# Installer un certificat tiers signé par une autorité de certification dans ISE

#### Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Informations générales
Configurer
Étape 1. Générer une demande de signature de certificat (CSR).
Étape 2. Importer une nouvelle chaîne de certificats.
Vérifier
Dépannage
Le demandeur n'approuve pas le certificat du serveur local ISE pendant une authentification dot1x
La chaîne de certificats ISE est correcte, mais le terminal rejette le certificat du serveur ISE pendant l'authentification
Informations connexes

# Introduction

Ce document décrit comment installer un certificat signé par une autorité de certification (CA) tierce dans Cisco Identity Services Engine (ISE).

# Conditions préalables

#### Exigences

Cisco vous recommande de connaître l'infrastructure à clé publique de base.

#### Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Identity Services Engine (ISE) version 3.0. La même configuration s'applique aux versions 2.X

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

# Informations générales

Ce processus est le même quel que soit le rôle de certificat final (authentification EAP, Portal, Admin et pxGrid).

## Configurer

Étape 1. Générer une demande de signature de certificat (CSR).

Afin de générer le CSR, accédez à Administration > Certificates > Certificate Signing Requests et cliquez sur Generate Certificate Signing Requests (CSR).

Certificate Management	Cei	Certificate Signing Requests				
Trusted Certificates	Gene	erate Certificate Si	gning Reque	ests (CSR)		
OCSP Client Profile	A Certif	A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click				
Certificate Signing Requests	request	request has been signed, click "bind" to bind the request to the signed certificate issued by that au				
Certificate Periodic Check Se	Q Viev	v 🛧 Export (	j Delete	Bind Certificate		
Certificate Authority	,	Friendly Name		Certificate Subject		

- 1. Dans la section Utilisation, sélectionnez le rôle à utiliser dans le menu déroulant. Si le certificat est utilisé pour plusieurs rôles, vous pouvez sélectionner Multi-use. Une fois le certificat généré, les rôles peuvent être modifiés si nécessaire.
- 2. Sélectionnez le noeud pour lequel le certificat peut être généré.
- 3. Renseignez les informations nécessaires (Unité organisationnelle, Organisation, Ville, État et Pays).
- Remarque : dans le champ Common Name (CN), ISE renseigne automatiquement le nom de domaine complet (FQDN) du noeud.

Caractères génériques :

- Si l'objectif est de générer un certificat générique, cochez la case Allow Wildcard Certificates.
- Si le certificat est utilisé pour les authentifications EAP, le symbole \* ne doit pas être dans le champ Objet CN car les demandeurs Windows rejettent le certificat du serveur.
- Même lorsque la validation de l'identité du serveur est désactivée sur le demandeur, la connexion SSL peut échouer lorsque le \* est dans le champ CN.

• À la place, un nom de domaine complet générique peut être utilisé dans le champ CN, puis le \*.domain.com peut être utilisé dans le champ Nom DNS alternatif du sujet (SAN).

Remarque : certaines autorités de certification peuvent ajouter automatiquement le caractère générique (\*) dans le CN du certificat, même s'il n'est pas présent dans le CSR. Dans ce scénario, une demande spéciale doit être émise pour empêcher cette action.

Exemple de certificat CSR de serveur individuel :

#### Usage

Allow Wildcard Certificates  i i Node(s) Generate CSR's for these Nodes: Node CSR Friendly Name	
Node(s) Generate CSR's for these Nodes: Node CSR Friendly Name	
Generate CSR's for these Nodes: Node CSR Friendly Name	
Node CSR Friendly Name	
abtomar30 abtomar30#Multi-Use	
Subject	
Common Name (CN) \$FQDN\$	
Organizational Unit (OU) Cisco TAC	
Organization (O) Cisco	
City (L) Bangalore	
State (ST) Karnataka	
Country (C)	
Subject Alternative Name (SAN)	
IP Address          10.106.120.87         =	0
* Key type	
RSA 🗸 🚺	

Exemple de CSR générique :

sage			~
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		,
ubject			
Common Name (CN)			
Mycluster.mydomain,com		(i)	
Organizational Unit (OU)			
Cisco TAC		(i)	
Organization (O)			
Cisco		<u>(</u> )	
City (L) Bangalore			
State (ST) Karnataka			
Country (C) IN			
Subject Alternative Name (SAN)			
IP Address	∽ 10.106.120.87		- +
DNS Name	✓ *.mydomain.com		- + 0
* Key type			
RSA	× (i)		

Remarque : chaque adresse IP de noeud de déploiement peut être ajoutée au champ SAN pour éviter un avertissement de certificat lorsque vous accédez au serveur via l'adresse IP.

Une fois le CSR créé, ISE affiche une fenêtre contextuelle avec l'option de l'exporter. Une fois exporté, ce fichier doit être envoyé à l'autorité de certification pour signature.





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



Étape 2. Importer une nouvelle chaîne de certificats.

L'autorité de certification renvoie le certificat de serveur signé avec la chaîne de certificats complète (racine/intermédiaire). Une fois reçus, procédez comme suit pour importer les certificats dans votre serveur ISE :

- 1. Afin d'importer tout certificat racine et (ou) intermédiaire fourni par l'autorité de certification, naviguez vers Administration > Certificates > Trusted Certificates.
- 2. Cliquez sur Import, puis sélectionnez le certificat racine et/ou le certificat intermédiaire et cochez les cases appropriées telles qu'elles ont été appliquées pour l'envoi.
- 3. Afin d'importer le certificat du serveur, naviguez à Administration > Certificates > Certificate Signing Requests.
- 4. Sélectionnez le CSR précédemment créé et cliquez sur Bind Certificate.
- 5. Sélectionnez le nouvel emplacement du certificat et ISE lie le certificat à la clé privée créée et stockée dans la base de données.
- Remarque : si le rôle admin a été sélectionné pour ce certificat, les services du serveur ISE spécifiques redémarrent.

Attention : si le certificat importé est destiné au noeud d'administration principal du déploiement et si le rôle Admin est sélectionné, les services sur tous les noeuds redémarrent l'un après l'autre. Ceci est prévu et une interruption est recommandée pour effectuer cet exercice.

#### Vérifier

Si le rôle admin a été sélectionné lors de l'importation du certificat, vous pouvez vérifier que le nouveau certificat est en place en chargeant la page admin dans le navigateur. Le navigateur doit faire confiance au nouveau certificat d'administration tant que la chaîne a été créée correctement et si la chaîne de certificats est approuvée par le navigateur.

Certificate	C Identity Services Engine
Certification path abtomar-WIN-231PNBS4IPH-CA abtomar30.abtomar.loca	cisco
	Identity Services Engine
View Certificate	Username
Certificate status: This certificate is OK.	Password
ОК	Login
	English   日本語 Problems logging in?

© 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 in View third-party licenses and notices

Pour une vérification supplémentaire, sélectionnez le symbole de verrouillage dans le navigateur et, sous le chemin d'accès du certificat, vérifiez que la chaîne complète est présente et approuvée par la machine. Il ne s'agit pas d'un indicateur direct indiquant que la chaîne complète a été transmise correctement par le serveur, mais d'un indicateur du navigateur capable d'approuver le certificat du serveur sur la base de son magasin d'approbation local.

### Dépannage

Le demandeur n'approuve pas le certificat du serveur local ISE pendant une authentification dot1x

Vérifiez qu'ISE passe la chaîne de certificats complète pendant le processus d'échange SSL.

Lorsque vous utilisez des méthodes EAP qui nécessitent un certificat de serveur (c'est-à-dire, PEAP) et que l'option Valider l'identité du serveur est sélectionnée, le demandeur valide la chaîne de certificats en utilisant les certificats qu'il a dans son magasin d'approbation local dans le cadre du processus d'authentification. Dans le cadre du processus de connexion SSL, ISE présente son certificat ainsi que tous les certificats racine et (ou) intermédiaires présents dans sa chaîne. Le demandeur ne pourra pas valider l'identité du serveur si la chaîne est incomplète. Pour vérifier que la chaîne de certificats est renvoyée à votre client, vous pouvez effectuer les étapes suivantes :

- 1. Afin d'effectuer une capture à partir d'ISE (TCPDump) pendant l'authentification, naviguez vers Operations > Diagnostic Tools > General Tools > TCP Dump.
- 2. Téléchargez/ouvrez la capture et appliquez le filtre ssl.handshake.certificates dans Wireshark et trouvez un défi d'accès.
- Une fois la sélection effectuée, naviguez vers Expand Radius Protocol > Attribute Value Pairs > EAP-Message Last segment > Extensible Authentication Protocol > Secure Sockets Layer > Certificate > Certificates.

Chaîne de certificats dans la capture.

le <u>E</u> di	t <u>V</u> iew <u>Go</u> <u>C</u> apture <u>Analyze</u> <u>Stat</u>	istics Telephony Iools Internals	Help	
® /	( = <u>A</u>   = = = X =   Q, + +			Frank
PHDer:	sschandshake.certificates	Expression	L. Cear Apply	save
33.	Time	Source	Destination	Protocol Length Info
3.34	13:39:41.13/2/4	14.36.157.20	14.30.137.21	ILSVI.2 992 Server Hello, Certificate, Server Hello Done
83/	13:39:33.138003	14.36.157.21	14.30.134.3	RADIUS 11/8 Access-challenge(11) (10-198, 1-1130)
86	13.50.53 313715	14.36.157.31	14.30.134.3	BADIUS 1174 Access Challenge(11) (1d-200, 1-1132)
86	12:50:52 221652	14.30.137.21	14 36 154 5	040105 11/4 Access - Challenge(11) (14-200, 1=1152)
126	14:00:01.253698	14.36.157.20	14.36.157.21	TLSv1.2 992 Server Hello, Certificate, Server Hello Done
a Al	/P: 1=255 t=EAP-Message(79	) Segment[2]		
i Al	<pre>/P: 1=255 t=EAP-Message(79)</pre>	) Segment[3]		
a Al	<pre>/P: 1=255 t=EAP-Message(79</pre>	) Last Segment[4]		
	EAP fragment			
8	Extensible Authentication	Protocol		
	td: 41			
	Length: 1012			
	Type: Protected EAP (EAP	-PEAP) (25)		
	EAP-TIS Flags: 0xc0	(20) (20)		
	EAP-TLS Length: 3141			
	# [4 EAP-TLS Fragments (31)	41 bytes): #857(1002), #	860(1002), #862(100	02), #864(135)]
	Secure Sockets Layer			
	III TLSv1 Record Layer: Har	ndshake Protocol: Server	Hello	
	B TLSv1 Record Layer: Has	ndshake Protocol: Certif	icate	
	Content Type: Handsha	ike (22)		
	Version: TLS 1.0 (0x0	301)		
	Length: 3048			
	Handshake Protocol: C	ertificate		
	Handshake Type: Cer	tificate (II)		
	Contificator Longth	2041		
	= Certificates (3041	hytes)		
	Certificate Length	1656		
	= Certificate (id-at	t-contooName=TORISE20A ct	tnaga net id-at-oro	nanizationalUnitName=RTPAAA_id-at-organizationName=CTSCO_id-at-localityName
	Certificate Length	1379	and and and and	and a second s
	E Certificate (id-at	t-commonName=rtpaaa-ca.de	=rtpaaa.dc=net)	
	TLSv1 Record Laver: Har	ndshake Protocol: Server	Hello Done	
		i i fact if a state		-

Si la chaîne est incomplète, accédez à ISE Administration > Certificates > Trusted Certificates et vérifiez que les certificats racine et (ou) Intermediate sont présents. Si la chaîne de certificats est passée avec succès, la chaîne elle-même doit être vérifiée comme étant valide à l'aide de la méthode décrite ici.

Ouvrez chaque certificat (serveur, intermédiaire et racine) et vérifiez la chaîne de confiance en faisant correspondre l'identificateur de clé de sujet (SKI) de chaque certificat à l'identificateur de

clé d'autorité (AKI) du certificat suivant dans la chaîne.

Exemple de chaîne de certificats.

Certificate 25	Certificate 2	Certificate
General Details Certification Path	General Details Certification Path	General Details Certification Path
Show <all></all>	Show <al></al>	Show <all></all>
Field Value ^	Field Value A	Field Volue *
Public key RSA (2048 8its)	CA Version V0.0	Dublic key RSA (4096 Bits)
E Subject Key Identifier da 39 a3 ee 5e 6b 4b 0d 32 55 bf ef 95 6	Subject Key Identifier fe 34 ca 8d 22 9b 6e d7 as 86 11 cl 18 1.	Key Usage Digital Signature, Certificate Signing, Off-I
Enhanced Key Usage Server Authentication (1.3.6.1.5.5.7.3.1)	E Certificate Templat SubCA	Subject Key Ident 52 2e e5 2c 38 29 d6 da 81 19 11 70 74 00
Subject Alternative IP Address=14.36.157.21	Authority Key Identif Key/D=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	CRL Distribution Pol [1]CRL 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-1	- Charles Contraction Contract
4 III. F	4	
V3	V3	V3
	M	14
	M	14
		14
Edit Descartion County File	Edit Descention Cours in Pile	Edit Dranastian
Eak Propercies Copy to Hie	Eat Properties Copy to File	Eak Properties Capy to Hie
Learn more about certificate details	Learn more about certificate details	Learn more about certificate details
OK	OK	OK

La chaîne de certificats ISE est correcte, mais le terminal rejette le certificat du serveur ISE pendant l'authentification

Si ISE présente sa chaîne de certificats complète lors de la connexion SSL et que le demandeur continue de rejeter la chaîne de certificats, l'étape suivante consiste à vérifier que les certificats racine et/ou intermédiaire se trouvent dans le magasin local d'approbations du client.

Afin de vérifier cela à partir d'un périphérique Windows, naviguez vers mmc.exe File > Add-Remove Snap-in. Dans la colonne Composants logiciels enfichables disponibles, sélectionnez Certificats et cliquez sur Ajouter. Sélectionnez Mon compte d'utilisateur ou Compte d'ordinateur selon le type d'authentification utilisé (Utilisateur ou Machine), puis cliquez sur OK.

Dans la vue de la console, sélectionnez Autorités de certification racines de confiance et Autorités de certification intermédiaires pour vérifier la présence des certificats racines et intermédiaires dans le magasin d'approbations local.

🖕 Console1 - [Console Root\Certificates - Current User\Trusted Root Certification Authorities\Certificates]

File Action View Favorites Window Help					
Console Root	Issued To	Issued By	Expiration	Intended Purpo	Friendly Name St
A P 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
<ul> <li>Trusted Root Certification Authorities</li> </ul>	Certum CA	Certum CA	6/11/2027	Server Authenti	Certum
Certificates	GCisco Root CA 2048	Cisco Root CA 2048	5/14/2029	<all></all>	<none></none>
Enterprise Trust	Gisco Root CA M1	Cisco Root CA M1	11/18/2033	<all></all>	<none></none>
Certificate Revocation List	Class 2 Primary CA	Class 2 Primary CA	7/6/2019	Secure Email, S.,	CertPlus Class 2
Certificates	Class 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
Third-Party Root Certification Authorities	DigiCert 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
Display the second s	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>
Image: Smart Card Trusted Roots	Entrust Root Certification	Entrust Root Certification	11/27/2026	Server Authenti	Entrust

Pour vérifier facilement qu'il s'agit d'un problème lié à la vérification de l'identité du serveur, désactivez la case à cocher Valider le certificat du serveur dans la configuration du profil du demandeur et testez-la à nouveau.

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

#### Informations connexes

- Guide de l'administrateur de Cisco Identity Services Engine, version 3.0
- <u>Assistance technique de Cisco et téléchargements</u>

#### À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.