# CCCSP v15 CCCSP-knooppunten aansluiten op SSM

## Inhoud

## uitgifte

Wanneer gebruikers proberen CCCSP-knooppunten te verbinden met SSM, kunnen ze problemen met het vertrouwen in certificaten tegenkomen, waardoor een succesvolle registratie van slimme licenties kan worden voorkomen. Dit heeft te maken met Cisco Bug ID CSCwv41814, waarbij de Java-certificaatopslag handmatige updates vereist om de SSM-certificaatketen te vertrouwen.

## milieu

- Cisco Contact Center Solution Platform (CCCSP) versie 15 (voorheen CUSP)
- Smart Software Manager (SSM)-connectiviteit vereist
- SFTP-server voor bestandsoverdrachten van certificaten

## resolutie

### GTM-certificaatvertrouwensprobleemoplossing (CSCwv41814)

Als u problemen ondervindt met het certificaatvertrouwen wanneer u verbinding maakt met SSM, volgt u deze stappen om het probleem met de Java-certificaatopslag op te lossen.

Stap 1: Toegang tot externe account inschakelen:

```
utils remote_account enable
```

Stap 2: Maak een externe account voor het oplossen van problemen:

```
utils remote_account create ciscotac 2
```

Stap 3: Navigeer naar de Java-beveiligingsdirectory:

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

Stap 4: Overdracht van de SSM-root- en intermediaire certificaten naar het CCCSP-systeem 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
```

Stap 5: Importeer het basiscertificaat in de Java keystore:

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

Stap 6: Importeer het tussenliggende certificaat in de Java keystore:

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

Stap 7: Start het CCCSP-systeem opnieuw op om wijzigingen toe te passen.

## Oorzaak

De CCCSP v15 CLI-beperking bestaat omdat de opdracht native crypto key certreq geen gedocumenteerde methode biedt om SAN-items toe te voegen aan een CSR. CCCSP v15 gebruikt SAN voor TLS-peer-verificatie wanneer SAN in het certificaat aanwezig is; anders wordt het certificaat Common Name (CN) gebruikt voor verificatie. Het probleem met de SSM-connectiviteit wordt veroorzaakt door Cisco Bug ID CSCwv41814, waarbij de Java-certificaatopslag op CCCSP niet automatisch de SSM-certificaatketen vertrouwt, waarvoor handmatige import van de root- en intermediaire certificaten vereist is.

## Gerelateerde inhoud

- CCCSP 15.0.1 CLI-configuratiegids - Een ondertekend certificaat maken en importeren
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.