Configure CA Signed Certificate on CVP Server for HTTPS Web Access

Contents

Introduction

This document describes how to configure and verify Certificate Authority (CA) signed certificate on the Cisco Voice Portal (CVP) Operation Administration and Management Portal (OAMP) server.

Prerequisites

Microsoft Windows based Certificate Authority server is already preconfigured.

Requirements

Cisco recommends that you have knowledge of the PKI infrastructure.

Components Used

The information in this document is based on these software and hardware versions:

CVP version 11.0

Windows 2012 R2 Server

Windows 2012 R2 Certificate Authority

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, make sure that you understand the potential impact of any command.

Configure

Command Reference List

```
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
```

Make a Backup

Navigate to the folder **c:\Cisco\CVP\conf\security** and archive all the files. If OAMP web access does not work, replace newly created files with the ones from the backup.

Generate CSR

Check your security password.

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

Navigate to **c:\Cisco\CVP\conf\security** folder.

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

> **Note**: In this article, Windows environment variable is used to make Keytool commands much shorter and more readable. Before any keytool command is added, ensure that the variable is initialized.

1. Create a temporary variable.

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

Enter the command to ensure that the variable is initialized. Enter correct password.

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

List the Certificates

List currently installed certificates in the keystore.

```
%kt% -list
```

> **Tip**: If you want to refine your list you can modify the command to display only self-signed

certificates.

```
%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 self-signed OAMP certification information.

```
%kt% -printcert -file oamp.crt
Owner: CN=CVP11, OU=TAC, O=Cisco, L=Krakow, ST=Malopolskie, C=PL Issuer: CN=CVP11, OU=TAC,
O=Cisco, L=Krakow, ST=Malopolskie, C=PL Serial number: 3f44f086 Valid from: Fri May 27 08:13:38
CEST 2016 until: Mon May 25 08:13:38 CEST 2026 Certificate 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
```

Remove the Existing OAMP Certificate

In order to generate a new key pair, remove the certificate that already exists.

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

Generate Key Pair

Run this command to generate a new key pair for the alias with selected key size.

```
%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]
```

Verify that the key pair was generated.

```
c:\Cisco\CVP\conf\security>dir | findstr oamp.key 05/27/2016 08:13 AM 1,724 oamp.key
```

Ensure to enter first and last name as your OAMP Server. The name must be resolvable to an IP address. This name will appear in the CN field of the certificate.

Generate New CSR

Run this command to generate the certificate request for the alias and save it to a file (for example, oamp.csr).

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

Verify that the CSR was generated successfully.

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

Issue the Certificate on the CA

To get the certificate you will need a Certificate Authority already configured.

Type the given URL in a browser

http://<CA ip address>/certsrv

Then select **Request certificate** and **Advanced certificate request**.

```
more oamp.csr -----BEGIN NEW CERTIFICATE REQUEST-----
MIIC/TCCAeUCAQAwgYcxIzAhBgkqhkiG9w0BCQEWFGFkbWluQGFsbGV2aWNoLmxvY2FsMQswCQYD
VQQGEwJQTDEUMBIGA1UECBMLTWFsb3BvbHNraWUxDzANBgNVBAcTBktyYWtvdzEOMAwGA1UEChMF
Q2lzY28xDDAKBgNVBAsTA1RBQzEOMAwGA1UEAxMFQ1ZQMTEwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQCvQEGmJPmzimqQA6zc1mbWnkzAj3PvGKe9Qg0REfOnHpLq+ddx66o6OGr6TTb1
BrqI8UeN1JDfuQj/m4HZvKsqRv1AWA5CtGRzjbOeNXPMCGOtkO0b9643M8DY0Q9LQ/+PxdzYGhie
CxnhQURcAIsViphV4yxUVJ4QcLkzkbM9T8DSoJSJAI4gY+tO3i0xxDTcxlaTQ1xkRYDba8JwzVHL
TkVwtSRK2jqIzJuBPZwpXMZc8RDkffBurrVXhFb8ylvR/Q7cAzHPgpPLuK6KmwpOKv8CRoWml3xA
EgRd39szkZfbawRzddTqw8hM/2cLSoUKx0NMFY5dXzIszQEYlK5XAgMBAAGgMDAuBgkqhkiG9w0B
CQ4xITAfMB0GA1UdDgQWBBRe8ul0CdlHckIm9VjD3ZL/uXhgGzANBgkqhkiG9w0BAQsFAAOCAQEA
c48VD1d/BJMaOXwxz5riT1BCjxzLIMTNzv3W00K7ehtmYVTTaRCXLZ/sOX5ws807kwnOaZeIpRzd
lGvumS+dUgun/2QO0rp+B44gRvgp9KUTvv5C6YoBslm4H2xp9yaQpgzLBJuKRgl8yIzYnIvoVuPx
racGSkyxKzxvrvxOX2qvxoVq71bf43Aps4+G85Cp3GWhIBQ+TtIKKxgZ/C64ThZgT9HtD9zbL3g0
U8bPlF6JNjztzjmuGEdqsNf0fAjpPsfShQl0o4qIMBi7hBQusAwNBEB1xaAlYumD09+R/BK2KfMv
Iy4CdsEfWlmjBb54lTJEYzwOh7tpRZkjOqyVMQ== -----END NEW CERTIFICATE REQUEST-----
```

Copy and paste the entire content of the CSR to the appropriate menu. Select **Web Server** as a certificate template and **Base 64 encoded**. Then click **Download certificate chain**.

You can export CA and web server generated certificate individually or download a full chain. In this example the full chain option is used.

Import CA Generated Certificate

Install the certificate from the file.

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

To apply new certificate restart **World Wide Web Publishing Service** and **Cisco CVP OPSConsoleServer** services.

Verify

Use this section in order to confirm that your configuration works properly.

Easiest way to verify is to login to CVP OAMP web server. You should not get an untrusted certificate warning message.

Another way is to check the OAMP certificate used with this command.

```
%kt% -list -v -alias oamp_certificate Alias name: oamp_certificate Creation date: Oct 20, 2016
Entry type: PrivateKeyEntry Certificate chain length: 2 Certificate[1]: Owner:
```

```
CN=cvp11.allevich.local, OU=TAC, O=Cisco, L=Krakow, ST=Malopolskie, C=PL Issuer: CN=pod1-POD1AD-
CA, DC=pod1, DC=ccemea, DC=tac Serial number: 130c0db6000000000017 Valid from: Thu Oct 20
12:48:08 CEST 2016 until: Sat Oct 20 12:48:08 CEST 2018 Certificate fingerprints: MD5:
BA:E8:FA:05:45:07:D0:3C:C8:81:1C:34:3D:21:AF:AC SHA1:
30:04:F2:EE:37:22:9D:8D:27:8F:54:D2:BA:D4:0F:33:74:34:87:D8 Signature algorithm name:
SHA1withRSA Version: 3 Extensions: #1: ObjectId: 1.3.6.1.4.1.311.20.2 Criticality=false 0000: 1E
12 00 57 00 65 00 62 00 53 00 65 00 72 00 76 ...W.e.b.S.e.r.v 0010: 00 65 00 72 .e.r #2:
ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false AuthorityInfoAccess [ [ accessMethod: caIssuers
accessLocation: URIName: ldap:///CN=pod1-POD1AD-CA,CN=AIA, ] ] #3: ObjectId: 2.5.29.35
Criticality=false AuthorityKeyIdentifier [ 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=false CRLDistributionPoints [ [DistributionPoint: [URIName: ldap:///CN=pod1-POD1AD-
CA,CN=POD1AD,CN=CDP] ]] #5: ObjectId: 2.5.29.37 Criticality=false ExtendedKeyUsages [ serverAuth
] #6: ObjectId: 2.5.29.15 Criticality=true KeyUsage [ DigitalSignature Key_Encipherment ] #7:
ObjectId: 2.5.29.14 Criticality=false SubjectKeyIdentifier [ 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=tac Issuer: CN=pod1-POD1AD-CA, DC=pod1,
DC=ccemea, DC=tac Serial number: 305dba13e0def8b474fefeb92f54acd Valid from: Thu Sep 08 18:06:37
CEST 2016 until: Wed Sep 08 18:16:36 CEST 2021 Certificate fingerprints: MD5:
50:04:5F:89:CA:7C:D6:71:82:10:C3:04:57:78:AB:AE SHA1:
A6:3B:07:29:AF:3A:07:73:9D:9B:4F:88:B5:A8:17:AC:0A:6D:C3:0D Signature algorithm name:
SHA1withRSA Version: 3 Extensions: #1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false 0000: 02
01 00 ... #2: ObjectId: 2.5.29.19 Criticality=true BasicConstraints:[ CA:true PathLen:2147483647
] #3: ObjectId: 2.5.29.15 Criticality=false KeyUsage [ DigitalSignature Key_CertSign Crl_Sign ]
#4: ObjectId: 2.5.29.14 Criticality=false SubjectKeyIdentifier [ 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 .... ] ]
```

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

If you need to verify the command syntax refer to the Configuration and Administration Guide for 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

Related Information

Configure CA Signed Certificate via CLI in Cisco Voice Operating System (VOS)

Procedure to obtain and upload Windows Server SelfSigned or Certificate Authority (CA) ...

Technical Support & Documentation - Cisco Systems