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.

System and Security	About	
← 🗁 × ↑ 💊 > Control Panel > System and Security	 Your PC is monitored and protected. 	lelated settings
Control Panel Home Security and Maintenance	B See details in Windows Security	htLocker settings
System and Security Review your computer's status and resolve issues Orange User Account Control settings Troubleshoot common computer problems	D	Jevice Manager
Network and Internet Hardware and Sound Windows Defender Firewall	Device specifications R	lemote desktop
Programs Allow an app through Windows Firewall	Device name DESKTOP-L2IL916 S	ystem protection
User Accounts	Processor Intel(R) Xeon(R) CPU E7-4820 v3 © 1.90GHz 1.90 GHz (2 processors)	Advanced system settings
System Properties X Computer Name / Names/Domain Changes X Computer Name / Names/Domain Changes X Computer Name / Names/Domain Changes X Windows uses the following information to deterfy your computer on the network. Names/Domain Changes X Computer description:		

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.

pciPassthru0 Properties ×	Protected EAP Properties ×	EAP MSCHAPv2 Properties X
Networking Authentication	When connecting: Uverify the server's identity by validating the certificate	When connecting:
Select this option to provide authenticated network access for this Ethemet adapter	Connect to these servers (examples:srv1;srv2;-*srv3com):	password (and domain if any).
C Enable IEEE 802 1X authentication	Trusted Boot Certification Activation:	OK Cancel
Choose a network authentication method: Microsoft: Protected EAP (PEAP) Settings	AAA Certificate Services ad-WINSERVER-CA	
Pemember my credentials for this connection each time I'm logged on Fallback to unauthorized network access	Baltmore Cyber Trust Root Class 3 Public Primary Certification Authority DigiCert Assured ID Root CA DigiCert Global Root CA DigiCert Global Root G2	
Additional Settings	Notifications before connecting:	
	Tell user if the server's identity can't be verified	
	Select Authentication Method:	
	Congure Congure Congure Congure Congure Osconnect if server does not present cryptabinding TLV	
OK Cancel	Enable Identity Privacy	
	OK Cancel	

Enable User Authentication

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

pciPassthru0 Properties	< Advanced settings	<
Networking Authentication Select this option to provide authenticated network access for this Ethemet adapter. Image: Choose a network authentication Choose a network authentication method: Image: Choose a network authentication method:	802.1X settings Specify authentication mode User or computer authentication Delete credentials for all users Delete credentials for all users Brable 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	OK Cancel	

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.





Step 2. Add Domain User

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

Active Directory Users and Computers File Action View Help						
💠 🔶 🙍 📷 🔏 🖬 🗶 🖬 🖉 📰 💲	🍬 (a) 🐨 📴 🔌					
Active Directory Users and Computers [winserver.ad.rem-rg Active Directory Users and Computers [winserver.ad.rem-rg Active Directory Users Computers Domain Controllers Domain Controllers Managed Service Accounts Users	Administrator Administrator Allowed RODC Password Replication Group Cloneable Domain Controllers DefaultAccount DenulpdateProxy Domain Computers Domain Computers Domain Computers Domain Computers Domain Controllers Domain Users Enterprise Read-only Domain Controllers Goup Policy Creator Owners Guest Key Admins Reference Result R	Type User Security Group - Domain Local Security Group - Domain Local Security Group - Global User Security Group - Domain Local Security Group - Global Security Group - Global User Security Group - Global User Security Group - Global User Security Group - Global User Security Group - Global Security Group - Global	Description Built-in acco Members in Members of A user acco Members in DNS clients user Properties Member Of Penote control neral Address trane: at name: aplay name: ecorption: fige:	unt for administering to this group can have the this group are permitte this group that are don unt managed by the syst this group cannot have strators Group who are permitted to per- permitted to per- permitt	he computer/ ir passwords o d to publish o nain controller term. their passwor ofform dunam ormert rose Profile Telephones	formain eplicated to entificates to s may be cl ds replicate ic updates o ? X Sessions COM+ Organization
	🔏 test user	User				

Add Domain User

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

a oper risperves				· ^	test user Properties				?	
Member Of	Dial-in	Enviro	onment	Sessions	Remote control	Remote	Desktop Se	ervices Profile	CO	M+
Remote control	Remote 0	esktop Sen	vices Profile	COM+	General Address	Account	Profile	Telephones	Organi	zatio
Seneral Address	Account	Profile	Telephones	Organization	Member Of	Dial-in	Env	ironment	Sessio	ns
lser logon name:					Member of:					
lestuser		@ad.rem	4,1.3m.com	\sim	Name	Active Direct	tory Domain	Services Folder	r	
lser logon name (pre	Windows 200	0):			Domain Admins	ad rem-syllin	m.com/Use	975		
AD\		testuser			Domain Users	ad.rem-sy-1.	m.com/Use	ers		
Uplock account		t and leave								
Uglock account coount gotions:	ge password a ange password r expires using reversibl	t next logon I	1	~	Add E Primary group: Do	jemove omain Users				
Uglock account ccount gotions: User must chan User cannot ch Password neve Store password Account expires Never End of:	ge password a ange password r expires using reversibl Thursday ,	t next logon t e encryption June 6	s, 2024	•	Add E Primary group: Do Set Primary Group	emove omain Users There is r you have applicatio	no need to Macintosh ons.	change Primary . clients or POSD	group unk K-compilar	ess

Domain Admins and Domain Users

Configuration in ISE

Step 1. Add Device

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

equences NAC Managers

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

≡	dentity Services	Engine Administration / Identity Management
н	Bookmarks	Identities Groups External Identity Sources Identity Source Sequences Settings
- 22	Dashboard	
1d	Context Visibility	External Identity Sources Connection Allowed Domains PassiveID Groups Attributes Advanced Settings
*	Operations	Certificate Authenticat Join Point Name AD_Join_Point
0	Policy	Active Directory ad.rem-s; i .m.com
20	Administration	AD_Join_Point

Add Active Directory

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

≡	dentity Services I	Engine Administration / Identity Management
Щ	Bookmarks	Identities Groups External Identity Sources Identity Source Sequences Settings
- 22	Dashboard	
0 ¹	Context Visibility	External Identity Sources Connection Allowed Domains PassiveID Groups Attributes Advanced Settings
×	Operations	Certificate Authenticat.
0	Policy	Select Groups From Directory
80	Administration	Add Group Control Assist ad.rem-sy 3m.com/S-1-5-32-579

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**.

≡	then the services	Engine		×	A. 100
н	Bookmarks	Identities Groups E	Select Directory Groups		
51	Dashboard	C Carterione Al	This dialog is used to select groups from the Directory.		
N	Context Visibility	1 AD_Join_Poin	Name SID Type ALL		
×	Operations	C LOAP	Berline Crours	_	
0	Policy	C RADIUS Trace			
2.	Administration	C RSA Securit	Name Group SID Group Ty	pe .	
2	Work Centers	SAME to Provide	adverse in contraction and a set of the set	· ·	
		🗅 Social Legin	ad ven-ay "en.com/Genuit Admine 5-1-5-21-4113/M2415-4133120024-20412299. GLOBAL	_	
	Interactive Help		ad nem-sy. 1, m. com/Users/Domain Computers 5-1-5-21-4193742415-4133520128-20442398. GLOBAL		
			at rem-1 st., m.com/Course/Domain Controllers 5-1-6-21-4132/92415-4133320028-20482398 GLOBAL		
			adven-4, 1191.2007/Jacob Domain Guess 5-1-5-21-4193742415-4133520126-20482399. 6L084L		
			ad.rem-ajm.com/Uwes/Domain Users 8+1-5-21-4193742415-4133920028-20442398GL0844		
			ativen-s) / m.com/coursi@respise.Aprills 5-1-6-21-4132192415-413322028-20482398 UNVDRSk		
			ad.rem-aj 1 m.com/Users/Energine Kay Admins 5-1-5-21-6110742415-4130520128-20482209 UNVDRSAL		
			ad.rem-s, v1:m.com/Shers/Enterprise Read-only	- 1	
			at remark, and conformations Printy County 5-1-5-21-41121N2415-4112122028-20482298 6L0844		
			Cance	ox	



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.



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

≡	diade Identity Services	Engine Administration / Identity Management
Щ	Bookmarks	Identities Groups External Identity Sources Identity Source Sequences Settings
53	Dashboard	Identity Source Sequences List > Identity AD
15	Context Visibility	Identity Source Sequence
×	Operations	
U	Policy	Identity Source Sequence Name
20	Administration	Identity_AD
ri-	Work Centers	Description
?	Interactive Help	Certificate Based Authentication Select Certificate Authentication Profile
		 Authentication Search List A set of identity sources that will be accessed in sequence until first authentication succeeds
		Available Selected
		Internal Endpoints AD_Join_Point
		Internal Users
		All_AD_Join_Points

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

≡	dentity Services E	Engine	Policy / Policy Elements	
Щ	Bookmarks	Dictionaries Conditions	tesults	
	Dashboard	Authentication >	Downloadable ACL List > MAR_Passed	
ь	Context Visibility	Authorization	Downloadable ACL	
- %	Operations	Authorization Profiles	* Nama MAP Dassed	
0	Policy	Downloadable ACLs	Description	
a.	Administration	Profiling >		
nili.	Work Centers	Posture >	* DACL Content 1234567 permit ip any host 1.(1),0,101	
		Client Provisioning >	8010111 permit ip any host 1.13 2 0.151 2131415 1617181	

Add DACL

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

- Name: MAR_Passed
- DACL Name: MAR_Passed

≡	disco Identity Services I	Engine			Policy / Policy Elements
Щ	Bookmarks	Dictionaries Conditions	Re	esults	
51	Dashboard	Authentication	~	Authorization Profiles > MAR	Passed
망	Context Visibility	Authorization		Authorization Profile	
×	Operations	Authorization Profiles	Ť	* Name	HAD Devend
0	Policy	Downloadable ACLs		Description	mmrassu
80	Administration	Profiling	>		
nii:	Work Centers	Posture	>	* Access Type	ACCESS_ACCEPT ~
		Client Provisioning	>	Network Device Profile	± Cisco ∨ ⊕
?	Interactive Help			Service Template	0
				Track Movement	•
				Agentless Posture	0
				Passive Identity Tracking	
				✓ Common Tasks	
				DACL Name	MAR_Passed V

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

≡	dealer Identity Services Er	ngine	Policy / Policy Sets	🛦 Ensembler Marke 18 Says 🔍 🎝 🕥 🗛 🙊
н	Bookmarks	Policy Sets		Click here to do visibility setup Do not show this again.
23	Dashboard	Status Policy Set Name Descri	n Conditions	Allowed Protocols / Server Sequence Hits Actions View
10	Context Visibility	Q Search		
*	Operations	MAR_Test	Www.802.1X	Default Network Access 🥒 + 15 🛞 🗲
8.	Administration	O Default Default	ty set	Default Network Access 🥜 🕂 o 🚳 🗲
ก็เ	Work Centers			Read Save

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

Authe	ntication	n Policy(2)				
۲	Status	Rule Name	Conditions	Use	Hits	Actions
Q	Search					
	٢	MAR_dot1x	Wind_802.1X	Identity_AD //	11	ŵ
	•	Default		All_User_ID_Stores /	0	¢

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

VAuthorization Policy(3)					
		Results			
🕒 Status Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
Q Search					
MAR_Passed	AND R AD_Join_Point ExternalGroups EQUALS ad rem-sy ' I'm com/Users/Domain Computers AND R AD_Join_Point ExternalGroups EQUALS ad rem-sy ' I'm com/Users/Domain Computers Image: Second Se	MAR_Passed	+ Select from list / +	1	\$
User_MAR_Passed	AND AND AD_Join_PointExternalGroups EQUALS True AD_Join_PointExternalGroups EQUALS ad.rem-sy tim.com/Users/Domain Users	PermitAccess	+ Select from list	1	ŵ
Oefault		DenyAccess	+ Select from list / +	9	@

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.



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: 0x000003C 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: 01C200650000049AA780D80 Acct Session ID: 0x000003D 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.

≡	dentity Services E	Engine					Operations	RADIUS				A Evaluation Mode Cays	۵ ۵	
н	Bookmarks	Live Lo	gs Live Sessions											
53	Dashboard		-											
명	Context Visibility	M	sconfigured Supplicants 🔘			Mise	configured Network Devices		RADIUS Drops	• •	Client Stopped Respondi	ng 😳		Repeat Counter 🕕
*	Operations		0				0		0		0			0
0	Policy										Refres	h Show r v Latest 20 re	cords 🗸 I	Athin ast 3 hours 🗸
-	Work Centers	e	E Reser Repear Courtes	\oplus Export To \vee										Filter 🗸 🛛 🛛
			Time	Status	Details	Repea	Identity	Endpoint ID	Endpoint	Authentication Policy	Authorization Policy	Authorization P IP Ad	dress	Network De
(?)	Interactive Help		×	~			Identity	Endpoint ID	Endpoint Pr	Authentication Policy	Authorization Policy	Authorization Profi IP Ad	dress 🗸	Network Devic
			May 07, 2024 04:36:14	٠	0	0	ADitestuser	84:96:91:15:84:	Intel-Devi	$MAR_{-}Test \mapsto MAR_{-}dot1x$	$MAR_Test \mapsto User_MAR_Passed$	PermitAccess 1.1	2.9	
			May 07, 2024 04:36:13	•	0		ADitestuser	84.96.91.15.84	Intel-Devi	MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed	PermitAccess 1.1	0.9	C1000
			May 07, 2024 04:35:12	2	ò		#ACSACL#-IP-MAR_Passed-6639ba20							C1000
			May 07, 2024 04:35:12	۲	ò		host/DESKTOP-L2IL96.ad.rem-s_ithm	84:96:91:15:84:	Intel-Devi	$MAR_Test \Rightarrow MAR_dot1x$	MAR_Test >> MAR_Passed	MAR_Passed 169.2	54.90.1	C1000

Radius Live Log

Confirm the detailed live log of machine authentication.

Cisco ISE

Overview					
Event	5200 Authentication succeeded				
Username	host/DESKTOP-L2IL9I6.ad.rem-s_s_sm.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 rom.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)

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

Steps

Detail of Machine Authentication

Confirm the detailed live log of user authentication.

Cisco ISE

Overview		Steps		
Event	5200 Authentication succeeded	Step ID	Description	Latency (ms)
		11001	Received RADIUS Access-Request - AD_Join_Point	
Username	AD\testuser	11017	RADIUS created a new session - ad.rem-sy .em.com	0
Endpoint Id	B4:96:91:15:84:CB ⊕	15049	Evaluating Policy Group - AD_Join_Point	0
Endpoint Profile	Intel-Device	15008	Evaluating Service Selection Policy	1
		11507	Extracted EAP-Response/Identity	7
Authentication Policy	MAR_Test >> MAR_dot1x	12500	Prepared EAP-Request proposing EAP-TLS with challenge	0
Authorization Policy	MAR_Test >> User_MAR_Passed	12625	Valid EAP-Key-Name attribute received	0
Authorization Result	PermitAccess	11006	Returned RADIUS Access-Challenge	0
		11001	Received RADIUS Access-Request	8
		11018	RADIUS is re-using an existing session	0
Authentication Details		12301	Extracted EAP-Response/NAK requesting to use PEAP instead	0
Source Timestamp	2024-05-07 16:36:13,748	12300	Prepared EAP-Request proposing PEAP with challenge	1
		12625	Valid EAP-Key-Name attribute received	0
Received Timestamp	2024-05-07 16:36:13.748	11006	Returned RADIUS Access-Challenge	0
Policy Server	ise33-01	11001	Received RADIUS Access-Request	11
Event	5200 Authentication succeeded	11018	RADIUS is re-using an existing session	0
Username	AD\testuser	12302	Extracted EAP-Response containing PEAP challenge- response and accepting PEAP as negotiated	0
Endpoint Id	B4:96:91:15:84:CB	61025	Open secure connection with TLS peer	0
		12318	Successfully negotiated PEAP version 0	1
Calling Station Id	B4-96-91-15-84-CB	12800	Extracted first TLS record; TLS handshake started	0
Endpoint Profile	Intel-Device	12805	Extracted TLS ClientHello message	0
IPv4 Address	1.111 0.9	12806	Prepared TLS ServerHello message	0
		12807	Prepared TLS Certificate message	0
Authentication Identity Store	AD_Join_Point	12808	Prepared TLS ServerKeyExchange message	28
		12810	Prepared TLS ServerDone message	0
Identity Group	Profiled	12305	Prepared EAP-Request with another PEAP challenge	1
Audit Session Id	01C2006500000049AA780D80	11006	Returned RADIUS Access-Challenge	0
Authentication Method	dot1x	11001	Received RADIUS Access-Request	30
		11018	RADIUS is re-using an existing session	0
Autnentication Protocol	PEAP (EAP-MSCHAPv2)	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: 0x000003D 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.

≡ deale. Identity Services E	ingine			Operations	RADIUS			A traduction Made Carps Q	A () A
JI Bookmarks	Live Logs Live Sessions								
Dashboard									
10 Context Visibility	Misconfigured Supplicants		Mis	configured Network Devices		RADIUS Drops	Client Stopped Responding	10	Repeat Counter 🕕
× Operations	0			0		0	0		0
Policy							Refresh	Show	Within
▲ Administration							Never	Catest 20 records Q	Cast 3 hours Q
Work Centers	😂 🖆 Reser Repear Counts	₫ Export To ∨							Filter V 0
	Time	Status I	Details Repea	Identity	Endpoint ID	Endpoint Authentication Policy	Authorization Policy	Authorization P IP Address	Network De
(7) Interactive Help	×			Identity	Endpoint ID	Endpoint Pr Authentication Policy	Authorization Policy	Authorization Profi IP Address	V Network Devic
0	May 07, 2024 04:42:05	•	à °	AD/(testuser	84:96:91:15:84:	Intel-Devi MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed	PermitAccess 1.1.1.1.1.9	
	May 07, 2024 04:42:04	2	ē.	AD/pestuser	84:96:91:15:84:	Intel-Devi MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed	PermitAccess 1	C1000
	May 07, 2024 04:36:13	8	ů.	AD/pestuser	84:96:91:15:84:	Intel-Devi MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed	PermitAccess 1.1, 0.9	C1000
	May 07, 2024 04:35:12	•	à	#ACSACL#-IP-MAR_Passed-6639ba20					C1000
	May 07, 2024 04:35:12		à	host/DESKTOP-L2IL9I6.ad.rem-s 1.am	84:96:91:15:84:	Intel-Devi MAR_Test >> MAR_dot1x	MAR_Test >> MAR_Passed	MAR_Passed 169.254.90.1	C1000

Radius Live Log

Confirm the detailed live log of user authentication.

Cisco ISE

Overview		Steps		
Event	5200 Authentication succeeded	Step ID	Description	Latency (ms)
		11001	Received RADIUS Access-Request - AD_Join_Point	
Username	AD\testuser	11017	RADIUS created a new session - ad.rem-s_u.em.com	0
Endpoint Id	B4:96:91:15:84:CB ⊕	15049	Evaluating Policy Group - AD_Join_Point	1
Endpoint Profile	Intel-Device	15008	Evaluating Service Selection Policy	0
Authoritantian Dellass		11507	Extracted EAP-Response/Identity	16
Authentication Policy	MAR_lest >> MAR_dot1x	12500	Prepared EAP-Request proposing EAP-TLS with challenge	2
Authorization Policy	MAR_Test >> User_MAR_Passed	12625	Valid EAP-Key-Name attribute received	0
Authorization Result	PermitAccess	11006	Returned RADIUS Access-Challenge	0
		11001	Received RADIUS Access-Request	5
		11018	RADIUS is re-using an existing session	0
Authentication Details		12301	Extracted EAP-Response/NAK requesting to use PEAP instead	0
Source Timestamp	2024-05-07 16:42:04.467	12300	Prepared EAP-Request proposing PEAP with challenge	0
Received Timestamp	2024-05-07 16:42:04 467	12625	Valid EAP-Key-Name attribute received	0
Received Timestamp	2024-03-07 10:42:04:407	11006	Returned RADIUS Access-Challenge	0
Policy Server	ise33-01	11001	Received RADIUS Access-Request	25
Event	5200 Authentication succeeded	11018	RADIUS is re-using an existing session	0
Username	AD\testuser	12302	Extracted EAP-Response containing PEAP challenge- response and accepting PEAP as negotiated	1
Endpoint Id	B4:96:91:15:84:CB	61025	Open secure connection with TLS peer	0
Calling Station Id	B4-96-91-15-84-CB	12318	Successfully negotiated PEAP version 0	0
		12800	Extracted first TLS record; TLS handshake started	0
Endpoint Profile	Intel-Device	12805	Extracted TLS ClientHello message	0
IPv4 Address	1.1 . 0.9	12806	Prepared TLS Certificate message	0
Authentication Identity	AD Jain Daint	12809	Prepared TLS Certificate message	26
Store	AD_JOIN_FOIN	12810	Prepared TLS ServerDone message	0
Identity Group	Profiled	12305	Prepared EAP-Request with another PEAP challenge	0
Audit Session Id	01C2006500000049AA780D80	11006	Returned RADIUS Access-Challenge	0
		11001	Received RADIUS Access-Request	14
Authentication Method	dot1x	11018	RADIUS is re-using an existing session	0
Authentication Protocol	PEAP (EAP-MSCHAPv2)	12304	Extracted EAP-Response containing PEAP challenge- response	1
Service Type	Framed	12305	Prepared EAP-Request with another PEAP challenge	0
Network Device	C1000		ISE has confirmed previous successful machine	_
	service-type=Framed,	24422	authentication for user in Active Directory	0
	audit-session-id=01C2006500000049AA780D80, method=dot1x.	15036	Evaluating Authorization Policy	0
CiscoAVPair	AuthenticationIdentityStore=AD_Join_Point, FQSubjectName=2ce19620-0842-11ef-a5ec-	24209	Looking up Endpoint in Internal Endpoints IDStore - AD\testuser	1
	362cec4b4f3d#testuser@ad.rem-sy_te_1.com, UniqueSubjectID=9273f674e52338d8f4807c495e1ff4c2ef92	24211	Found Endpoint in Internal Endpoints IDStore	3
	17/9	24432	Looking up user in Active Directory - AD\testuser	
AD-Groups-Names	ad.rem-sy: :m.com/Builtin/Users	24355	LDAP fetch succeeded	
AD Crowns Names	ed som en Duilte (Adecisioner	24416	User's Groups retrieval from Active Directory succeeded	
AD-Groups-Names	ad.rem-sim.com/builun/Administrators	15048	Queried PIP - AD_Join_Point.ExternalGroups	11
AD-Groups-Names	ad.rem-synt: n.com/Users/Denied RODC Password Replication Group	15016	Selected Authorization Profile - PermitAccess	5
	rogenouries stronge	22081	Max sessions policy passed	0
AD-Groups-Names	ad.rem-spate.n.com/Users/Domain Admins	22080	New accounting session created in Session cache	0
AD-Groups-Names	ad.rem-synthem.com/Users/Domain Users	12306	PEAP authentication succeeded	0
		61026	Snutdown secure connection with TLS peer	
		11002	Returned RADIUS Access-Access	2
Result		11002	Returned RADIOS Access-Accept	

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,CPMSessionI

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,CPMSessionII

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

Related Information

Machine Access Restriction Pros and Cons