Konfigurieren der EAP-TLS-Authentifizierung mit OCSP in der ISE

Inhalt

Einleitung
<u>Voraussetzungen</u>
Anforderungen
Verwendete Komponenten
<u>Netzwerkdiagramm</u>
Hintergrundinformationen
Konfigurationen
Konfiguration in C1000
Konfiguration auf Windows-PCs
Schritt 1: Benutzerauthentifizierung konfigurieren
Schritt 2: Clientzertifikat bestätigen
Konfiguration in Windows Server
Schritt 1: Benutzer hinzufügen
Schritt 2: OCSP-Dienst bestätigen
Konfiguration in der ISE
Schritt 1: Gerät hinzufügen
Schritt 2: Active Directory hinzufügen
Schritt 3: Zertifikatauthentifizierungsprofil hinzufügen
Schritt 4: Identitätsquelltext hinzufügen
Schritt 5: Zertifikat in ISE bestätigen
Schritt 6: Zulässige Protokolle hinzufügen
Schritt 7. Policy Set hinzufügen
Schritt 8: Authentifizierungsrichtlinie hinzufügen
Schritt 9. Autorisierungsrichtlinie hinzufügen
Überprüfung
Schritt 1: Authentifizierungssitzung bestätigen
Schritt 2: RADIUS-Live-Protokoll bestätigen
Fehlerbehebung
1. Debug-Protokoll
2. TCP-Dump
Zugehörige Informationen

Einleitung

In diesem Dokument werden die erforderlichen Schritte zum Einrichten der EAP-TLS-Authentifizierung mit OCSP für Echtzeit-Clientzertifikatwiderrufsprüfungen beschrieben.

Voraussetzungen

Anforderungen

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

- Konfiguration der Cisco Identity Services Engine
- Konfiguration des Cisco Catalyst
- Online-Zertifikatstatusprotokoll

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Identity Services Engine Virtual 3.2 Patch 6
- C1000-48FP-4G-L 15,2(7)E9
- Windows Server 2016
- Windows 10

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.



Hintergrundinformationen

In EAP-TLS stellt ein Client dem Server sein digitales Zertifikat als Teil des Authentifizierungsprozesses dar. In diesem Dokument wird beschrieben, wie die ISE das Client-Zertifikat validiert, indem der Common Name (CN) des Zertifikats mit dem AD-Server abgeglichen wird und bestätigt wird, ob das Zertifikat mithilfe des OCSP (Online Certificate Status Protocol) widerrufen wurde, das den Echtzeit-Protokollstatus bereitstellt.

Der unter Windows Server 2016 konfigurierte Domänenname ist ad.rem-xxx.com. Dies wird in diesem Dokument als Beispiel verwendet.

Die in diesem Dokument erwähnten OCSP- (Online Certificate Status Protocol) und AD-Server (Active Directory) werden für die Zertifikatsvalidierung verwendet.

- · Active Directory-FQDN: winserver.ad.rem-xxx.com
- URL der Zertifikatsperrlisten-Verteilung: http://winserver.ad.rem-xxx.com/ocsp-ca.crl
- URL der Behörde: <u>http://winserver.ad.rem-xxx.com/ocsp</u>

Dies ist die Zertifikatskette mit dem allgemeinen Namen jedes im Dokument verwendeten Zertifikats.

- CA: ocsp-ca-common-name
- Client-Zertifikat: clientcertCN
- Serverzertifikat: ise32-01.ad.rem-xxx.com
- OCSP-Signaturzertifikat: ocspSignCommonName

Konfigurationen

Konfiguration in C1000

Dies ist die minimale Konfiguration in C1000 CLI.

aaa new-model radius server ISE32 address ipv4 1.x.x.181 key cisco123

aaa group server radius AAASERVER server name ISE32

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 Vlan12 ip address 192.168.10.254 255.255.255.0 interface Vlan14
ip address 1.x.x.101 255.0.0.0

interface GigabitEthernet1/0/1
Switch port access vlan 14
Switch port mode access

interface GigabitEthernet1/0/3
switchport access vlan 12
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: Benutzerauthentifizierung konfigurieren

Navigieren Sie zuAuthentication, aktivieren SieEnable IEEE 802.1X authentication, und wählen Sie Microsoft: Smart Card oder sonstiges Zertifikat aus.

Klicken Sie auf die Schaltfläche Einstellungen, aktivieren SieZertifikat auf diesem Computer verwenden, und wählen Sie die vertrauenswürdige Zertifizierungsstelle von Windows PC aus.

pciPassthru0 Properties	× Smart Card or other Certificate Properties ×
Networking Authentication Select this option to provide authenticated network access for this Ethemet adapter. Enable IEEE 802.1X authentication Choose a network authentication method:	When connecting: Use my gmart card Use a certificate on this computer Use simple certificate selection (Recommended) Verify the server's identity by validating the certificate Connect to these servers (examples:srv1;srv2;.*\srv3\.com):
Microsoft: Smart Card or other certificate Settings	Trusted Boot Certification Authorities:
	< >
	Don't grompt user to authorize new servers or trusted certification authorities.
OK Cance	Use a different user name for the connection

Navigieren Sie zuAuthentifizierung, und aktivieren SieZusätzliche Einstellungen. Wählen SieBenutzer- oder Computerauthentifizierung aus der Dropdown-Liste aus.

pciPassthru0 Properties ×	Advanced settings ×
Networking Authentication	802. 1X settings
Select this option to provide authenticated network access for this Ethemet adapter.	Specify authentication mode User or computer authentication Save credentials Delete credentials for all users
Choose a network authentication <u>m</u> ethod: Microsoft: Smart Card or other certificate \checkmark <u>Settings</u>	Enable single sign on for this network O Perform immediately before user logon Deform immediately before user logon
 <u>Remember my credentials for this connection each time I'm logged on</u> ✓ <u>Fallback to unauthorized network access</u> Additional Settings 	 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

Authentifizierungsmodus angeben

Schritt 2: Clientzertifikat bestätigen

Navigieren Sie zu Certificates - Current User > Personal > Certificates, und überprüfen Sie das Client-Zertifikat, das für die Authentifizierung verwendet wird.

Console1 - [Console Root\Certificates - Current U	Iser\Personal\Certificates]								– 🗆 X
File Action View Favorites Window He	lp								- 8 ×
◆ → 2 (() 4 %) 🗙 🗊 🕞 🖬 🗂								Ū.	
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te	Actions	
 Personal 	Clastcart CN	0/10-/3-/000000-03004	6/4/2025	Client Authentication	occountient	1		Certificates	-
Certificates		to contract the second			verp energ			More Actions	,
Certificates								clientcertCN	-
> 🛄 Enterprise Trust								More Actions	,

Clientzertifikat bestätigen

Doppelklicken Sie auf das Clientzertifikat, navigieren Sie zu Details, überprüfen Sie die Details zu Subject (Betreff), CRL Distribution Points (Zertifikatsperrlisten) und Authority Information Access (Zugriff auf Autoritätsinformationen).

- Betrifft: CN = clientcertCN
- CRL Distribution Points: <u>http://winserver.ad.rem-xxx.com/ocsp-ca.crl</u>

Zugriff auf Behördeninformationen: <u>http://winserver.ad.rem-xxx.com/ocsp</u>

Certificate		X 🔲 Certificate	×	Certificate	×
General Details Certification P	ath	General Details Certification Pa	th	General Details Certification Pat	ħ
Show: <all></all>	~	Show: <all></all>	~	Show: <all></all>	~
Field Subject Public key parameters Basic Constraints Subject Key Identifier Authority Key Identifier	Value Wednesday, June 4, 2025 7:4 dientcertCN RSA (2048 Bits) 05 00 Subject Type=End Entity, Pat d1 af 68 6c 3e b6 90 f4 c1 80 KeyID=43 0e c8 58 5c 99 2d 2 Vietable Second	Field	Value Client Authentication (1.3.6.1 [1]CRL Distribution Point: Distr 5 [1]Authority Info Access: Acc xca certificate sha1 62 46 9a 98 57 95 e8 30 39 a5 ocsp-client	Field Financed Key Usage CDL Distribution Doiste Authority Information Access Wire usage Comment Thumbprint algorithm Thumbprint Friendly name	Value Client Authentication (1.3.6.1 [1]Di Dictribution Delate Distr [1]Authority Info Access: Acc xua cer uncare sha 1 62 46 9a 98 57 95 e8 30 39 a5 ocsp-client
CN = dientcertCN	1	[1]CRL Distribution Point Distribution Point Name:	ad.remic /	[1]Authority Info Access Access Method=On-line Certifi (1 36.15.5.7.48.1) Alternative Name: URL=http://winserver.ad.re	cate Status Protocol em-s, il m.com/ocsp

Details zum Client-Zertifikat

Konfiguration in Windows Server

Schritt 1: Benutzer hinzufügen

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

clientcert CN Properti	es		? ×	clientcert CN Properti	es			?	×
Member Of	Dial-In	Environment	Sessions	Remote control	Remote	Desktop Se	rvices Profile	CO	M+
Remote control	Remote [esktop Services Profile	COM+	General Address	Account	Profile	Telephones	Organia	ation
General Address	Account	Profile Telephones	Organization	Member Of	Dial-in	Envi	ronment	Sessio	ns
User logon name:				Member of:					
clientcertCN		@ad.rem-s_::sm.com	~	Name	Active Direct	tory Domain	Services Folder		
User logon name (pre	Windows 200	0):		Domain Admins	ad rem-s	m.com/Use	ns		
AD\		clientcertCN		Domain Users	ad.rem-s; ()	m.com/Use	rs		
User must chan User cannot ch Password neve Store password Account expires	ge password a ange password rexpires using reversibl	t next logon d e encryption	~	Add	Remove Iomain Users There is r	no need to a	change Primary	group unle	
● Ne <u>v</u> er ○ End of:	Friday .	July 5, 2024		Set Primary Group	you have applicatio	Macintosh ns.	clients or POSI)	(-complian	t
0	К	Cancel Apply	Help	0	K	Cancel	Apply	He	lp

Benutzername für Anmeldung

Schritt 2: OCSP-Dienst bestätigen

Navigieren Sie zu Windows, und klicken Sie auf Online-Responder-Verwaltung. Bestätigen Sie den Status des OCSP-Servers.

Stocsp - [Online Responder: winserver.ad.rem-system.o	om)					
Eile Action Yiew Help						
Online Responder: winserver.ad.rem-s,r*1.n.com Prevocation Configuration Pray Configuration winserver.ad.rem-s;rt.t.n.com	serverad.rem=s,r="_incom retion n m=ry:ts.n.com Online Responder Configuration Use this snap-in to configure and manage one or more certificate revocation responders.					
	Overview	•				
	The Online Responder Management snap-in helps you configure and manage online certificate status protocol (OCSP) responders with one or more certification authorities. Use this tool to: • Manage certificate revocation configurations for an Online Responder Array. • Monitor the operating status of each member of an Online Responder Array. • Manage Online Responder Array members.					
	Revocation Configuration Status	•				
	The Status pane identifies Online Responder configurations that are working properly or that may need administrator attention. To get more information, select the Array members. Note: You may need to click Refresh if recent configuration changes or other administrative actions are not represented here. For more information, see Verifying that a revocation configuration is functioning properly.					

Status des OCSP-Servers

Klicken Sie auf winserver.ad.rem-xxx.com, und überprüfen Sie den Status des OCSP-Signaturzertifikats.



Status des OCSP-Signaturzertifikats



Schritt 1: Gerät hinzufügen

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

■ Cisco ISE					Δ	dministration · Netw	ork Resources		
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS S	Servers	RADIUS Server Sequences	NAC Managers	External MDM	pxGrid Direct Connectors	Location Services
Network Devices Default Device Device Security Settings	Network Devices List Network Device	> c1000							
	Namo	C1000							
	Description								
	IP Address	*IP: 1,10, \101	′ <u>32</u> 🐡						
	Device Profile	# Свсо	~ 0						
	Model Name		~						
	Software Version		~						
	Network Device	Group							
	Location	All Locations	~	Set To De	fault				
	IPSEC	No	~	Set To De	fault				
	Device Type	All Device Types	×	Set To Del	fault				
	RAD	IUS Authentication Settir	ıgs						
	RADIU	S UDP Settings							
	Protoco	RADIUS							
	Shared	Secret cisco123		Hide					
	Us	e Second Shared Secret 🕕							
Gerät hinzufüg	gen								

Schritt 2: Active Directory hinzufügen

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

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

≡ Cisco ISE	Administration - Identity Management
Identities Groups External Ide	entity Sources Identity Source Sequences Settings
External Identity Sources	Connection Allowed Domains PassiveID Groups Attributes Advanced Settings
Certificate Authentication F	Join Point Name AD_Join_Point
Active Directory	* Active Directory Domain ad.rem-s_t* (n.com
C LDAP	+ Join + Leave Q Test User 🕺 Diagnostic Tool 🛛 Refresh Table
ODBC RADIUS Token	ISE Node ^ ISE Node R Status Domain Controller Site
C RSA SecurID	ise32-01.ad.rem-sy um.c STANDALONE 🗹 Operational winserver.ad.rem-s, ste Default-First-Site-Na
SAML Id Providers	
Social Login	

Active Directory hinzufügen

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

≡ Cisco ISE	Administration - Identity Management					
Identities Groups	External Identity Sources	Identity Source Sequences	Settings			
External Identity Sources	Connection	Allowed Domains PassivelD	Groups	Advanced Settings		
> 🗖 Certificate Auth	entication f	Ndd 🔿 📋 Delete Group Update Sil	D Values			
Active Directory		Select Groups From Directory	∧ SID			

Gruppen aus Verzeichnis auswählen

Klicken Sie auf Gruppen aus der Dropdown-Liste abrufen. Checkad.rem-xxx.com/Users/Cert Publisher und klicken Sie auf OK.

Cisco ISE		Administration - Identity Management	
Identities Groups External Ide	entity Sources Identity Sc	Select Directory Groups	×
Extende Identity Sources Extende Identity Sources	Connection Allowed Dom	Select Directory Groups Interest in select groups from the Directory Domain at select groups from the Directory Name Sole Interest in select groups from the Directory Name Sole Interest in select groups from the Directory Interest in selectory of Groups from the Directory Interest in mean/Directory Orests S-1-S-21-41193742415-413352000-30442396 Interest in mean/Directory Orests	
		Cancel	~

Zertifikatverleger überprüfen

Schritt 3: Zertifikatauthentifizierungsprofil hinzufügen

Navigieren Sie zu Administration > External Identity Sources > Certificate Authentication Profile, und klicken Sie auf die Schaltfläche Add, um ein neues Zertifikatauthentifizierungsprofil hinzuzufügen.

- Name: cert_authen_profile_test
- Identitätsspeicher: AD_Join_Point
- Identität aus Zertifikatattribut verwenden: Betreff Allgemeiner Name.
- Zuordnen des Clientzertifikats zum Zertifikat im Identitätsspeicher: Nur zur Behebung von Identitätsmehrdeutigkeiten.

=	Cisco ISE	Administration - Identity Management	
lde	entities Groups External Ide	tity Sources Identity Source Sequences Settings	
	External Identity Sources	Certificate Authentication Profiles List > cert_authen_profile_test	
	< <u>₩</u> •	Certificate Authentication Profile	
	Certificate Authentication F		
	<pre>ert_authen_profile_test</pre>	* Name cert_authen_profile_test	
	2 Preloaded_Certificate_Prof	Description	
	Active Directory		
	AD_Join_Point		
	🗖 LDAP		
	C ODBC	Identity Store AD_Join_Point V 🕡	
	RADIUS Token		
	RSA SecuriD	Use Identity From O Certificate Attribute Subject - Common Name V ()	
	SAML Id Providers	Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)	
	Social Login	👻 na fore foren nome recent for a new recent in a new recent for and the new of a monor for the 👻	
		Match Client Certificate Against Certificate In Identity Store () Only to resolve identity ambiguity O Always perform binary comparison	

Zertifikatauthentifizierungsprofil hinzufügen

Schritt 4: Identitätsquelltext hinzufügen

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

- Name: Identity_AD
- Wählen Sie Certificate Authentication Profile: cert_authen_profile_test
- Authentifizierungs-Suchliste: AD_Join_Point

Cisco ISE

Identities	Groups	External Identity	Sources	Identity Source Seque	ences	Settings
Identity Source	e Sequences List	> Identity_AD				
 Identity Name Description 	/ Source Se Identi	quence y_AD	_			
						li.
 ✓ Certifi ✓ Se ✓ Auther A s 	cate Based lect Certificate A ntication Se et of identity s	Authentication uthentication Profile earch List ources that will be ad	cert_aut	then_profil⊷ quence until first authentic	ation su	ucceeds
	Available		Sel	lected		
	Internal Endpo	ints	AD	_Join_Point	^	
	Guest Users					
	All_AD_Join_I	Points	>			
			» «			

Identitätsquellensequenzen hinzufügen

Schritt 5: Zertifikat in ISE bestätigen

Navigieren Sie zu Administration > Certificates > System Certificates, und bestätigen Sie, dass das Serverzertifikat von der vertrauenswürdigen Zertifizierungsstelle signiert wurde.

Cisco ISE	Administration - System	🛕 Evaluation Mode 1 (Days Q 🔿 💭 🐡
Deployment Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings	
Certificate Management ~ System Certificates	Default self-signed samt server cer SAML tificate - CN+SAML_Ise32-01.ad.rem-sy. um.co SAML_Ise32-01.ad.rem-sy. m.co Thu, 2 May 2024 Tu tificate - CN+SAML_Ise32-01.ad.re m m m-sy. sm.com	e, 1 May 2029 Z
Trusted Certificates OCSP Client Profile Certificate Signing Requests	CN+Ise32-01ad rem-ry: em.com, ISE Messaging Service Ise32-01ad rem-rsj: I m.com Certificate Services Endpoint Sub C Wed, 1 May 2024 We A - Ise32-01 ad rem-rsj: I m.com Certificate Services Endpoint Sub CA - Ise 32-0180001	rd, 2 May 2029 Z Active
Certificate Periodic Check Se Certificate Authority >	CN+ise32-01ad rem-sy, t.m.com, Not in use OU-Certificate Services Endpoint Sub C. Wed, 1 May 2024 OU-Certificate Services Endpoint Sub C. Wed, 1 May 2024 I officiate Services Endpoint Int Sub CA - Ise32-01 Int Sub CA - Ise32-01	rd, 2 May 2029 Z Active
	CN+Ise32-01.ad zem-s, Im.comil Portal Default Portal Certificate Group 🕥 Ise32-01.ad zem-s, Im.com rootCACommonName Tue, 4 Jun 2024. We rootCACommonName#00004	id, 4 Jun 2025 C
	ise-server-cert-friendly-name Admin, EAP () ise32-01.ad.rem-s it m.com ocsp-ca-common-name Tue, 4 Jun 2024 We Autoentication, BADIUS DTLS, publid, Portal	id, 4 Jun 2025 C

Serverzertifikat

Navigieren Sie zu Administration > Certificates > OCSP Client Profile, und klicken Sie auf Add

(Hinzufügen), um ein neues OCSP-Clientprofil hinzuzufügen.

- Name: ocsp_test_profile
- URL des OCSP-Responders konfigurieren: <u>http://winserver.ad.rem-xxx.com/ocsp</u>

≡ Cisco ISE	Administration - System	
Deployment Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Acces	s Settings
Certificate Management ~ System Certificates Trusted Certificates OCSP Cilent Profile Certificate Signing Requests Certificate Periodic Check Se	Edit OCSP Profile * Name ocsp_test_profile Description	
Certificate Authority >	 Server Connection Enable Secondary Server Always Access Primary Server First Failback to Primary Server After Interval 5 Minutes () 	
	Verificity of the second support Use OCSP URLs specified in Authority Information Access (AIA) Content State Response Support Content State Sta	✓ Secondary Server URL http:// ☑ Enable Nonce Extension Support ☑ Validate Response Signature
	Vandate Response Signature	

OCSP-Clientprofil

Navigieren Sie zu Administration > Certificates > Trusted Certificates, und bestätigen Sie, dass die vertrauenswürdige Zertifizierungsstelle in die ISE importiert wurde.

E Cisco ISE				Administra	tion - System				Evaluation Mode	Days Q	O	<u>7</u>
Deployment Licensing	Certificates	Logging Maintenance U	Ipgrade Health	Checks Bac	kup & Restore Admin A	ccess Settings						
	C	Sisco Manufacturing CA SHA2	Infrastructure	02	Cisco Manufacturing CA SH	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2	Enabled			10
Certificate Management \sim	c	lisco Root CA 2048	Endpoints Infrastructure	5F F8 7B 28 2	Cisco Root CA 2048	Cisco Root CA 2048	Sat, 15 May 2004	Tue, 15 May 2 @	Disabled			1
System Certificates	0 0	lisco Root CA 2099	Cisco Services	01 9A 33 58 7	Cisco Root CA 2099	Cisco Root CA 2099	Wed, 10 Aug 2016	Mon, 10 Aug 🖬	Enabled			
Trusted Certificates		Sisco Root CA M1	Cisco Services	2E D2 0E 73 4	Cisco Root CA M1	Cisco Root CA M1	Wed, 19 Nov 2008	Sat, 19 Nov 2	Enabled			
Certificate Signing Requests		Sisco Root CA M2	Infrastructure Endpoints	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2	Enabled			1
Certificate Periodic Check Se	0 0	lisco RXC-R2	Cisco Services	01	Cisco RXC-R2	Cisco RXC-R2	Thu, 10 Jul 2014	Mon, 10 Jul 2 🖬	Enabled			1
Certificate Authority	c	N=root_ca_common_name, OU=cisc	Infrastructure Cisco Services Endpoints AdminAuth	20 BF 12 86 F	root_ca_common_name	root_ca_common_name	Thu, 16 May 2024	Tue, 16 May 2 🛛	Enabled			
	c	N=rootCACommonName#rootCACom	Infrastructure Cisco Services Endpoints AdminAuth	21 31 D3 DE	rootCACommonName	rootCACommonName	Tue, 4 Jun 2024	Sun, 4 Jun 20 🛛	Enabled			
		efault self-signed server certificate	Endpoints Infrastructure	37 66 FC 29	ise32-01.ad.rem-system.com	ise32-01.ad.rem-system.com	Thu, 2 May 2024	Sat, 2 May 20	Enabled			
		NgiCert Global Root CA	Cisco Services	08 38 E0 56 9	DigiCert Global Root CA	DigiCert Global Root CA	Fri, 10 Nov 2006	Mon, 10 Nov 🗧	Enabled			
		NgiCert Global Root G2 CA	Cisco Services	03 3A F1 E6	DigiCert Global Root G2	DigiCert Global Root G2	Thu, 1 Aug 2013	Fri, 15 Jan 20 🖬	Enabled			1
		NgiCert root CA	Endpoints Infrastructure	02 AC 5C 26	DigiCert High Assurance EV	DigiCert High Assurance EV	Fri, 10 Nov 2006	Mon, 10 Nov 🛛	Enabled			1
		NgiCert SHA2 High Assurance Server	Endpoints Infrastructure	04 E1 E7 A4	DigiCert SHA2 High Assuran	DigiCert High Assurance EV	Tue, 22 Oct 2013	Sun, 22 Oct 2 🛛	Enabled			
		denTrust Commercial Root CA 1	Cisco Services	0A 01 42 80 0	IdenTrust Commercial Root	IdenTrust Commercial Root	Fri, 17 Jan 2014	Tue, 17 Jan 2 🖬	Enabled			1
	•	csp-ca-friendly-name	Cisco Services Endpoints	1A 12 1D 58	ocsp-ca-common-name	ocsp-ca-common-name	Tue, 4 Jun 2024	Sun, 4 Jun 20 🖪	Enabled			

Vertrauenswürdige Zertifizierungsstelle

Überprüfen Sie die Zertifizierungsstelle, und klicken Sie auf die Schaltfläche Bearbeiten, und geben Sie die Details der OCSP-Konfiguration für die Zertifikatsstatusvalidierung ein.

- Validierung gegenüber OCSP-Service: ocsp_test_profile
- Anfrage ablehnen, wenn OCSP den Status UNBEKANNT zurückgibt: prüfen
- Lehnen Sie die Anfrage ab, wenn der OCSP-Responder nicht erreichbar ist: Überprüfen

= Cisco ISE			Administration - Sys	stem	
Deployment Licensing	Certificates Logging Ma	intenance Upgrade H	ealth Checks Backup & Re	store Admin Access	Settings
	Issuer				
Certificate Management					
System Certificates	* Friendly Name	ocsp-ca-friendly-name			
Trusted Certificates					
OCSP Client Profile	Status	Enabled 🗸			
Certificate Signing Requests	Description				
Certificate Periodic Check Se					
	Subject	CN=ocsp-ca-common-name			
Certificate Authority	Issuer	CN=ocsp+ca-common-name			
	Valid From	Tue, 4 Jun 2024 13:52:00 JST			
	Valid To (Expiration)	Sun, 4 Jun 2034 13:52:00 JST			
	Serial Number	1A 12 1D 58 59 6C 75 1B			
	Signature Algorithm	SHA256withRSA			
	Key Length	2048			
	ing congr	2010			
	Usage				
		Trusted For:			
		Trust for authentication within ISE	1		
		Trust for client authenticatio	n and Syslog		
		Trust for certificate be	ased admin authentication		
		Trust for authentication of Cisco	Services		
	Certificate Status Validation				
		To verify certificates, enable the	methods below. If both are enabled	d, OCSP will always be tried fir	ist.
		OCSP Configuration			
		Validate against OCSP Service	ocsp_test_profile ~		
		Reject the request if OCSP	returns UNKNOWN status		
		Reject the request if OCSP	Responder is unreachable		
		Certificate Revocation List Cor	figuration		
		Download CRL			
		CRL Distribution URL			
			Automatically 5	Minutes	 before expiration.
		Retrieve CRL		marystra	. verere ergerditett.
			C Every 1	Hours	~
		If download failed wait	10	Minutes	 before retry.
Validiarung das Zartifik	i ataatatu a				

Validierung des Zertifikatsstatus

Schritt 6: Zulässige Protokolle hinzufügen

Navigieren Sie zu Policy > Results > Authentication > Allowed Protocols, bearbeiten Sie die Liste der Standard-Netzwerkzugriffsdienste, und aktivieren Sie dann Allow EAP-TLS.

Cisco ISE

Policy · Policy Elements

Dictionaries	Conditions	Results
Authentication Allowed Protocols	Ň	Allowed Protocols Services List > Default Network Access Allowed Protocols
Authorization	>	Name Default Network Access
Profiling	>	Description Default Allowed Protocol Service
Posture	>	
Client Provisioning	>	V Allowed Protocols
		Authentication Bypass Process Host Lookup () Authentication Protocols Allow PAP/ASCII Allow CHAP Allow MS-CHAPv1 Allow MS-CHAPv2 Allow EAP-MDS Allow EAP-MDS Allow EAP-TLS Allow EAP-TLS Proactive session ficket update will occur after 90 % of Time To Live has expired Allow LEAP Proactive session ticket update will occur after 90 % of Time To Live has expired Allow EAP-ADS Allow EAP-ADS Allow EAP-ADS Allow EAP-TLS Proactive session ticket update will occur after 90 % of Time To Live has expired Allow LEAP PAP Inner Methods Allow EAP-ADS-CHAPv2 Allow EAP-ADS-CHAPv2 Allow EAP-GTC Allow EAP-TLS Allow EAP-TLS Allow EAP-TLS Allow EAP-GTC Allow EAP-TLS Allow EAP-TLS Allow EAP-TLS Allow EAP-TLS Allow EAP-TLS Allow EAP-GTC Allow EAP-TLS Allow EAP-TLS



Schritt 7. Policy Set hinzufügen

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

- Richtliniensatzname: EAP-TLS-Test
- Bedingungen: Network Access Protocol ENTSPRICHT RADIUS
- · Zulässige Protokolle/Serversequenz: Standard-Netzwerkzugriff

≡ Cisco ISE	Policy - Policy Sets	🛕 Evaluation Mode : 1 Days Q. 🛞 👾
Policy Sets		Reset Reset Policyset Hitcounts Save
Status Policy Set Name Description	Conditions	Allowed Protocols / Server Sequence Hits Actions View
Q Search		
Satulläules	2 Network Access Protocol EQUALS RACIUS	Default Network Access 🥒 + 🤧 🚳 🕨

Policy Set hinzufügen

Schritt 8: Authentifizierungsrichtlinie hinzufügen

Navigieren Sie zu Policy Sets, und klicken Sie auf EAP-TLS-Test, um eine Authentifizierungsrichtlinie hinzuzufügen.

- Regelname: EAP-TLS-Authentifizierung
- Bedingungen: Network Access EAPAuthentication ENTSPRICHT EAP-TLS UND Wired_802.1 X
- Verwenden: Identity_AD

\sim Authentication Policy (2)				
Status Rule Name	Conditions	Use	Hits	Actions
Q Search				
	22 Network Access EasAuthentication EQUALS EAP-TLS	Identity_AD		
EAP-TLS-Authentication	AND Weed_802.1X	> Options	26	傪

Authentifizierungsrichtlinie hinzufügen

Schritt 9. Autorisierungsrichtlinie hinzufügen

Navigieren Sie zu Policy Sets, und klicken Sie auf EAP-TLS-Test, um eine Autorisierungsrichtlinie hinzuzufügen.

- Regelname: EAP-TLS-Autorisierung
- Bedingungen: ZERTIFIKAT Betreff Common Name EQUALS clientcertCN
- Ergebnisse: PermitAccess

✓ Authorization Pol	icy (2)							
			Results					
Status R	ule Name	Conditions	Profiles		Security Groups		Hits	Actions
Q Search								
O E	AP-TLS-Authorization	CERTIFICATE-Subject - Common Name EQUALS clientcertCN	PermitAccess	0 +	Select from list	<i>e</i> +	17	

Autorisierungsrichtlinie hinzufügen

Überprüfung

Schritt 1: Authentifizierungssitzung bestätigen

Führenshow authentication sessions interface GigabitEthernet1/0/3 details Sie den Befehl aus, um die Authentifizierungssitzung in C1000 zu bestätigen.

<#root>

Switch#

show authentication sessions interface GigabitEthernet1/0/3 details

Interface: GigabitEthernet1/0/3 MAC Address: b496.9114.398c IPv6 Address: Unknown IPv4 Address: 192.168.10.10 User-Name: clientcertCN 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: 111s Common Session ID: 01C2006500000933E4E87D9 Acct Session ID: 0x0000078 Handle: 0xB6000043 Current Policy: POLICY_Gi1/0/3 Local Policies: Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150) Server Policies: Method status list: Method State dot1x Authc Success

Schritt 2: 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 zur Authentifizierung.

■ Cisco ISE		Operations - RADIUS	Evaluation Mode 70 Days	Q (0) 59 (4)
Live Logs Live Sessions				
Misconfigured Supplicants 🕕	Misconfigured Network Devices ①	RADIUS Drops 💿	Client Stopped Responding 🕡	Repeat Counter ①
0	0	0	0	0
\mathcal{G} $\begin{tabular}{lllllllllllllllllllllllllllllllllll$			Refresh Show Latest 50 reco	✓ Within Last 24 hours ↓ Filter ↓ ②
Time Status	Details Repea Identity	Endpoint ID Endpoint Authentication Policy	Authorization Policy Authorizatio	IP Address
×	✓ Identity	Endpoint ID Endpoint Pr Authentication Policy	Authorization Policy Authorization Pi	IP Address 🗸 🗸
Jun 05, 2024 09:43:36.3 🔵	a 0 clientcertCN	84:96:91:14:3 Intel-Device EAP-TLS-Test >> EAP-TLS-Authentication	EAP-TLS-Test >> EAP-TLS-Authorization PermitAccess	192.168.10.10
Jun 05, 2024 09:43:33.2	a clientcertCN	84:96:91:14:3 Intel-Device EAP+TLS+Test >> EAP+TLS+Authentication	EAP-TLS-Test >> EAP-TLS-Authorization PermitAccess	

Radius-Live-Protokoll

Bestätigen Sie das detaillierte Live-Protokoll der Authentifizierung.

Cisco ISE

Overview	
Event	5200 Authentication succeeded
Username	clientcertCN
Endpoint Id	B4:96:91:14:39:8C @
Endpoint Profile	Intel-Device
Authentication Policy	EAP-TLS-Test >> EAP-TLS-Authentication
Authorization Policy	EAP-TLS-Test >> EAP-TLS-Authorization
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2024-06-05 09:43:33.268
Received Timestamp	2024-06-05 09:43:33.268
Policy Server	ise32-01
Event	5200 Authentication succeeded
Username	clientcertCN
Endpoint Id	B4:96:91:14:39:8C
Calling Station Id	B4-96-91-14-39-8C
Endpoint Profile	Intel-Device
Authentication Identity Store	AD_Join_Point
Identity Group	Profiled
Audit Session Id	01C20065000000933E4E87D9
Other Australia	
Other Attributes	
ConfigVersionId	167
DestinationPort	1645
Protocol	Radius
NAS-Port	50103
Framed-MTU	1500
State	37CPMSessionID=01C20065000000933E4E87D9;31SessionI D=ise32-01/506864164/73;
AD-User-Resolved-Identities	clientcertCN@ad.rem-s;=:em.com
AD-User-Candidate- Identities	clientcertCN@ad.rem-sy:.tem.com
TotalAuthenLatency	324
ClientLatency	80
AD-User-Resolved-DNs	CN=clientcert CN,CN=Users,DC=ad,DC=rem- st- <tem,dc=com< th=""></tem,dc=com<>
AD-User-DNS-Domain	ad.rem-sy ; tem.com
AD-User-NetBios-Name	AD
IsMachineldentity	false
AD-User-SamAccount-Name	clientcertCN
AD-User-Qualified-Name	clientcertCN@ad.rem-sy:::+m.com
AD-User-SamAccount-Name	clientcertCN
AD-User-Qualified-Name	clientcertCN@ad.rem-sy*t:m.com
TLSCipher	ECDHE-RSA-AES256-GCM-SHA384
TLSVersion	TLSv1.2
DTLSSupport	Unknown
Subject	CN=clientcertCN

CN+ocsp-ca-common-name

Steps 11001 Received RADIUS Access-Request 11017 RADIUS created a new session 15049 Evaluating Policy Group 15008 Evaluating Service Selection Policy 11507 Extracted EAP-Response/Identity 12500 Prepared EAP-Request proposing EAP-TLS with challenge 12625 Valid EAP-Key-Name attribute received 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request 11018 RADIUS is re-using an existing session 12502 Extracted EAP-Response containing EAP-TLS challengeresponse and accepting EAP-TLS as negotiated 12800 Extracted first TLS record; TLS handshake started 12545 Client requested EAP-TLS session ticket The EAP-TLS session ticket received from supplicant 12542 while the stateless session resume is disabled. Performing full authentication 12805 Extracted TLS ClientHello message 12806 Prepared TLS ServerHello message 12807 Prepared TLS Certificate message 12808 Prepared TLS ServerKeyExchange message 12809 Prepared TLS CertificateRequest message 12810 Prepared TLS ServerDone message 12505 Prepared EAP-Request with another EAP-TLS challenge 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request 11018 RADIUS is re-using an existing session 12504 Extracted EAP-Response containing EAP-TLS challengeresponse 12988 Take OCSP servers list from OCSP service configuration -certificate for clientcertCN 12550 Sent an OCSP request to the primary OCSP server for the CA - External OCSP Server 12553 Received OCSP response - certificate for clientcertCN 12554 OCSP status of user certificate is good - certificate for clientcertCN 12811 Extracted TLS Certificate message containing client certificate 12812 Extracted TLS ClientKevExchange message

12813 Extracted TLS CertificateVerify message

12803 Extracted TLS ChangeCipherSpec message

24432 Looking up user in Active Directory - AD_Join_Point 24325 Resolving identity - clientcertCN

- 24313
 Search for matching accounts at join point ad.remsr. imm.com

 24319
 Single matching account found in forest - ad.remsr. thm.com

 24323
 Identity resolution detected single matching account
- 24700 Identity resolution by certificate succeeded -AD_Join_Point 22037 Authentication Passed
- 12506
 EAP-TLS authentication succeeded

 24715
 ISE has not confirmed locally previous successful machine authentication for user in Active Directory

 15036
 Evaluating Authorization Policy
- 24209 Looking up Endpoint in Internal Endpoints IDStore clientcertCN 15036 Evaluating Authorization Policy
- 24209 Looking up Endpoint in Internal Endpoints IDStore clientcertCN 24211 Found Endpoint in Internal Endpoints IDStore
- 15016 Selected Authorization Profile PermitAccess

22081 Max sessions policy passed

- 22080 New accounting session created in Session cache
- 11503 Prepared EAP-Success
- 11002 Returned RADIUS Access-Accept

Authentifizierungsdetails

Issuer

Crypto,2024-06-05 09:43:33,064,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, CryptoLib.CSSL.OCSP Callback -

starting OCSP request to primary

,SSL.cpp:1444 Crypto,2024-06-05 09:43:33,064,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe

Start processing OCSP request

,

URL=<u>http://winserver.ad.rem-xxx.com/ocsp</u>

, use nonce=1,0cspClient.cpp:144

Crypto, 2024-06-05 09:43:33, 104, DEBUG, 0x7f9822961700, NIL-CONTEXT, Crypto::Result=0, Crypto.0cspClient::pe

Received OCSP server response

,0cspClient.cpp:411 Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.0cspClient::pe

Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe

Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe

Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe

User certificate status: Good

,OcspClient.cpp:598
Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, CryptoLib.CSSL.OCSP C

perform OCSP request succeeded

, status: Good,SSL.cpp:1684

// Radius session
Radius,2024-06-05 09:43:33,120,DEBUG,0x7f982d7b9700,cntx=0000017387,sesn=ise32-01/506864164/73,CPMSessi

Code=1(AccessRequest)

Identifier=238 Length=324 [1] User-Name - value: [

clientcertCN

] [4] NAS-IP-Address - value: [1.x.x.101] [5] NAS-Port - value: [50103] [24] State - value: [37CPMSessionID=01C20065000000933E4E87D9;31SessionID=ise32-01/506864164/73;] [87] NAS-Port-Id - value: [GigabitEthernet1/0/3]

Radius, 2024-06-05 09:43:33, 270, DEBUG, 0x7f982d9ba700, cntx=0000017387, sesn=ise32-01/506864164/73, CPMSessi

Code=2(AccessAccept)

Identifier=238 Length=294
[1] User-Name - value: [clientcertCN]

Radius, 2024-06-05 09:43:33, 342, DEBUG, 0x7f982d1b6700, cntx=0000017401, sesn=ise32-01/506864164/74, CPMSessie

Code=4(AccountingRequest)

```
Identifier=10 Length=286
[1] User-Name - value: [clientcertCN]
[4] NAS-IP-Address - value: [1.x.x.101]
[5] NAS-Port - value: [50103]
[40] Acct-Status-Type - value: [Interim-Update]
[87] NAS-Port-Id - value: [GigabitEthernet1/0/3]
[26] cisco-av-pair - value: [audit-session-id=01C2006500000933E4E87D9]
[26] cisco-av-pair - value: [method=dot1x] ,RADIUSHandler.cpp:2455
```

Radius, 2024-06-05 09:43:33, 350, DEBUG, 0x7f982e1be700, cntx=0000017401, sesn=ise32-01/506864164/74, CPMSessi

Code=5(AccountingResponse)

Identifier=10 Length=20,RADIUSHandler.cpp:2455

2. TCP-Dump

Im TCP-Dump in der ISE erwarten Sie Informationen zur OCSP-Antwort und zur Radius-Sitzung.

OCSP-Anfrage und -Antwort:

No.	Time	Identification	Source	S.Port Destination	D.Port Time	to Live Protocol	Length TCP	Se Next se	CP.Ac Info	
+	140 2024-06-05 00:43:33.093523	0x0295 (661)	1.1181	25844 1.1 1	80	64 OCSP	262	1 197	1 Request	
•	141 2024-06-05 00:43:33.104108	0x0117 (279)	1.1 ? 0.57	80 1.1 181	25844	128 OCSP	1671	1 1607	197 Response	

Paketerfassung von OCSP-Anfragen und -Antworten

>	Frame 141: 1671 bytes on wire (13368 bits), 1671 bytes captured (13368 bits)												
>	Ethernet II, Src: VMware_98:c9:91 (00:50:56:98:c9:91), Dst: VMware_98:57:1c (00:50:56:98:57:1c)												
>	Internet Protocol Version 4, Src: 1.1. 1.57, Dst: 1.131.181												
>	ransmission Control Protocol, Src Port: 80, Dst Port: 25844, Seq: 1, Ack: 197, Len: 1605												
>	Hypertext Transfer Protocol												
v	Online Certificate Status Protocol												
	responseStatus: successful (0)												
	✓ responseBytes												
	ResponseType Id: 1.3.6.1.5.5.7.48.1.1 (id-pkix-ocsp-basic)												
	✓ BasicOCSPResponse												
	✓ tbsResponseData												
<pre>> responderID: byKey (2) producedAt: Jun 5, 2024 09:43:33.000000000 > responses: 1 item > SingleResponse > contID</pre>													
								> certStatus: good (0)					
							cnisopoace: Jun 4, 2024 16:05:00.00000000						
								nextUpdate: Jul 4, 2024 16:05:00.000000000					
								✓ responseExtensions: 1 item					

Erfassen der Details der OCSP-Antwort

Radius-Sitzung:

146 2024-06-05 00:43:33.118175	0x9bc6 (39878)	1.177.101	67181 1.17	1645	255 RADIUS	366	Access-Request id=238
185 2024-06-05 00:43:33.270244	0x033d (829)	1.1	67181 1.:^^.^.101	1645	64 RADIUS	336	Access-Accept id=238
187 2024-06-05 00:43:33.341233	0x9bc7 (39879)	1.1.1.1.1.101	1646 1	1646	255 RADIUS	328	Accounting-Request id=10
188 2024-06-05 00:43:33.350936	0x037a (890)	1.17181	1646 1.:)101	1646	64 RADIUS	62	Accounting-Response id=10
267 2024-06-05 00:43:36.359621	0x9bc8 (39880)	1.104.0.101	1646 1.1JK.J.181	1646	255 RADIUS	334	Accounting-Request id=11
268 2024-06-05 00:43:36.369035	0x0489 (1161)	1.1 1.1.181	1646 1.174).101	1646	64 RADIUS	62	Accounting-Response id=11

Paketerfassung der RADIUS-Sitzung

Zugehörige Informationen

Konfigurieren der EAP-TLS-Authentifizierung mit der ISE

Konfigurieren von TLS/SSL-Zertifikaten in der ISE

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.