

Probleemoplossing Foutmelding in Unity Connection voor onderhoud

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Fasen om te troubleshooten](#)

[Proces 1](#)

[Proces 2](#)

[Proces 3](#)

[Herstelproces:](#)

[Proces 4](#)

[Omgeving 1](#)

[Oplossing 2](#)

[Workaround 3](#)

[Proces 5](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u een veelvoorkomende foutmelding van Cisco Unity Connection op de onderhoudspagina kunt oplossen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Unity Connection (CUC)
- Certificaatbeheer voor Unified servers

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

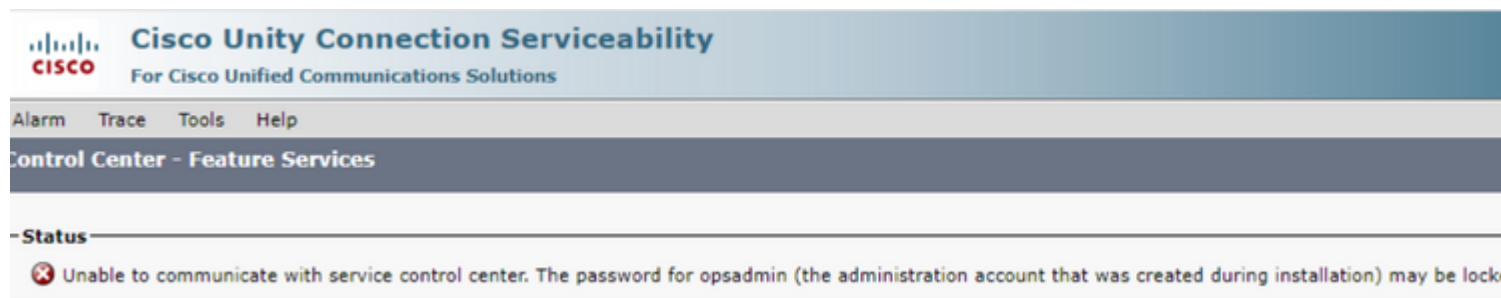
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

In Cisco Unity Connection wanneer een nieuw knooppunt is geïnstalleerd, moeten een gebruiker en

wachtwoord worden toegewezen, wordt deze gebruiker gemaakt en opgeslagen in de Cisco Unity-database.

Deze fout verschijnt om verschillende redenen, en maakt het onmogelijk om de servicemogelijkheden pagina te gebruiken.



Fasen om te troubleshooten

Om het probleem op te lossen, moet u eerst naar de beheerder gaan die werd gemaakt toen Unity werd geïnstalleerd:

Proces 1

Navigeren naar **Cisco Unity Connection Administration > Go > Gebruikers > Selecteer een beheergebruiker > Bewerken > Wachtwoordinstellingen**

Schakel het aanvinkvakje **Vergrendeld door beheerder uit** om de gebruikersaccount te ontgrendelen.

Schakel het aanvinkvakje **Niet verlopen** in om te voorkomen dat het wachtwoord vervalt.

Edit Password Settings (Web Application)

User Edit Refresh Help

Choose Password
 Web Application ▼
 Save

Web Applications Password Settings

Locked by Administrator

User Cannot Change

User Must Change at Next Sign-In

Does Not Expire

Authentication Rule: Recommended Web Application Authentication Rule ▼

Time Last Changed: 7/12/22 10:32 AM

Failed Sign-In Attempts: 0

Time of Last Failed Sign-In Attempt: 6/14/23 5:49 PM

Time Locked by Administrator: [Empty field]

Time Locked Due to Failed Sign-In Attempts: [Empty field]

Unlock Password

Save

Klik op **Wachtwoord** voor **ontgrendelen** > **Opslaan**.

Navigeer naar de pagina Cisco Unity Connection Servicability.

Proces 2

Als het probleem nog kan worden gereproduceerd:

Ga naar **Cisco Unity Connection Administration** > **Go** > **Gebruikers** > **Selecteer de beheerder** > **Bewerken** > **Wachtwoord wijzigen** en voer een nieuw wachtwoord in.

Navigeer naar de pagina Cisco Unity Connection Servicability en controleer of deze toegankelijk is.

Proces 3

Als het probleem zich blijft voordoen:

Navigeer naar **Cisco Unified OS-beheer** > **Ga** > **Beveiliging** > **certificaatbeheer** en controleer of de IPsec- en Tomcat-certificaten niet zijn verlopen.

Als de certificaten zijn verlopen, moeten de certificaten worden geregenereerd.

Herstelproces:

- Zelfondertekend: [Zelfondertekend proces voor certificaatregeneratie](#)
- CA-signed: [CA-getekend proces voor certificaatregeneratie](#)

Proces 4

Als de certificaten CA zijn ondertekend, moet u controleren of Cisco Unity Connection niet overeenkomt met Cisco bug-id [CSCvp31528](#).

Als Unity overeenkomsten heeft, voert u de volgende tijdelijke oplossingen uit:

Omgeving 1

Vraag de CA om het servercertificaat te ondertekenen zonder de kritische uitbreiding van de X509v3 Onderwerpalternatieve Naam en Laat andere extensies ongewijzigd blijven.

Oplossing 2

Vraag de CA om het servercertificaat te ondertekenen en de extensie toe te voegen die naast wordt gespecificeerd om het te laten werken.

X509v3 basisbeperkingen: kritiek

Workaround 3

Gebruik zelfondertekende certificaten, het is niet altijd de juiste oplossing voor iedereen.

Workaround 4

Als een van de laatste beschikbare workarounds, upgrade naar release die de oplossing van het defect bevat en Generate de CSR op vaste release en krijgen het ondertekend door CA zoals het bekend is met het normale proces.

Proces 5

Op CUC CLI:

1. De objectID van de standaardtoepassingsbeheerder ophalen uit de Unity Connection-database.

```
run cuc dbquery unitydirdb select name, value from vw_configuration where name='DefaultAdministrator'
```

Opdrachtoutput:

name	value
-----	-----

DefaultAdministrator XXXX-XXXX-XXXXX-XXXX

2. De alias ophalen die gekoppeld is aan de standaard applicatie beheerder objectID. Vervang bij query het veld objectid='XXXX-XXXX-XXXXX-XXXX' door de waarde in de vorige uitvoer.

```
run cuc dbquery unitydirdb select alias,objectid from vw_user where objectid='XXXX-XXXX-XXXXX-XXXX'
```

Opdrachtoutput:

```
alias  objectid
-----
admin  XXXX-XXXX-XXXXX-XXXX
```

3. Bevestig dat het coderingstype 4 is voor webverificatie voor de standaardgebruiker van de toepassingsbeheerder (Credentialtype 3 is voor het wachtwoord van de webtoepassing).

```
run cuc dbquery unitydirdb select objectid, userobjectid, credentialtype, encryptiontype from tbl_creden
```

Opdrachtoutput:

objectid	userobjectid	credentialtype	encryptiontype
ZZZZZ-ZZZZZ-ZZZZZ-ZZZZZ	XXXX-XXXX-XXXXX-XXXX	3	4
TTTTT-TTTTT-TTTTT-TTTTT	XXXX-XXXX-XXXXX-XXXX	4	3

Als encryptie type = 3, verander in 4.

```
run cuc dbquery unitydirdb update tbl_credential set encryptiontype = "4" where objectid = "ZZZZZ-ZZZZZ-
```

5. Wachtwoord moet worden gewijzigd omdat met het oude wachtwoord de gebruiker is versleuteld met

type 3

```
utils cuc reset password <accountalias>
```

6. Start Tomcat opnieuw via CLI

```
utils service restart Cisco Tomcat
```

Controleer of de onderhoudspagina toegankelijk is.

Als het probleem blijft bestaan, verzamel dan CUC Tomcat-logs van RTMT.

Dit doet u zo:

1. Open RTMT.
2. Plaats Cisco Unity Connection IP/Hostname.
3. Plaats de gebruiker en het wachtwoord.
4. Dubbelklik **op Bestanden verzamelen**. Het venster Bestanden verzamelen wordt geopend om UCM-services/toepassingen te selecteren.
5. In Selecteer UCM-services/toepassingen klikt u op het aanvinkvakje in de kolom Alle servers voor:
 - Cisco Tomcat

Gerelateerde informatie

- [Cisco technische ondersteuning 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.