Installeer een door derden ondertekend certificaat in ISE

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Configureren Stap 1. Generate certificaataanvraag (CSR). Stap 2. Voer een nieuwe certificaatketen in. Verifiëren Problemen oplossen Leverancier heeft geen vertrouwen in het ISE Local Server Certificate tijdens een dot1x-verificatie ISE certificaatketen is correct maar endpoint wijst ISE's servercertificaat tijdens verificatie af Gerelateerde informatie

Inleiding

Dit document beschrijft de installatie van een door derden ondertekend certificaat in Cisco Identity Services Engine (ISE). Dit proces is hetzelfde ongeacht de uiteindelijke certificeringsrol (EAP-verificatie, Portal, Admin en PxGrid).

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van de Basisinfrastructuur van de Openbare Sleutel.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Identity Services Engine (ISE) release 3.0. Dezelfde configuratie is van toepassing op releases 2.X

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configureren

Stap 1. Generate certificaataanvraag (CSR).

Om de CSR te genereren, navigeer dan naar Administratie > Certificaten > Aanvragen van certificaatsignalering en klik op Aanvragen van certificaatsignalering genereren (CSR).

Certificate Management System Certificates	~	Certificate Signing Requests		
Trusted Certificates		Generate Certificate Signing Reque	sts (CSR)	
OCSP Client Profile		A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click request has been signed, click "bind" to bind the request to the signed certificate issued by that au		
Certificate Signing Requests				
Certificate Periodic Check Se		Q View ₫ Export 💼 Delete	Bind Certificate	
Certificate Authority	>	Friendly Name	Certificate Subject	

- Selecteer onder het gedeelte Gebruik de rol die u wilt gebruiken in het vervolgkeuzemenu. Als het certificaat wordt gebruikt voor meerdere rollen, kunt u Meervoudig gebruik selecteren. Zodra het certificaat is gegenereerd kunnen de rollen indien nodig worden gewijzigd.
- 2. Selecteer het knooppunt waarvoor het certificaat wordt gegenereerd.
- 3. Vul de vereiste informatie in (organisatie-eenheid, organisatie, stad, staat en land).

Opmerking: Onder Common Name (CN) - veld ISE vult de Full Qualified Domain Name (FQDN) van het knooppunt automatisch in.

Wildcards:

- Als het doel is om een certificaat met jokerteken te genereren, controleer dan het vakje Wildcard Certificaten toestaan.
- Indien het certificaat wordt gebruikt voor MAP-authenticaties, mag het*-symbool niet in het veld Onderwerp GN worden aangebracht, aangezien Windows-aanvragers het servercertificaat afwijzen.
- Zelfs wanneer Validering Server Identity op de aanvrager uitgeschakeld is, kan de SSLhanddruk falen wanneer de * in het GN-veld staat.
- In plaats daarvan kan een generieke FQDN in het GN-veld worden gebruikt, en vervolgens kan het ***.domain.com** worden gebruikt in het veld Naam Onderwerp Alternative Name (SAN) DNS Name.

Opmerking: Sommige certificaatinstanties (CA) kunnen de wildkaart (*) automatisch toevoegen aan de GN van het certificaat, zelfs als deze niet in het CSR aanwezig is. In dit geval is een speciaal verzoek vereist om deze actie te voorkomen.

Individueel servercertificaat CSR voorbeeld:

Usage

Certificate(s) will be used for	Multi-Use	~	You can use a single certificate for multiple services, but doing so is not a recommended practice. Rather, you should obtain individual certificates specifically for each service (for example, one certificate each for Guest Portals, EAP, and pxGrid).
Allow Wildcard Certificates	0		
Node(s)			
Generate CSR's for these Nodes:			
Node	CSR Friendly Name		
✓ abtomar30	abtomar30#Multi-Use		
Subject			
Common Name (CN) \$FQDN\$		0	
Organizational Unit (OU) Cisco TAC		<u>.</u>	
Organization (O) Cisco		<u>(</u>)	
City (L) Bangalore			
State (ST) Karnataka			
Country (C) IN			
Subject Alternative Name (SAN)			
IP Address	∨ 10.106.120.87		- + 0
* Key type			
RSA	~ (i)		

Voorbeeld van jokerteken CSR:

lsage			\sim
Certificate(s) will be used for	Multi-Use	× \Lambda	You can use a single certificate for multiple services, but doing so is not a recommended practice. Rather, you should obtain individual
			certificates specifically for each service (for example, one certificate each for Guest Portals, EAP, and pxGrid).
Allow Wildcard Certificates 🗸	0		
ubject			
Common Name (CN) Mycluster.mydomain,com		<u>(</u>)	
Organizational Unit (OU) Cisco TAC		(i)	
Organization (O) Cisco		i	
City (L) Bangalore			
State (ST) Karnataka			
Country (C)			
Subject Alternative Name (SAN)			
IP Address	∽ 10.106.120.87		- +
DNS Name	*.mydomain.com		- + ()
* Key type			
RSA	~ (i)		

Opmerking: Het IP-adres van elk van de implementatieknooppunten kan aan het SAN-veld worden toegevoegd om een certificaatwaarschuwing te voorkomen wanneer u de server via het IP-adres benadert.

Zodra de CSR is gemaakt, geeft ISE een pop-upvenster weer met de optie om deze te exporteren. Als dit bestand eenmaal geëxporteerd is, moet dit naar de CA worden verzonden voor het ondertekenen.

 \sim



Certificate Signing request(s) generated:

abtomar30.abtomar.local#Multi-Use

Click Export to download CSR(s) or OK to return to list of CSR(s) screen



Stap 2. Voer een nieuwe certificaatketen in.

De certificaatinstantie retourneert het ondertekende servercertificaat samen met de volledige certificeringsketen (Root/Intermediate). Nadat u de certificaten hebt ontvangen, volgt u de volgende stappen om deze in uw ISE-server te importeren:

- 1. Om alle door de CA verstrekte wortelcertificaten en (of) certificaten via tussenweg in te voeren, navigeer dan naar Administratie > Certificaten > Vertrouwde certificaten.
- 2. Klik op **Importeren** en kies vervolgens het (middelste) certificaat en/of de bijbehorende selectievakjes in te schakelen.
- 3. Als u het servercertificaat wilt importeren, navigeer dan naar Administratie > Certificaten > Aanvragen voor certificaatsignalering.
- 4. Selecteer de CSR die eerder is gemaakt en klik op Bind-certificaat.
- 5. Selecteer de nieuwe certificaatlocatie en ISE bindt het certificaat aan de privé sleutel die in de database gecreëerd en opgeslagen wordt.

Opmerking: Als de Admin Rol voor dit certificaat is geselecteerd, start de specifieke ISE serverdiensten opnieuw.

Voorzichtig: Als het geïmporteerde certificaat bedoeld is voor het knooppunt Primair beheer van de implementatie en als de Admin-rol is geselecteerd, starten de services op alle knooppunten het ene na het andere opnieuw. Dit wordt verwacht en voor het uitvoeren van deze activiteit wordt een downtime aanbevolen.

Verifiëren

Als de admin-rol is geselecteerd tijdens de certificaatinvoer, kunt u controleren of het nieuwe certificaat is geïnstalleerd door de admin-pagina in de browser te laden. De browser dient het nieuwe admin certificaat te vertrouwen zolang de keten correct gebouwd is en als de certificeringsketen door de browser wordt vertrouwd.

÷	🛞 🏈 https://abtomar30.abtomar.local/admin/login.jsp 🖉 🗸 🗎 😋 🥔 Identity Services Engine 🛛 🛪
1	Certificate X
	General Details Certification Path
	Certification path abtomar -WIN-231PNBS4IPH-CA abtomar 30.abtomar.local CISCO
P	Identity Services Engine
	Intuitive network security
	Username
	View Certificate
_	Certificate status: Password
	This certificate is OK.
	Login
	ок
	English 日本語
	Problems logging in?
6	2020 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S and certain other countries. Cisco ISE

Selecteer voor extra verificatie het symbool van het slot in de browser en controleer of de volledige keten aanwezig is en betrouwbaar is in de machine. Dit is geen directe indicator dat de volledige keten correct door de server werd doorgegeven maar een indicator van de browser die het servercertificaat kan vertrouwen op basis van zijn lokale vertrouwenswinkel.

View third-party licenses and notice

Problemen oplossen

Leverancier heeft geen vertrouwen in het ISE Local Server Certificate tijdens een dot1x-verificatie

Controleer of ISE tijdens het SSL-handschudproces de volledige certificatieketen passeert.

Bij het gebruik van MAP-methoden waarbij een servercertificaat (d.w.z. PEAP) vereist is en **de** naam **van de** bevestigde **serveridentiteit** wordt geselecteerd, bevestigt de aanvrager de certificeringsketen met behulp van de certificaten die hij in zijn lokale trustwinkel heeft als onderdeel van het verificatieproces. Als onderdeel van het SSL-handdrukproces presenteert ISE zijn certificaat en ook alle Root- en (of) intermediaire certificaten die in zijn keten aanwezig zijn. De aanvrager kan de serveridentiteit niet valideren als de keten niet volledig is. U kunt de volgende stappen uitvoeren om te controleren of de certificeringsketen naar uw client is teruggestuurd:

- 1. Om een opname van ISE (TCPDump) te nemen tijdens de authenticatie, navigeer naar Operations > diagnostische tools > General Tools > TCP dump.
- 2. Download/open de opname en pas het filter **toe.**sl.**handshake.certificaten** in Wireshark en vind een access-challenge.
- Nadat u deze optie hebt geselecteerd, navigeer u om Radius Protocol uit te vouwen > Waarde van kenmerken > EAP-Message Laatste segment > Extensible Authentication Protocol > Secure Socket Layer > Certificate > Certificates.

certificaatketen in de opname.

Ele Edit View Go Capture Analyze Statistic	s Telephony Iools Internals Help 9 ኛ 🛓 🔲 🕞 🔍 🔍 🖾	, ∰ ⊠ ¶§ % ∰	
Filter: ssl.handshake.certificates	 Expression 	Clear Apply Save	
No. Time	Source	Destination	Protocol Length Info
334 13:59:41.137274	14.36.157.20	14.36.157.21	TLSv1.2 992 Server Hello, Certificate, Server Hello Done
857 13:59:53.158063	14.36.157.21	14.36.154.5	RADIUS 1178 Access-Challenge(11) (id=198, 1=1136)
860 13:59:53.193912	14.36.157.21	14.36.154.5	RADIUS 1174 Access-Challenge(11) (id=199, l=1132)
862 13:59:53.213715	14.36.157.21	14.36.154.5	RADIUS 1174 Access-Challenge(11) (id=200, 1=1132)
864 13:59:53.231653	14.36.157.21	14.36.154.5	RADIUS 301 Access-Challenge(11) (id=201, 1=259)
1265 14:00:01.253698	14.36.157.20	14.36.157.21	TLSv1.2 992 Server Hello, Certificate, Server Hello Done

1	11 III
ſ	I AVP: I=255 t=EAP-Message(/9) Segment[1]
	B AVP: 1=255 t=EAP-Message(79) Segment[2]
	# AVP: 1=255 t=EAP-Message(79) Segment[3]
	B AVP: 1=255 t=EAP-Message(79) Last Segment[4]
	EAP fragment
	Extensible Authentication Protocol
	Code: Request (1)
	Id: 41
	Length: 1012
	Type: Protected EAP (EAP-PEAP) (25)
	# EAP-TLS Flags: 0xc0
	EAP-TLS Length: 3141
	@ [4 EAP-TLS Fragments (3141 bytes): #857(1002), #860(1002), #862(1002), #864(135)]
	⊖ Secure Sockets Layer
	I TLSVI Record Layer: Handshake Protocol: Server Hello
	ILSVI Record Layer: Handshake Protocol: Certificate
	Content (ype: Handshake (22)
	Version: ILS 1.0 (0x0301)
	Length: 3048
	Handshake Protocol: Certificate (11)
	Lancha 2046
	Contribution Jonatha 2041
	e Certificates (2041 hutes)
	Certificate length: 1656
	<pre>Certificate (id-at-componenterDRISE20A, rtpaga, not, id-at-organizationalUnitName=RTPAAA, id-at-organizationName=CISCO, id-at-localityName=R1</pre>
	Certificate Length: 1379
	# Certificate (id-at-componiane=rtpaaa-ca.dc=rtpaaa.dc=net)
	ILSv1 Record Laver: Handshake Protocol: Server Hello Done

Als de ketting niet volledig is, navigeer dan naar **ISE-administratie > Certificaten > Trusted Certificates** en controleer of de Root en (of) Intermediate certificaten aanwezig zijn. Indien de certificeringsketen succesvol is doorlopen, moet de keten zelf als geldig worden gecontroleerd met behulp van de hier beschreven methode.

Open elk certificaat (server, intermediair en wortel) en controleer de vertrouwensketen door de onderwerpsleutel (SKI) van elk certificaat te koppelen aan de doorsnede van de Autoriteit (AKI) van het volgende certificaat in de keten.

Voorbeeld van een certificeringsketen.

Certificate 25	Certificate 25	Certificate 25
General Details Certification Path	General Details Certification Path	General Details Certification Path
Show <all></all>	Show <all></all>	Show <a>l>
Field Value ^	Field Value *	Field Value ^
Public key RSA (2048 84s)	CA Version V0.0	Public key RSA (4096 Bits)
Enhanced Key Joerdner da 39 a3 ee 5e 60 40 00 32 33 dt er 95 6	Certificate Templat SubCA	Subject Key Ident., 52 Ze e5 Zc 38 Z9 d6 da 81 19 11 70 74 00.
Subject Alternative IP Address=14.36.157.21	Authority Key Identif KeyiD=52 2e e5 2c 38 29 d6 da 81 19 11	CA Version V0.0
Authority Key Identi KeyID=fe 34 ca 8d 22 9b 6e d7 a6 86 11	CRI. Distribution Pol [1]CRI. Distribution Point: Distribution Pol.	Basic Constraints Subject Type=CA, Path Length Constraint= 🚊
CRL Distribution Pol [1]CRL Distribution Point: Distribution Pol	Authority Informatio [1] Authority Info Access: Access Method	Thumbprint algori sha1
Authority Informati [1] Authority Info Access: Access Method +	Key Usage Digital Signature, Certificate Signing, Off-L -	() Thumbprint cb 24 48 a5 30 11 72 a3 da 9e 31 d1 f3 f6 +
· · · ·	· · · · ·	· · · · ·
V3 Edit Properties Copy to File Learn more about conficute details	Edit Properties Copy to File	Edit Properties Copy to File
ОК	OK	ок

ISE certificaatketen is correct maar endpoint wijst ISE's servercertificaat tijdens verificatie af

indien ISE tijdens de SSL-handdruk haar volledige certificatieketen presenteert en de aanvrager de certificeringsketen nog steeds afwijst; de volgende stap is te controleren of de certificaten van de hoofdsom en/of de tussenpersoon in de plaatselijke trustwinkel van de cliënt zijn opgeslagen.

Om dit vanuit een Windows-apparaat te controleren, navigeer naar **mmc.exe File > Add-Remove Magnetisch-in**. Selecteer in de kolom Beschikbare invoegtoepassingen **Certificaten** en klik op **Toevoegen**. Selecteer **Mijn gebruikersaccount** of **computeraccount**, afhankelijk van het gebruikte verificatietype (gebruiker of machine), en klik vervolgens op **OK**.

Selecteer onder de console-weergave de **Trusted Root-certificeringsinstanties** en de **Intermediate Certified-certificeringsinstanties** om de aanwezigheid van een certificaat voor wortel en tussenkomst in de plaatselijke trustwinkel te controleren.

🛶 Console1 - [Console Root\Certificates - Current User\Truste	d Root Certification Authorities\0	[ertificates]			
💊 File Action View Favorites Window Help					
♦ ⇒ 2					
Console Root	Issued To	Issued By	Expiration	Intended Purpo	Friendly Name Sta
A 🖓 Certificates - Current User	AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authenti	USERTrust
Personal	Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Server Authenti	Baltimore Cybe
 Trusted Root Certification Authorities 	Certum CA	Certum CA	6/11/2027	Server Authenti	Certum
Certificates	Gisco Root CA 2048	Cisco Root CA 2048	5/14/2029	<all></all>	<none></none>
Enterprise Trust	Cisco Root CA M1	Cisco Root CA M1	11/18/2033	<all></all>	<none></none>
Certificate Revocation List	Gass 2 Primary CA	Class 2 Primary CA	7/6/2019	Secure Email, S	CertPlus Class 2
Certificates	Glass 3 Public Primary Ce	Class 3 Public Primary Certi	8/1/2028	Secure Email, C	VeriSign Class 3
Active Directory User Object	COMODO RSA Certificati	COMODO RSA Certificatio	1/18/2038	Server Authenti	COMODO
Trusted Publishers	Copyright (c) 1997 Micro	Copyright (c) 1997 Microso	12/30/1999	Time Stamping	Microsoft Time
Untrusted Certificates	DigiCert Assured ID Root	DigiCert Assured ID Root C	11/9/2031	Server Authenti	DigiCert
Dirac Internation Party Root Certification Authorities	GDigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Server Authenti	DigiCert
Trusted People	DigiCert High Assurance	DigiCert High Assurance E.,	11/9/2031	Server Authenti	DigiCert
Other People	DST Root CA X3	DST Root CA X3	9/30/2021	Secure Email, S.,	DST Root CA X3
Certificate Enrollment Requests	DST Root CA X3	DST Root CA X3	9/30/2021	<all></all>	<none></none>
E Smart Card Trusted Roots	Entrust Root Certification	Entrust Root Certification	11/27/2026	Server Authenti	Entrust

Een makkelijke manier om te controleren of dit een probleem is met de identiteitscontrole van de server, **valideren van het servercertificaat** uit te schakelen onder de configuratie van het flexibele profiel en het opnieuw testen.

Connection Security Security type: WPA2-Enterprise	When connecting: Validate server certificate Connect to these servers:
Choose a network authentication method: Microsoft: Protected EAP (PEAP) Settings Remember my credentials for this connection each time I'm logged on	Trusted Root Certification Authorities: AddTrust External CA Root Baltimore CyberTrust Root Certum CA Cisco Root CA 2048 Cisco Root CA 2048 Cisco Root CA M1 Class 2 Primary CA Class 3 Public Primary Certification Authority Control Root Cattlement Authority

Gerelateerde informatie

- Administrator-gids voor Cisco Identity Services Engine, release 3.0
- Technische ondersteuning en documentatie Cisco Systems