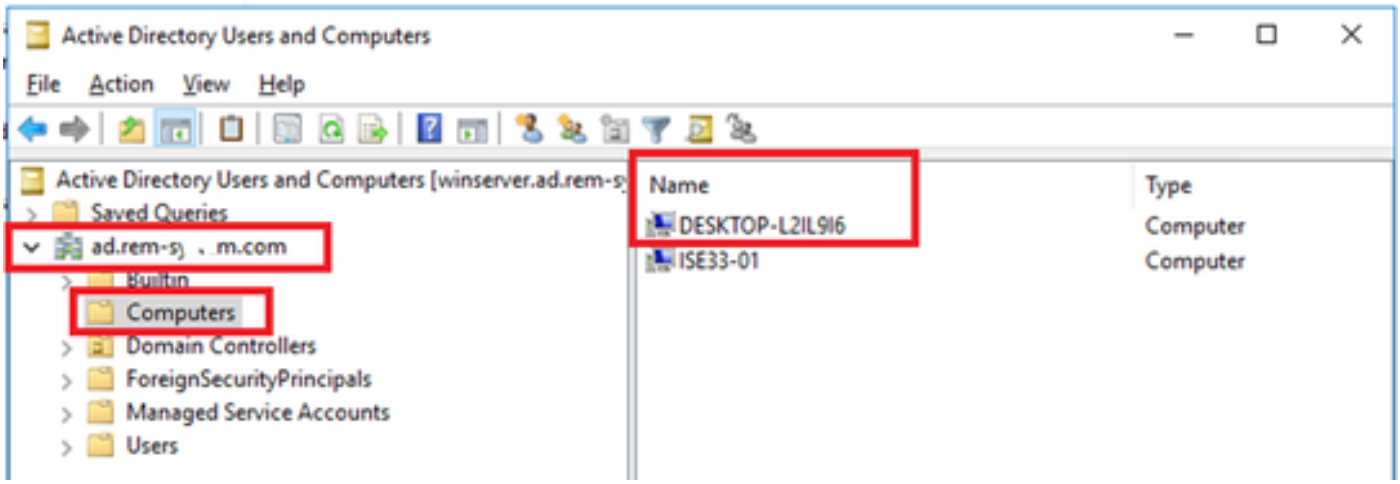


Authentifizierungsmodus angeben

Konfiguration in Windows Server

Schritt 1: Domänencomputer bestätigen

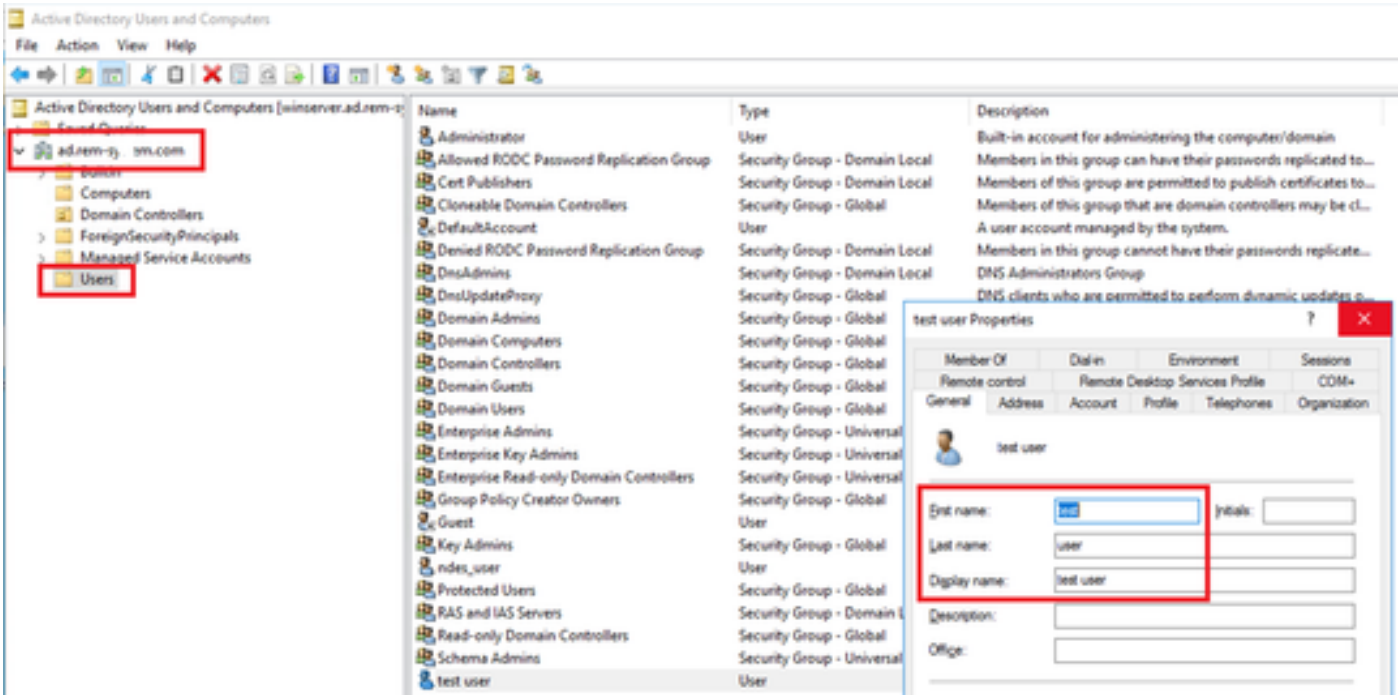
Navigieren Sie zu Active Directory-Benutzer und -Computer, und klicken Sie auf Computer. Vergewissern Sie sich, dass Win10 PC1 in der Domäne aufgeführt ist.



Domänencomputer bestätigen

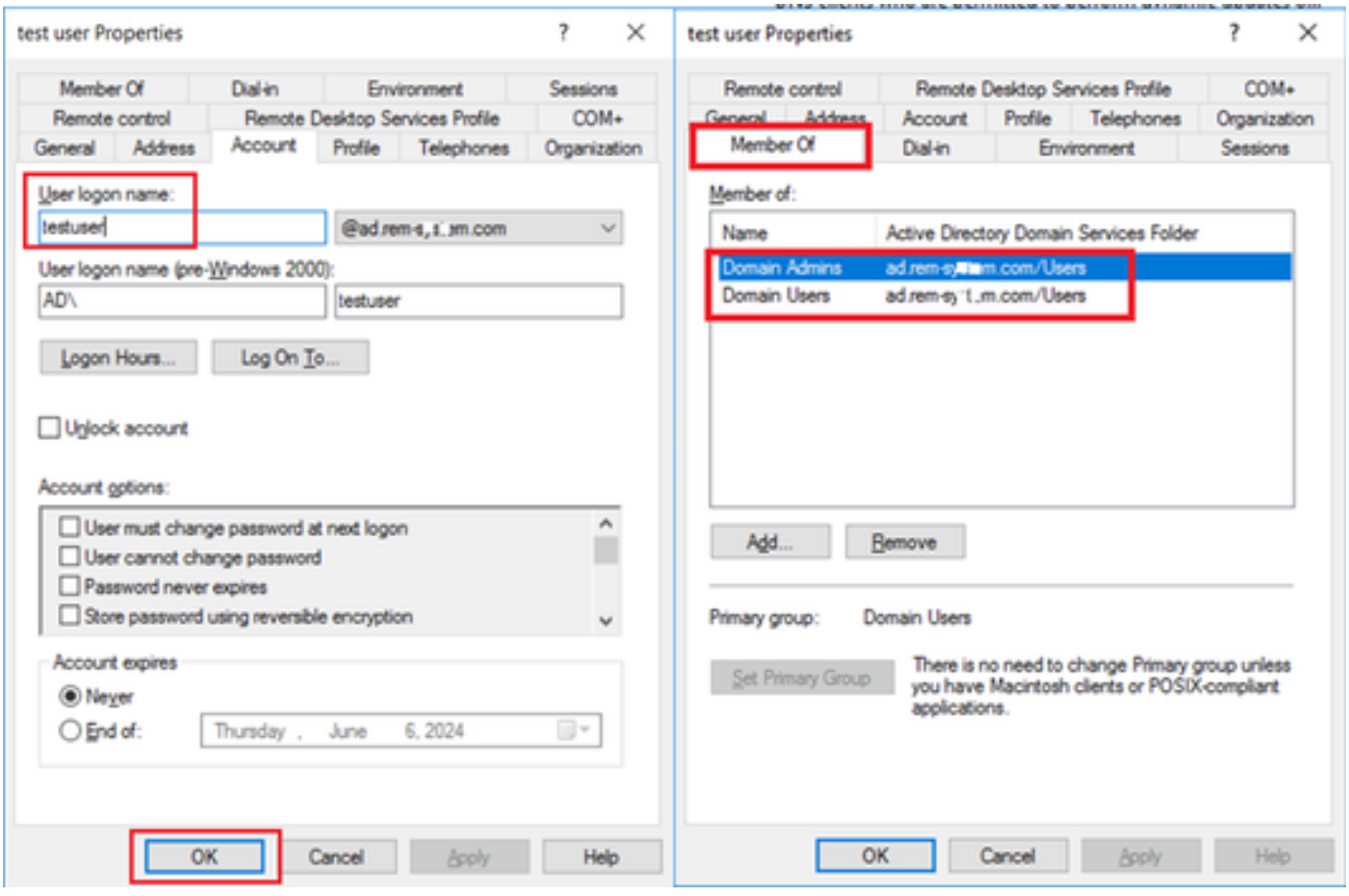
Schritt 2: Domänenbenutzer hinzufügen

Navigieren Sie zu Active Directory-Benutzer und -Computer, und klicken Sie auf Benutzer. Fügen Sie testuser als Domänenbenutzer hinzu.



Domänenbenutzer hinzufügen

Fügen Sie den Domänenbenutzer einem Mitglied von Domänenadministratoren und Domänenbenutzern hinzu.

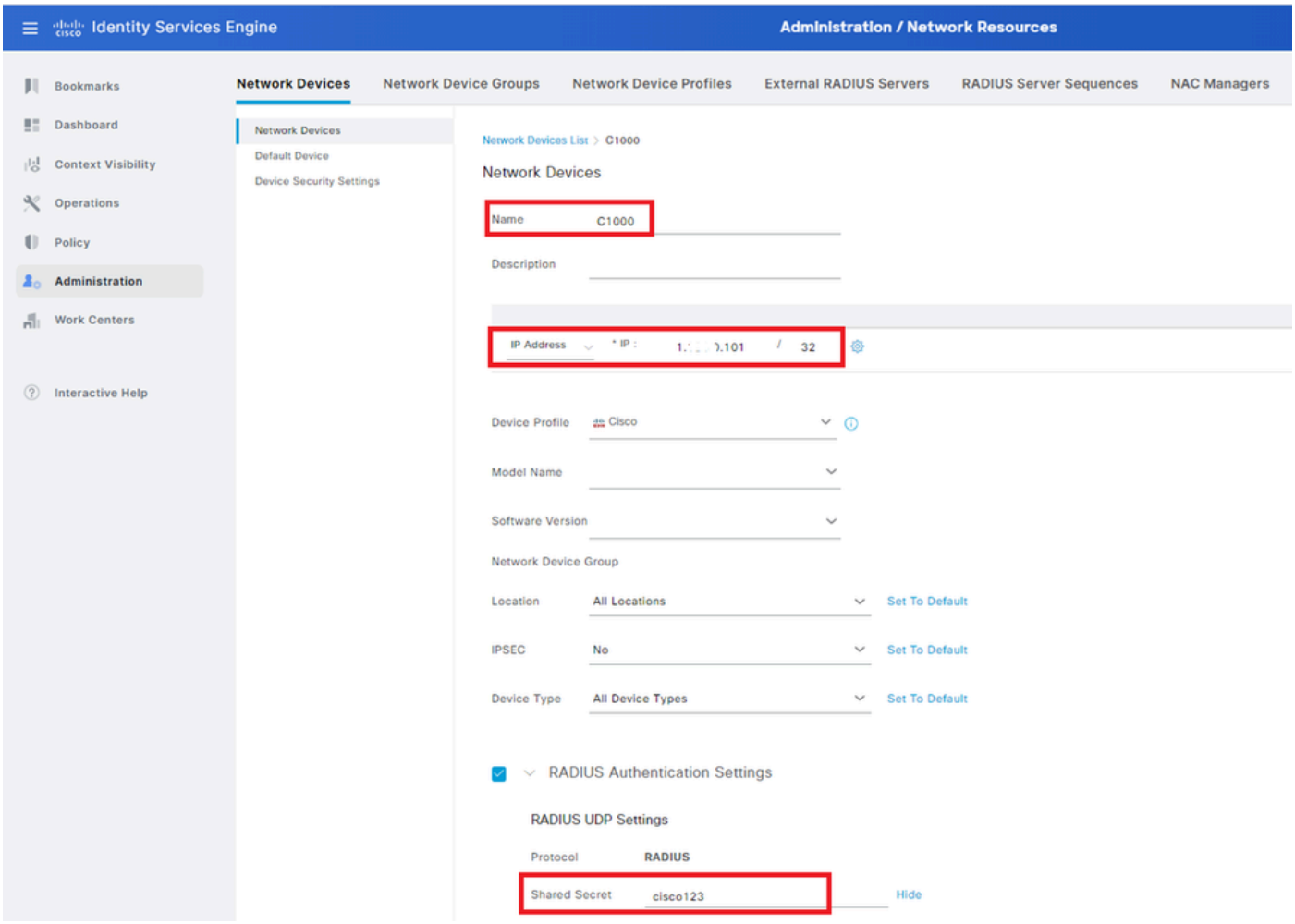


Domänenadministratoren und Domänenbenutzer

Konfiguration in der ISE

Schritt 1: Gerät hinzufügen

Navigieren Sie zu Administration > Network Devices, und klicken Sie auf Add (Hinzufügen), um ein C1000-Gerät hinzuzufügen.

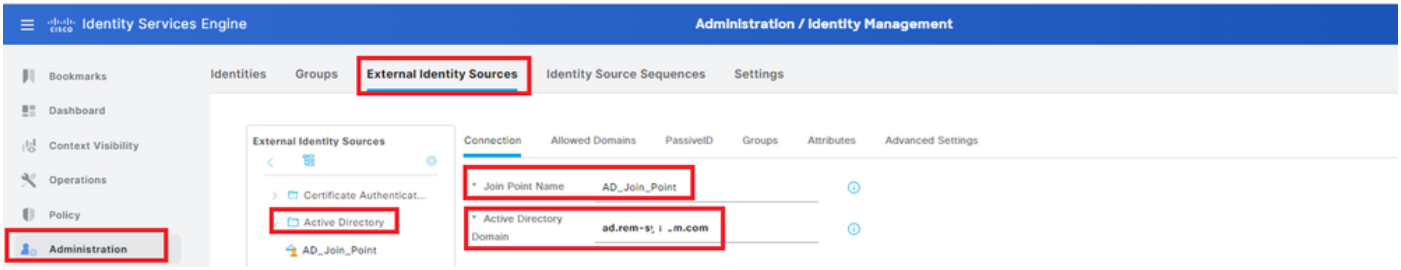


Gerät hinzufügen

Schritt 2: Active Directory hinzufügen

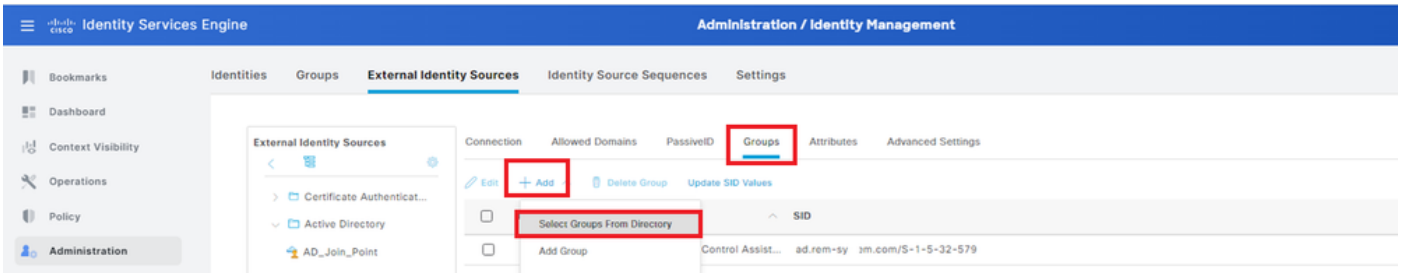
Navigieren Sie zu Administration > External Identity Sources > Active Directory, klicken Sie auf die Registerkarte Connection, und fügen Sie Active Directory zur ISE hinzu.

- Verknüpfungspunkt-Name: AD_Join_Point
- Active Directory-Domäne: ad.rem-xxx.com



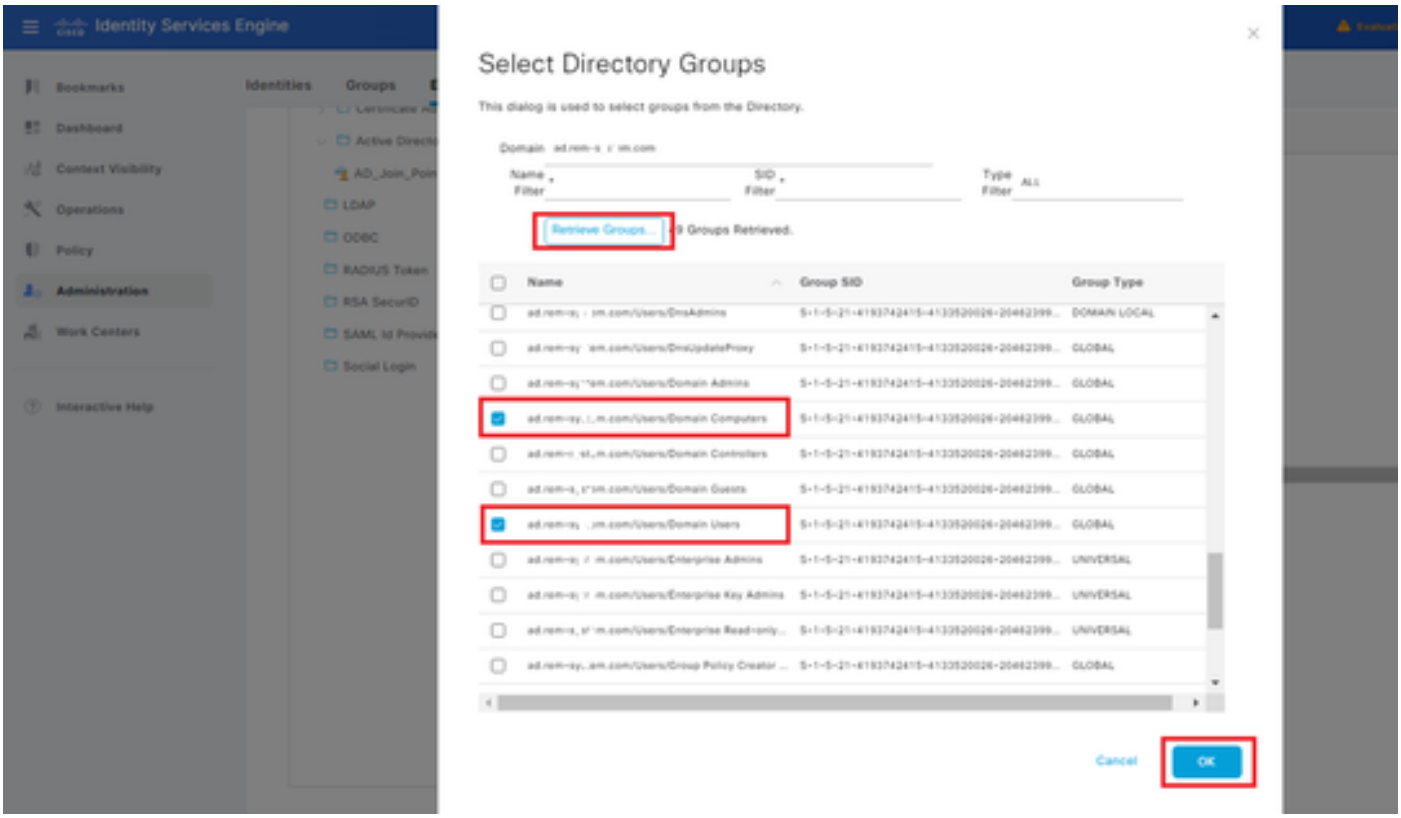
Active Directory hinzufügen

Navigieren Sie zur Registerkarte Gruppen, und wählen Sie Gruppen aus Verzeichnis aus der Dropdown-Liste aus.



Gruppen aus Verzeichnis auswählen

Klicken Sie auf Gruppen aus Dropdown-Liste abrufen. Aktivieren Sie ad.rem-xxx.com/Users/Domain Computers and ad.rem-xxx.com/Users/Domain Users, und klicken Sie auf OK.



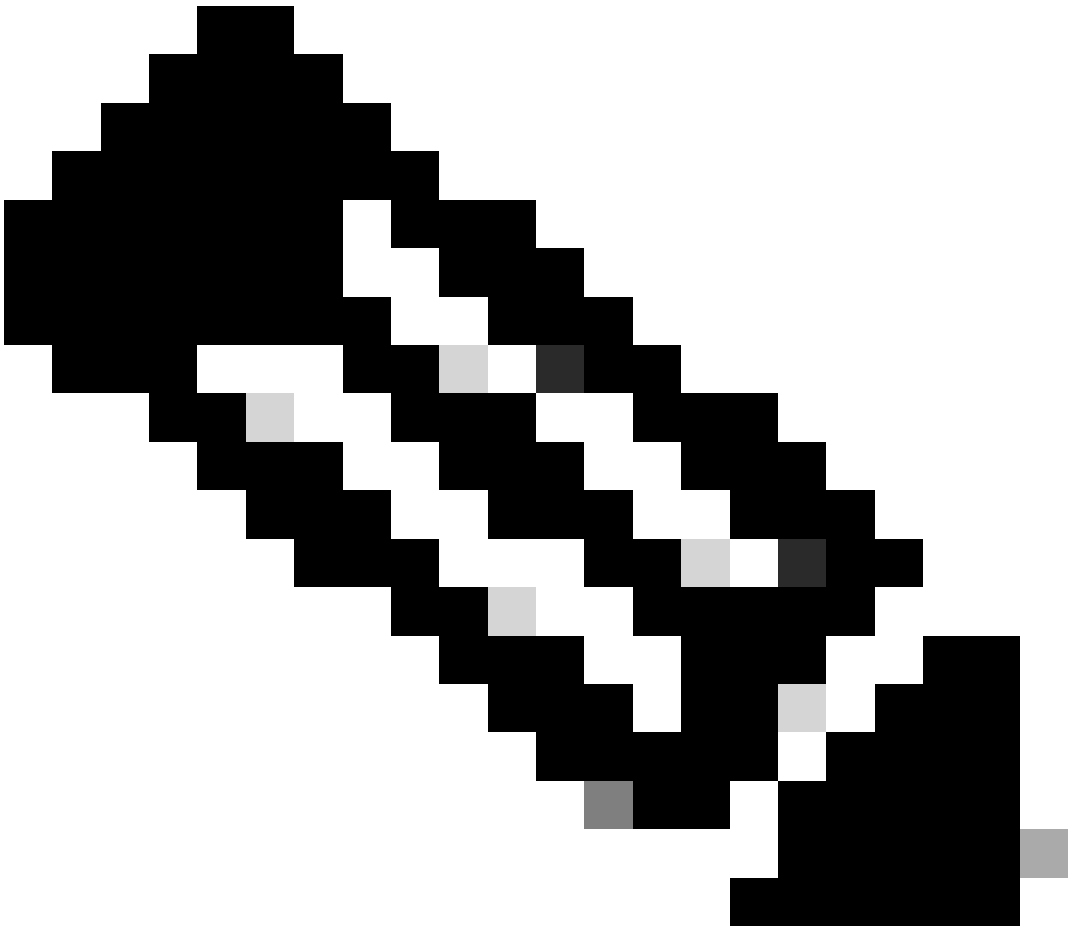
Domänencomputer und -benutzer hinzufügen

Schritt 3: Einstellungen für die Computerauthentifizierung bestätigen

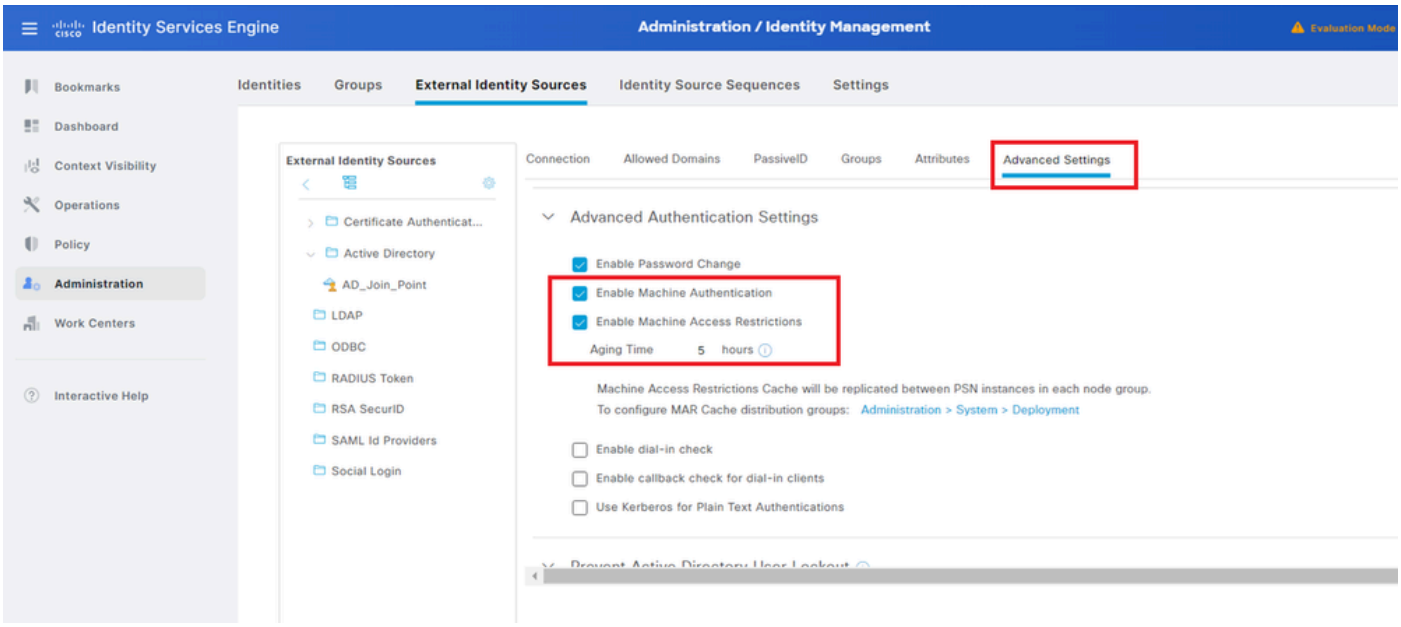
Navigieren Sie zur Registerkarte Erweiterte Einstellungen, und bestätigen Sie die Einstellung der Computerauthentifizierung.

- Computerauthentifizierung aktivieren: So aktivieren Sie die Computerauthentifizierung
- Aktivieren der Einschränkung des Computerzugriffs: So kombinieren Sie Benutzer- und Computerauthentifizierung vor der Autorisierung

---



Hinweis: Der gültige Bereich für die Alterungszeit liegt zwischen 1 und 8760.

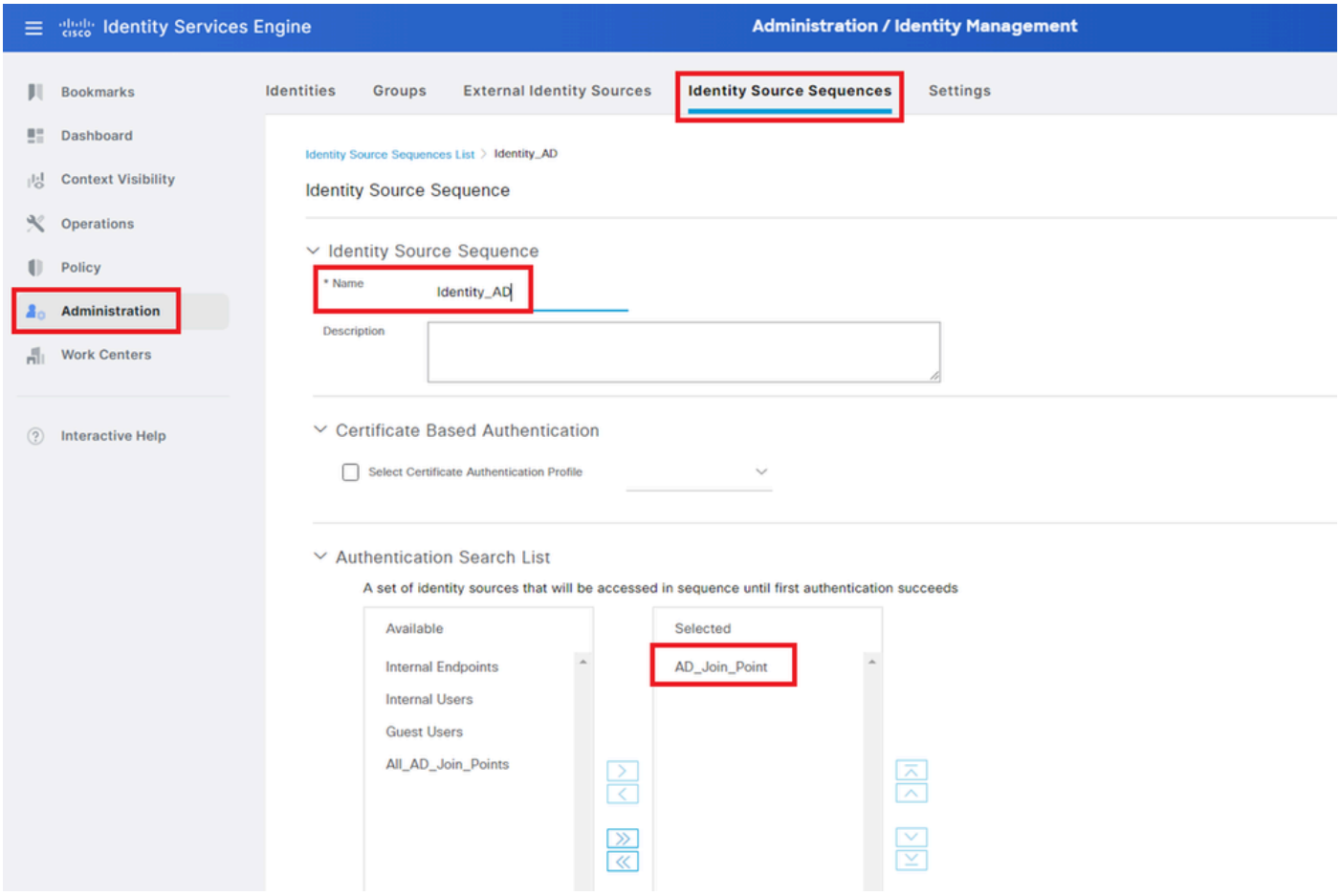


Einstellungen für die Computerauthentifizierung

Schritt 4: Identitätsquellensequenzen hinzufügen

Navigieren Sie zu Administration > Identity Source Sequences, und fügen Sie eine Identity Source Sequence hinzu.

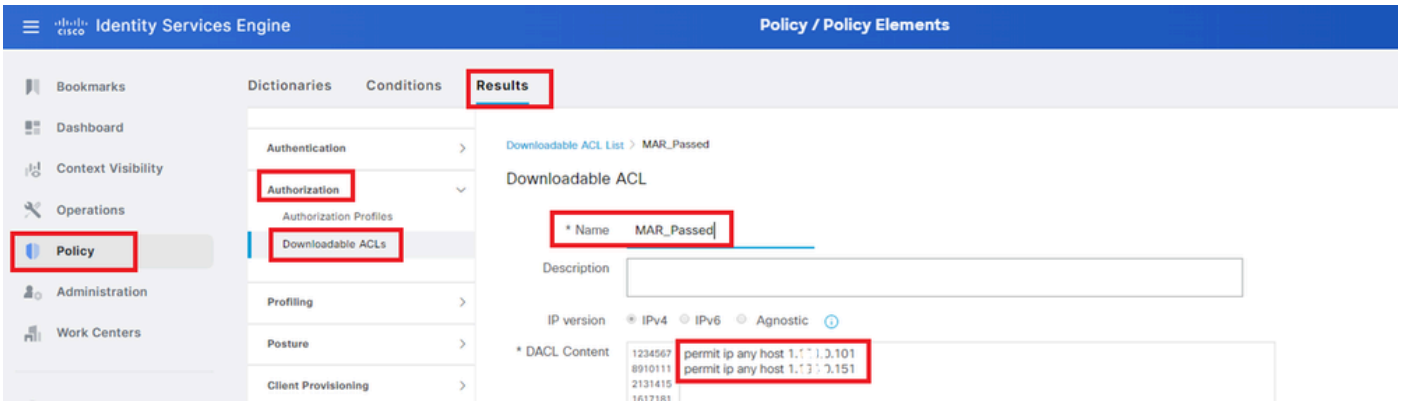
- Name: Identity_AD
- Authentifizierungs-Suchliste: AD_Join_Point



Schritt 5: DACL und Autorisierungsprofil hinzufügen

Navigieren Sie zu Richtlinie > Ergebnisse > Autorisierung > Herunterladbare ACLs, und fügen Sie eine DACL hinzu.

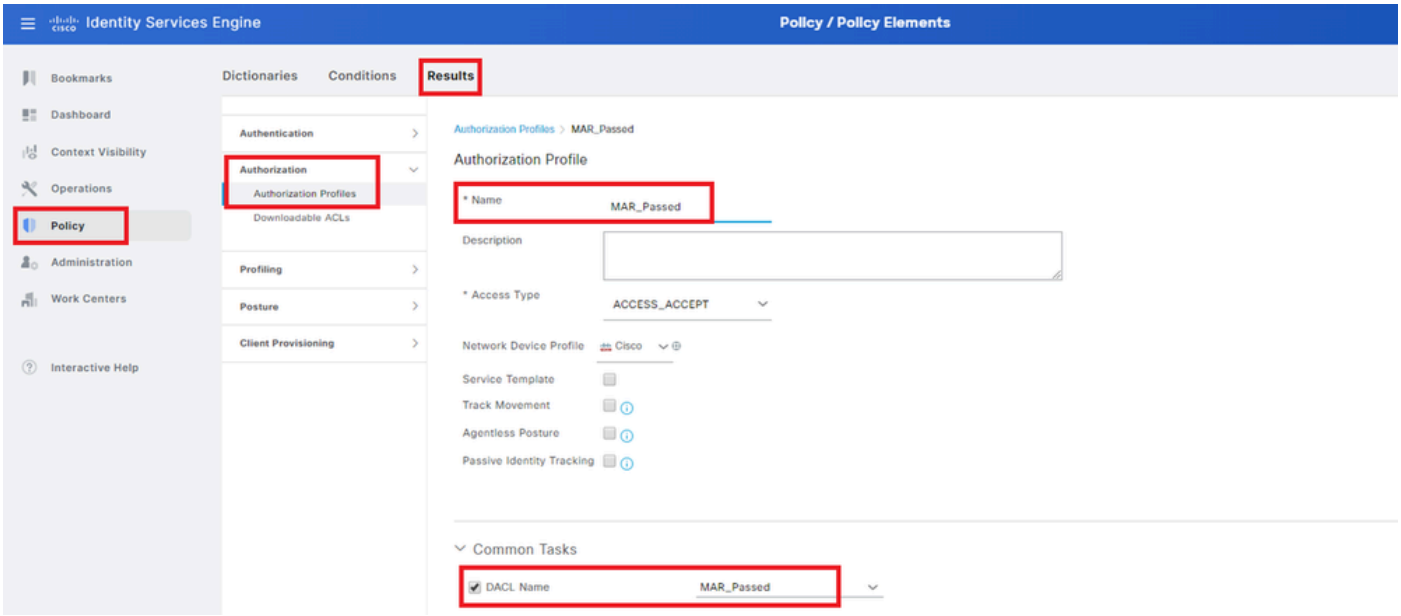
- Name: MAR_Passed
- DACL Content: permit ip any host 1.x.x.101 and permit ip any host 1.x.x.105



DACL hinzufügen

Navigieren Sie zu Richtlinie > Ergebnisse > Autorisierung > Autorisierungsprofile, und fügen Sie ein Autorisierungsprofil hinzu.

- Name: MAR_Passed
- DACL-Name: MAR_Passed

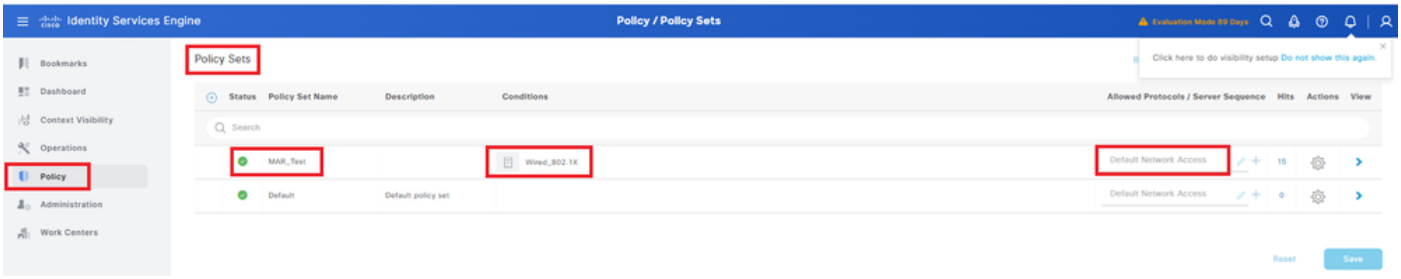


Autorisierungsprofil hinzufügen

Schritt 6: Policy Set hinzufügen

Navigieren Sie zu Policy > Policy Sets, und klicken Sie auf +, um einen Policy Set hinzuzufügen.

- Richtliniensatzname: MAR_Test
- Bedingungen: Wired_802.1X
- Zulässige Protokolle/Serversequenz: Standard-Netzwerkzugriff

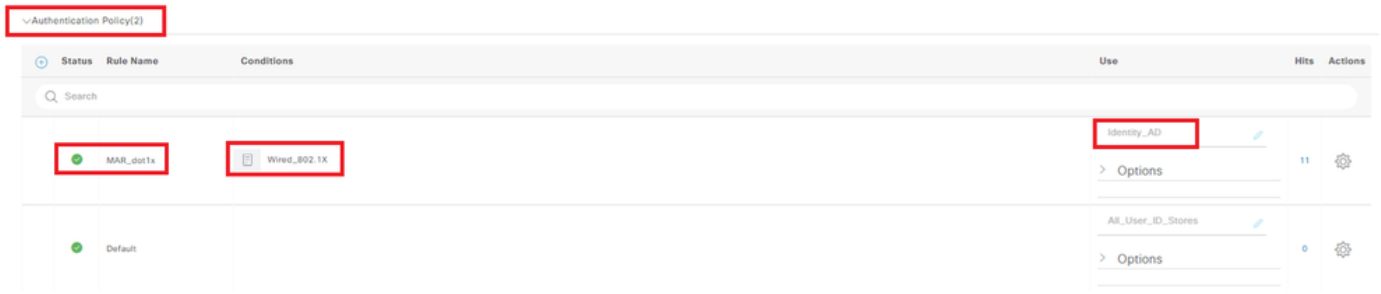


Policy Set hinzufügen

Schritt 7. Authentifizierungsrichtlinie hinzufügen

Navigieren Sie zu Policy Sets, und klicken Sie auf MAR_Test, um eine Authentifizierungsrichtlinie hinzuzufügen.

- Regelname: MAR_dot1x
- Bedingungen: Wired_802.1X
- Verwenden: Identity_AD



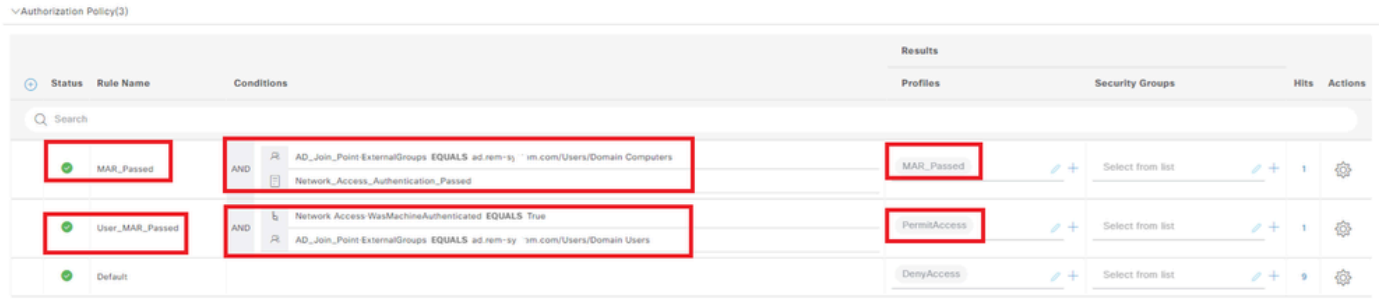
Authentifizierungsrichtlinie hinzufügen

Schritt 8: Autorisierungsrichtlinie hinzufügen

Navigieren Sie zu Policy Sets, und klicken Sie auf MAR_Test, um eine Autorisierungsrichtlinie hinzuzufügen.

- Regelname: MAR_Passed
- Bedingungen: AD_Join_Point· ExternalGroups GLEICHT ad.rem-xxx.com/Users/Domain Computers AND Network_Access_Authentication_Passed
- Ergebnisse: MAR_Passed

- Regelname: User_MAR_Passed
- Bedingungen: Netzwerkzugriff· WasMachineAuthenticated ENTSPRICHT True UND AD_Join_Point· ExternalGroups ENTSPRICHT ad.rem-xxx.com/Users/Domain
- Ergebnisse: PermitAccess



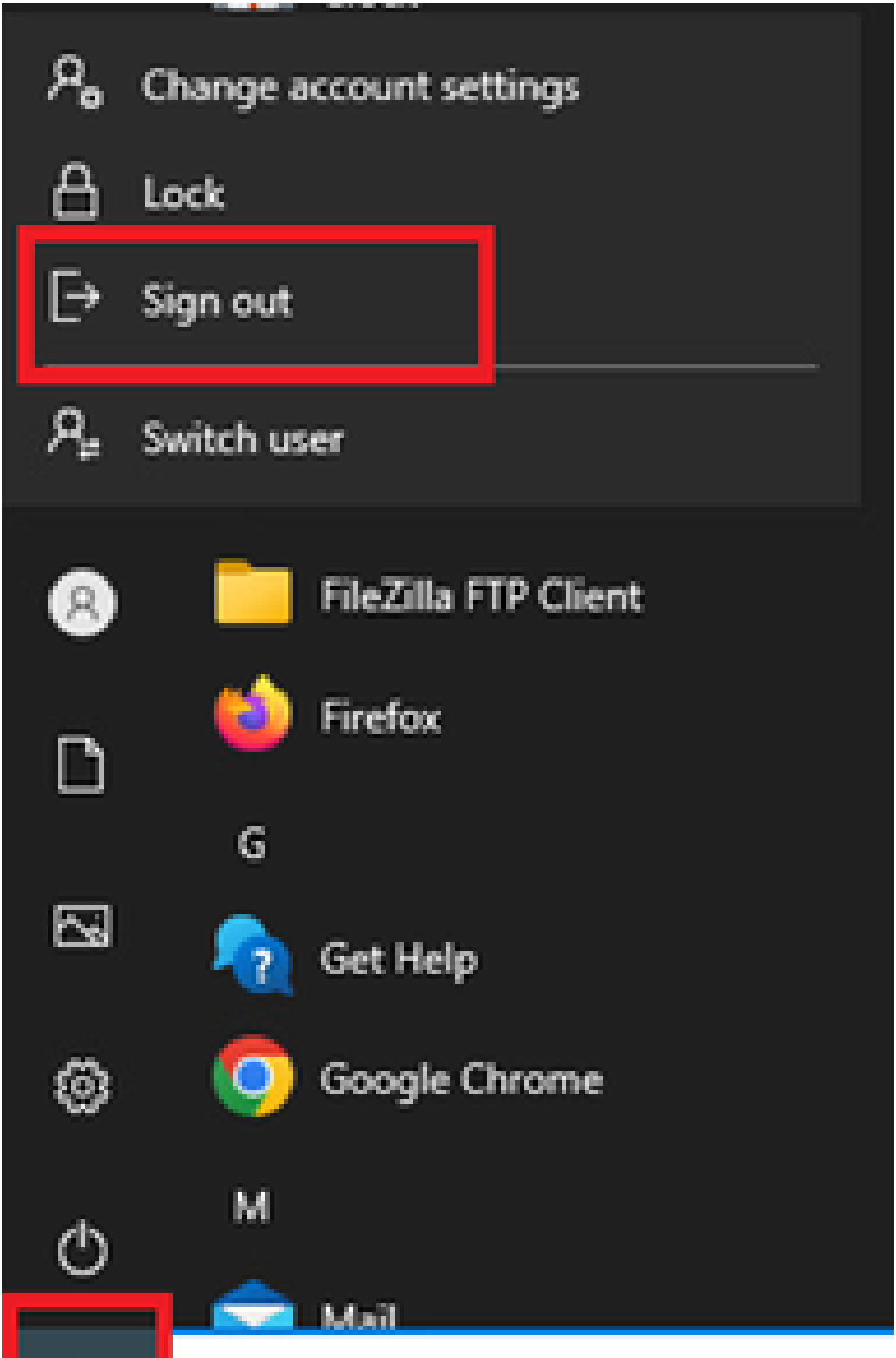
Autorisierungsrichtlinie hinzufügen

Überprüfung

Muster 1. Systemauthentifizierung und Benutzerauthentifizierung

Schritt 1: Abmelden von Windows-PC

Klicken Sie auf Abmelden in Win10 PC1, um die Computerauthentifizierung auszulösen.


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

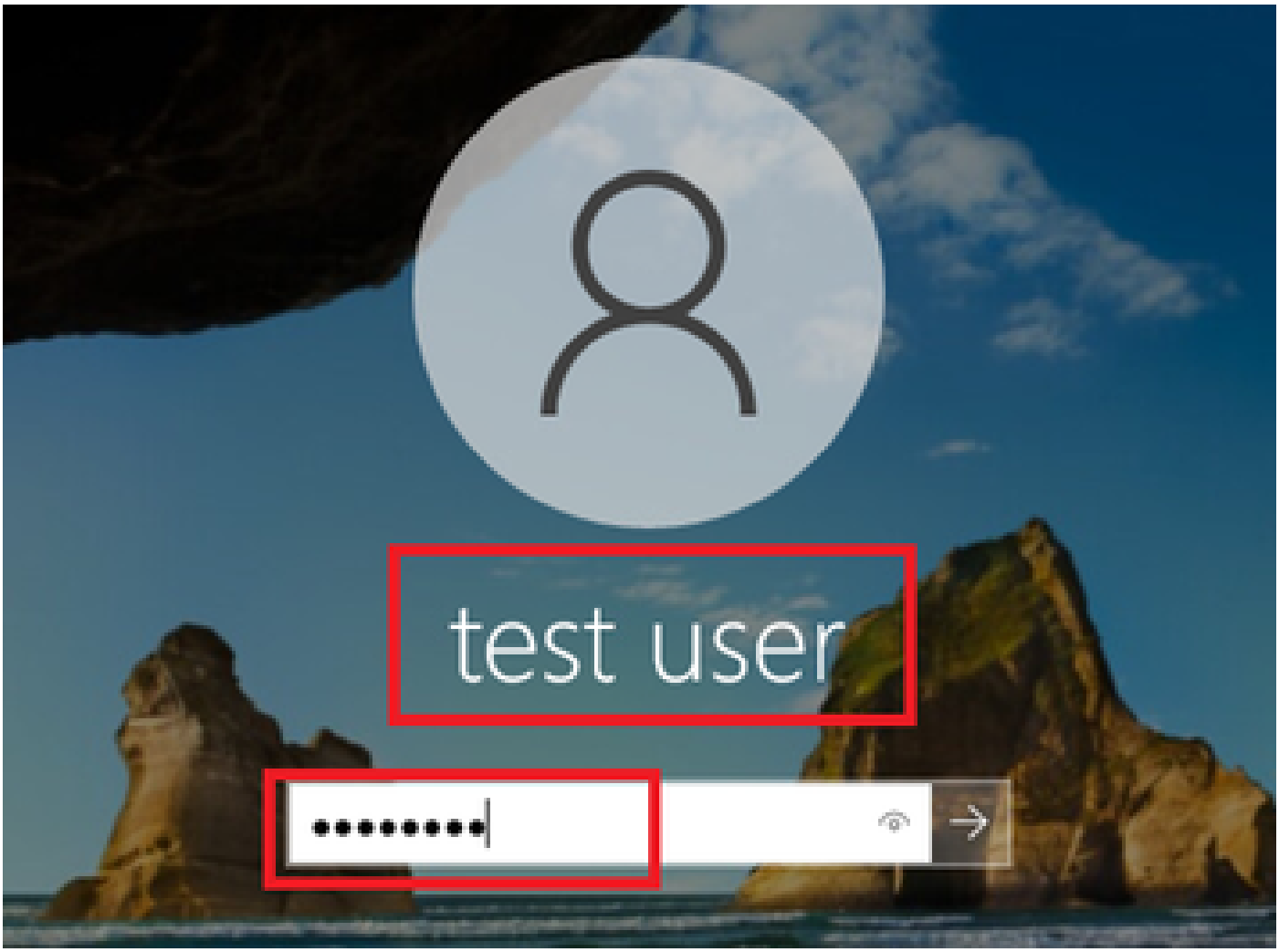
```
Interface: GigabitEthernet1/0/2
MAC Address: b496.9115.84cb
IPv6 Address: Unknown
IPv4 Address: 1.x.x.9
User-Name:
```

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
```

Schritt 3: Windows-PC anmelden

Melden Sie sich bei Win10 PC1 an, geben Sie Benutzername und Kennwort ein, um die Benutzerauthentifizierung auszulösen.



Windows-PC anmelden

Schritt 4: Authentifizierungssitzung bestätigen

show authentication sessions interface GigabitEthernet1/0/2 details Führen Sie den Befehl aus, um die Benutzerauthentifizierungssitzung in C1000 zu bestätigen.

<#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:
```

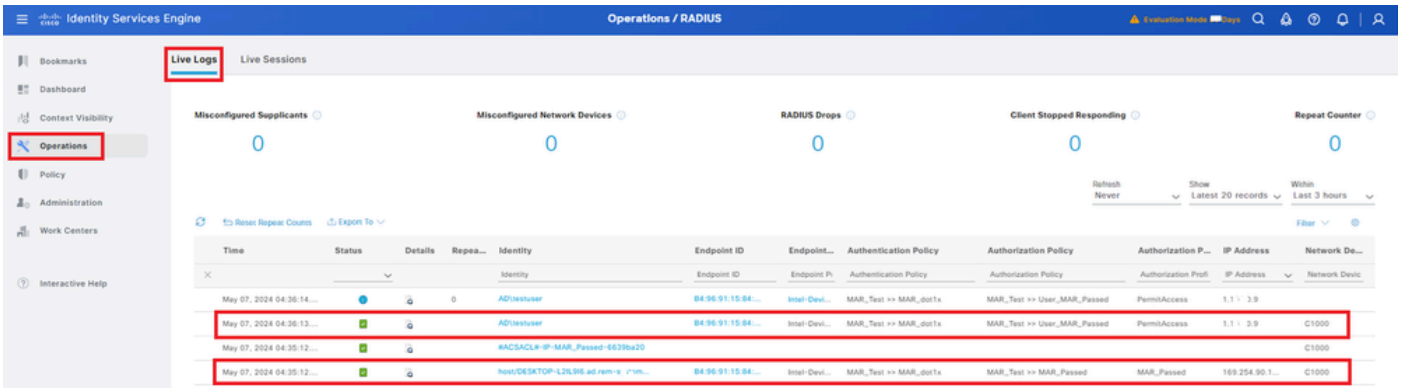
AD\testuser

```
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
```

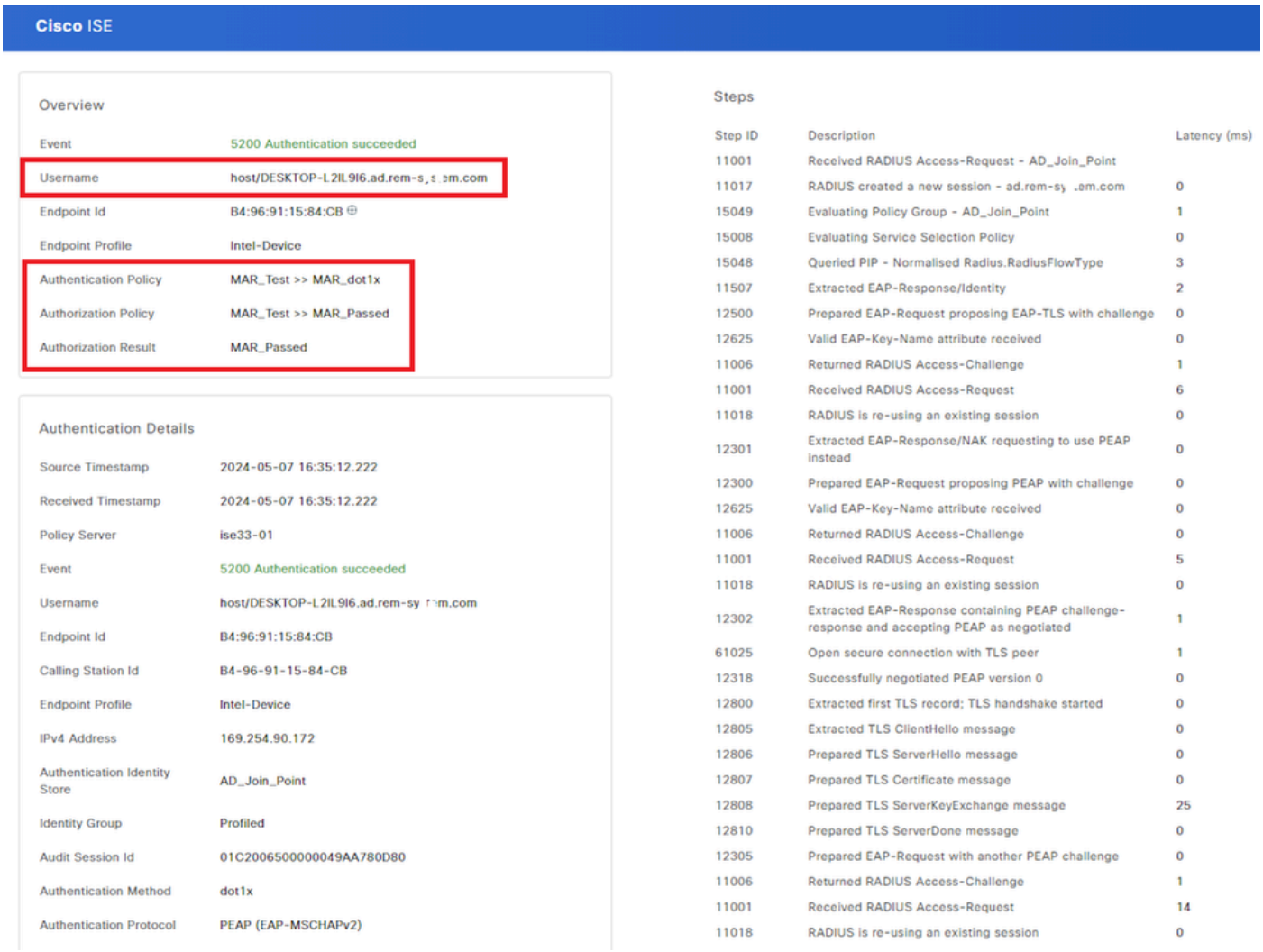
Schritt 5: RADIUS-Live-Protokoll bestätigen

Navigieren Sie zu **Operations > RADIUS > Live Logs (Vorgänge > RADIUS > Live-Protokolle**) in der ISE-GUI, und bestätigen Sie das Live-Protokoll für die Computer- und Benutzerauthentifizierung.



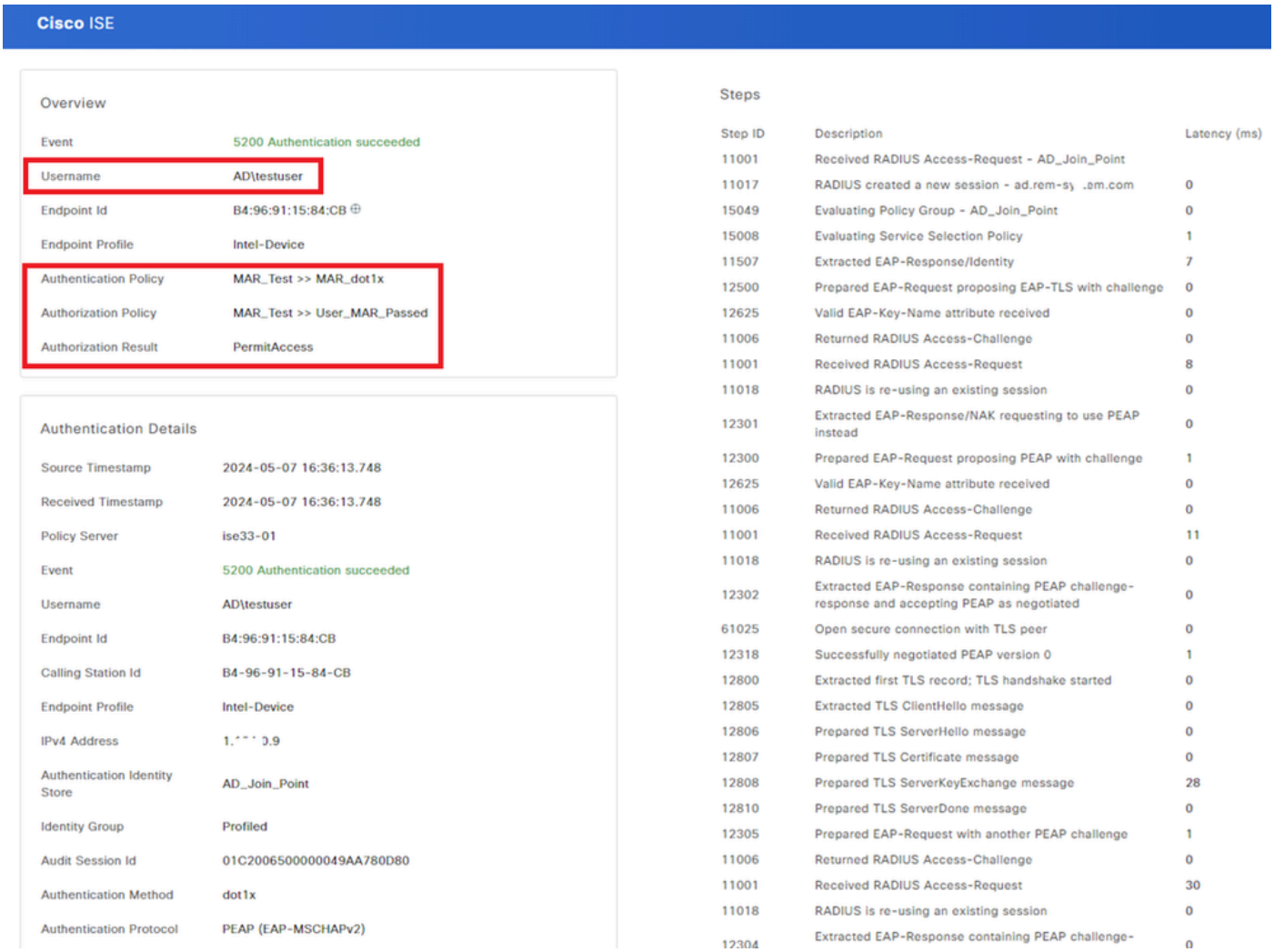
Radius-Live-Protokoll

Bestätigen Sie das detaillierte Live-Protokoll der Computerauthentifizierung.



Details zur Computerauthentifizierung

Bestätigen Sie das detaillierte Live-Protokoll der Benutzerauthentifizierung.



Details zur Benutzerauthentifizierung

Muster 2. Nur Benutzerauthentifizierung

Schritt 1: Deaktivieren und Aktivieren der Netzwerkkarte von Windows PC

Um die Benutzerauthentifizierung auszulösen, deaktivieren und aktivieren Sie die Netzwerkkarte von Win10 PC1.

Schritt 2: Authentifizierungssitzung bestätigen

show authentication sessions interface GigabitEthernet1/0/2 details Führen Sie den Befehl aus, um die Benutzerauthentifizierungssitzung in C1000 zu bestätigen.

<#root>

Switch#

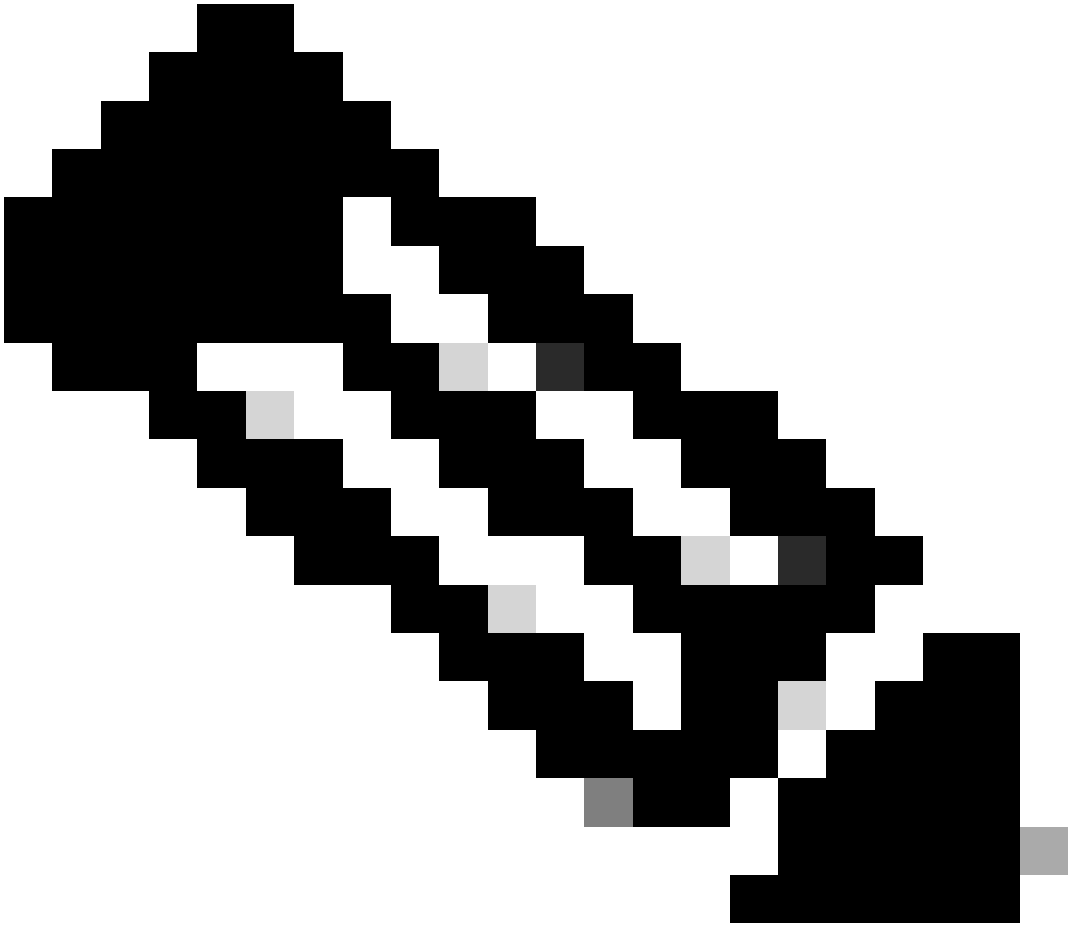
```
show authentication sessions interface GigabitEthernet1/0/2 details
```

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

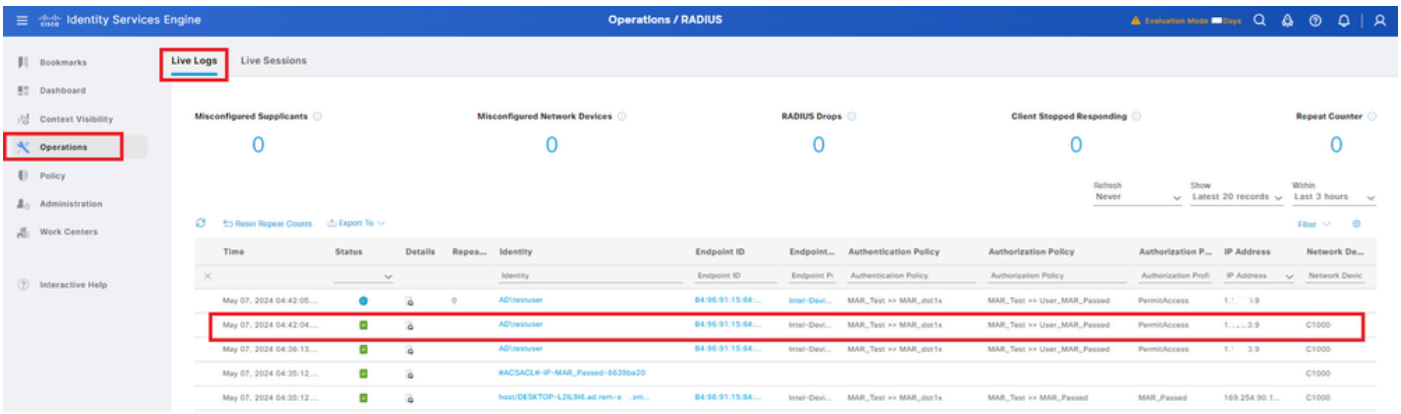
```
User-Name: AD\testuser
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 419s
Common Session ID: 01C2006500000049AA780D80
Acct Session ID: 0x0000003D
Handle: 0x66000016
Current Policy: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

Schritt 3: RADIUS-Live-Protokoll bestätigen

Navigieren Sie zu **Operations > RADIUS > Live Logs (Vorgänge > RADIUS > Live-Protokolle** in der ISE-GUI), und bestätigen Sie das Live-Protokoll für die Benutzerauthentifizierung.

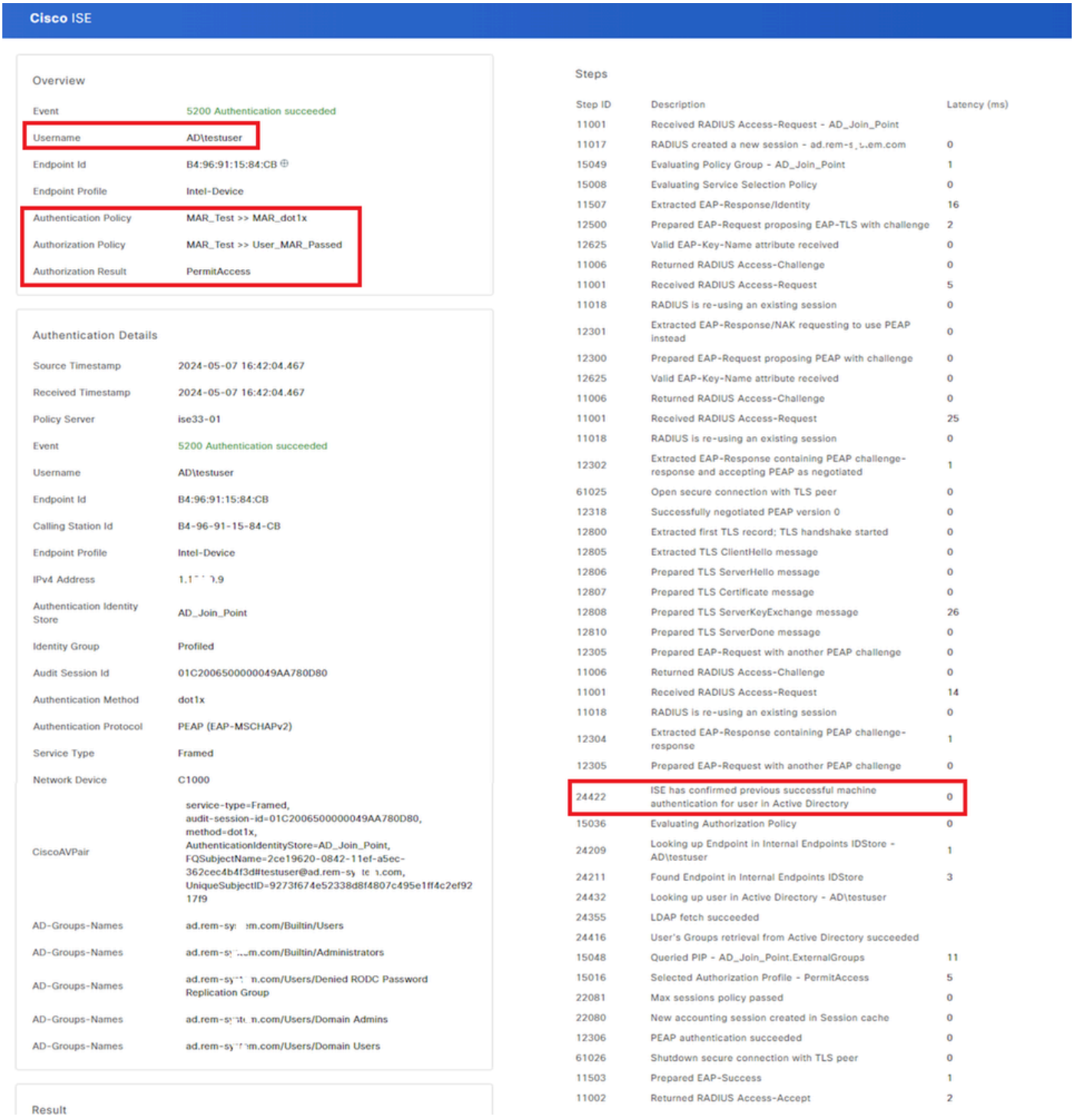


Hinweis: Da der MAR-Cache in der ISE gespeichert ist, ist nur eine Benutzerauthentifizierung erforderlich.



Radius-Live-Protokoll

Bestätigen Sie das detaillierte Live-Protokoll der Benutzerauthentifizierung.



Details zur Benutzerauthentifizierung

Fehlerbehebung

Diese Debug-Protokolle (prrt-server.log) helfen Ihnen, das detaillierte Verhalten der Authentifizierung in der ISE zu bestätigen.

- Laufzeitkonfiguration

- Laufzeitprotokollierung

- Laufzeit-AAA

Dies ist ein Beispiel für das Debug-Protokoll für **Muster 1. Systemauthentifizierung und Benutzerauthentifizierung** in diesem Dokument.

<#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

Zugehörige Informationen

Vor- und Nachteile der Einschränkung des Systemzugriffs

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.