CCCSP v15 Connecting CCCSP Nodes to SSM

Contents

Issue

When attempting to attempting to connect CCCSP nodes to SSM, users can encounter certificate trust issues, which can prevent successful smart licensing registration. This is related to Cisco Bug ID CSCwv41814, where the Java certificate store requires manual updates to trust the SSM certificate chain.

Environment

- Cisco Contact Center Solution Platform (CCCSP) version 15 (formerly known as CUSP)
- Smart Software Manager (SSM) connectivity required
- SFTP server for certificate file transfers

Resolution

SSM Certificate Trust Issue Resolution (CSCwv41814)

If encountering certificate trust issues when connecting to SSM, follow these steps to resolve the Java certificate store issue.

Step 1: Enable remote account access:

```
utils remote_account enable
```

Step 2: Create remote account for troubleshooting:

```
utils remote_account create ciscotac 2
```

Step 3: Navigate to the Java security directory:

```
cd $JAVA_HOME/jre/lib/security
```

Step 4: Transfer the SSM root and intermediate certificates to the CCCSP system via SFTP:

```
sftp root@X.X.X.X
sftp> get sub-root.cer
sftp> get SSM-Root.cer
sftp> exit

# Check if the certificates are there.

[root@hostname security]# ls -ltr
-rw-r--r--. 1 root root  56050 Aug 17 15:55 java.security
-rw-------. 1 root root   2031 Sep  8 13:43 sub-root.cer
-rw-------. 1 root root   1396 Sep  8 13:43 SSM-Root.cer
```

Step 5: Import the root certificate into the Java keystore:

```
$JAVA_HOME/bin/keytool -storetype JKS -import -alias SSM-Root -keystore $JAVA_HOME/jre/lib/security/cac
```

Step 6: Import the intermediate certificate into the Java keystore:

```
$JAVA_HOME/bin/keytool -storetype JKS -import -alias sub-root -keystore $JAVA_HOME/jre/lib/security/cac
```

Step 7: Reboot the CCCSP system to apply changes.

Cause

The CCCSP v15 CLI limitation exists because the native crypto key certreq command does not provide a documented method to add SAN entries into a CSR. CCCSP v15 uses SAN for TLS peer verification when SAN is present in the certificate; otherwise, the certificate Common Name (CN) is used for verification. The SSM connectivity issue is caused by Cisco Bug ID CSCwv41814, where the Java certificate store on

CCCSP does not automatically trust the SSM certificate chain, requiring manual import of the root and intermediate certificates.

Related Content

- CCCSP 15.0.1 CLI Configuration Guide - Create and Import a Signed Certificate
- Cisco Technical Support & Downloads