CVP Smart License CSSM Certificate Import Procedure

Contents

Issue

CVP Call Server is experiencing smart licensing "verify signature" errors in the SmartAgent logs. The system requires the CSSM (Cisco Smart Software Manager) certificate to be imported into the CVP keystore to resolve signature verification failures during normal licensing status update processes. Without the proper CSSM certificate chain, CVP cannot validate licensing transactions with the Cisco Smart Software Manager, resulting in licensing compliance issues.

Environment

- Cisco Customer Voice Portal (CVP) Call Server version 12.6.2
- Contact Center Software - Packaged Contact Center Enterprise (PCCE)
- CVP services: Call Server, WSM (Web Service Manager), VXML Server
- Java JCEKS keystore format for certificate management
- Smart Licensing integration with Cisco Smart Software Manager (CSSM)

Resolution

Follow these detailed steps to import the CSSM certificate into the CVP Call Server keystore.

Step 1: Identify Keystore Password

Open a command window as administrator and navigate to the CVP home directory to decrypt the keystore password:

```
cd %CVP_HOME%\bin
DecryptKeystoreUtil.bat
```

Record the password displayed by this utility as it is required for all subsequent keytool commands.

Step 2: Backup Current Keystore

Create a backup of the existing keystore from the security directory:

```
cd %CVP_HOME%\conf\security
copy .keystore backup.keystore
```

Step 3: Export Current Keystore Contents

Generate a list of all current certificates in the keystore for reference:

```
cd %CVP_HOME%\jre\bin
keytool -list -v -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" > C:\temp\certs_cvp.tx
```

Review the generated file to understand the current certificate inventory.

Step 4: Download CSSM Certificates

Obtain the required CSSM certificate chain from the Transport URL on the CVP Licensing page. The certificate requirements depend on the certificate type:

For CA-signed certificates: Download the Root and Intermediate certificates individually in .cer format

For self-signed certificates: Download the CSSM certificate directly

Save the certificate files to the CVP security directory:

```
%CVP_HOME%\conf\security
```

Step 5: Import CSSM Root Certificate (CA-signed)

For CA-signed certificates, import the root certificate first:

```
"%CVP_HOME%\jre\bin\keytool.exe" -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" -impor
```

Step 6: Import CSSM Intermediate Certificate (CA-signed)

If an intermediate certificate exists, import it using this command:

```
"%CVP_HOME%\jre\bin\keytool.exe" -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" -impor
```

Step 7: Import Self-Signed CSSM Certificate (Alternative)

For self-signed certificates, import the CSSM certificate directly:

```
"%CVP_HOME%\jre\bin\keytool.exe" -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" -impor
```

Step 8: Verify Certificate Import

Confirm the new certificates are present in the keystore:

```
cd %CVP_HOME%\jre\bin
keytool -list -v -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" > C:\temp\certs_cvp_ne
```

Review the new certificate list to verify the CSSM certificates have been successfully imported.

Step 9: Reboot and Service Verification

Reboot the CVP server and record the restart time. After reboot, confirm all CVP services have started:

- Call Server
- WSM (Web Service Manager)
- VXML Server

Wait approximately 20 minutes after service startup before proceeding to validation.

Step 10: Validate Resolution

Perform these validation steps:

Check SmartAgent Logs:

Navigate to **C:\Cisco\CVP\logs\WSM** and sort by Date Modified. Examine the most recent 15-minute status reports in the SmartAgent logs. The verify signature exception must no longer appear after the restart time.

Verify Licensing Status:

Access the CVP licensing page and confirm the system shows "registered" and "in compliance" status with no errors.

Rollback Procedure (If Issues Occur)

If problems are encountered during the certificate import process, follow these rollback steps:

Step 1: Stop all CVP services (Call Server, WSM, VXML)

Step 2: Navigate to the security directory:

```
cd %CVP_HOME%\conf\security
```

Step 3: Delete the modified keystore:

```
del .keystore
```

Step 4: Restore the backup keystore:

```
rename backup.keystore .keystore
```

Step 5: Restart all CVP services

Cause

The CVP Call Server keystore does not contain the required CSSM certificate chain needed to validate digital signatures from the Cisco Smart Software Manager. During smart licensing operations, CVP attempts to verify the authenticity of licensing communications using certificate-based signature validation. Without the proper CSSM certificates in the Java JCEKS keystore, these signature verification attempts fail, resulting in licensing transaction errors and potential compliance issues.

Related Content

- Cisco Technical Support & Downloads