

Configureer de orkestratie voor UCS

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Versievereisten](#)

[Overzicht](#)

[Stappen voor installatie en configuratie](#)

[Stap 1. Genereer de Artifactory API-toets](#)

[Stap 2. De Artifactory URL en API-toets op Cloud Connect configureren](#)

[Stap 3. Onboard VOS-knooppunten voor orkestratie en controle knooppunt](#)

[Stap 4: Aan boord van Windows-knooppunten voor orkestratie en controle knooppunt](#)

[Stap 5: update het bestand inventaris.conf](#)

[Stap 6: valideren van onboard knooppunten voor orkestratie](#)

Inleiding

Dit document beschrijft de stappen voor het configureren van contactcenters voor ondernemingsorkestratie.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Unified Contact Center Enterprise (UCS) 12.x
- Packaged Contact Center Enterprise (PCCE) 12.x
- Cisco Voice Portal (CVP) 12.x
- Finesse 12.x
- Cisco Unified Intelligence Center (CUIC) 12.x
- Virtual Voice Browser (VVB) 12.x

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- Cloud Connect 12.6(1) ES3
- UCS 12.5(1)
- Finesse 12.5(1)
- CUIC 12.5(1)
- CVP 12.5(1)
- VVB 12,5(1)

Opmerking: In het gehele document verwijst CUIC naar zowel gelijktijdige installatie van CUIC, Live Data (LD) en Identity Server (IDS). Alleen wanneer een instructie specifiek is voor een subcomponent, wordt naar die component verwezen.

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.

Versievereisten

UCCE/PCCE 12.5(1) (ofwel)

- ES66 (ES55 is een verplichte installatie voorafgaand aan de installatie van ES66)
- UCS 12.5(2) MR

UCS/PCE 12.6(1)

- Geen extra vereisten

Cloud Connect versie: 12.6(1)

- ES3

Finesse, CUIC, VVB: 12.5(1)

- `ucos.orchestration.enable-12.5.1.cop.sgn`
- `ucos.keymanagement.cop.sgn`

Finesse, CUIC, VVB: 12.6(1)

- `ucos.keymanagement.cop.sgn`

CVP 12.5(1)

- ES23

CVP 12.6(1)

- Geen extra vereisten

Speciale opmerkingen voor Cloud Connect-upgrades.

Opmerking: wanneer u Cloud Connect van 12.5 naar 12.6 upgraden, is het verplicht om eerst `ucos.keymanagement.cop.sgn` te installeren. Upgrade mislukt als dit niet is gebeurd.

Opmerking: wanneer u Cloud Connect van 12.5 naar 12.6 upgradt, is het verplicht om de schijf te verhogen van 146GB naar 246GB. Als deze stap voor de upgrade niet is uitgevoerd, voert u de volgende stappen uit:

Stap 1: Stop de Cloud Connect-server.

Stap 2: Breid de schijf in vSphere uit naar 246GB.

Stap 3: Start de Cloud Connect-server.

VOS breidt de partities automatisch uit. Dit zorgt ervoor dat de gedownloade updates geen uit ruimtevoorwaarde op de gemeenschappelijke verdeling veroorzaken.

Overzicht

CCE Orchestration wordt vanaf Cloud Connect 12.6(1) ondersteund.

Cloud Connect-serverversie 12.6 (1) ondersteunt orkestratie in deze scenario's:

- CCE 12.5 ES/COP en Windows Updates kunnen worden georkestreerd vanaf 12.6 Cloud Connect server
- CCE 12.5 tot 12.6 software upgrade kan worden georkestreerd vanaf 12.6 Cloud Connect server

Stappen voor installatie en configuratie

Stap 1. Genereer de Artifactory API-toets

1. Login aan <https://devhub-download.cisco.com/console/> met uw Naam en Wachtwoord van de Gebruiker van CCO.
2. Selecteer de optie Download sleutel beheren op de consolepagina zoals in de afbeelding.



Dev Hub Console

Welcome to the console for **devhub-download.cisco.com**.

Dev Hub Download enables API-driven distribution of Cisco software.

Usage Instructions

- Generate a Download Key via the **Manage Download Key** page.
- Use your **Email Address** and the **Download Key** from this page as credentials with devhub-download.cisco.com APIs.
- You must log into devhub-download.cisco.com/console once every **6 months** to the Download Key.

3. Klik op Generate Key optie om de API-toets te genereren. De optie om de sleutel te bekijken en in te trekken is beschikbaar in de pagina Downloadsleutel beheren.




Dev Hub Download


Manage Download Key

Use the key below to authenticate to **devhub-download.cisco.com** repositories to r

Download Key

.....

 Generate Key

 Revoke Key

4. Selecteer de knop Kopiëren om de API-toets naar het klembord te kopiëren.

Opmerking: het is verplicht dat de CCO-id die wordt gebruikt om API-sleutels te genereren, over de nodige software-upgraderechten beschikt. De CCO-id die u gebruikt, moet een geldig SSS- (servicecontract) of Flex-abonnement hebben om de benodigde rechten te hebben.

Opmerking: u dient zich eens in de zes maanden in te loggen op <https://devhub-download.cisco.com/console> om de geldigheid van de API-sleutel te verlengen.

Stap 2. De Artifactory URL en API-toets op Cloud Connect configureren

- Cisco host alle software-artefacten in een cloudgebaseerde artefactorij die wordt gebruikt door Cloud Connect-server om nieuwe updates te downloaden en te melden.
- Cloud Connect-server moet worden geconfigureerd met Cisco gehoste software Artifactory URL, naam van opslagplaats en API-sleutel.

1. Start de opdracht, **maakt gebruik van de Image Repository ingesteld** om artefactdownload te configureren zoals getoond in de afbeelding.

```
admin:
admin:utils image-repository set
Please Enter Artifactory URL:https://devhub-download.cisco.com/binaries
Please Enter Artifactory Repository Name [ent-platform-release-external]:
Please Enter API Key:*****

CCO ID used to generate API key has access to export restricted and unrestricted software, select 'yes' to download export restricted software (yes/no): yes

Configuration settings has been saved and connection to artifactory is successful.
Artifacts required for orchestration will be downloaded locally to the Cloud Connect at 2 AM server time. Cloud connect server can be restarted, download starts 10 minutes post restart. Usage of orchestration related CLI are blocked during download, and this duration depends on the size of the artifacts.
admin:
```

- a. Geef de artefactorale URL op: <https://devhub-download.cisco.com/binaries>.
 - b. Geef de naam van de artefactoropslagplaats, net-platform-release-extern.
 - c. Plakt de API-toets die u hebt gegenereerd. De API-sleutel wordt om veiligheidsredenen als sterretjes weergegeven.
2. Voer de opdracht uit, **maakt gebruik van image-repository tonen** om de geconfigureerde Artifactory URL, naam van de repository en API-sleutel in de Cloud Connect-server te bekijken zoals in de afbeelding.

```
admin:
admin:utils image-repository show
Artifactory URL: https://devhub-download.cisco.com/binaries
Artifactory Repository Name: ent-platform-release-external
Artifactory API Key: ****W28W
admin:
```

Opmerking: Voordat de opdracht **Image Repository set** op de CLI wordt uitgevoerd, navigeer u naar de **EULA URL** (<https://software.cisco.com/download/eula>) en accepteer de EULA. Als dit niet gebeurt, mislukt de opdracht **image-repository instellen** met fout: *CCO-id gebruikt om API-sleutel te genereren is niet conform de Gebruiksrechtovereenkomst, gebruik dan een geldige CCO-id.* Zie Cisco bug-id [CSC78680](https://tools.cisco.com/bugcenter/bug/?bugID=CSC78680) voor meer informatie.



Products & Services

Support

How to Buy

Training & Events

Cisco's End User Software License Agreement

In order to download software, Please confirm that you have read and agree to be bound by the [Cisco End User License Agreement and any Supplemental Terms](#), if applicable.

Accept License Agreement

Decline

Opmerking: beide opdrachten kunnen alleen worden uitgevoerd vanuit de uitgeversknooppunt van de Cloud Connect-server.

De replicatie van de configuratie van de beeldopslagplaats gebeurt automatisch van de uitgeversknooppunt naar de abonneeknooppunt wanneer de **optie image-repository set** commando wordt uitgevoerd met succesvolle resultaten op de uitgeversknooppunt.

Opmerking: de **afbeeldingsopslagplaats set** CLI kan op elk moment worden gebruikt om de export beperkte versus onbeperkte software optie in de implementatie te wijzigen. Start de Cloud Connect-server opnieuw om de opschonen en downloaden van beperkte vs onbeperkte software af te dwingen. Download start 10 minuten na het opnieuw opstarten.

Toelichting: Toelichting op artefactoperaties:

Na een succesvolle configuratie van artefactgegevens worden artefacten lokaal gedownload naar de Cloud Connect-server op 02:00 A.M. servertijd.

Orchestratiebewerkingen, zoals installatie van patches, terugdraaien of upgrades, kunnen alleen worden uitgevoerd nadat de artefacten zijn gedownload.

Als de artefacten direct na de configuratiestappen moeten worden gedownload, kan de Cloud Connect-server opnieuw worden opgestart en begint de download 10 minuten na het opnieuw opstarten.

Het gebruik van orkestratie gerelateerde CLI-opdrachten wordt geblokkeerd bij het starten van de download en deze duur is afhankelijk van het aantal te downloaden artefacten.

Opmerking: als de Cloud Connect-server een proxy nodig heeft voor toegang tot internet, dan moet ES3 of hoger worden geïnstalleerd. Zie de Installatie- en upgrade-handleiding voor UCS voor meer informatie over proxyconfiguratie.

Stap 3. Onboard VOS-knooppunten voor orkestratie en controle knooppunt

Voorwaarden:

- Controleer of aan alle vereisten voor de systeemversie is voldaan.
- Importeer de certificaten van de Cloud Connect-cluster (Pub en Sub) in het tomcat-trust op alle doelVOS-servers (tomcat voor zelfondertekend en root/tussenpersoon voor CA-ondertekend)

Aan boord van elk Finesse, CUIC, VVB, IDS, LD-systeem naar een Cloud Connect-server, voer de opdracht uit, **maakt gebruik van het systeem aan boord** vanaf de uitgeversknooppunt van de respectieve VOS-cluster zoals getoond in de afbeelding.

```
admin:
admin:utils system onboard initiate
You can onboard a cluster to a Cloud Connect node. Enter the details of the Cloud Connect node.
Cloud Connect FQDN:cloudconnect1.dcloud.cisco.com
Cloud Connect Application User:appadmin
Cloud Connect Application User's Password:*****
The cluster has been successfully onboarded.
admin:
```

1. Verstrek FQDN van de de uitgeversknoop van Cloud Connect.
2. Geef de gebruikersnaam voor de toepassing op voor de Cloud Connect-server.
3. Geef het gebruikerswachtwoord van de toepassing op de Cloud Connect-server op.
 - De uitgeversknooppunt van de Cloud Connect-server moet online zijn wanneer de on-board initiatie

wordt uitgevoerd vanaf de VOS-knooppunt.

- Wanneer de on-board initiatie wordt uitgevoerd vanaf de VOS-knooppunt, moet FQDN van de Cloud Connect-uitgeversserver worden gebruikt.
- **Het gebruikssysteem aan boord** moet op alle VOS-uitgevers (Finesse, CUIC, LD, IDs, alle VVB's) worden uitgevoerd

Opmerking: Als het systeem (cluster) onboards op de Cloud Connect-server met partiële fout, controleer dan de reden voor de fout en corrigeer deze. Voer vervolgens de **updateopdracht van het utils-systeem aan boord** uit in plaats van de **opdracht** initiëren van het **utils-systeem aan boord**.

Opmerking: Onboard is alleen toegestaan wanneer zowel de uitgever als de abonneeknooppunten in de Cloud Connect-server bereikbaar zijn.

Opmerking: Als de Cloud Connect-server beschadigd is en opnieuw wordt ingezet met een nieuwe installatie, moet de beheerder het **utils-systeem aan boord** uitvoeren om uit de VOS-knooppunt te **verwijderen** en vervolgens het **utils-systeem aan boord** uitvoeren om weer aan boord van de VOS-knooppunten te **komen**.

Opmerking: Om de gebruikersnaam voor de toepassing Cloud Connect Servers te verifiëren/vinden, voert u de opdracht **run sql select * uit applicationuser** op de Cloud Connect Servers' CLI uit.

Stap 4: Aan boord van Windows-knooppunten voor orkestratie en controle knooppunt

Het ingebouwde proces helpt een verbinding zonder wachtwoord tot stand te brengen tussen de Cloud Connect-knooppunt en de Windows-knooppunten. Voer de volgende stappen uit om de op Windows gebaseerde knooppunten voor de Orchestration-besturingsknooppunt te activeren:

Openbare SSH-toets op de Windows-knooppunten configureren:

- a. Navigeer naar `%Gebruikers%\ en maak een bestand met geautoriseerde_toetsen als het niet bestaat. (Het extensie type geautoriseerde_keys is File en kan niet worden aangepast)`

Opmerking: de gebruiker mag niet uit het systeem worden verwijderd en moet een domeingebruiker zijn met domeinbeheerder of lokale beheerrechten.

- b. Open de browser en voer de **Cloud Connect-uitgever URL in:**
`https://<CloudConnectIP>:8445/inventaris/controleknooppunt/sleutel`

- c. Verstrek uw Cloud Connect-gebruikersreferenties. Na succesvolle verificatie haalt een REST API-respons de Cloud Connect Public SSH-sleutel.

- d. Kopieer deze openbare toetswaarde naar het geautoriseerde_keys-bestand in `%Gebruikers%\.`

Er wordt een voorbeeld weergegeven van de uitvoer van de URL. Kopieer in het uitvoerdocument alleen het gedeelte dat begint met **ssh-rsa** en eindigt met **root@localhost** naar het geautoriseerde_keys bestand.

```
{"category": "PUBLISHER", "hostName": "cc125clouda.uclabservices.com", "publicKey": "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDfJD17RUZ/Umdflp5r3IqMaoV8WSrr7iLB0WindC0lGeGPYkprVW2xq6H6I8F
```

Het bestand `authorised_keys` bij het voorbeeld wordt weergegeven.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDfJD17RUZ/Umdflp5r3IqMaoV8WSrr7iLB0WindC0lGeGPYkprVW2xq6H6I8F
```

e. Herhaal stap b, c en d om de openbare sleutel van Cloud Connect Subscriber op te halen (als Cloud Connect een HA-instelling is).

Opmerking: de Cloud Connect-uitgever en de abonnee openbare sleutels moeten worden gekopieerd naar één `geautoriseerd_keys`-bestand. De uitgever en de abonnee-vermeldingen moeten in aparte regels staan en mogen geen extra ruimte, komma's of speciale tekens aan het einde van de regel gebruiken.

f. Start de OpenSSH-services opnieuw:
- **OpenSSH-server**
- **OpenSSH-verificatieagent**

Probleemoplossing voor de SSH-aanmelding met deze stappen:

- Navigeer naar **C:\ProgramData\ssh** en open het bestand `sshd_config` in een teksteditor.
- Zoek de sectie van dit bestand die begint met **# Vastlegging**
- Niet-commentaar bij zowel de `SyslogFacility`- als de `LogLevel`-lijnen.
- Verander de `SyslogFacility` in `LOCAL0` en de `LogLevel` te `DEBUG` zoals in het voorbeeld

```
# Logging
SyslogFacility LOCAL0
LogLevel DEBUG
```

- Sla het bestand `sshd_config` op en start de service **OpenSSH SSH Server** opnieuw.
- Het logbestand wordt geschreven naar **C:\ProgramData\ssh\logs\sshd.log**

Stap 5: update het bestand `inventaris.conf`

- Voer de opdracht uit, **maakt gebruik van `systeminventaris export`** om de inventaris te uploaden naar een SFTP server zoals in de afbeelding.


```
admin:utils
admin:utils system inventory export
You can export an inventory to a SFTP server location. Enter the details of the SFTP server
SFTP Server:10.128.157.150
SFTP User:johndoe
SFTP User's Password:*****
SFTP Directory:/voice/ipcc/Enterprise/Orchestration

Inventory successfully exported.
admin:
```

- a. Geef het IP-adres of FQDN van een SFTP-server op.
- b. Geef de gebruikersnaam op die lees-/schrijftoegang heeft tot de SFTP-server.
- c. Voer het wachtwoord in voor de gebruiker.
- d. Geef de directory op om het inventarisbestand in UNIX/Linux-indeling te schrijven.

Voorbeeld: /voice/IPCC/Enterprise/Orchestration

2. Bewerk de inventaris om de VOS- en Windows-componenten op te nemen.

- De syntaxis, uitlijning en inspringing moeten exact hetzelfde zijn als in het inventarisbestand.
- CRLF-lijnuiteinden moeten UNIX-Style zijn. Daarom kan een Linux-gebaseerde of een Mac OS-gebaseerde editor worden gebruikt om het Windows-inventarisbestand te maken. Een programma als Notepad++ kan ook worden gebruikt.
- De namen van de componenten, zoals CVPREPORT, ROgger, PG, enzovoort, moeten in hoofdletters zijn.

Opmerking: Het bestand inventaris.conf is gevoelig voor inkepingen, raadpleeg/gebruik afbeeldingen en voorbeeld configuratiebestanden

Hier kunnen voorbeeldbestanden met de juiste indeling worden gedownload:

<https://github.com/CXCCSummit/Repository>

Het voorbeeld van de VOS-server wordt in de afbeelding getoond:

```

CUIC: {}
CUIC_LiveData_IdS:
  CUIC_LiveData_IdS-Cluster-1:
    hosts:
      - name: "125cuicpub"
        side: "A"
        type: "Publisher"
      - name: "125cuicsub"
        side: "B"
        type: "Subscriber"
Finesse:
  Finesse-Cluster-1:
    hosts:
      - name: "125finpub"
        side: "A"
        type: "Publisher"
      - name: "125finsub"
        side: "B"
        type: "Subscriber"
IdS: {}
LiveData: {}
VVB:
  VVB-Cluster-1:
    hosts:
      - name: "125vvb1"
        side: "A"
        type: "Publisher"
  VVB-Cluster-2:
    hosts:
      - name: "125vvb2"
        side: "B"
        type: "Publisher"

```

Het voorbeeld van Windows Server wordt in de afbeelding getoond:

```

Windows:
CVFGAMP: {}
CVFPREPORTING: {}
CVFSEVER:
  CVFCALLSERVER:
    hosts:
      - name: "125scvp1"
        side: "A"
        user: "administrator@domain.local"
      - name: "125scvp2"
        side: "B"
        user: "administrator@domain.local"
  DISTRIBUTOR:
    AM-HDS-DDS1:
      hosts:
        - name: "125awhdsa"
          side: "A"
          user: "administrator@domain.local"
    AM-HDS-DDS2:
      hosts:
        - name: "125awhdsb"
          side: "B"
          user: "administrator@domain.local"
  LOGGER: {}
  PG1:
    hosts:
      - name: "125pga"
        side: "A"
        user: "administrator@domain.local"
      - name: "125pgb"
        side: "B"
        user: "administrator@domain.local"
  ROgger:
    ROgger1:
      hosts:
        - name: "125rgra"
          side: "A"
          user: "administrator@domain.local"
        - name: "125rgrb"
          side: "B"
          user: "administrator@domain.local"
  ROUTER: {}

```

3. Bewerk de strings in het inventarisbestand, zoals vereist.

placementName: Geef een unieke naam voor de inzet.

- Deze naam wordt weergegeven in de onderwerpregel van het e-mailbericht. Als het niet is geconfigureerd, bevat de onderwerpregel van het e-mailbericht alleen het type procedure en de

algemene status.

placementType: Dit veld wordt gebruikt voor compatibiliteitscontrole in de upgrade-, terugdraai- of switch-doorstuurprocedures.

```
-----  
deploymentName: "UnifiedCCE"  
deploymentType: "UCCE-2000-Agents"
```

De ondersteunde implementatietypen zijn:

- UCS E-2000-A agents
- UCS E-4000-A agents
- PCE-2000-A agents
- PCE-4000-A agents
- HCS-CC-2000-A agents
- HCS-CC-4000-X agents

Opmerking: bekijk deze opmerkingen over de ondersteunde implementatietypen. Orchestratie wordt niet ondersteund voor 12000-, 24000- en 26000-agent implementatiemodellen. Het implementatiemodel van HCS-SCC (Small Contact Center) wordt momenteel niet ondersteund voor Orchestratie. Zorg ervoor dat de waarden die in dit veld worden ingevoerd, overeenkomen met de ondersteunde indeling voor implementatietypen. Het implementatietype is hoofdlettergevoelig.

Opmerking: de beheerder kan de standaardwaarden, indien nodig, bijwerken of bewerken op basis van het type implementatie en de voorkeursnaam van de implementatie.

4. Voer de opdracht uit, **maakt gebruik van systeeminventaris importeren** op de Cloud Connect-uitgeversknooppunt om de bijgewerkte inventaris te importeren van de SFTP-server zoals in de afbeelding wordt getoond.

```
admin:  
admin:utils system inventory import  
You can import an inventory from SFTP server location. Enter the details of the SFTP server  
SFTP Server:10.128.10.1:11  
SFTP User:johndoe  
SFTP User's Password:*****  
SFTP Directory:/voice/ipcc/Enterprise/Orchestration  
  
Import will replace the existing inventory config. Do you want to continue(yes/no): yes  
Inventory successfully imported. Components in the deployment will be validated as part of 1  
Please use "file get activelog ansible/component_cache_update.log" command to check the log f  
admin:
```

- Geef het IP-adres of FQDN van een SFTP-server op.
- Geef de gebruikersnaam op die lees-/schrijftoegang heeft tot de SFTP-server.
- Voer het wachtwoord in voor de gebruiker.
- Geef de directory op om het inventarisbestand in UNIX/Linux-indeling te schrijven.

Voorbeeld: /voice/IPCC/Enterprise/Orchestration

e. Antwoord "ja" om toe te staan dat het nieuwe inventarisbestand de huidige inventaris vervangt.

Stap 6: valideren van onboard knooppunten voor orkestratie

Om de VOS- en Windows-knooppunten te valideren, is met succes aan boord gegaan en om te controleren of de Orchestration-functie klaar is voor gebruik, voert u de opdracht uit, **maakt u gebruik van een testverbinding voor de implementatie** zoals in de afbeelding wordt getoond.

```
admin:
admin:utils deployment test-connection

Select the option:

1) VOS
2) Windows
q) quit

Please select an option (1 - 2 or "q" ): 1
Select the option:

1) CUIC_LiveData_IdS
2) Finesse
3) VVB
p) previous
q) quit

Please select an option (1 - 3, "p" or "q" ): 1
Select the option:

1) CUIC_LiveData_IdS-Cluster-1
2) Side A CUIC_LiveData_IdS nodes in the inventory
3) Side B CUIC_LiveData_IdS nodes in the inventory
4) All CUIC_LiveData_IdS nodes in the inventory
p) previous
q) quit

Please select an option (1 - 4, "p" or "q" ): 4

Do you want to test_connection on All the nodes of CUIC_LiveData_IdS ('yes' or 'no'): yes
Checking on selected hosts...

Test connection successful for below nodes:
125cuicpub
125cuicsub

admin:
```

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.