Automate CVP Certificate Commands

Contents

[Introduction]
[Prerequisites]
[Requirements]
[Components Used]
[Configure]
[Command Explanation]
[Commands]
[Alias Backup]
[Export Keystore]
[Delete Alias]
[Create New Self-Signed Certificate]
[Export Self-Signed Certificate]
[Generate Certificate Signing Request (CSR)]
[Import CA Signed Certificates]
[Verify]
[Troubleshoot]

Introduction

This document describes a way to automate the various commands used with CVP certificates. This also provides options to make the certificate compliant with RFC.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Voice Portal (CVP)
- Java Keytool
- Public Key Infrastructure (PKI) Certificates

Components Used

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

- Cisco Voice Portal (CVP) 12.5(1)
- Unified Contact Center Enterprise (UCCE)
- Packaged Contact Center Enterprise (PCCE)
- Operation and Administration Management Portal (OAMP)

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, ensure that you understand the potential impact of any command.

Configure

Command Explanation

These commands were built to largely automate the commands used in the of management certificates with CVP. These are not officially supported, but are tested.

Example security.properties output:

```
Security.keystorePW = xt_PXM-*4Z!!ZQID7YX*6K(3iii
```

The part of these commands that makes them able to be automated is the first part of the line. This section shows the line and then explains how it works.

```
FOR /f "tokens=3" %i IN ('more %CVP_HOME%\conf\security.properties') DO <command>
```

Command parts:

Command Section	Explanation
FOR /f	This is the DOS FOR command with a switch used to process the content of f for specific matches.
"tokens=3"	This indicates that we need the 3rd token or word. With the example security.properties file shown in this section, the 3 tokens a Token 1: Security.keystorePW Token 2: = Token 3: xt_PXM-*4Z!!ZQID7YX*6K(3iii
%i	This is the variable where the value of the IN command that matches the FOR parameter is stored.
IN ('more %CVP_HOME%\conf\security.properties')	Execute the command, "more %CVP_HOME%\conf\security.properties" and the contents into the FOR command.
DO <command>	Execute the command and pass the value for %i.

The commands shown in this document read the password in security.properties and automate the entry in the keystore commands. This ensures that the end user does not need to type or copy/paste this password an elminates the errors this can cause.

Commands

The example commands all work with an arbritrary alias named cvp_certificate. Ensure that you replace the alias name as required.

Alias Backup

This command is not typically used, but is helpful to make a backup of the old certificate and private key.

The example renames the cvp_certificate to cvp_certificate_back.

```
FOR /f "tokens=3" %i IN ('more %CVP_HOME%\conf\security.properties') DO
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
storepass %i -changealias -alias cvp_certificate -destalias cvp_certificate_back
```

Export Keystore

This command exports the entire keystore to a text file. This allows a user to inspect the contents of the keystore.

```
FOR /f "tokens=3" %i IN ('more %CVP_HOME%\conf\security.properties') DO
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
storepass %i -list -v > %CVP_HOME%\conf\security\cvp_keystore.txt
```

Delete Alias

This command deletes the current alias and certificate. This process is irrevokable, it is strongly recommended that you make a backup of the keystore.

```
FOR /f "tokens=3" %i IN ('more %CVP_HOME%\conf\security.properties') DO
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
storepass %i -delete -alias cvp_certificate
```

Create New Self-Signed Certificate

This command creates a new, self-signed certificate. This command is required even if you choose to have the certificate signed by a certificate authority (CA), as this creates the private key required for the certificate.

For RSA Certificates without SAN (typical):

```
FOR /f "tokens=3" %i IN ('more %CVP_HOME%\conf\security.properties') DO
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
storepass %i -genkeypair -alias cvp_certificate -keysize 2048 -keyalg RSA -validity 1825
```

For RSA Certificates with SAN:

```
FOR /f "tokens=3" %i IN ('more %CVP_HOME%\conf\security.properties') DO
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
storepass %i -genkeypair -alias cvp_certificate -keysize 2048 -keyalg RSA -validity 1825 -ext
san=dns:mycvp.mydomain.com,dns:localhost
```

Subject Alternative Name

The -ext paramenter allows a user to specific extensions. The example shown adds a subject alternative name (SAN) with the fully qualified domain name (FQDN) of the server as well as localhost. Additional SAN fields can be added as comma separated values.

Valid SAN Types are:

```
ip:192.168.0.1
dns:myserver.mydomain.com
```

```
email:name@mydomain.com
```

Each of these commands requires 6 values to be provided. In order they are, Common Name, Organizational Unit, Organization, City, State, and Country. Copy the answers and update them to match your specific requirements. You can then paste them into the command prompt when required.

```
myserver.mydomain.com
My Organizational Unit
My Company
City
My State
US
```

Export Self-Signed Certificate

This command exports the self-signed certificate. This allows the certificate to be imported to other components such as OAMP, or the PCCE Administration Data Server.

```
FOR /f "tokens=3" %i IN ('more %CVP_HOME%\conf\security.properties') DO
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
storepass %i -export -alias cvp_certificate -file %CVP_HOME%\conf\security\cvp.crt
```

Generate Certificate Signing Request (CSR)

This command creates a CSR so that you can have a CA sign the request.For Certificates without SAN:

```
FOR /f "tokens=3" %i IN ('more %CVP_HOME%\conf\security.properties') DO
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
storepass %i -certreq -alias cvp_certificate -file %CVP_HOME%\conf\security\cvp.csr
```

For Certificates with SAN:

```
FOR /f "tokens=3" %i IN ('more %CVP_HOME%\conf\security.properties') DO
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
storepass %i -certreq -alias cvp_certificate -file %CVP_HOME%\conf\security\cvp.csr -ext
san=dns:mycvp.mydomain.com,dns:localhost
```

> **Note**: You must include the SAN extension in the CSR request for the certificate to contain a SAN.

Import CA Signed Certificates

These commands import the CA root, intermediate, and server certificates in turn.

Copy the certificates to the %CVP_HOME%\conf\security\ directory.

Ensure that you update the alias name and certificate name as required.

```
FOR /f "tokens=3" %i IN ('more %CVP_HOME%\conf\security.properties') DO
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
storepass %i -import -v -trustcacerts -alias myrootca -file %CVP_HOME%\conf\security\root.crt
```

```
FOR /f "tokens=3" %i IN ('more %CVP_HOME%\conf\security.properties') DO
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
storepass %i -import -v -trustcacerts -alias myintermediate -file
%CVP_HOME%\conf\security\intermediate.crt
FOR /f "tokens=3" %i IN ('more %CVP_HOME%\conf\security.properties') DO
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
storepass %i -import -v -trustcacerts -alias cvp_certificate -file
%CVP_HOME%\conf\security\cvp.crt
```

Verify

There are no steps to verify this procedure.

Troubleshoot

There are no steps to troubleshoot this procedure.