为请求方访问配置计算机双因素身份验证

目录

简介

本文档介绍使用计算机和dot1x身份验证配置双因素身份验证所需的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科身份服务引擎的配置
- Cisco Catalyst的配置
- IEEE802.1X

使用的组件

- 身份服务引擎虚拟3.3补丁1
- C1000-48FP-4G-L 15.2(7)E9

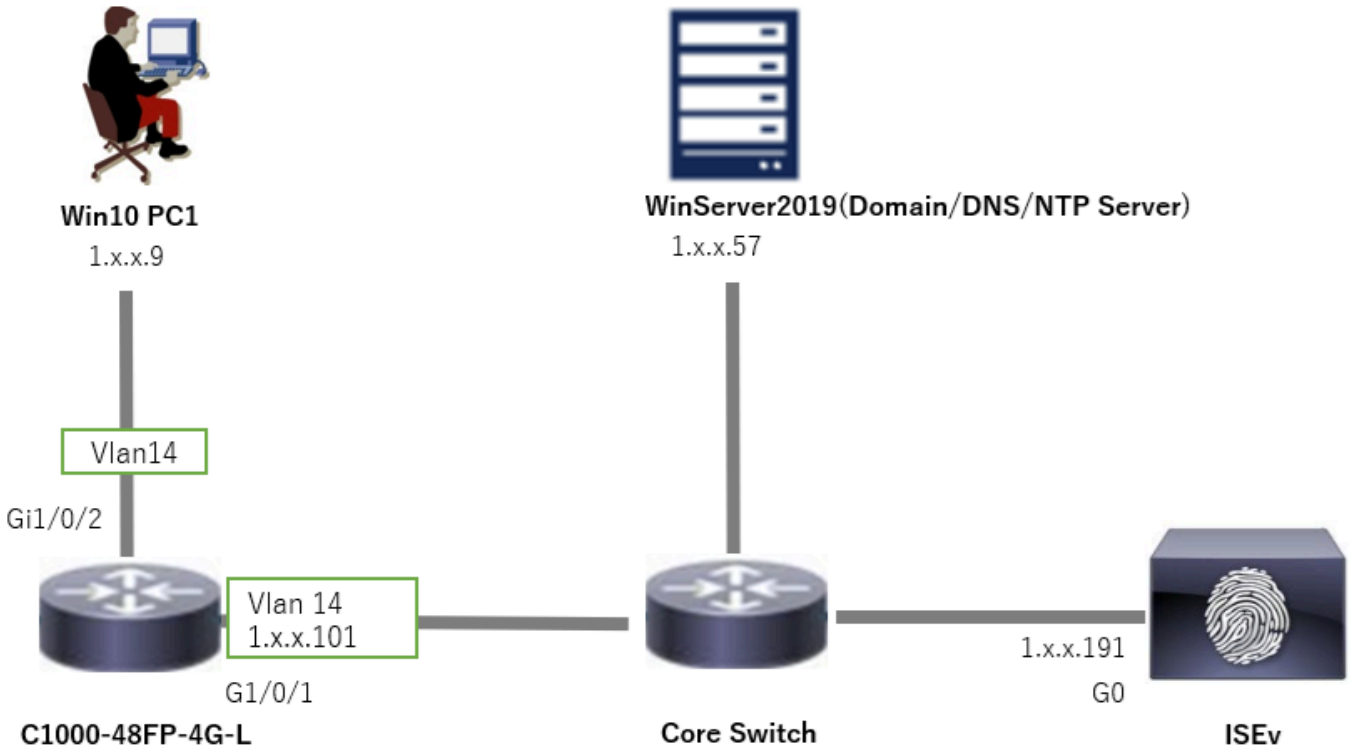
- Windows Server 2019

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

网络图

下图显示本文档示例中使用的拓扑。

在Windows Server 2019上配置的域名是ad.rem-xxx.com，本文档中将其用作示例。



网络图

背景信息

计算机身份验证是验证寻求访问网络或系统的设备的身份的安全过程。用户身份验证根据用户名和密码等凭证验证个人身份，而计算机身份验证则不同，它侧重于验证设备本身。这通常使用设备独有的数字证书或安全密钥来完成。

通过将机器和用户身份验证结合使用，组织可以确保只有经过授权的设备和用户才能访问其网络，从而提供更加安全的环境。这种双因素身份验证方法对于保护敏感信息和遵守严格的法规标准特别有用。

配置

C1000中的配置

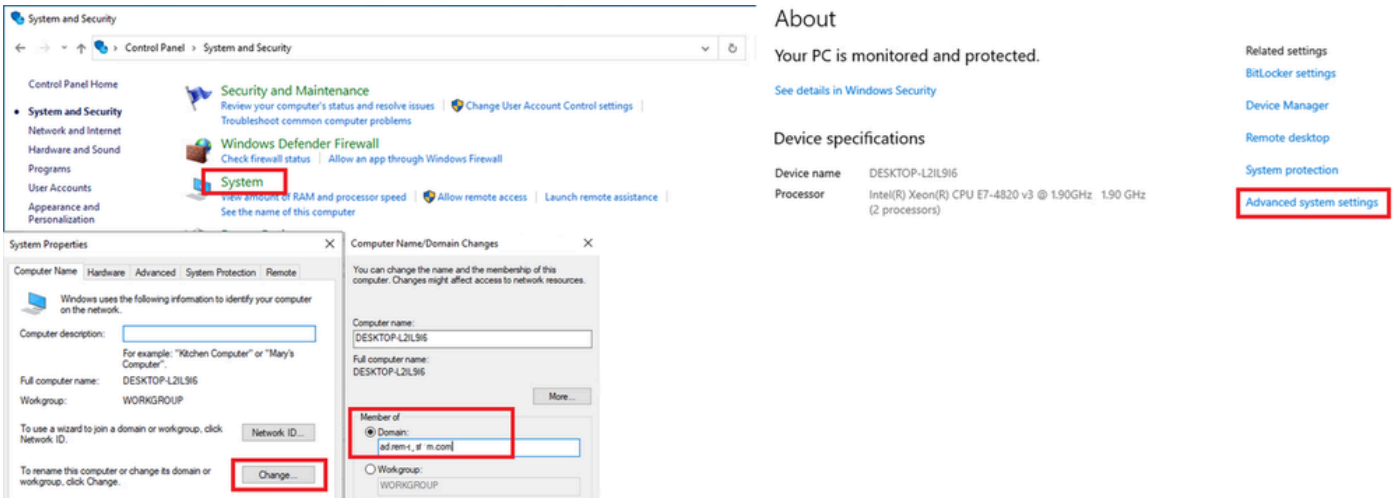
这是C1000 CLI中的最低配置。

```
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中的配置

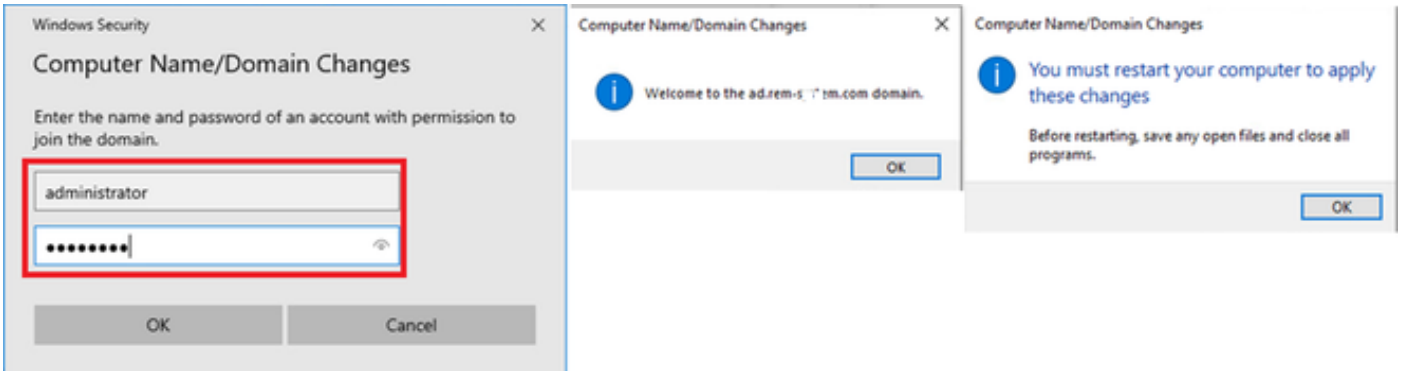
步骤1:将PC添加到AD域

导航到控制面板>系统和安全，单击系统，然后单击高级系统设置。在“System Properties”窗口中，单击Change，选择Domain并输入域名。



将PC添加到AD域

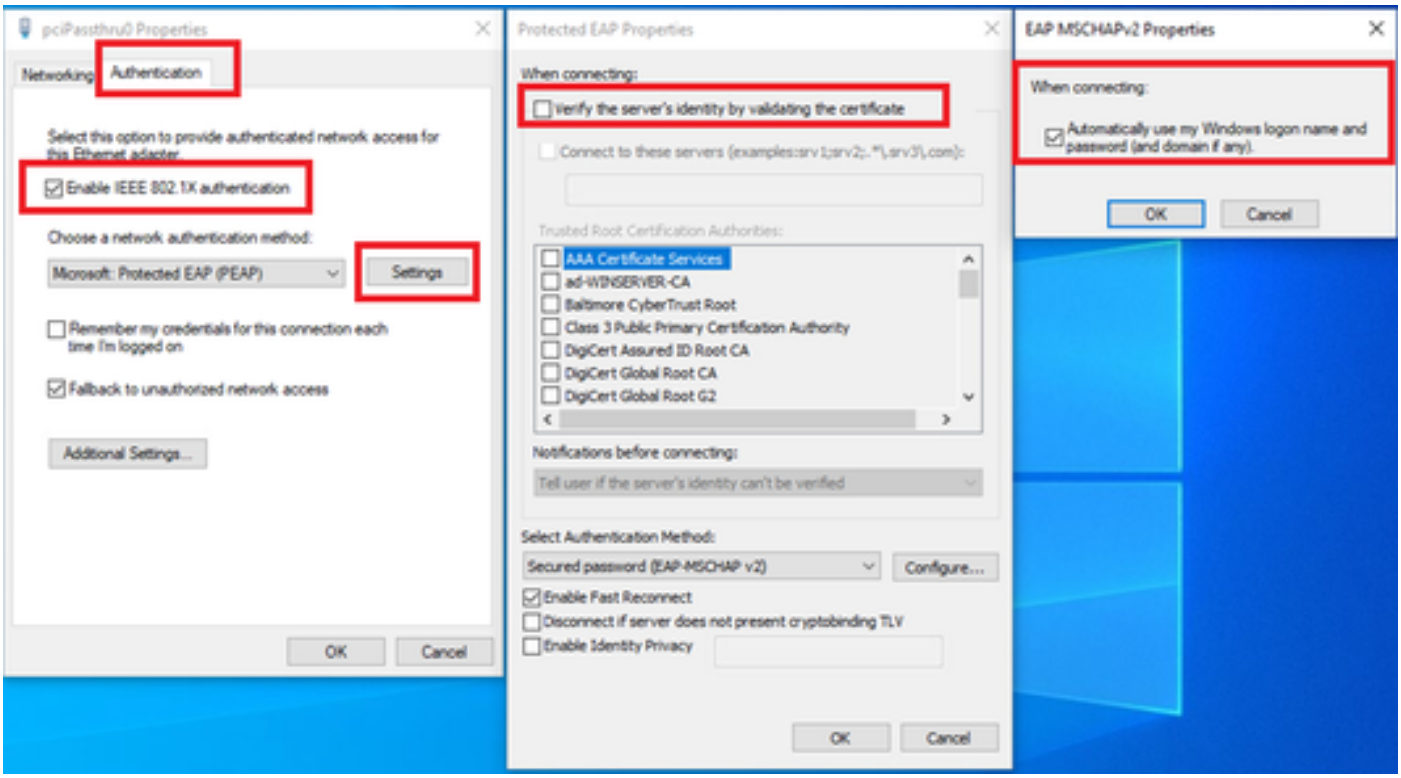
在“Windows安全”窗口中，输入域服务器的用户名和密码。



输入用户名和密码

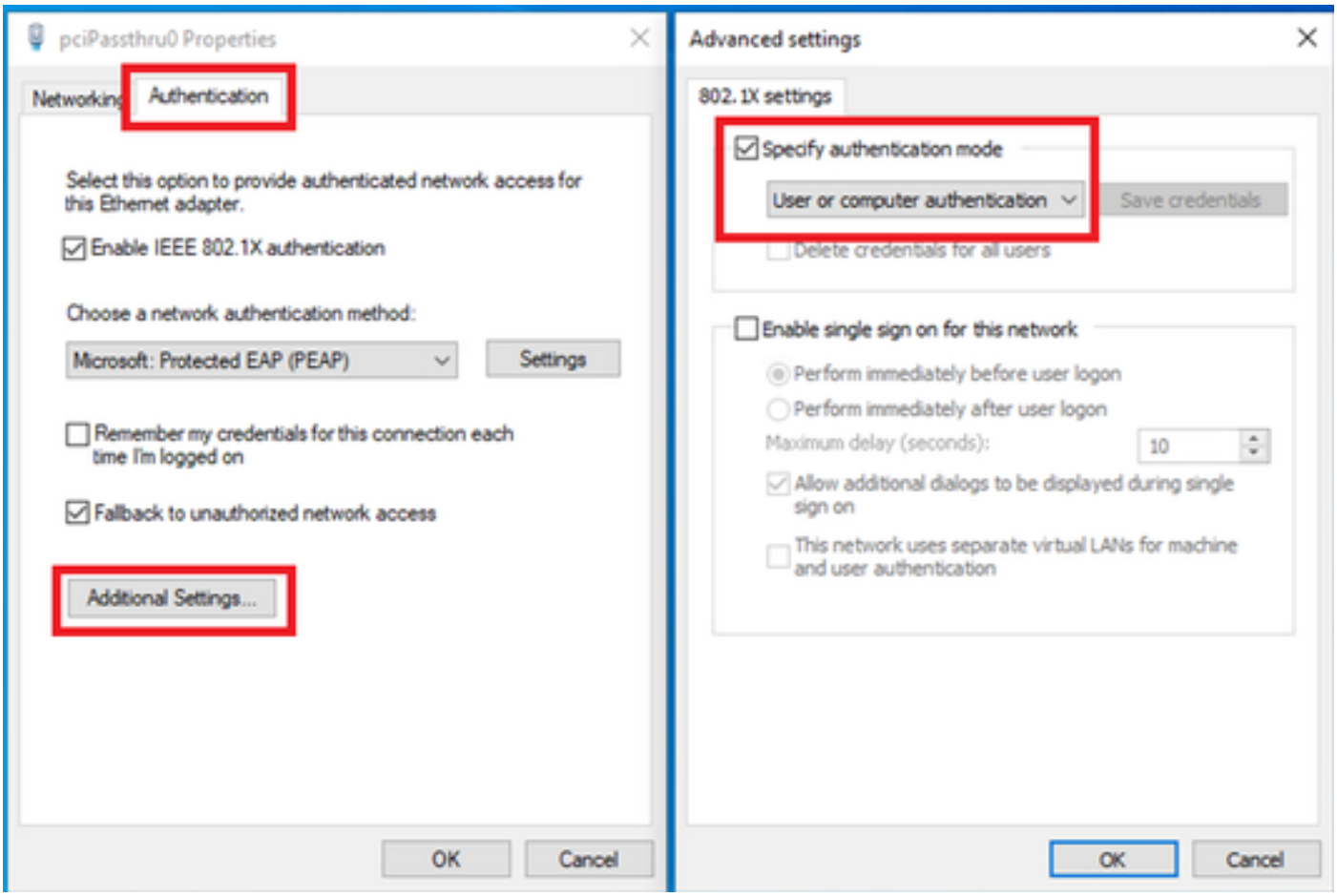
第二步：配置用户身份验证

导航到身份验证，选中启用IEEE 802.1X身份验证。 在“受保护的EAP属性”窗口中单击设置，取消选中通过验证证书验证服务器身份，然后单击配置。在“EAP MSCHAPv2 Properties”窗口中，选中Automatically use my Windows logon name and password (and domain if any)，以使用在Windows计算机登录期间输入的用户名进行用户身份验证。



启用用户验证

导航到身份验证，选中其他设置。从下拉列表中选择User or computer authentication。

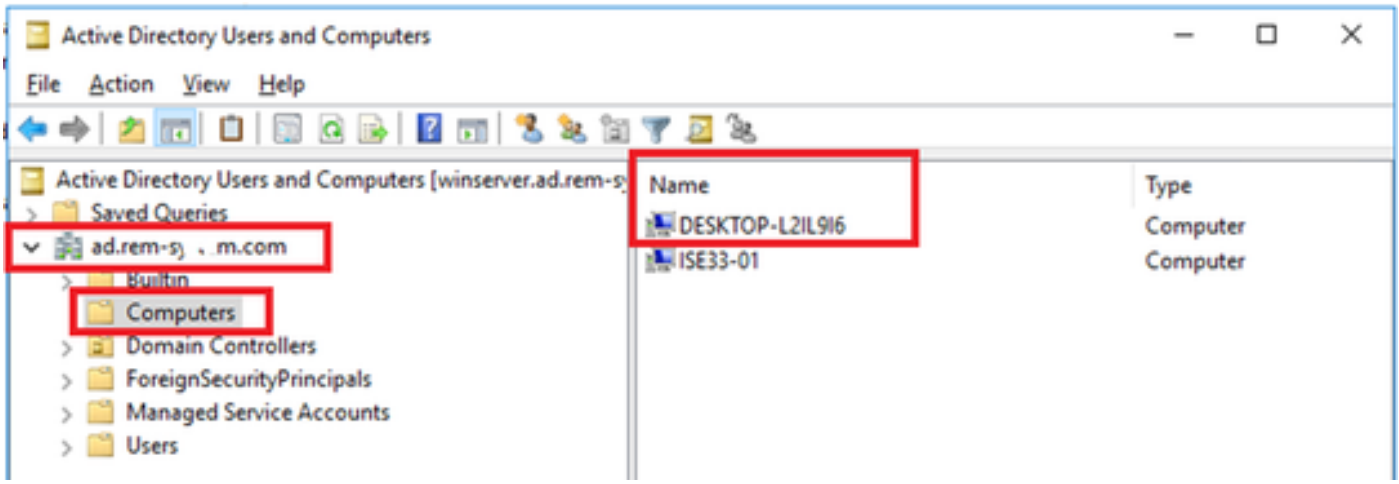


指定身份验证模式

Windows Server中的配置

步骤1:确认域计算机

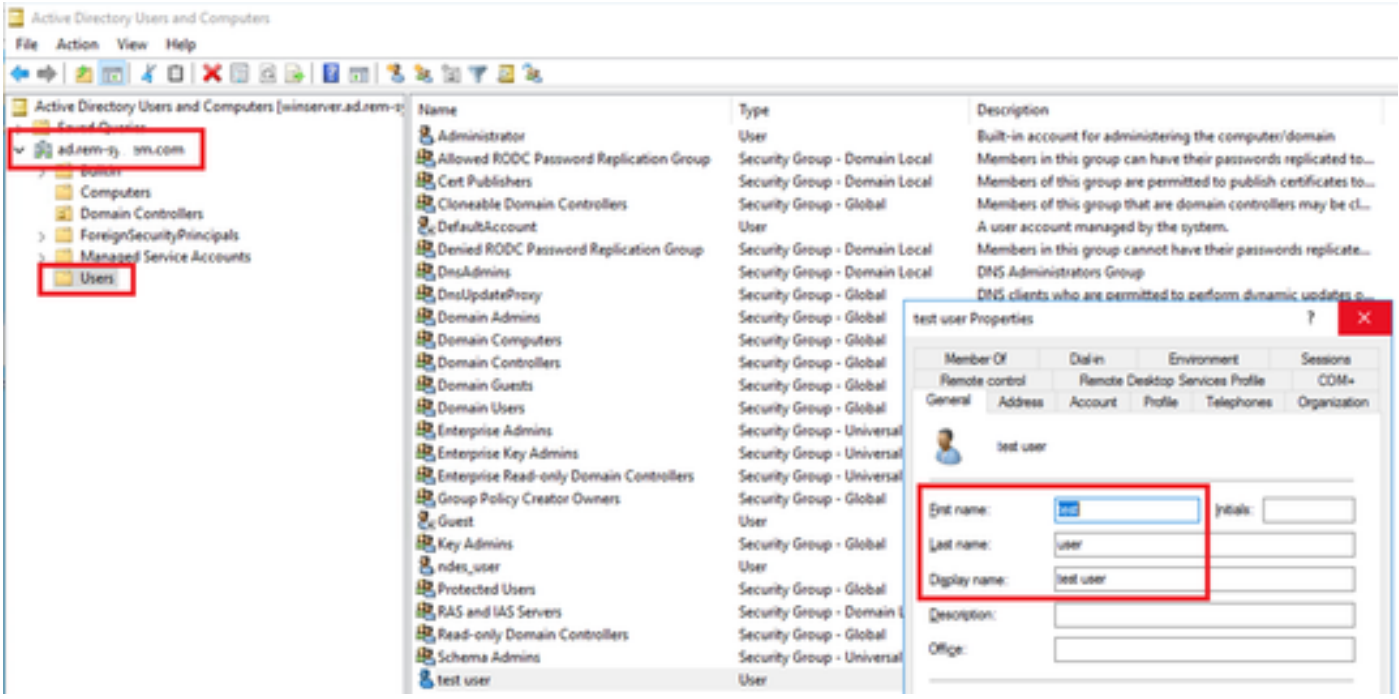
导航到Active Directory用户和计算机，单击计算机。确认域中列出了Win10 PC1。



确认域计算机

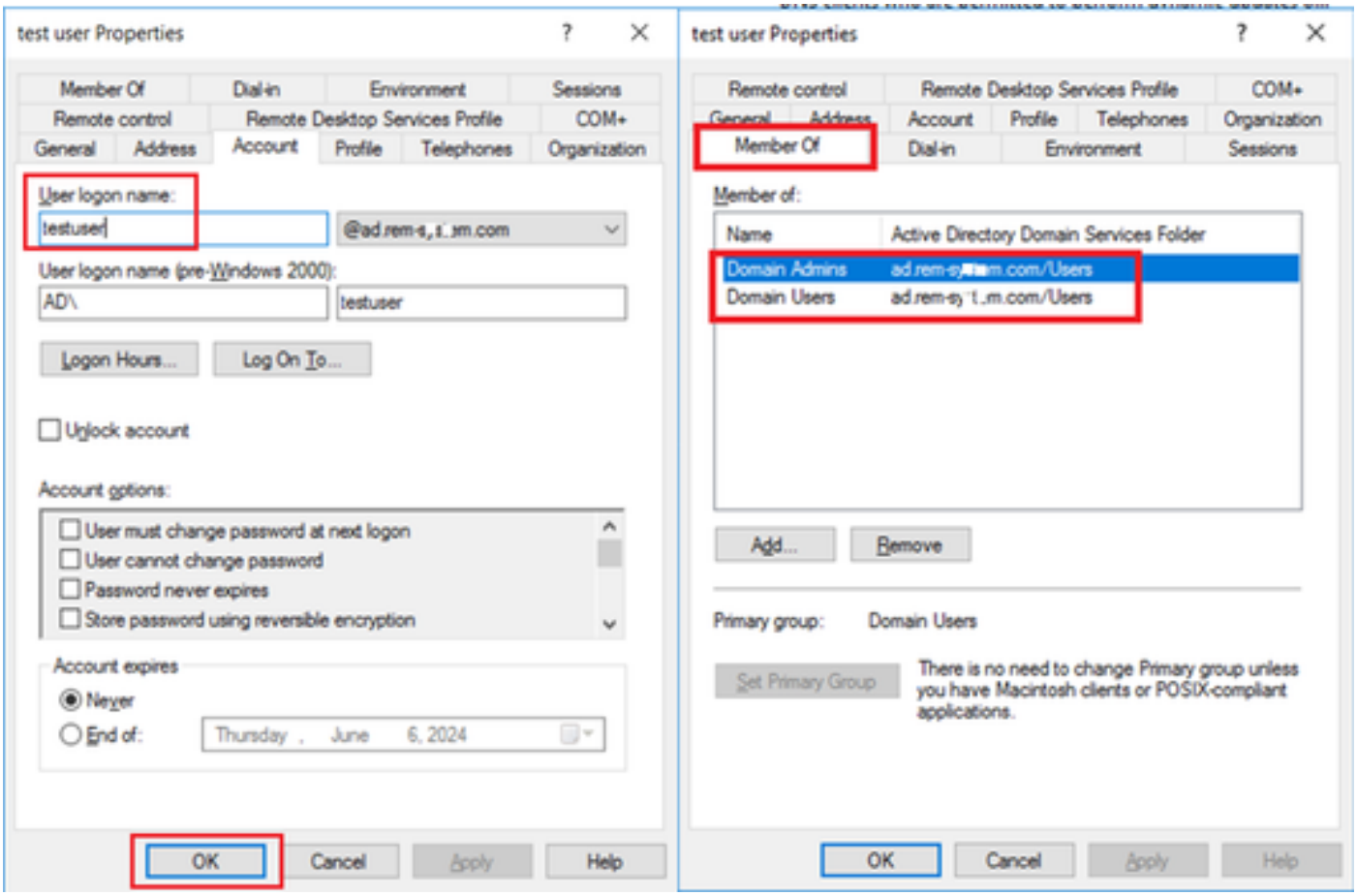
第二步：添加域用户

导航到Active Directory用户和计算机，单击用户。将testuser添加为域用户。



添加域用户

将域用户添加到域管理员和域用户的成员。

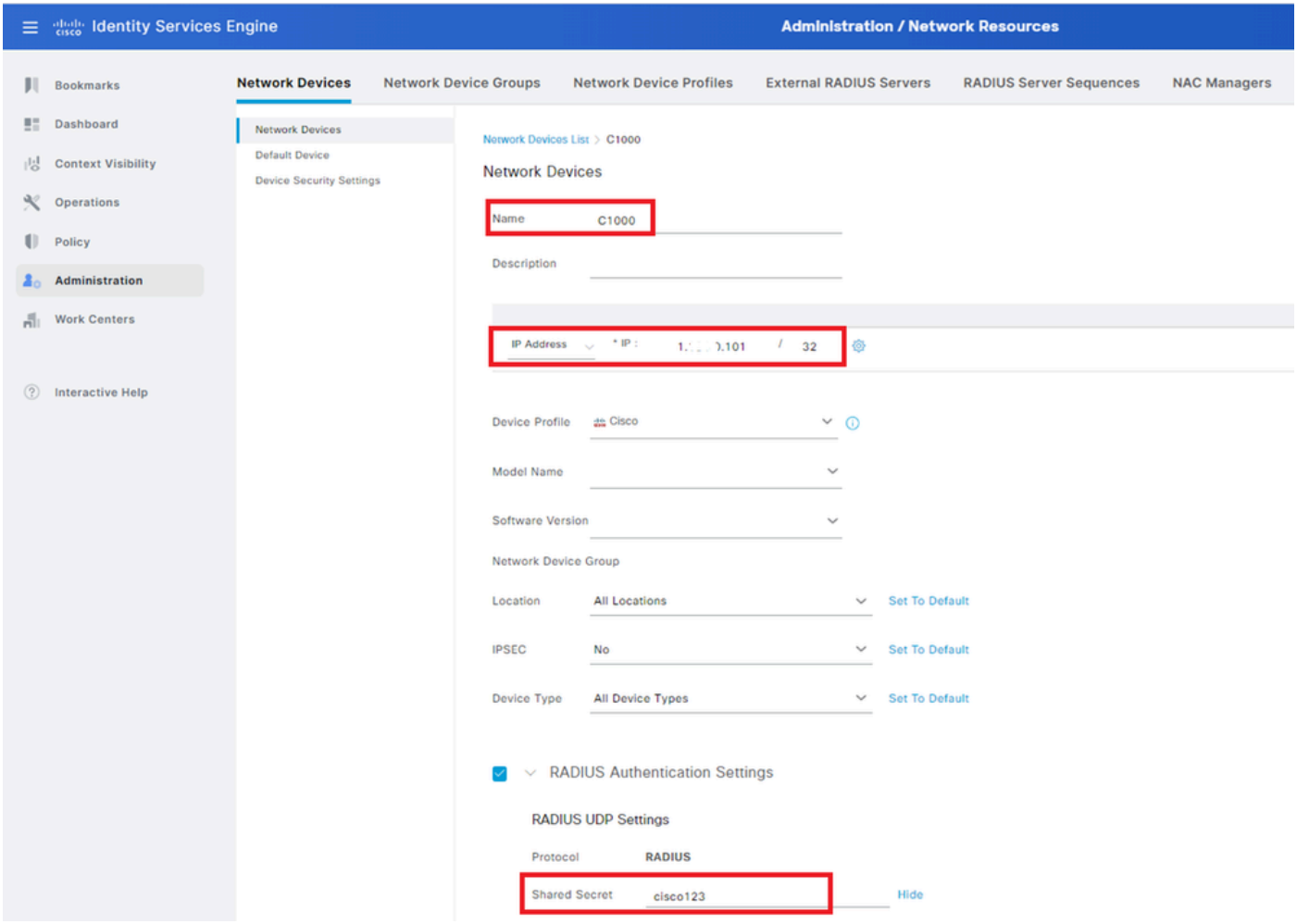


域管理员和域用户

ISE中的配置

步骤1:添加设备

导航到管理>网络设备，点击添加按钮以添加C1000设备。

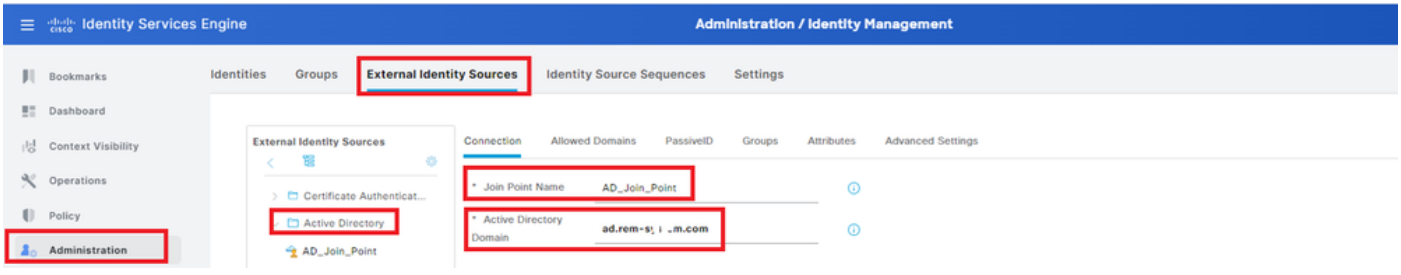


添加设备

第二步：添加Active Directory

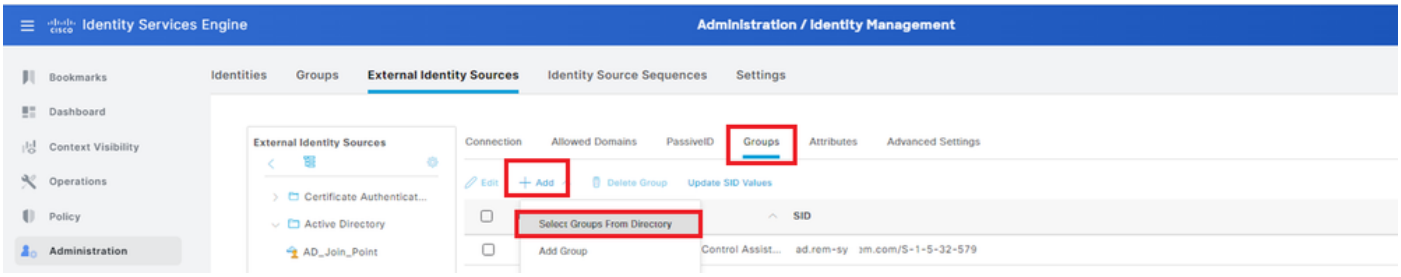
导航到管理>外部身份源> Active Directory，点击连接选项卡，将Active Directory添加到ISE。

- 加入点名称：AD_Join_Point
- Active Directory域：ad.rem-xxx.com



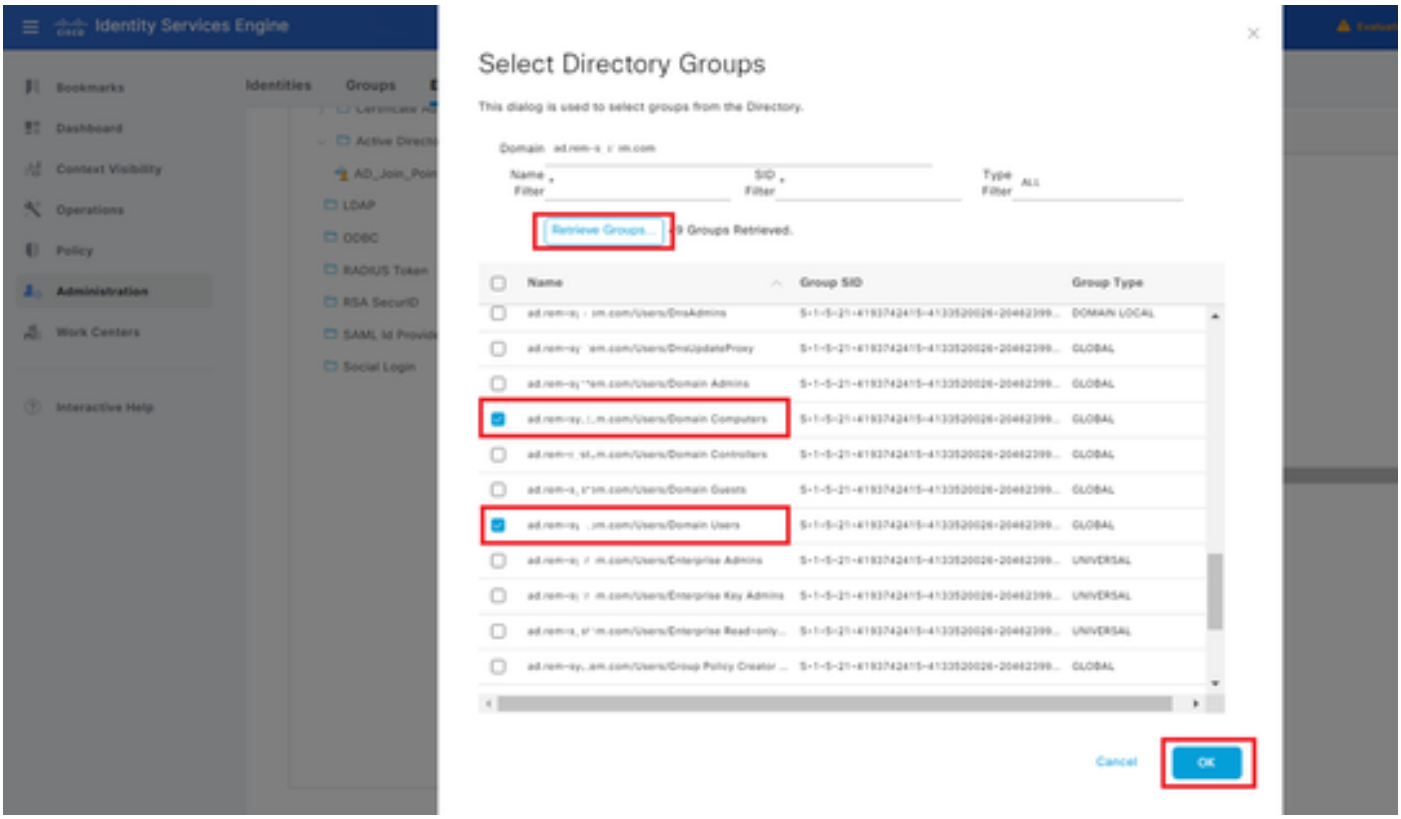
添加Active Directory

导航到Groups选项卡，从下拉列表中选择Select Groups From Directory。



从目录中选择组

从下拉列表中单击Retrieve Groups。选中ad.rem-xxx.com/Users/Domain计算机和ad.rem-xxx.com/Users/Domain用户，然后单击确定。

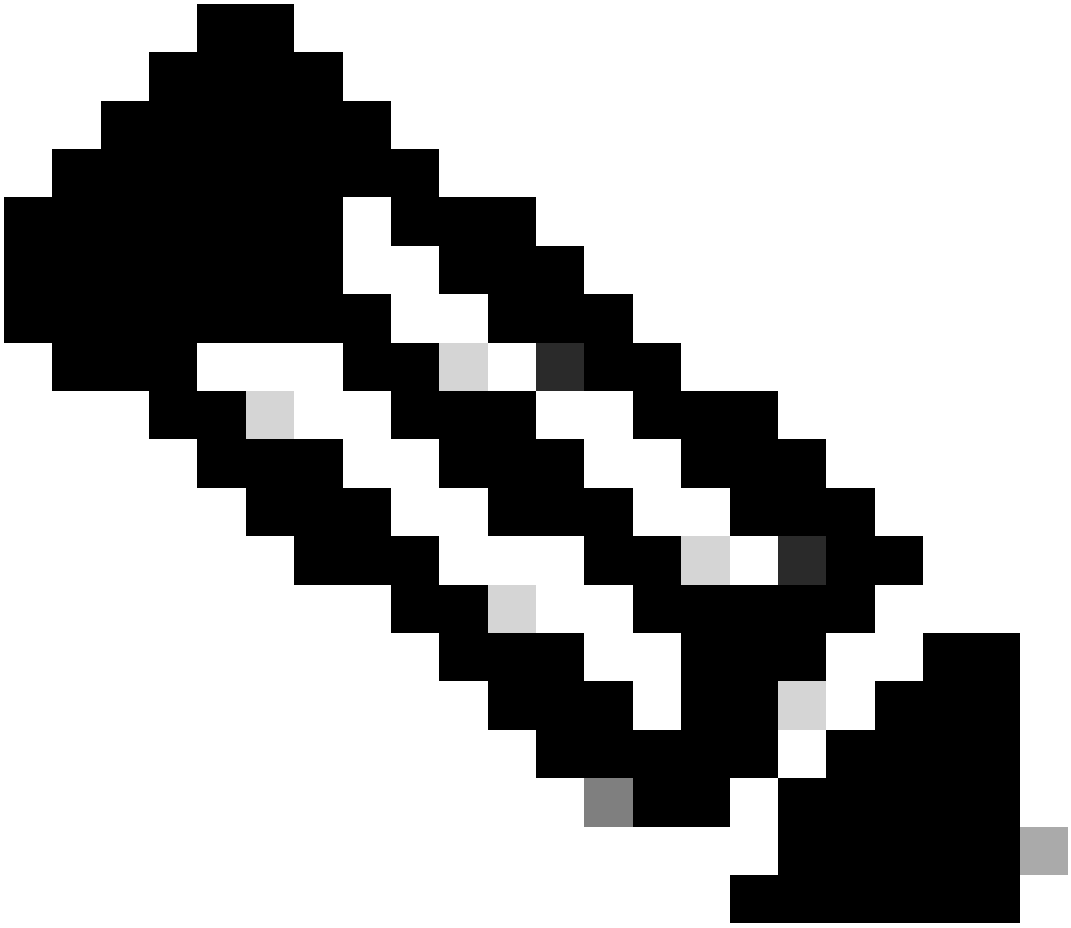


添加域计算机和用户

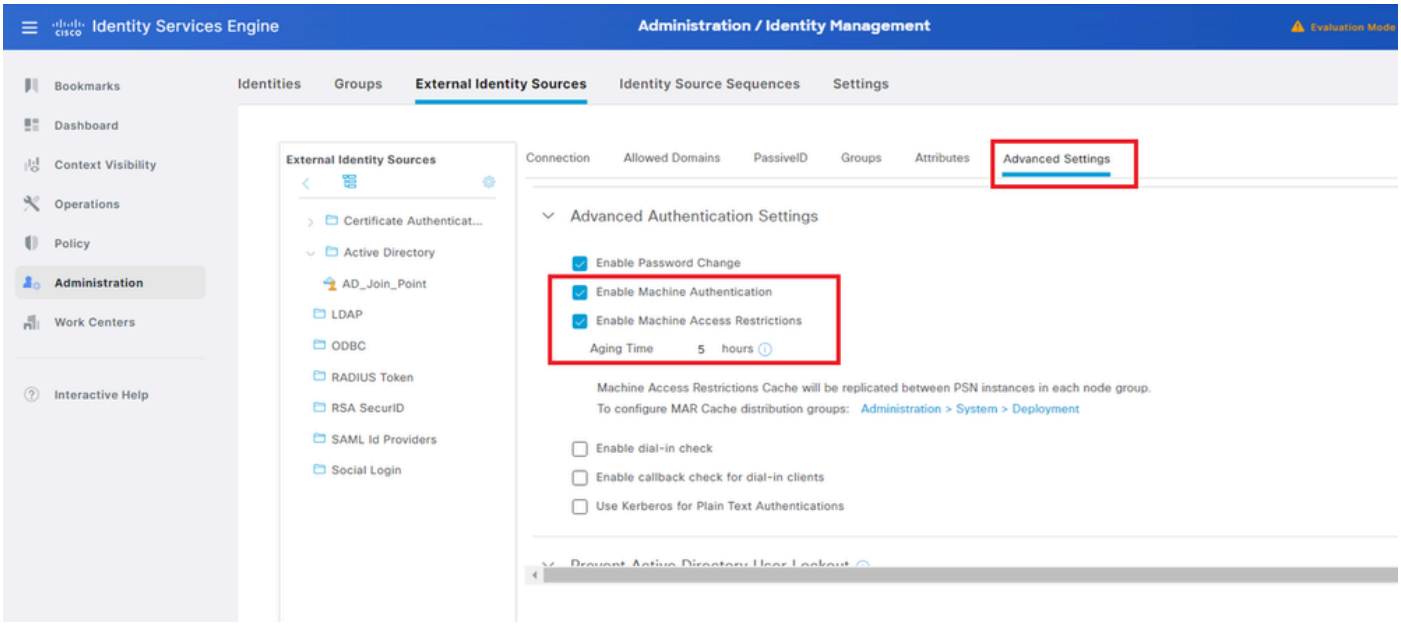
第三步：确认计算机身份验证设置

导航到高级设置选项卡，确认计算机身份验证的设置。

- 启用计算机身份验证：启用计算机身份验证
- Enable Machine Access Restriction：在授权之前将用户和计算机身份验证结合起来



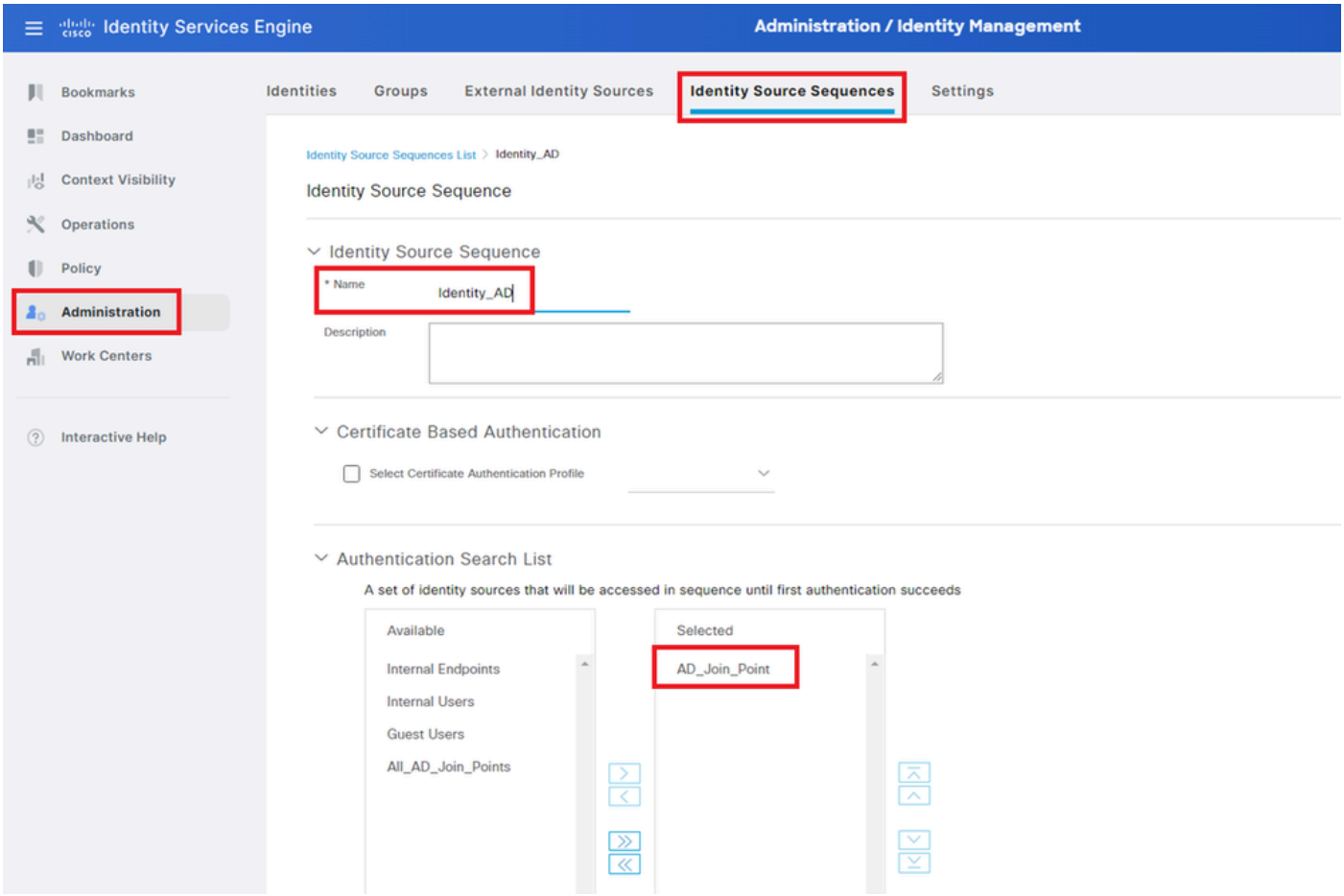
注意：有效的老化时间范围是1到8760。



第四步：添加身份源序列

导航到管理>身份源序列，添加身份源序列。

- 名称：Identity_AD
- 身份验证搜索列表：AD_Join_Point

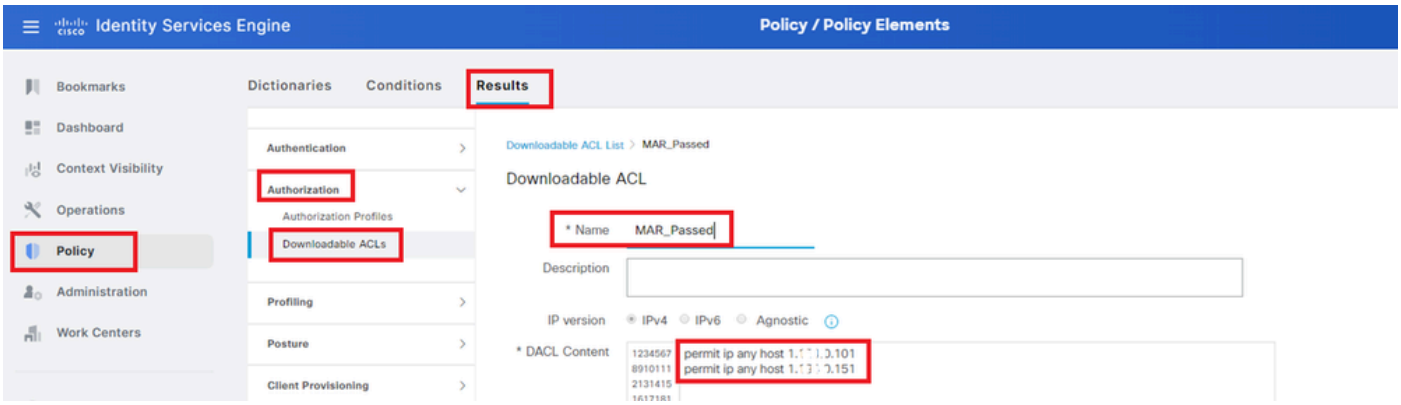


添加身份源序列

第五步：添加DACL和授权配置文件

导航到策略>结果>授权>可下载ACL，添加DACL。

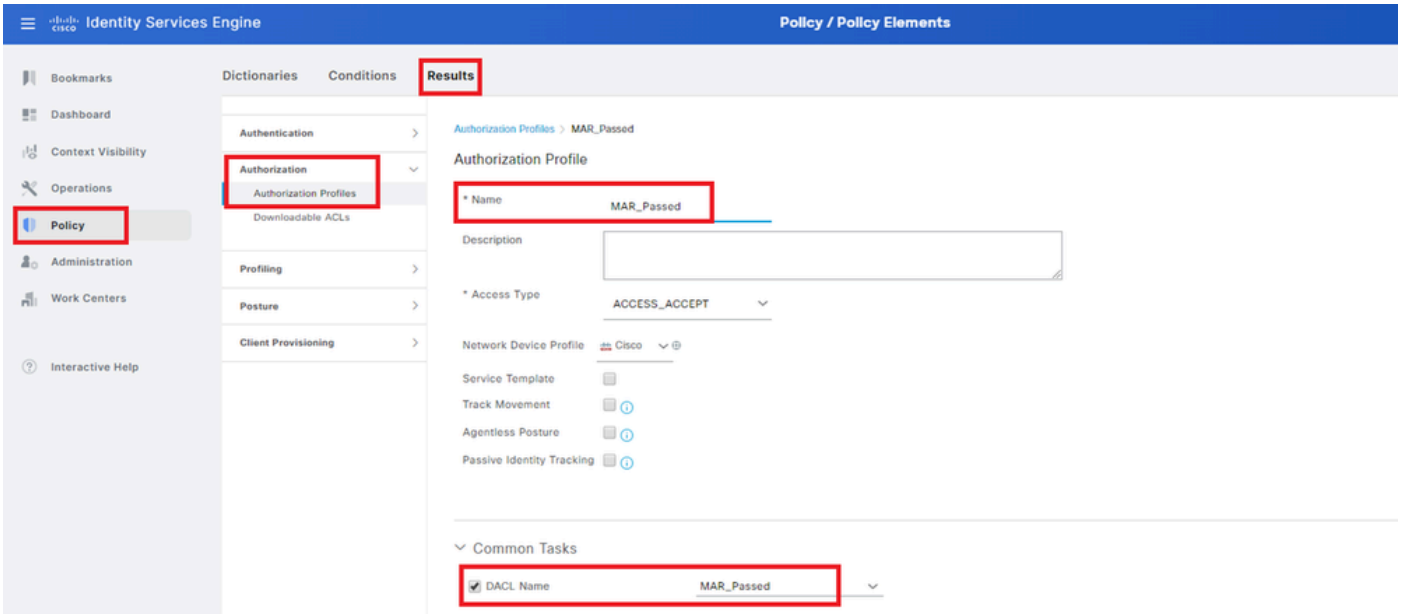
- 名称：MAR_Passed
- DACL内容：permit ip any host 1.x.x.101和permit ip any host 1.x.x.105



添加DACL

导航到策略>结果>授权>授权配置文件，添加授权配置文件。

- 名称：MAR_Passed
- DACL名称：MAR_Passed

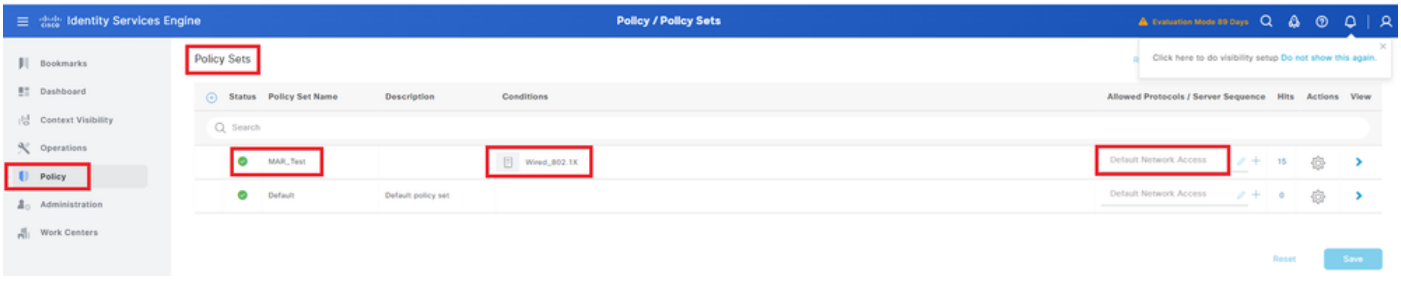


添加授权配置文件

第六步：添加策略集

导航到策略>策略集，点击+ 添加策略集。

- 策略集名称：MAR_Test
- 条件：Wired_802.1X
- 允许的协议/服务器序列：默认网络访问



添加策略集

步骤 7.添加身份验证策略

导航到策略集，点击MAR_Test添加身份验证策略。

- 规则名称：MAR_dot1x
- 条件：Wired_802.1X
- 使用：Identity_AD

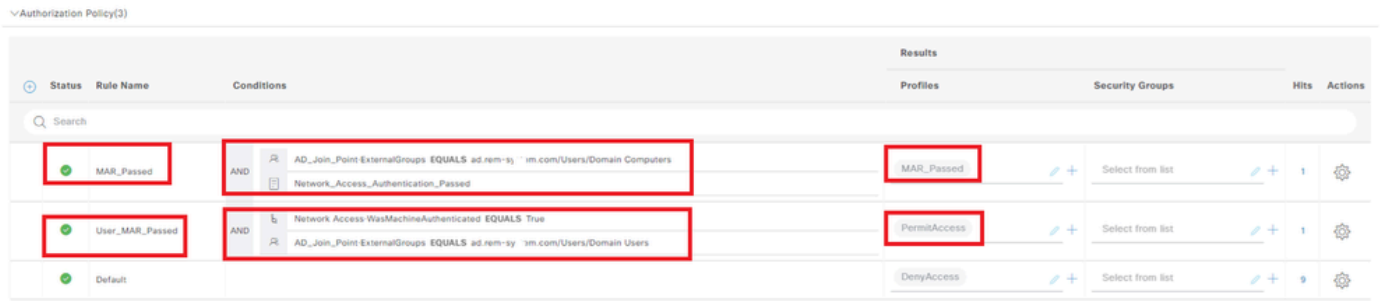
添加身份验证策略

步骤 8添加授权策略

导航到策略集，点击MAR_Test添加授权策略。

- 规则名称：MAR_Passed
- 条件：AD_Join_Point·ExternalGroups 等于ad.rem-xxx.com/Users/Domain计算机和 Network_Access_Authentication_Passed
- 结果：MAR_Passed

- 规则名称：User_MAR_Passed
- 条件：网络访问·WasMachineAuthenticated EQUALS True 和AD_Join_Point·ExternalGroups EQUALS ad.rem-xxx.com/Users/Domain用户
- 结果：PermitAccess



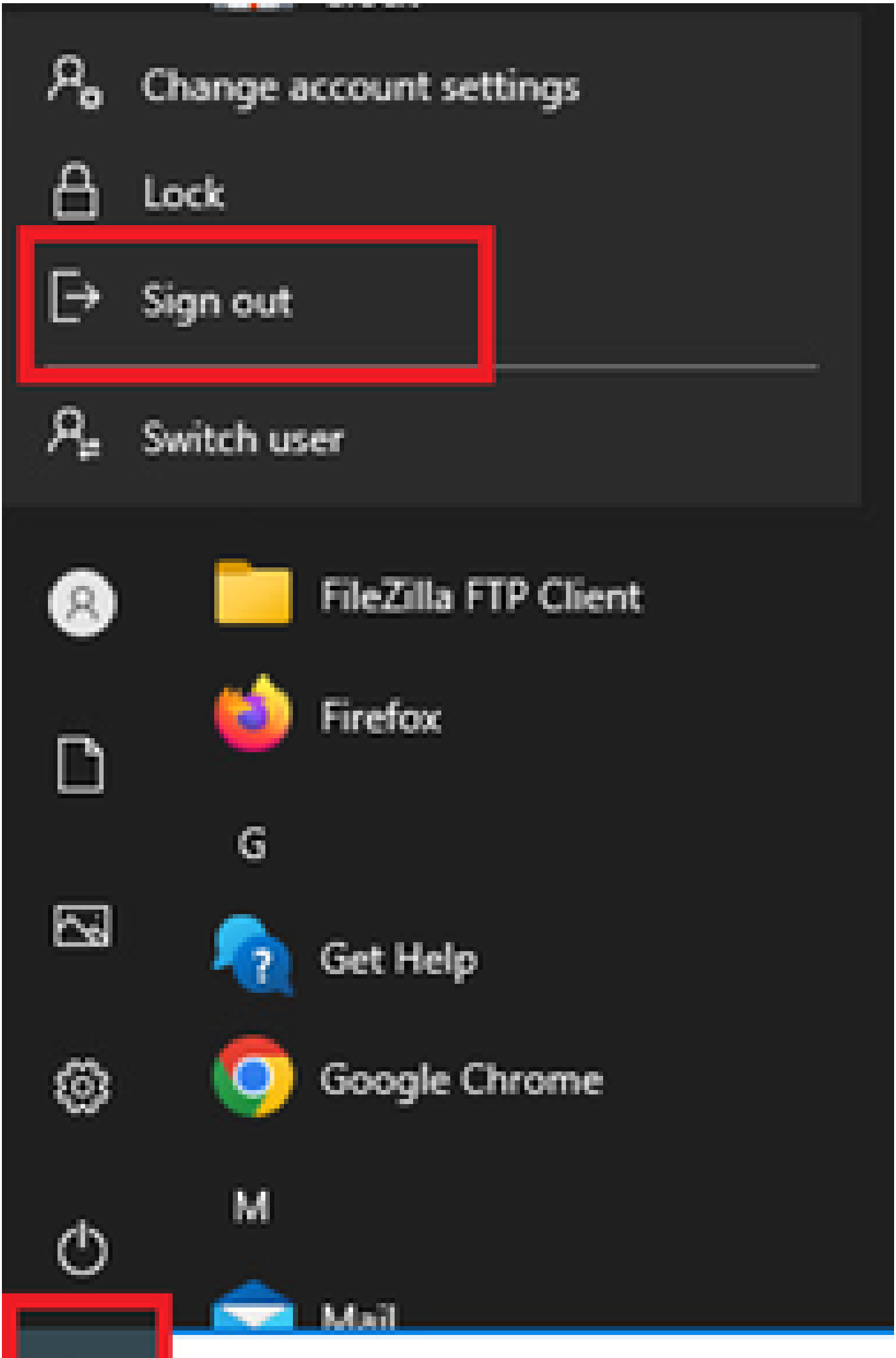
添加授权策略

验证

模式1。计算机身份验证和用户身份验证

步骤1:注销Windows PC

单击Win10 PC1的注销按钮以触发计算机身份验证。


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

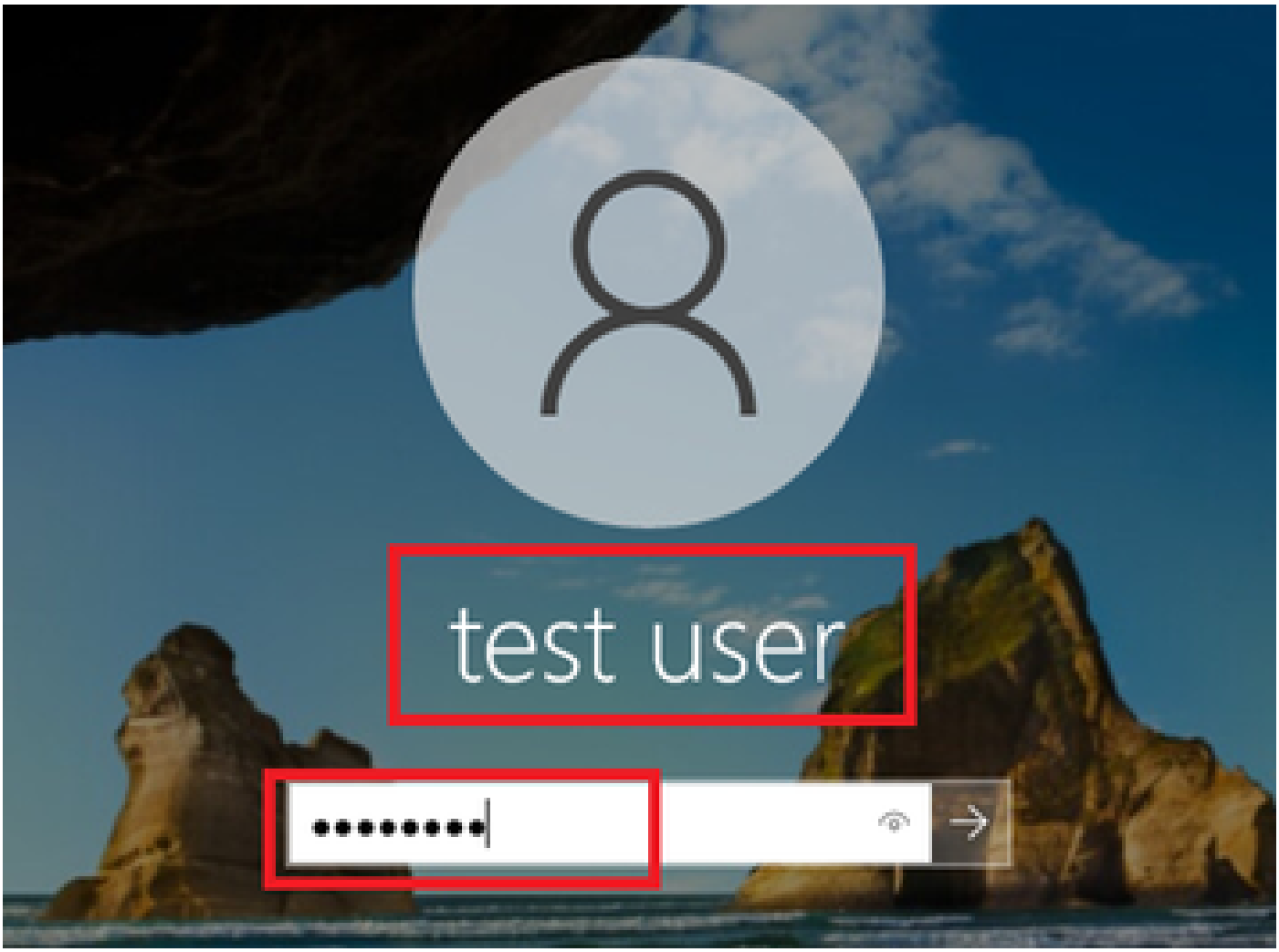
```
Interface: GigabitEthernet1/0/2
MAC Address: b496.9115.84cb
IPv6 Address: Unknown
IPv4 Address: 1.x.x.9
User-Name:
```

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
```

第三步：登录Windows PC

登录Win10 PC1，输入用户名和密码以触发用户身份验证。



登录*Windows PC*

第四步：确认身份验证会话

在C1000中运行show authentication sessions interface GigabitEthernet1/0/2 details命令以确认用户身份验证会话。

<#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:
```

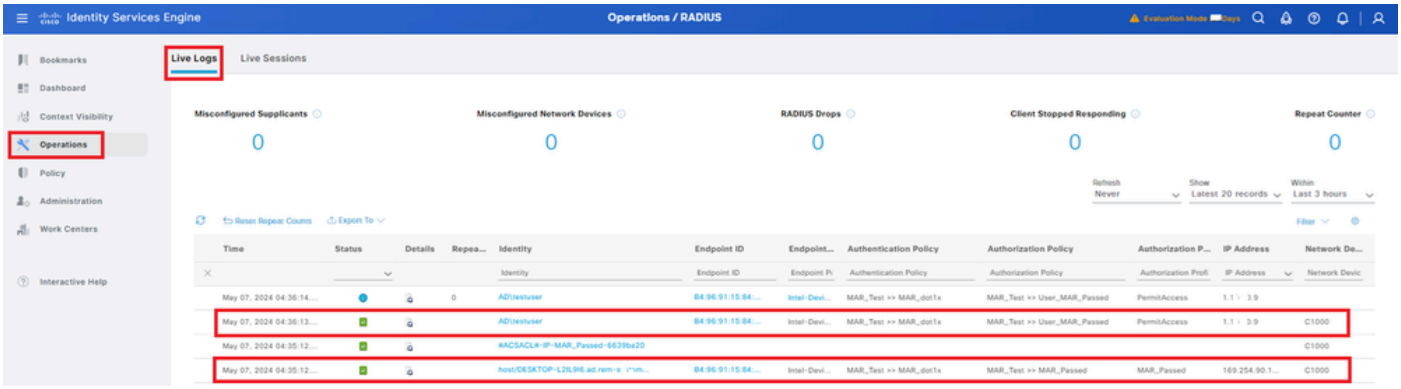
AD\testuser

```
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
```

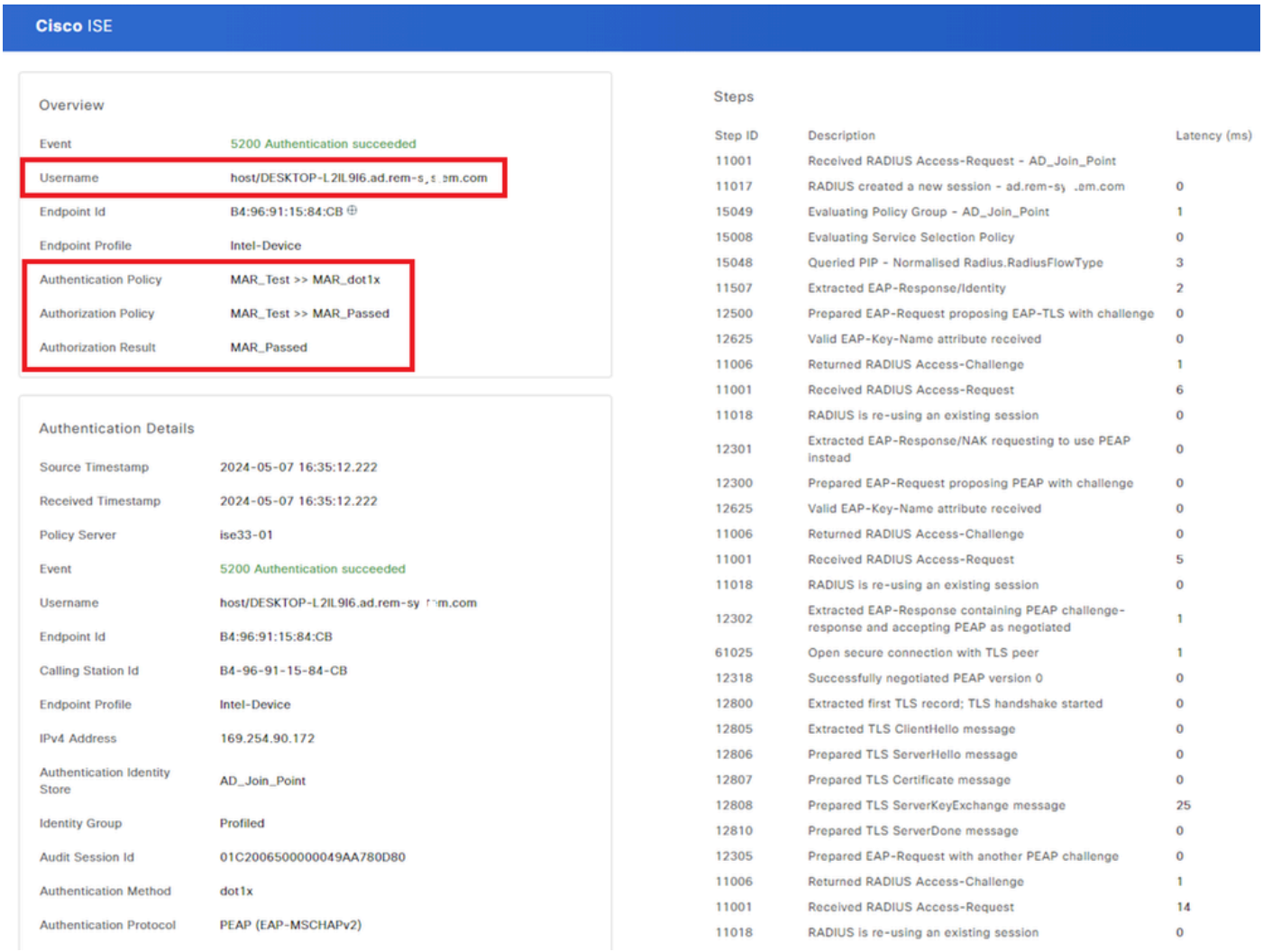
第五步：确认Radius实时日志

导航到ISE GUI中的**操作> RADIUS** >实时日志，确认计算机身份验证和用户身份验证的实时日志。



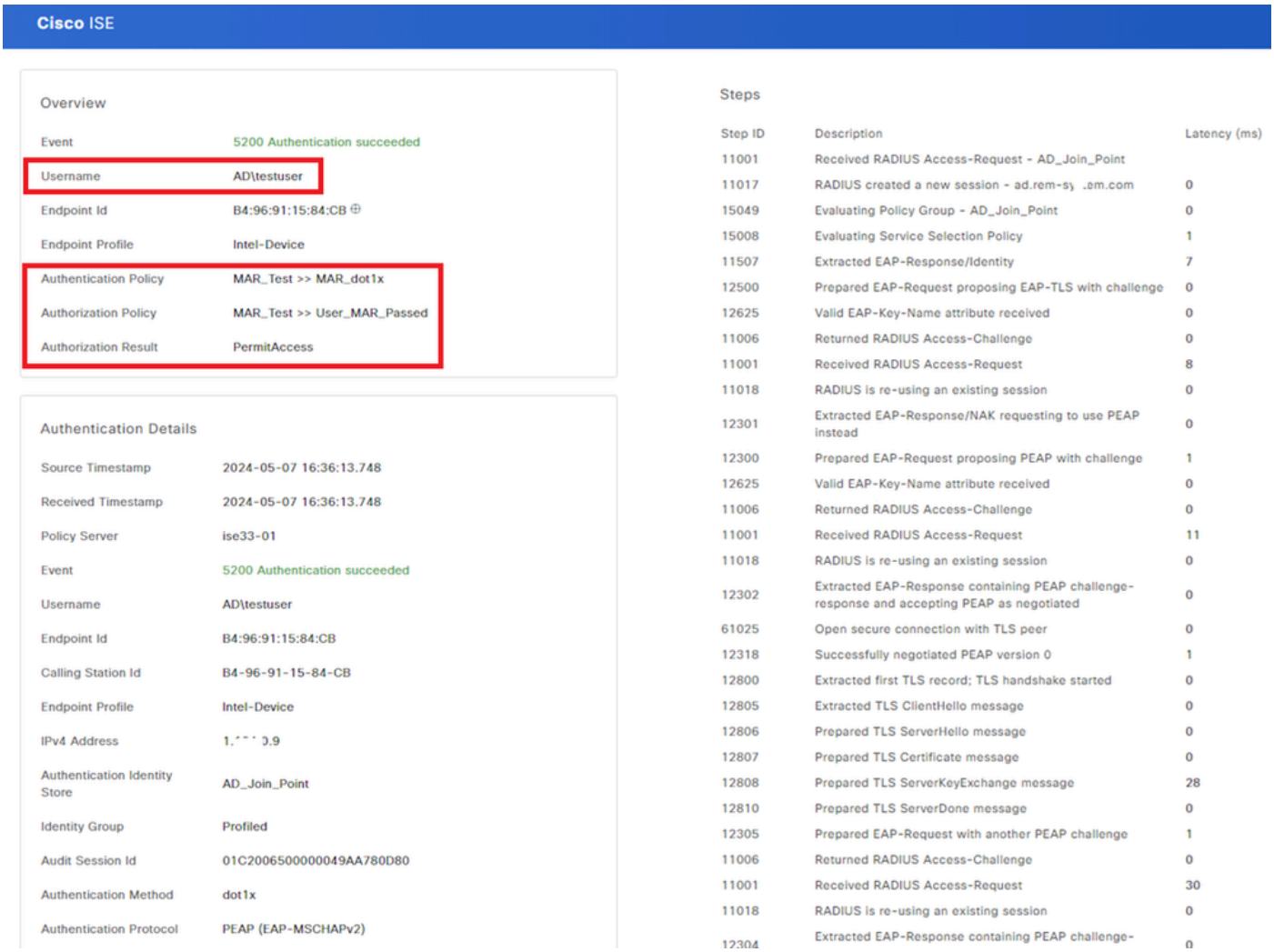
*Radius*实时日志

确认计算机身份验证的详细实时日志。



计算机身份验证的详细信息

确认用户身份验证的详细实时日志。



用户身份验证的详细信息

模式2.仅用户身份验证

步骤1:禁用和启用Windows PC的网卡

要触发用户身份验证，请禁用和启用Win10 PC1的NIC。

第二步：确认身份验证会话

在C1000中运行show authentication sessions interface GigabitEthernet1/0/2 details命令以确认用户身份验证会话。

<#root>

Switch#

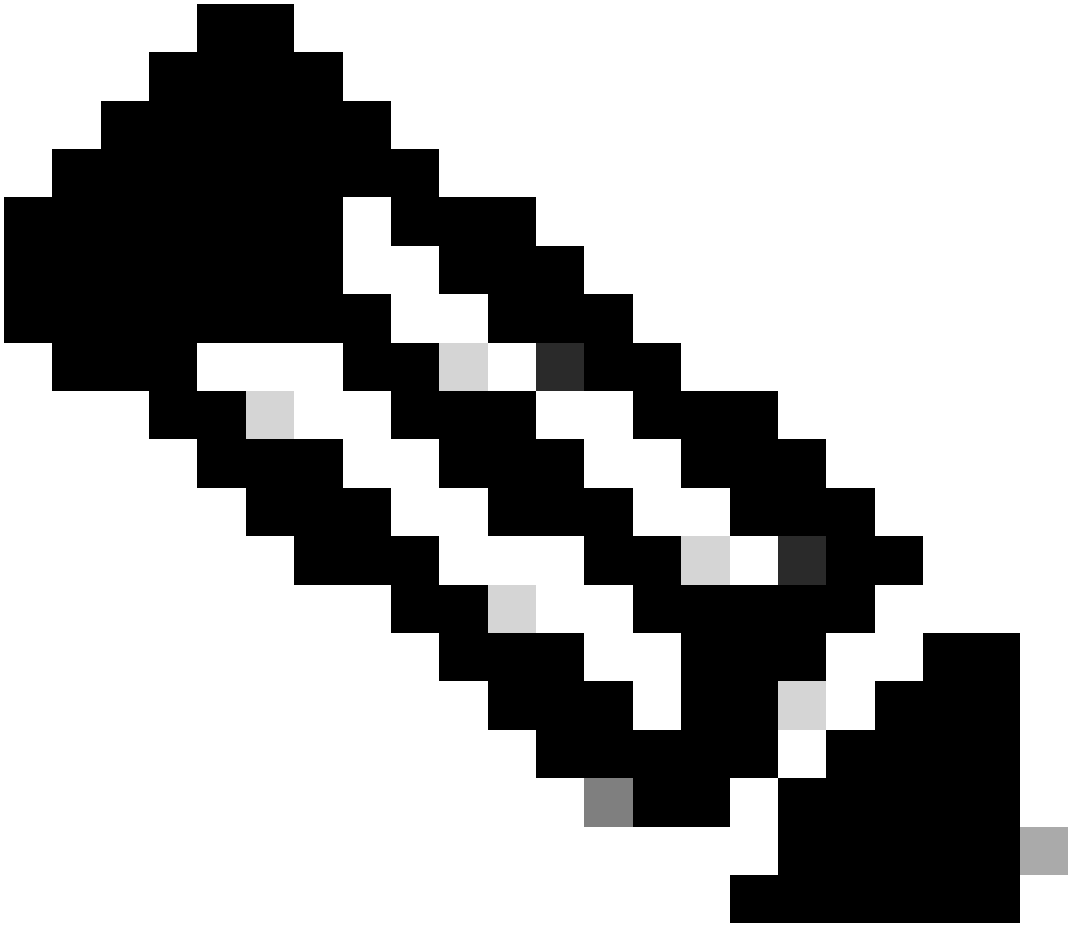
show authentication sessions interface GigabitEthernet1/0/2 details

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

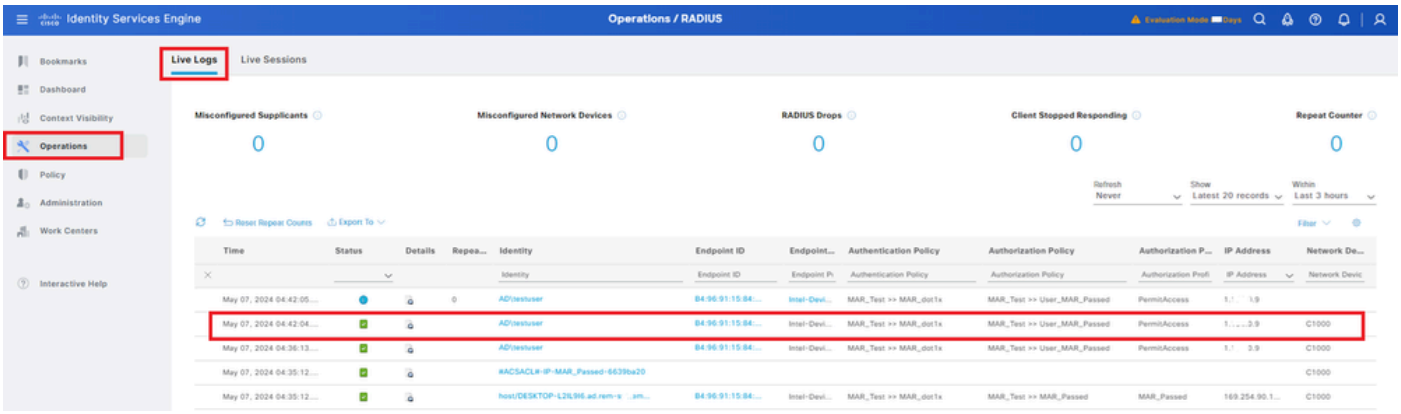
```
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 419s
Common Session ID: 01C2006500000049AA780D80
Acct Session ID: 0x0000003D
Handle: 0x66000016
Current Policy: POLICY_Gi1/0/2

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:


Method status list:
Method State

dot1x Authc Success
```

第三步：确认Radius实时日志

导航到ISE GUI中的**操作> RADIUS** >实时日志，确认用户身份验证的实时日志。



注意：由于MAR缓存存储在ISE中，因此只需要用户身份验证。



*Radius*实时日志

确认用户身份验证的详细实时日志。

用户身份验证的详细信息

故障排除

这些调试日志(prrt-server.log)可帮助您确认ISE中身份验证的详细行为。

- 运行时配置
- 运行日志
- 运行时AAA

这是**模式1**的调试日志示例。计算机身份验证和用户身份验证。

<#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

相关信息

[计算机访问限制的优缺点]

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。