

Configure Machine Two Factor Authentication for Supplicant Access

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Network Diagram](#)

[Background Information](#)

[Configurations](#)

[Configuration in C1000](#)

[Configuration in Windows PC](#)

[Step 1. Add PC to AD Domain](#)

[Step 2. Configure User Authentication](#)

[Configuration in Windows Server](#)

[Step 1. Confirm Domain Computers](#)

[Step 2. Add Domain User](#)

[Configuration in ISE](#)

[Step 1. Add Device](#)

[Step 2. Add Active Directory](#)

[Step 3. Confirm Machine Authentication Setting](#)

[Step 4. Add Identity Source Sequences](#)

[Step 5. Add DACL and Authorization Profile](#)

[Step 6. Add Policy Set](#)

[Step 7. Add Authentication Policy](#)

[Step 8. Add Authorization Policy](#)

[Verify](#)

[Pattern 1. Machine Authentication and User Authentication](#)

[Step 1. Sign Out of Windows PC](#)

[Step 2. Confirm Authentication Session](#)

[Step 3. Login Windows PC](#)

[Step 4. Confirm Authentication Session](#)

[Step 5. Confirm Radius Live Log](#)

[Pattern 2. User Authentication Only](#)

[Step 1. Disable and Enable NIC of Windows PC](#)

[Step 2. Confirm Authentication Session](#)

[Step 3. Confirm Radius Live Log](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

This document describes the steps required to configure Two-Factor authentication with machine and dot1x

authentication.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

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

Components Used

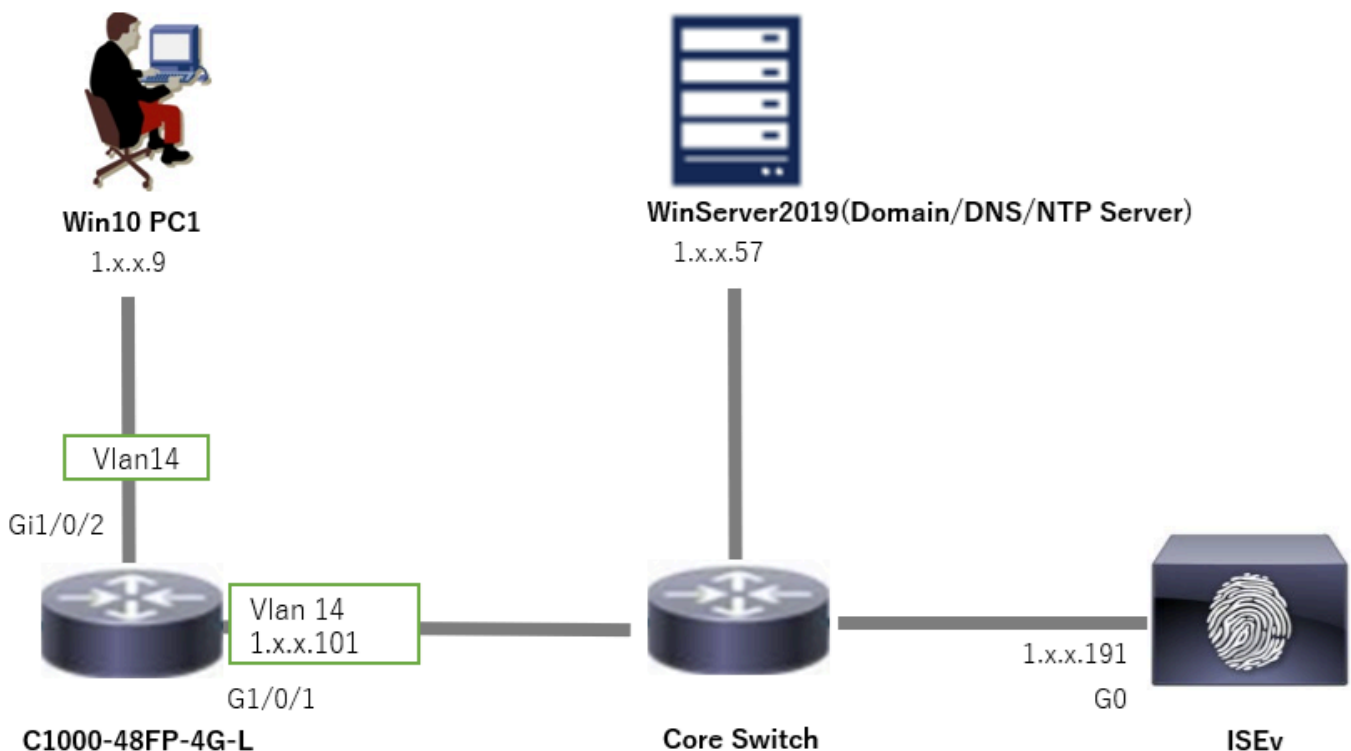
- Identity Services Engine Virtual 3.3 Patch 1
- C1000-48FP-4G-L 15.2(7)E9
- Windows Server 2019

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Network Diagram

This image shows the topology that is used for the example of this document.

The domain name configured on Windows Server 2019 is ad.rem-xxx.com, which is used as an example in this document.



Background Information

Machine authentication is a security process that verifies the identity of a device seeking access to a network or system. Unlike user authentication, which verifies the identity of a person based on credentials like a username and password, machine authentication focuses on validating the device itself. This is often done using digital certificates or security keys that are unique to the device.

By using machine and user authentication together, an organization can ensure that only authorized devices and users can access its network, thereby providing a more secure environment. This Two-Factor authentication method is particularly useful for protecting sensitive information and complying with strict regulatory standards.

Configurations

Configuration in C1000

This is the minimal configuration 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

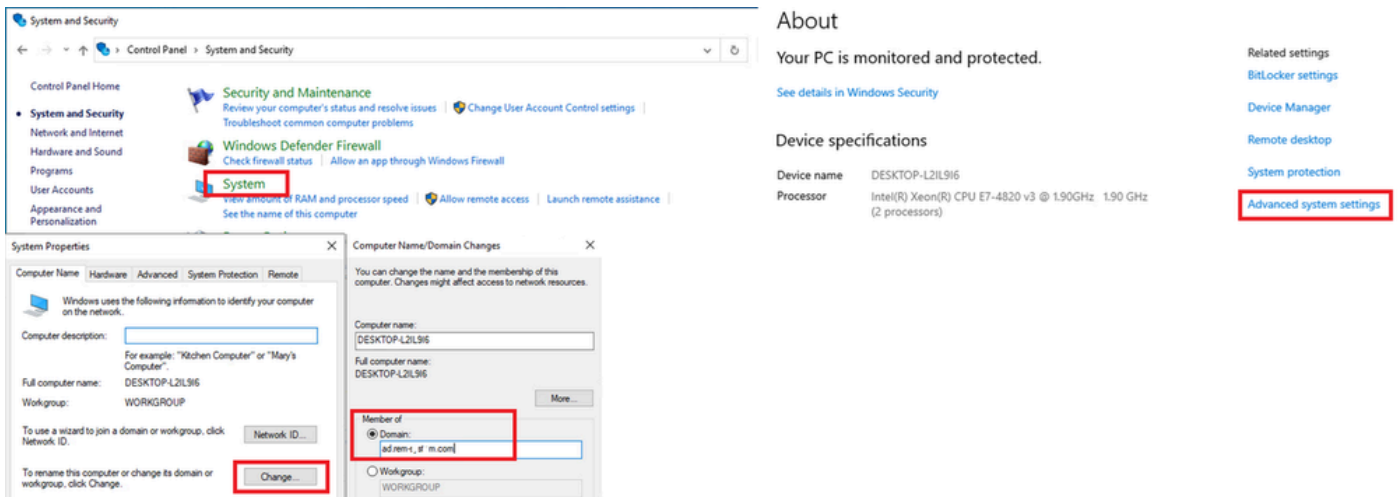
interface GigabitEthernet1/0/1
switchport access vlan 14
switchport mode access

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
```

Configuration in Windows PC

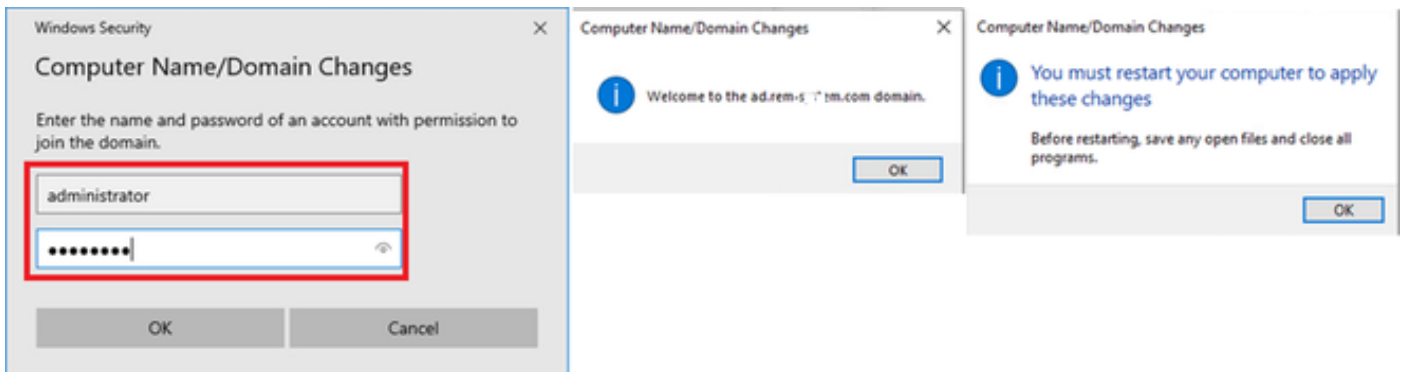
Step 1. Add PC to AD Domain

Navigate to **Control Panel > System and Security**, click **System**, and then click **Advanced system settings**. In System Properties window, click **Change**, select **Domain** and input the domain name.



Add PC to AD Domain

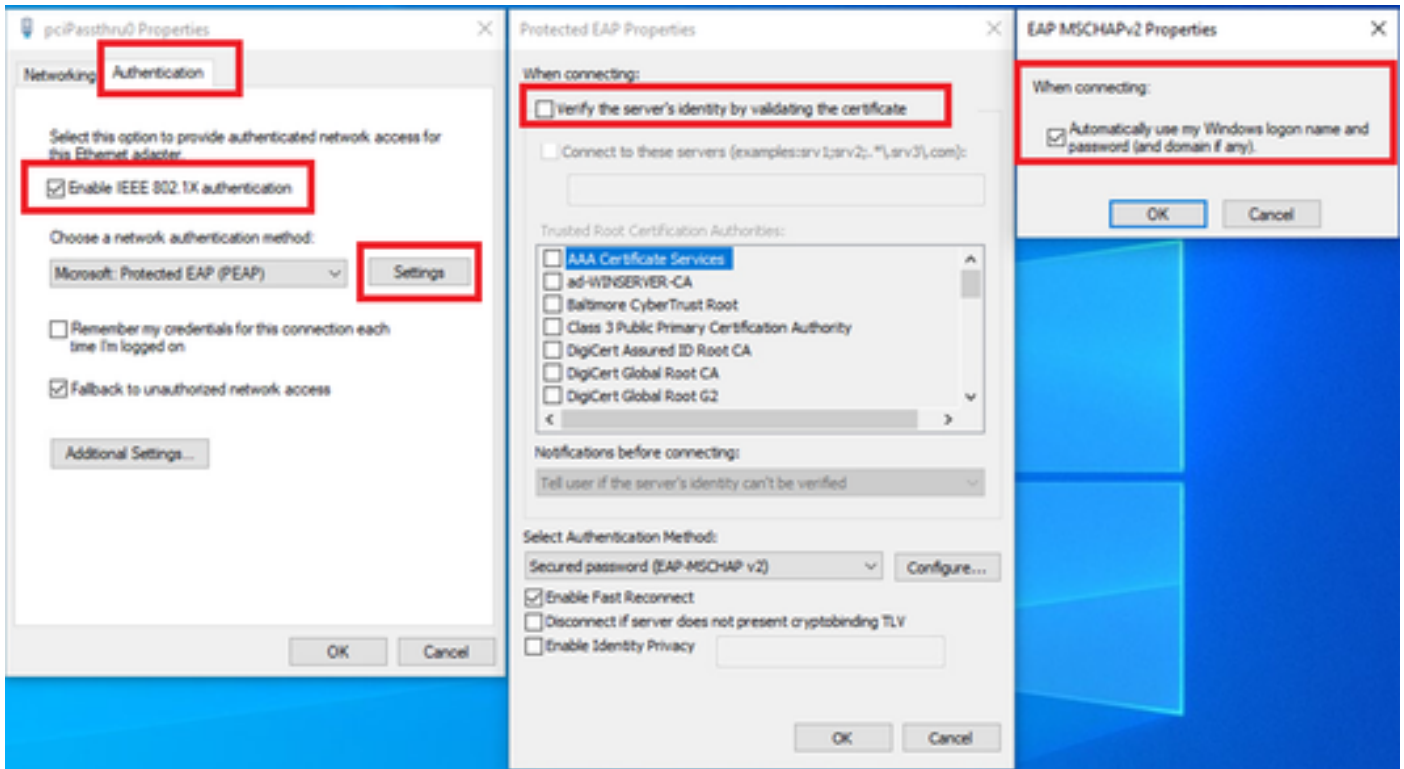
In Windows Security window, input username and password of domain server.



Input Username and Password

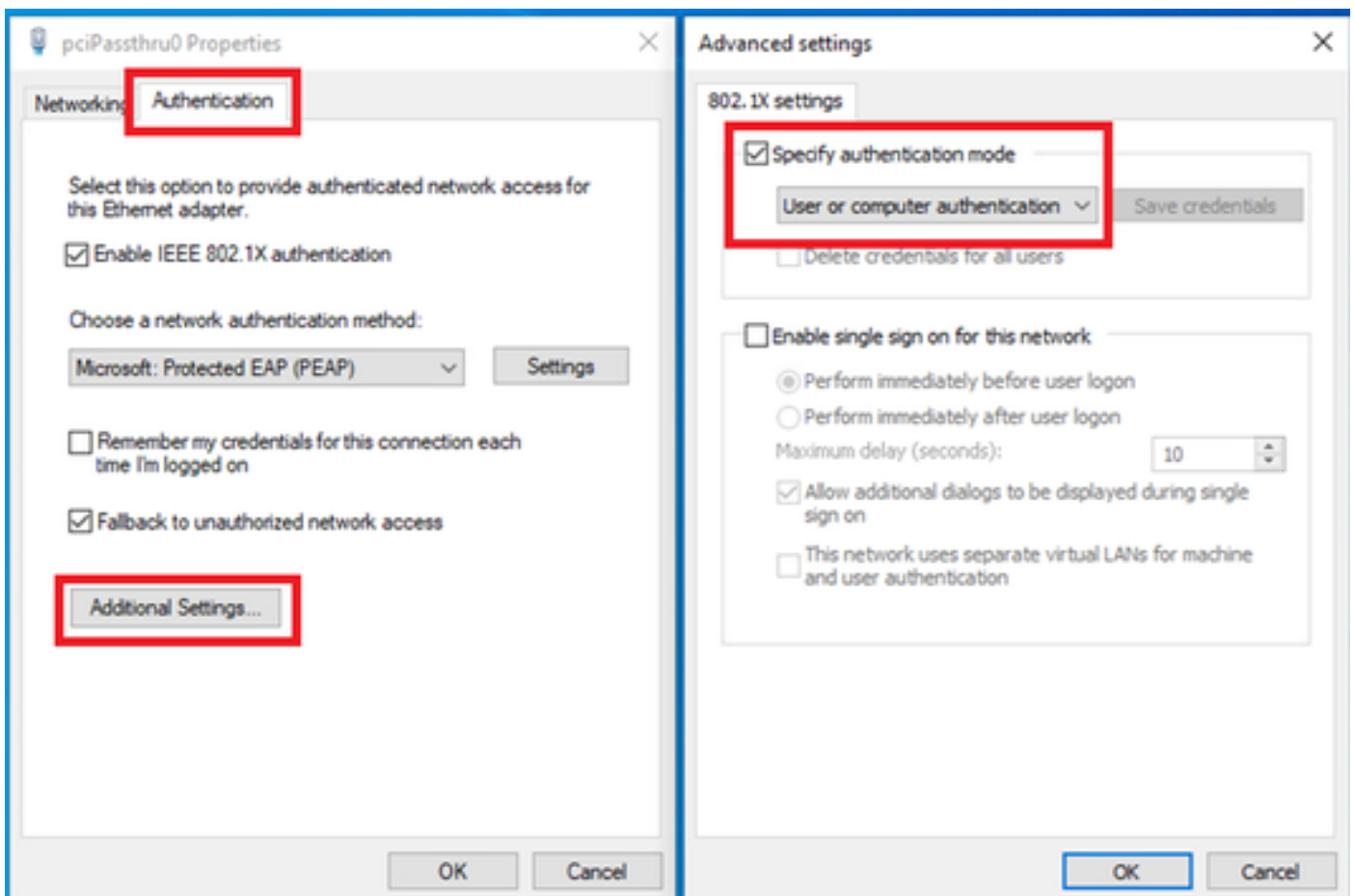
Step 2. Configure User Authentication

Navigate to **Authentication**, check **Enable IEEE 802.1X authentication**. Click **Settings** in Protected EAP Properties window, uncheck **Verify the server's identity by validating the certificate** and then click **Configure**. In EAP MSCHAPv2 Properties window, check **Automatically use my Windows logon name and password (and domain if any)** to use the username entered during the windows machine login for user authentication.



Enable User Authentication

Navigate to **Authentication**, check **Additional Settings**. Select **User or computer authentication** from drop-down list.

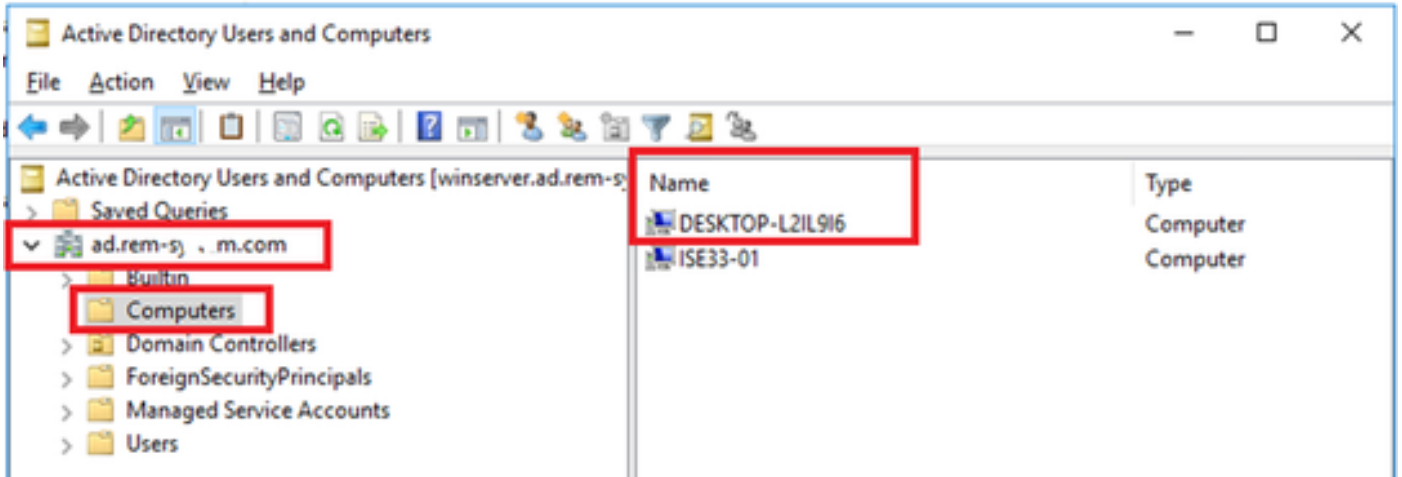


Specify Authentication Mode

Configuration in Windows Server

Step 1. Confirm Domain Computers

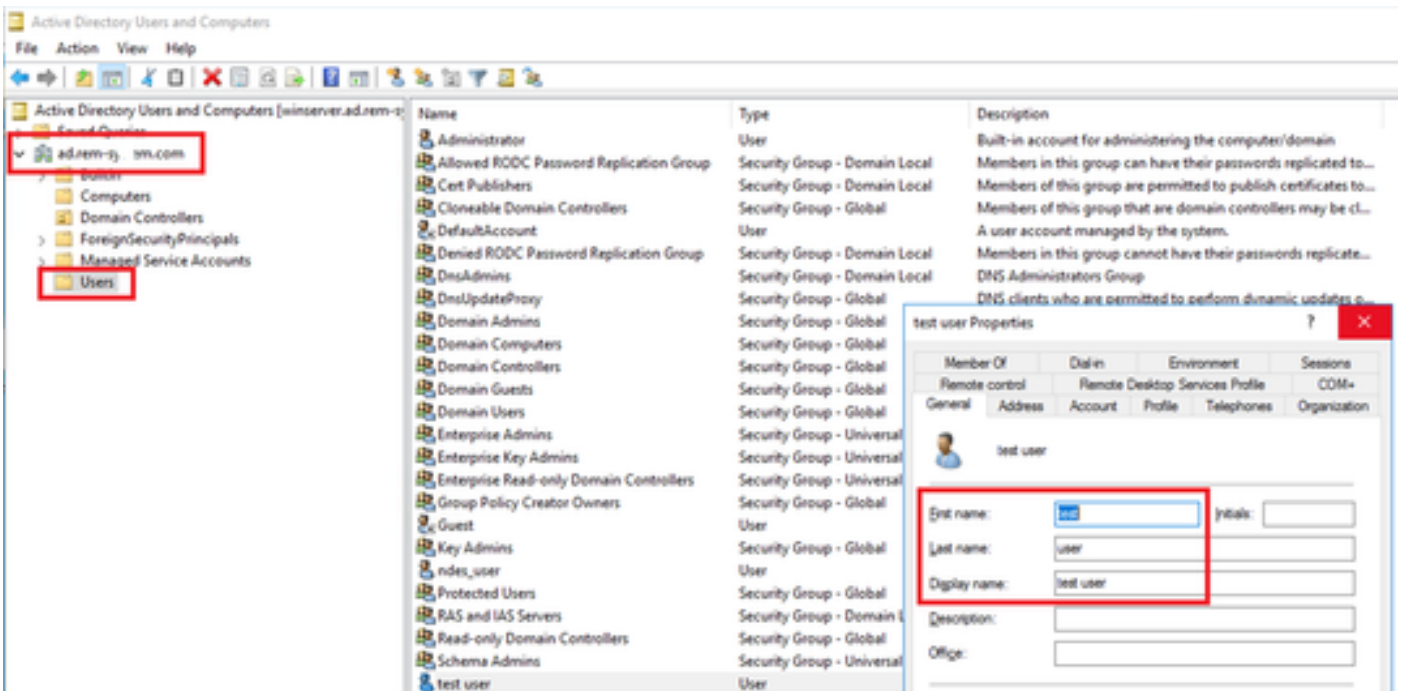
Navigate to **Active Directory Users and Computers**, click **Computers**. Confirm that Win10 PC1 is listed in the domain.



Confirm Domain Computer

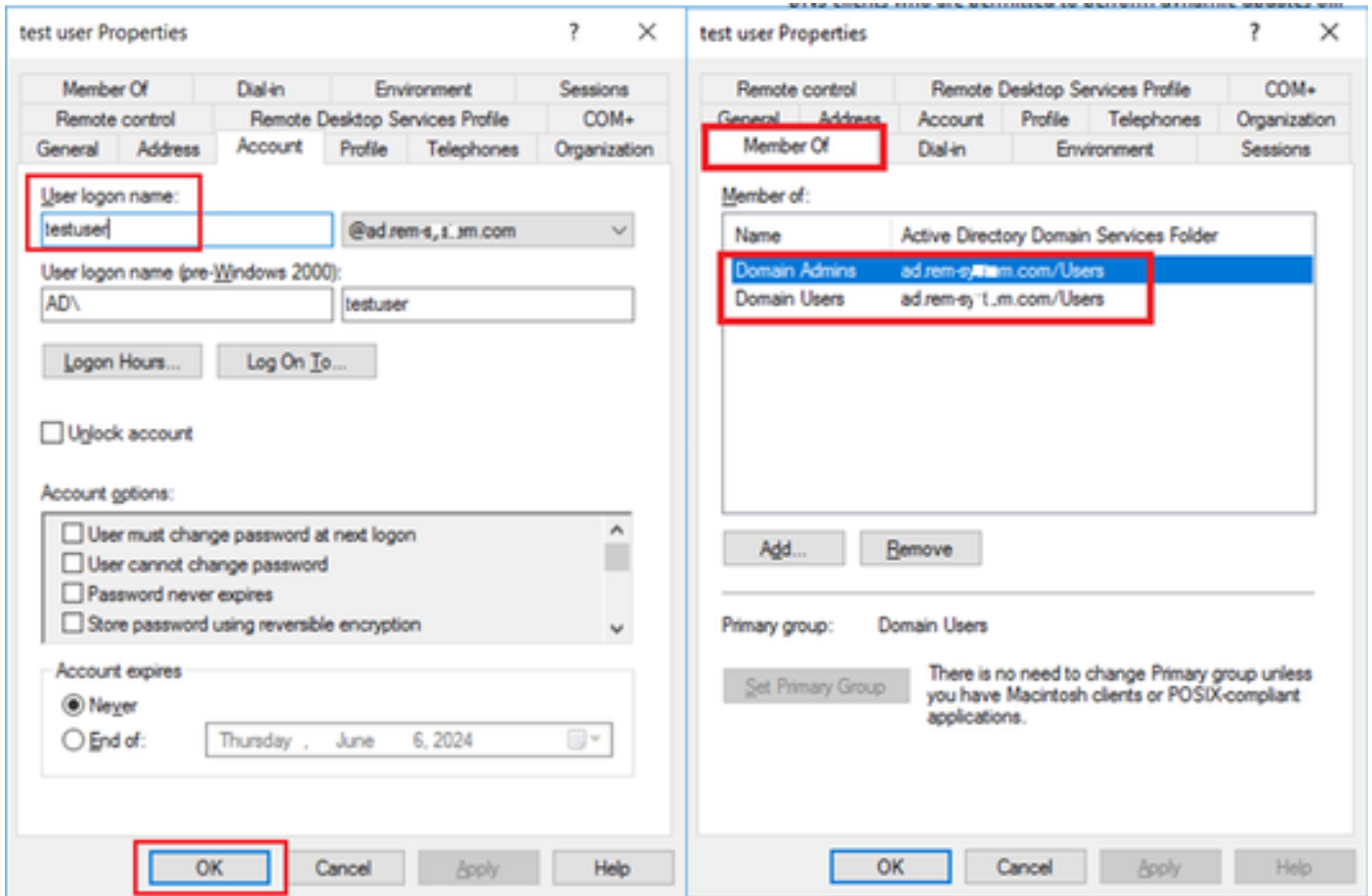
Step 2. Add Domain User

Navigate to **Active Directory Users and Computers**, click **Users**. Add testuser as domain user.



Add Domain User

Add the domain user to member of **Domain Admins** and **Domain Users**.

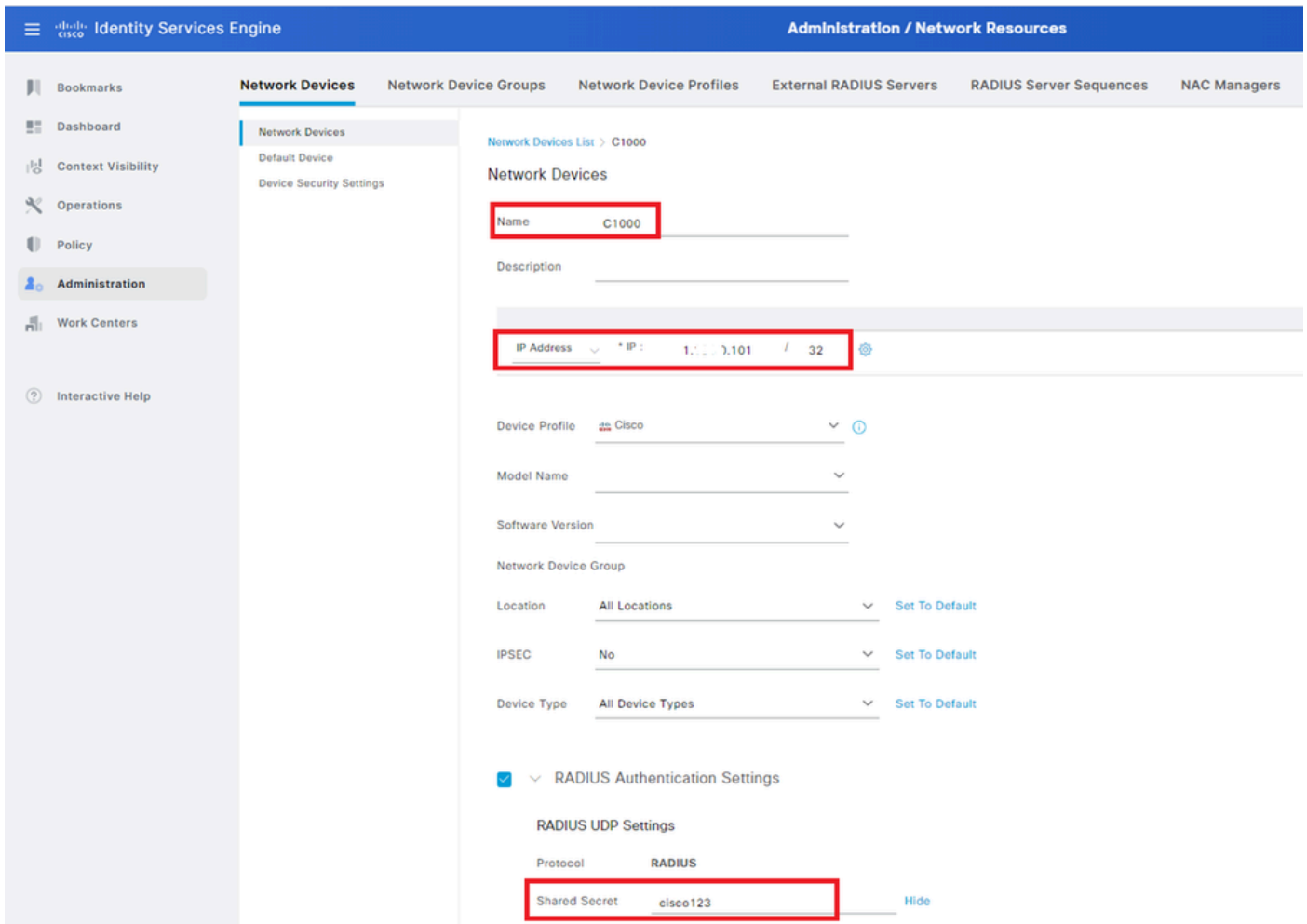


Domain Admins and Domain Users

Configuration in ISE

Step 1. Add Device

Navigate to **Administration > Network Devices**, click **Add** button to add C1000 device.

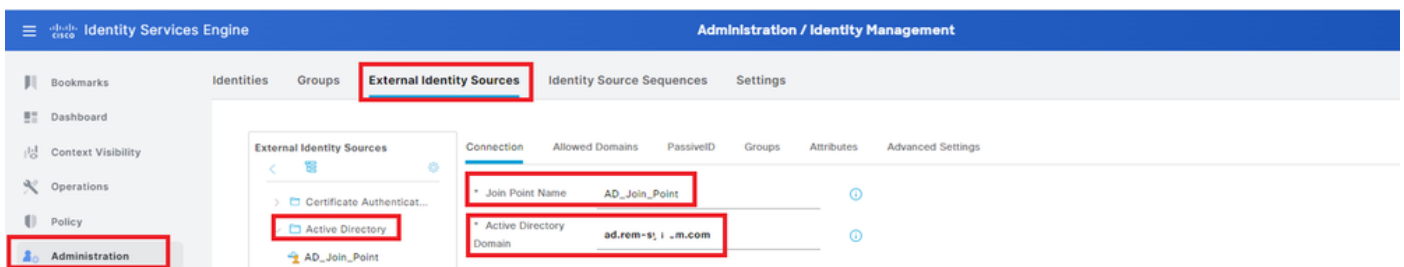


Add Device

Step 2. Add Active Directory

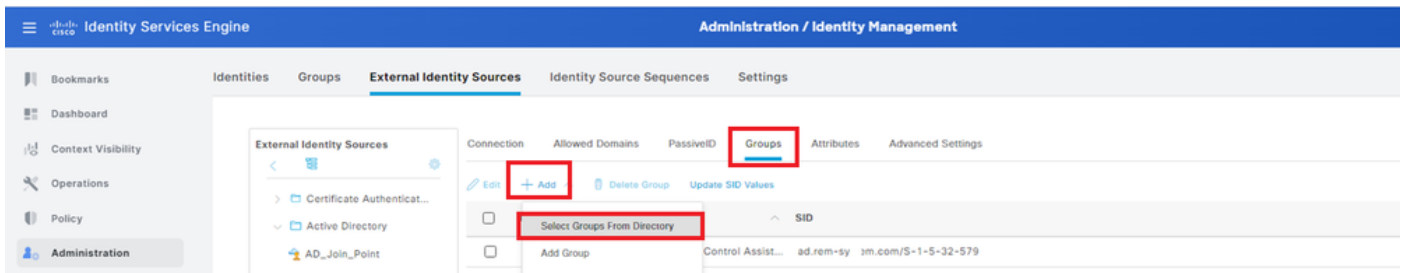
Navigate to **Administration > External Identity Sources > Active Directory**, click **Connection** tab, add Active Directory to ISE.

- Join Point Name: AD_Join_Point
- Active Directory Domain: ad.rem-xxx.com



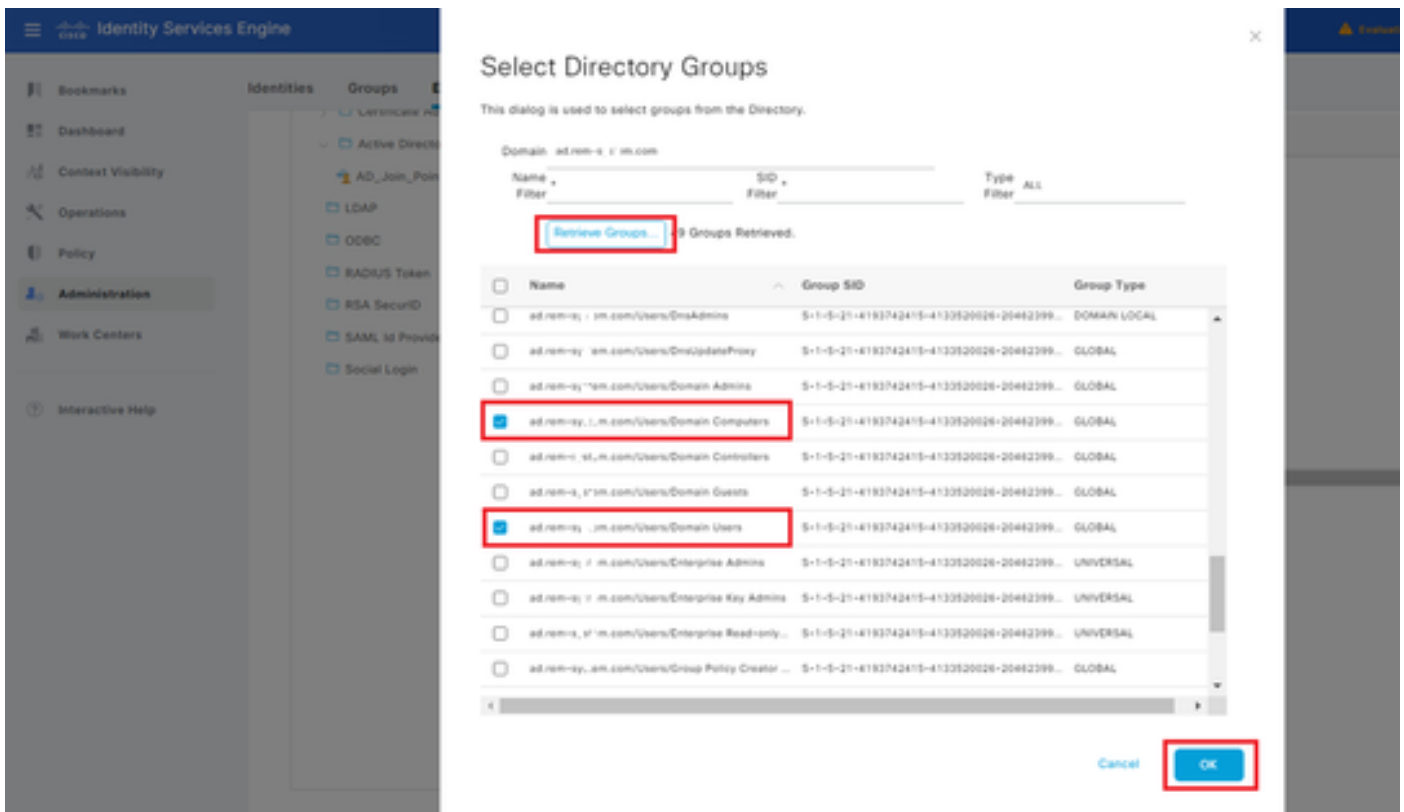
Add Active Directory

Navigate to **Groups** tab, select **Select Groups From Directory** from drop-down list.



Select Groups from Directory

Click **Retrieve Groups** from drop-down list. Check **ad.rem-xxx.com/Users/Domain Computers** and **ad.rem-xxx.com/Users/Domain Users** and click **OK**.



Add Domain Computers and Users

Step 3. Confirm Machine Authentication Setting

Navigate to **Advanced Settings** tab, confirm the setting of machine authentication.

- Enable Machine Authentication: To enable machine authentication
- Enable Machine Access Restriction: To combine user and machine authentication before authorization

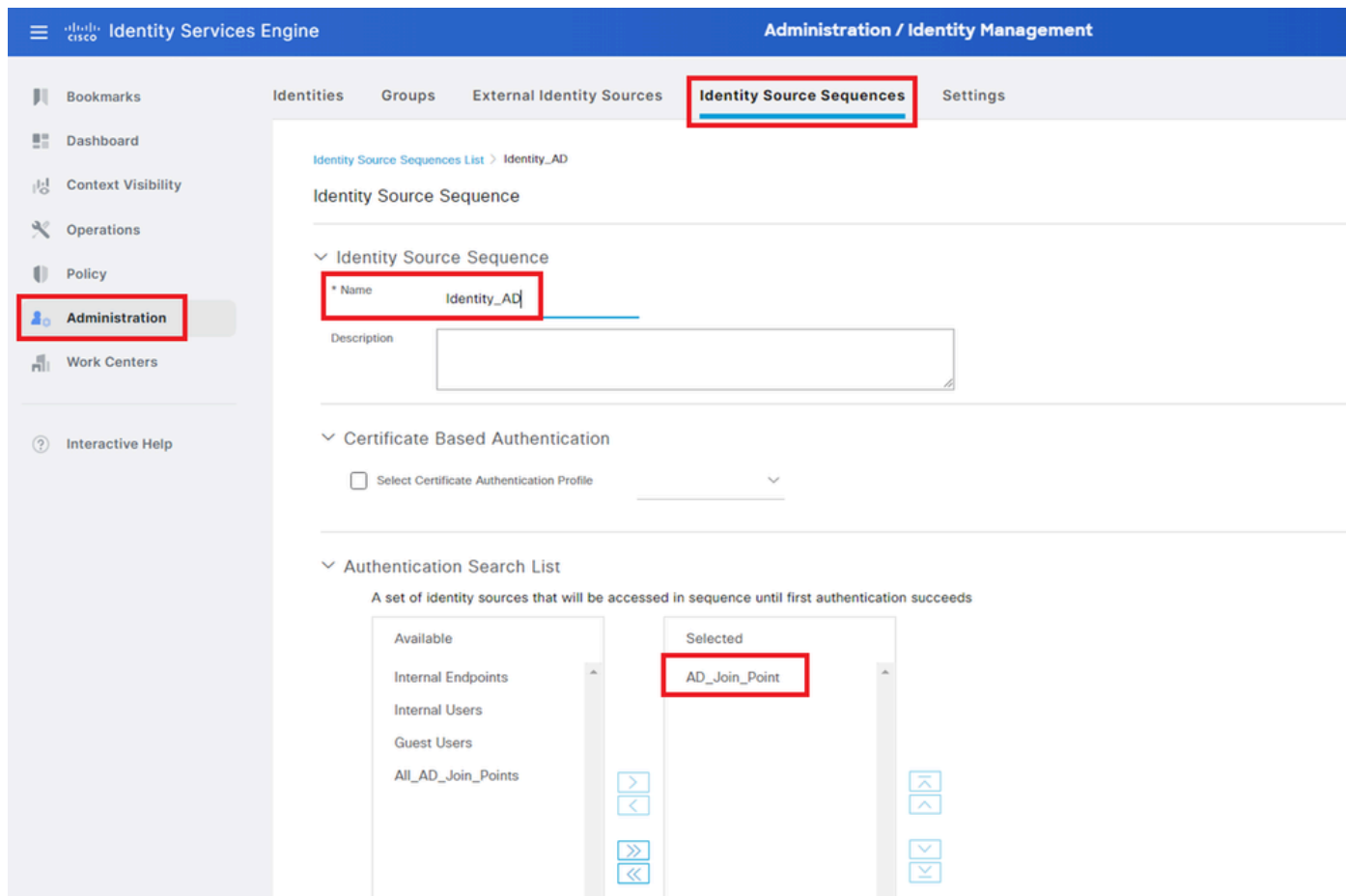
Note: Valid range of aging time is 1 to 8760.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The main navigation bar at the top indicates the current page is 'Administration / Identity Management'. Below this, a secondary navigation bar shows 'External Identity Sources' as the active section, with other options like 'Identities', 'Groups', 'Identity Source Sequences', and 'Settings'. On the left, a sidebar menu lists various administrative functions, with 'Administration' highlighted. The main content area is divided into tabs: 'Connection', 'Allowed Domains', 'PassiveID', 'Groups', 'Attributes', and 'Advanced Settings', with the latter being selected and highlighted with a red box. Under the 'Advanced Authentication Settings' section, several options are listed: 'Enable Password Change' (checked), 'Enable Machine Authentication' (checked and highlighted with a red box), and 'Enable Machine Access Restrictions' (checked and highlighted with a red box). Below these, the 'Aging Time' is set to '5 hours' with a dropdown arrow. A note states: 'Machine Access Restrictions Cache will be replicated between PSN instances in each node group. To configure MAR Cache distribution groups: Administration > System > Deployment'. Other unchecked options include 'Enable dial-in check', 'Enable callback check for dial-in clients', and 'Use Kerberos for Plain Text Authentications'.

Step 4. Add Identity Source Sequences

Navigate to **Administration > Identity Source Sequences**, add an Identity Source Sequence.

- Name: Identity_AD
- Authentication Search List: AD_Join_Point

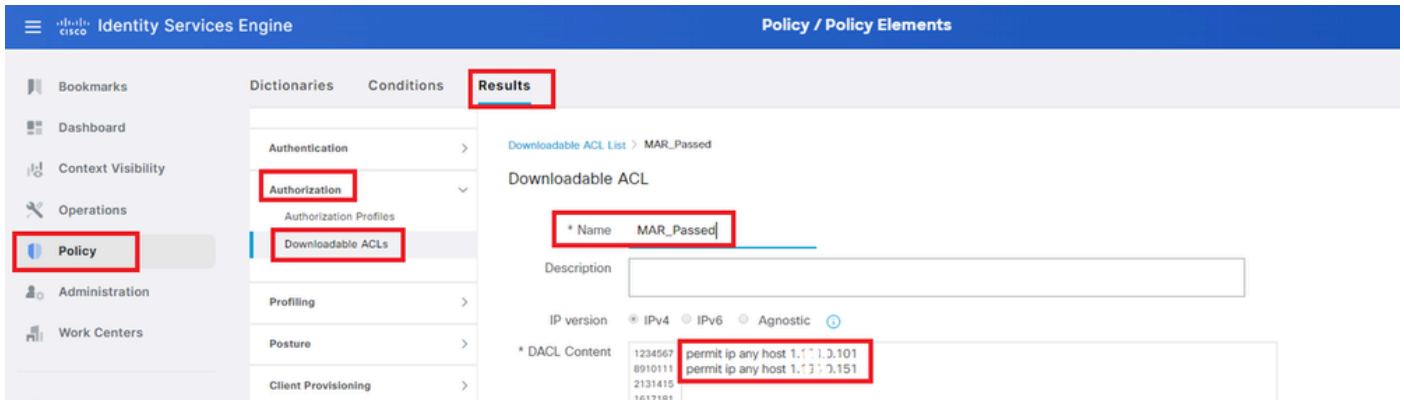


Add Identity Source Sequences

Step 5. Add DACL and Authorization Profile

Navigate to **Policy > Results > Authorization > Downloadable ACLs**, add a DACL.

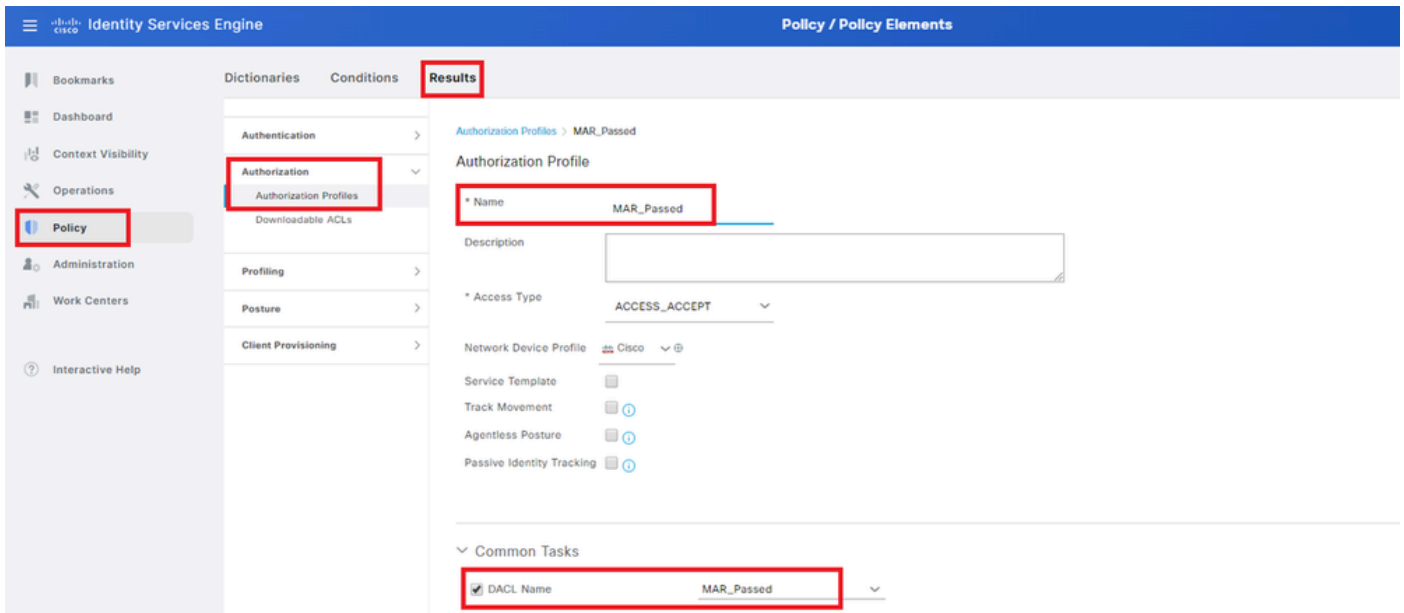
- Name: MAR_Passed
- DACL Content: permit ip any host 1.x.x.101 and permit ip any host 1.x.x.105



Add DACL

Navigate to **Policy > Results > Authorization > Authorization Profiles**, add a authorization profile.

- Name: MAR_Passed
- DACL Name: MAR_Passed

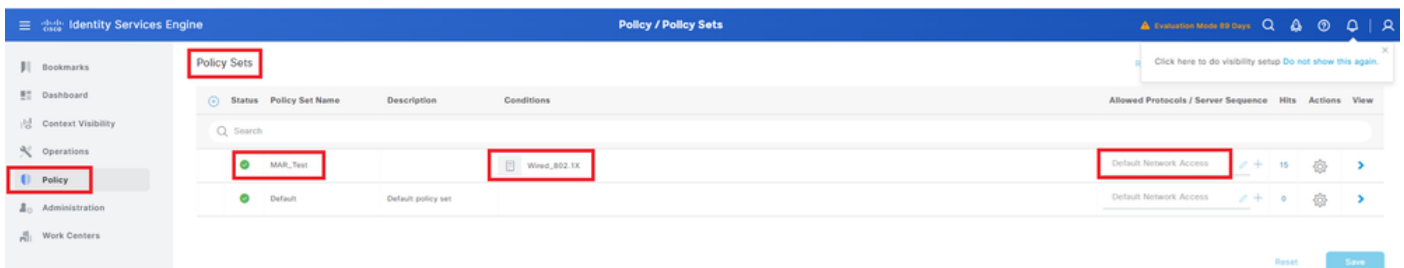


Add Authorization Profile

Step 6. Add Policy Set

Navigate to **Policy > Policy Sets**, click + to add a policy set.

- Policy Set Name: MAR_Test
- Conditions: Wired_802.1X
- Allowed Protocols / Server Sequence: Default Network Access

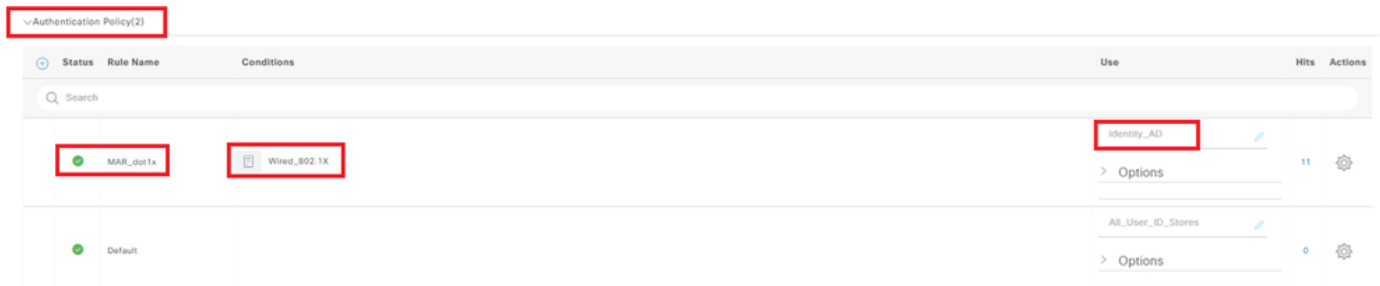


Add Policy Set

Step 7. Add Authentication Policy

Navigate to **Policy Sets**, click **MAR_Test** to add an authentication policy.

- Rule Name: MAR_dot1x
- Conditions: Wired_802.1X
- Use: Identity_AD



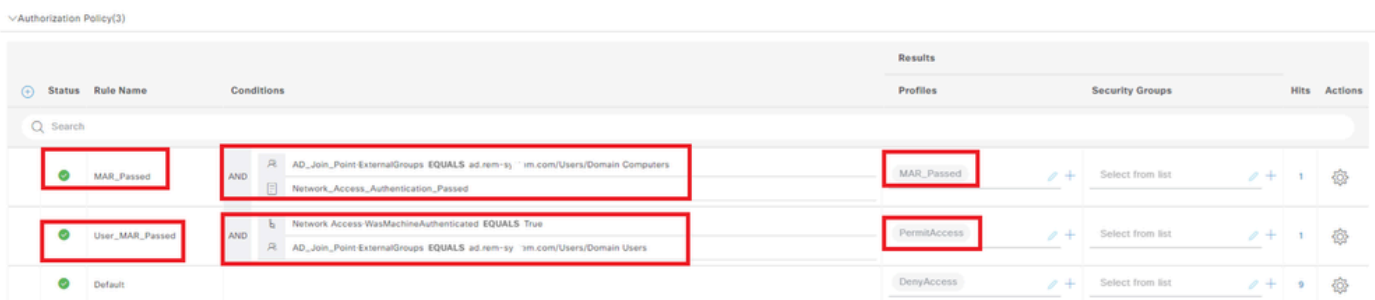
Add Authentication Policy

Step 8. Add Authorization Policy

Navigate to **Policy Sets**, click **MAR_Test** to add an authorization policy.

- Rule Name: MAR_Passed
- Conditions: AD_Join_Point·ExternalGroups **EQUALS** ad.rem-xxx.com/Users/Domain Computers **AND** Network_Access_Authentication_Passed
- Results: MAR_Passed

- Rule Name: User_MAR_Passed
- Conditions: Network_Access·WasMachineAuthenticated **EQUALS** True **AND** AD_Join_Point·ExternalGroups **EQUALS** ad.rem-xxx.com/Users/Domain Users
- Results: PermitAccess



Add Authorization policy

Verify

Pattern 1. Machine Authentication and User Authentication

Step 1. Sign Out of Windows PC

Click **Sign out** button from Win10 PC1 to trigger machine authentication.

 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)

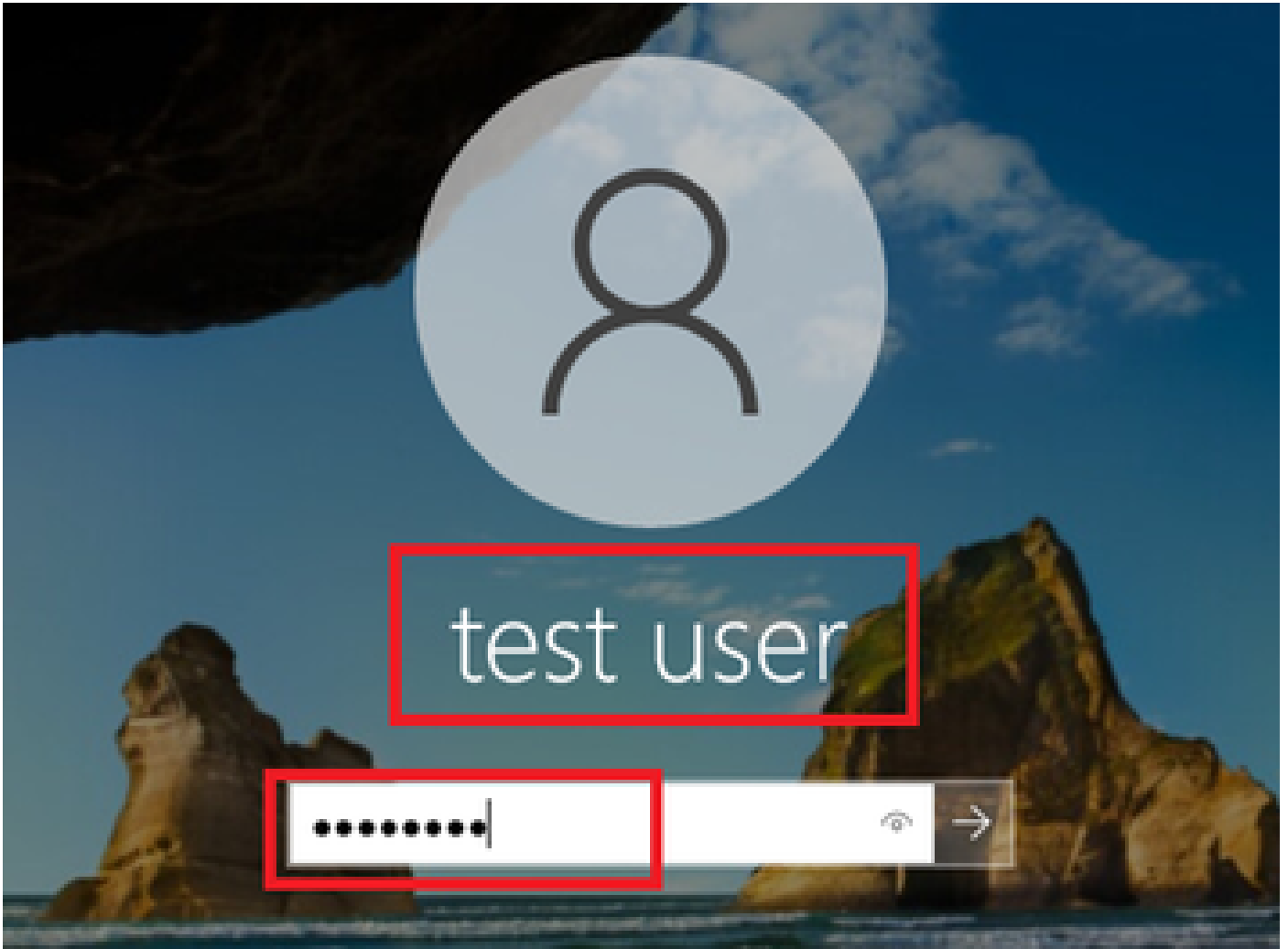
Server Policies:
ACS ACL: xACSACLx-IP-MAR_Passed-6639ba20

Method status list:
Method State

dot1x Authc Success

Step 3. Login Windows PC

Login Win10 PC1, input username and password to trigger user authentication.



Login Windows PC

Step 4. Confirm Authentication Session

Run `show authentication sessions interface GigabitEthernet1/0/2 details` command to confirm user authentication session 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

Step 5. Confirm Radius Live Log

Navigate to **Operations > RADIUS > Live Logs** in ISE GUI, confirm the live log for machine authentication and user authentication.

The screenshot shows the ISE GUI interface for RADIUS Live Logs. The left sidebar has 'Live Logs' and 'Operations' highlighted. The main area shows a table of log entries. Three entries are highlighted with red boxes:

Time	Status	Details	Repeats	Identity	Endpoint ID	Endpoint IP	Authentication Policy	Authorization Policy	Authorization Profile	IP Address	Network Device
May 07, 2024 04:36:14...	Success		0	AD/tesuser	84.96.91.15.84...	Intel-Dev...	MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed	PermitAccess	1.1.1.3.9	C1000
May 07, 2024 04:35:12...	Success			HSSO\DESKTOP-L2L96.ad.net	84.96.91.15.84...	Intel-Dev...	MAR_Test >> MAR_dot1x	MAR_Test >> MAR_Passed	MAR_Passed	169.254.90.1...	C1000

Radius Live Log

Confirm the detailed live log of machine authentication.

Overview

Event	5200 Authentication succeeded
Username	host/DESKTOP-L2IL916.ad.rem-sy .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-L2IL916.ad.rem-sy .em.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	01C200650000049AA780D80
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

Detail of Machine Authentication

Confirm the detailed live log of user authentication.

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.x.x.9
Authentication Identity Store	AD_Join_Point
Identity Group	Profiled
Audit Session Id	01C200650000049AA780D80
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 .am.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

Detail of User Authentication

Pattern 2. User Authentication Only

Step 1. Disable and Enable NIC of Windows PC

In order to trigger user authentication, disable and enable the NIC of Win10 PC1.

Step 2. Confirm Authentication Session

Run `show authentication sessions interface GigabitEthernet1/0/2 details` command to confirm user authentication session 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

Step 3. Confirm Radius Live Log

Navigate to **Operations > RADIUS > Live Logs** in ISE GUI, confirm the live log for user authentication.

Note: Because the MAR cache is stored in ISE, only user authentication is needed.

The screenshot shows the Identity Services Engine (ISE) Operations / RADIUS Live Logs interface. The 'Live Logs' tab is selected, and the 'Operations' menu item is highlighted. The interface displays several summary cards for metrics like Misconfigured Supplicants, Misconfigured Network Devices, RADIUS Drops, Client Stopped Responding, and Repeat Counter, all showing zero. Below these is a table of log entries with columns for Time, Status, Details, Repeats, Identity, Endpoint ID, Endpoint P., Authentication Policy, Authorization Policy, Authorization P., IP Address, and Network De... The following table represents the data shown in the screenshot:

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint P.	Authentication Policy	Authorization Policy	Authorization P...	IP Address	Network De...
May 07, 2024 04:42:05...	Success		0	AD\testuser	84-96-91:15:84...	Intel-Devi...	MAR_Test => MAR_dotx	MAR_Test => User_MAR_Passed	PermiAccess	1.1	1.9
May 07, 2024 04:42:04...	Success			AD\testuser	84-96-91:15:84...	Intel-Devi...	MAR_Test => MAR_dotx	MAR_Test => User_MAR_Passed	PermiAccess	1.1	3.9
May 07, 2024 04:36:13...	Success			AD\testuser	84-96-91:15:84...	Intel-Devi...	MAR_Test => MAR_dotx	MAR_Test => User_MAR_Passed	PermiAccess	1.1	3.9
May 07, 2024 04:35:12...	Success			WACSACL#-IP-MAR_Passed-6639ba20							C1000
May 07, 2024 04:35:12...	Success			host/DESKTOP-L2696.ad.rem-v...sm...	84-96-91:15:84...	Intel-Devi...	MAR_Test => MAR_dotx	MAR_Test => MAR_Passed	MAR_Passed	169.254.90.1...	C1000

Radius Live Log

Confirm the detailed live log of user authentication.

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	1.1.1.9
Authentication Identity Store	AD_Join_Point
Identity Group	Profiled
Audit Session Id	01C200650000049AA780D80
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	C1000
CiscoAVPair	service-type=Framed, audit-session-id=01C200650000049AA780D80, method=dot1x, AuthenticationIdentityStore=AD_Join_Point, FQSubjectName=2ce19620-0842-11ef-a5ec-362cec4b4f3d@testuser@ad.rem-sys.com, UniqueSubjectID=9273f674e52338d8f4807c495e1ff4c2ef9217f9
AD-Groups-Names	ad.rem-sys.com/Builtin/Users
AD-Groups-Names	ad.rem-sys.com/Builtin/Administrators
AD-Groups-Names	ad.rem-sys.com/Users/Denied RODC Password Replication Group
AD-Groups-Names	ad.rem-sys.com/Users/Domain Admins
AD-Groups-Names	ad.rem-sys.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-sys.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

Detail of User Authentication

Troubleshoot

These debug logs (prrt-server.log) help you to confirm the detailed behavior of authentication in ISE.

- runtime-config
- runtime-logging
- runtime-AAA

This is an example of the debug log for **Pattern 1. Machine Authentication and User Authentication** in this document.

<#root>

// machine authentication

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

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,CPMSessionID=

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 and

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

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

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

// user authentication

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

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,CPMSessionID=

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

Related Information

[Machine Access Restriction Pros and Cons](#)