

Configurez le certificat signé CA sur le serveur CVP pour l'accès au Web HTTPS

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurez](#)

[Liste de référence de commandes](#)

[Faites une sauvegarde](#)

[Générez le CSR](#)

[Répertoriez les Certificats](#)

[Retirez le certificat existant OAMP](#)

[Générez la paire de clés](#)

[Générez le nouveau CSR](#)

[Délivrez le certificat sur le CA](#)

[Certificat généré par CA d'importation](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer et vérifier le certificat signé d'Autorité de certification (CA) sur le serveur du portail de gestion et de Gestion d'exécution du port voix de Cisco (CVP) (OAMP).

Conditions préalables

Microsoft Windows a basé l'autorité de certification que le serveur est déjà préconfiguré.

Conditions requises

Cisco recommande que vous ayez la connaissance de l'infrastructure de PKI.

[Composants utilisés](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

Version 11.0 CVP

Serveur R2 de Windows 2012

Autorité de certification R2 de Windows 2012

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Liste de référence de commandes

```
more c:\Cisco\CVP\conf\security.properties
cd c:\Cisco\CVP\conf\security
```

```
%kt% -list
%kt% -list | findstr Priv
%kt% -list -v -alias oamp_certificate
```

```
%kt% -genkeypair -alias oamp_certificate -v -keysize 2048 -keyalg RSA
%kt% -import -v -trustcacerts -alias oamp_certificate -file oamp.p7b
```

Faites une sauvegarde

Naviguez vers le répertoire **c:\Cisco\CVP\conf\security** et archivez tous les fichiers. Si l'accès de Web OAMP ne fonctionne pas, remplacez les fichiers de création récente par ceux de la sauvegarde.

Générez le CSR

Vérifiez votre mot de passe de Sécurité.

```
more c:\Cisco\CVP\conf\security.propertiesSecurity.keystorePW = fc]@2zfe*Ufe2J,.0uM$Ff
```

Naviguez vers le répertoire de **c:\Cisco\CVP\conf\security**.

```
cd c:\Cisco\CVP\conf\security
```

Remarque: En cet article, la variable d'environnement Windows est utilisée pour rendre des commandes de Keytool beaucoup plus courtes et plus accessibles en lecture. Avant que n'importe quelle commande de keytool soit ajoutée, assurez-vous que la variable est initialisée.

1. Créez une variable temporaire.

```
set kt=c:\Cisco\CVP\jre\bin\keytool.exe -storepass fc]@2zfe*Ufe2J,.0uM$Ff -storetype JCEKS -keystore .keystore
```

Sélectionnez la commande de s'assurer que la variable est initialisée. Entrez le mot de passe correct.

```
echo %kt%
c:\Cisco\CVP\jre\bin\keytool.exe -storepass fc]@2zfe*Ufe2J,.0uM$Ff -storetype JCEKS -keystore .keystore
```

Répertoriez les Certificats

Certificats actuellement installés de liste dans le keystore.

```
%kt% -list
```

Conseil : Si vous voulez affiner votre liste vous pouvez modifier la commande d'afficher seulement les Certificats auto-signés.

```
%kt% -list | findstr Priv
```

```
vxml_certificate, May 27, 2016, PrivateKeyEntry,oamp_certificate, May 27, 2016,  
PrivateKeyEntry,wsm_certificate, May 27, 2016, PrivateKeyEntry,callserver_certificate, May 27,  
2016, PrivateKeyEntry,
```

Verify auto-a signé les informations sur la certification OAMP.

```
%kt% -printcert -file oamp.crt
```

```
Owner: CN=CVP11, OU=TAC, O=Cisco, L=Krakow, ST=Malopolskie, C=PLIssuer: CN=CVP11, OU=TAC,  
O=Cisco, L=Krakow, ST=Malopolskie, C=PLSerial number: 3f44f086Valid from: Fri May 27 08:13:38  
CEST 2016 until: Mon May 25 08:13:38 CEST 2026Certificate fingerprints: MD5:  
58:F5:D3:18:46:FE:9A:8C:14:EA:73:0F:5F:12:E7:43 SHA1:  
51:7F:E7:FF:25:B6:B8:02:CD:18:84:E7:50:9E:F2:ED:B1:9E:78:40 Signature algorithm name:  
SHA1withRSA Version: 3
```

Retirez le certificat existant OAMP

Afin de générer une nouvelle paire de clés, retirez le certificat qui existe déjà.

```
%kt% -delete -alias oamp_certificate
```

Générez la paire de clés

Exécutez cette commande de générer une nouvelle paire de clés pour le pseudonyme avec la taille de clé sélectionnée.

```
%kt% -genkeypair -alias oamp_certificate -v -keysize 2048 -keyalg RSA
```

```
What is your first and last name?
```

```
[Unknown]: cvp11.allevich.local
```

```
What is the name of your organizational unit?
```

```
[Unknown]: TAC
```

```
What is the name of your organization?
```

```
[Unknown]: Cisco
```

```
What is the name of your City or Locality?
```

```
[Unknown]: Krakow
```

```
What is the name of your State or Province?
```

```
[Unknown]: Malopolskie
```

```
What is the two-letter country code for this unit?
```

```
[Unknown]: PL
```

```
Is CN=cvp11, OU=TAC, O=Cisco, L=Krakow, ST=Malopolskie, C=PL correct?
```

```
[no]: yes
```

```
Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA)
```

```
with a validity of 90 days for: CN=cvp11, OU=TAC, O=Cisco, L=Krakow, ST=Malopolskie, C=PL
```

```
(RETURN if same as keystore password):
```

```
[Storing .keystore]
```

Vérifiez que la paire de clés a été générée.

```
c:\Cisco\CVP\conf\security>dir | findstr oamp.key05/27/2016 08:13 AM 1,724 oamp.key
```

Assurez pour entrer d'abord et nom de famille en tant que votre serveur OAMP. Le nom doit être résoluble à une adresse IP. Ce nom apparaîtra dans le domaine NC du certificat.

Générez le nouveau CSR

Exécutez cette commande de générer la demande de certificat du pseudonyme et de la sauvegarder à un fichier (par exemple, oamp.csr).

```
%kt% -certreq -alias oamp_certificate -file oamp.csr
```

Vérifiez que le CSR a été généré avec succès.

```
dir oamp.csr 08/25/2016 08:13 AM 1,136 oamp.csr
```

Délivrez le certificat sur le CA

Pour obtenir le certificat vous aurez besoin d'une autorité de certification déjà configurée.

Tapez l'URL donné dans un navigateur

IP address >/certsrv de http:// <CA

Sélectionnez alors le **certificat de demande** et la **demande avancée de certificat**.

```
more oamp.csr-----BEGIN NEW CERTIFICATE REQUEST-----
MIIC/TCCAeUCAQAwYcxIzAhBgkqhkiG9w0BCQEWFkGkbWluQGfSbGV2aWN0LmxvY2FsMQswCQYDVQQGEwJQTDEUMBIGA1UE
CBMLTWFsb3BvbHNraWUxZDZANBgNVBAcTBktyYWtvdzEOMAwGA1UEChMFQ2l2Y28xDDAKBgNVBAsTAlRBQzEOMAwGA1UEAxMF
Q1ZQMTEwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCvQEGmJPmzimqQA6zc1mbWnkzAj3PvGKe9Qg0RefOnHpLq
+ddx66o60Gr6TTb1BrqI8UeN1JDFuQj/m4HZvKsqRv1AWA5CtGRzjbOeNXPMCGotk00b9643M8DY0Q9LQ/+PxdzYGhieCxnH
QURcAIsViphV4yxUVJ4QcLkzkbM9T8DSOJSJAI4gY+tO3i0xxDTcXlaTQ1xkRYDba8JwzVHLTkVwtSRK2jqIzJuBPZwpXMZc
8RDkffBurrVXhFb8ylvR/Q7cAzHPgpPLuK6KmwP0Kv8CRoWml3xAEGrd39szkZfbawRzddTqw8hM/2cLSouKx0NMFY5dXzIs
zQEYlK5XAgMBAAGgMDAuBgkqhkiG9w0BCQ4xITAFMB0GA1UdDgQWBRe8u10Cd1HckIm9VjD3ZL/uXhgGzANBgkqhkiG9w0B
AQsFAAOCAQEAc48VD1d/BJMaOXwxz5riT1BCjxzLIMTNzv3W00K7ehtmYVTaRCXLZ/sOX5ws807kwnOaZeIprzdlGvumS+d
Ugun/2Q00rp+B44gRv9KUTvv5C6YoBslm4H2xp9yaQpgzLBjuKRgl8yIzYnIvoVuPxracGSkyxKzxvrvxOX2qvxoVq71bf
43Aps4+G85Cp3GWhIBQ+TtIKKxgZ/C64ThZgT9HtD9zbL3g0U8bP1F6JNjztzjmuGEDqsNF0fAjpPsfShQ10o4qIMBi7hBQu
sAwNBEB1xaAlYumD09+R/BK2KfMvIy4CdsEfWlmjBb541TJEYzwOh7tpRZkjOqyVMQ=====END NEW CERTIFICATE
REQUEST-----
```

Copiez et collez le contenu entier du CSR au menu approprié. **Serveur Web** choisi comme modèle et **base 64 de certificat encodés**. Cliquez sur Download alors la **chaîne de certificat**.

Vous pouvez exporter le CA et le certificat généré par web server individuellement ou télécharger une pleine chaîne. Dans cet exemple l'option de pleine chaîne est utilisée.

Certificat généré par CA d'importation

Installez le certificat à partir du fichier.

```
%kt% -import -v -trustcacerts -alias oamp_certificate -file oamp.p7b
```

Pour appliquer le nouveau certificat redémarrez les services de **service** et de **Cisco CVP OPSConsoleServer d'édition de World Wide Web**.

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Le moyen le plus simple de vérifier est d'ouvrir une session au web server CVP OAMP. Vous ne devriez pas recevoir un message d'avertissement de certificat non approuvé.

Une autre manière est de vérifier le certificat OAMP utilisé avec cette commande.

```
%kt% -list -v -alias oamp_certificateAlias name: oamp_certificateCreation date: Oct 20,
2016Entry type: PrivateKeyEntryCertificate chain length: 2Certificate[1]:Owner:
CN=cvp11.allevich.local, OU=TAC, O=Cisco, L=Krakow, ST=Malopolskie, C=PLIssuer: CN=pod1-POD1AD-
CA, DC=pod1, DC=ccemea, DC=tacSerial number: 130c0db6000000000017Valid from: Thu Oct 20 12:48:08
CEST 2016 until: Sat Oct 20 12:48:08 CEST 2018Certificate fingerprints:MD5:
BA:E8:FA:05:45:07:D0:3C:C8:81:1C:34:3D:21:AF:ACSHA1:
30:04:F2:EE:37:22:9D:8D:27:8F:54:D2:BA:D4:0F:33:74:34:87:D8Signature algorithm name:
SHA1withRSAVersion: 3Extensions:#1: ObjectId: 1.3.6.1.4.1.311.20.2 Criticality=false0000: 1E 12
00 57 00 65 00 62 00 53 00 65 00 72 00 76 ...W.e.b.S.e.r.v0010: 00 65 00 72 .e.r#2: ObjectId:
1.3.6.1.5.5.7.1.1 Criticality=falseAuthorityInfoAccess [[accessMethod: caIssuersaccessLocation:
URIName: ldap:///CN=pod1-POD1AD-CA,CN=AIA,]]#3: ObjectId: 2.5.29.35
Criticality=falseAuthorityKeyIdentifier [KeyIdentifier [0000: 9B 33 47 9E 76 DB F3 92 B2 F8 F9
86 3A 59 BA DE .3G.v.....:Y..0010: C5 0B E5 E4 ....]]#4: ObjectId: 2.5.29.31
Criticality=falseCRLDistributionPoints [[DistributionPoint:[URIName: ldap:///CN=pod1-POD1AD-
CA,CN=POD1AD,CN=CDP]]]#5: ObjectId: 2.5.29.37 Criticality=falseExtendedKeyUsages [serverAuth]#6:
ObjectId: 2.5.29.15 Criticality=trueKeyUsage [DigitalSignatureKey_Encipherment]#7: ObjectId:
2.5.29.14 Criticality=falseSubjectKeyIdentifier [KeyIdentifier [0000: CD FC 95 D1 60 44 9A 34 A9
EE 0E 3F C7 F5 5D 3C ....`D.4...?..]<0010: 46 DF 47 D9 F.G.]]Certificate[2]:Owner: CN=pod1-
POD1AD-CA, DC=pod1, DC=ccemea, DC=tacIssuer: CN=pod1-POD1AD-CA, DC=pod1, DC=ccemea, DC=tacSerial
number: 305dba13e0def8b474fefeb92f54acdValid from: Thu Sep 08 18:06:37 CEST 2016 until: Wed Sep
08 18:16:36 CEST 2021Certificate fingerprints:MD5:
50:04:5F:89:CA:7C:D6:71:82:10:C3:04:57:78:AB:AESHA1:
A6:3B:07:29:AF:3A:07:73:9D:9B:4F:88:B5:A8:17:AC:0A:6D:C3:0DSignature algorithm name:
SHA1withRSAVersion: 3Extensions:#1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false0000: 02 01
00 ...#2: ObjectId: 2.5.29.19 Criticality=trueBasicConstraints:[CA:truePathLen:2147483647]#3:
ObjectId: 2.5.29.15 Criticality=falseKeyUsage [DigitalSignatureKey_CertSignCrl_Sign]#4:
ObjectId: 2.5.29.14 Criticality=falseSubjectKeyIdentifier [KeyIdentifier [0000: 9B 33 47 9E 76
DB F3 92 B2 F8 F9 86 3A 59 BA DE .3G.v.....:Y..0010: C5 0B E5 E4 ....]]
```

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Si vous devez vérifier la syntaxe de commande référez-vous à la configuration et au guide d'administration pour CVP.

http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/customer_voice_portal/cvp8_5/configuration/guide/ConfigAdminGuide_8-5.pdf

Informations connexes

[Configurez le certificat signé CA par l'intermédiaire du CLI dans le système d'exploitation de Voix de Cisco \(VOS\)](#)

[Procédure pour obtenir et télécharger l'individu de Windows Server ? Signé ou Autorité de certification \(CA\)...](#)

Support et documentation techniques - Cisco Systems