

Configuración de la orquestación para UCCE

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Requisitos de versión](#)

[Overview](#)

[Pasos de configuración](#)

[Paso 1. Generación de la clave API artificial](#)

[Paso 2. Configuración de la URL artificial y la clave de API en Cloud Connect](#)

[Paso 3. Nodos VOS integrados a nodo de control de orquestación](#)

[Paso 4: Incorporación de nodos de Windows al nodo de control de orquestación](#)

[Paso 5: Actualice el archivo Inventory.conf](#)

[Paso 6: Validar nodos incorporados para la orquestación](#)

Introducción

Este documento describe los pasos para configurar Contact Center Enterprise Orchestration.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Unified Contact Center Enterprise (UCCE) 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 (VB) 12.x

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Conexión a la nube 12.6(1) ES3
- UCCE 12.5(1)
- Finesse 12.5(1)
- CUIC 12.5(1)
- CVP 12.5(1)
- VB 12.5(1)

Nota: En todo el documento, CUIC hace referencia tanto a instalaciones de co-residentes como a instalaciones independientes de CUIC, Live Data (LD) e Identity Server (IDS). Sólo cuando una instrucción es específica de un subcomponente, se hace referencia a ese componente.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Requisitos de versión

UCCE/PCCE 12.5(1) (ya sea)

- ES66 (ES55 es una instalación obligatoria antes de la instalación de ES66)
- UCCE 12.5(2) MR

UCCE/PCCE 12.6(1)

- Sin requisitos adicionales

Cloud Connect Versión: 12.6(1)

- ES3

Finesse, CUIIC y VB: 12.5(1)

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

Finesse, CUIIC y VVB: 12.6(1)

- `ucos.keymanagement.cop.sgn`

CVP 12.5(1)

- ES23

CVP 12.6(1)

- Sin requisitos adicionales

Notas especiales para las actualizaciones de Cloud Connect.

Nota: al actualizar Cloud Connect de 12.5 a 12.6, es obligatorio instalar primero `ucos.keymanagement.cop.sgn`. La actualización falla si no se realiza.

Nota: al actualizar Cloud Connect de 12.5 a 12.6, es obligatorio aumentar el disco de 146 GB a 246 GB. Si este paso se ha omitido antes de la actualización, siga estos pasos:

Paso 1: Detenga el servidor de Cloud Connect.

Paso 2: Amplíe el disco de vSphere a 246 GB.

Paso 3: Inicie el servidor de Cloud Connect.

VOS expande las particiones automáticamente. Esto garantiza que las actualizaciones descargadas no causen una condición de falta de espacio en la partición común.

Overview

CCE Orchestration es compatible a partir de Cloud Connect 12.6(1).

El servidor Cloud Connect versión 12.6 (1) admite la orquestación en los siguientes escenarios:

- CCE 12.5 ES/COP y las actualizaciones de Windows se pueden organizar desde el servidor 12.6 Cloud Connect
- La actualización de software de CCE 12.5 a 12.6 se puede organizar desde el servidor 12.6 Cloud Connect

Pasos de configuración

Paso 1. Generación de la clave API artificial

1. Inicie sesión en <https://devhub-download.cisco.com/console/> con su nombre de usuario y contraseña de CCO.
2. Seleccione Administrar clave de descarga en la página de la consola, como se muestra en la imagen.



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. Haga clic en la opción Generate Key (Generar clave) para generar la clave API. La opción Ver y revocar clave está disponible en la página Administrar clave de descarga.




Dev Hub Download


Manage Download Key

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

Download Key

.....

 Generate Key

 Revoke Key

4. Seleccione el botón Copiar para copiar la clave de la API en el portapapeles.

Nota: es obligatorio que la ID de CCO utilizada para generar claves de API tenga los derechos de actualización de software necesarios. La ID de CCO que utilice debe tener una suscripción SWSS (contrato de servicio) o Flex válida para tener los derechos necesarios.

Nota: Debe iniciar sesión en <https://devhub-download.cisco.com/console> una vez cada seis meses para ampliar la validez de la clave de la API.

Paso 2. Configuración de la URL artificial y la clave de API en Cloud Connect

- Cisco aloja todos los artefactos de software en un artefacto basado en la nube que utiliza el servidor de Cloud Connect para descargar y notificar nuevas actualizaciones.
- El servidor de Cloud Connect debe configurarse con la URL artificial del software alojado de Cisco, el nombre del repositorio y la clave de la API.

1. Ejecute el comando, *utils image-repository set* para configurar la descarga artificial como se muestra en la imagen.

```
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 artifacts.
admin:
```

- a. Proporcione la URL artificial, <https://devhub-download.cisco.com/binaries>.
- b. Proporcione el nombre del repositorio artificial, ent-platform-release-external.
- c. Pegue la clave de API que ha generado. La clave API se muestra como asteriscos por motivos de seguridad.

2. Ejecute el comando, **utils image-repository show** para ver la URL artificial, el nombre del repositorio y la clave de API configurados en el servidor de Cloud Connect, como se muestra en la imagen.

```
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:
```

Nota: Antes de ejecutar el comando **utils image-repository set** en la CLI, navegue hasta la **URL de EULA** (<https://software.cisco.com/download/eula>) y acepte el EULA. Si esto no se realiza, el comando **utils image-repository set** falla con el error: *ID de CCO utilizada para generar la clave de API no cumple con el Acuerdo de licencia del usuario final, utilice una ID de CCO válida.* Consulte Cisco bug ID [CSCvy78680](https://tools.cisco.com/bugcenter/bug/?bugID=CSCvy78680) para obtener más información.



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 terms of the [Cisco End User License Agreement and any Supplemental Terms](#), if applicable.

Accept License Agreement

Decline

Nota: estos dos comandos solo se pueden ejecutar desde el nodo de editor del servidor de Cloud Connect.

La replicación de la configuración del repositorio de imágenes se produce automáticamente desde el nodo del editor al nodo del suscriptor cuando se ejecuta el comando **utils image-repository set** con resultados satisfactorios en el nodo del editor.

Nota: La CLI **utils image-repository set** se puede utilizar en cualquier momento para cambiar la opción de exportación de software restringido frente a no restringido en la implementación. Reinicie el servidor de Cloud Connect para aplicar la limpieza y la descarga del software restringido frente al no restringido. La descarga comienza 10 minutos después del reinicio.

Nota: Notas sobre operaciones artificiales:

Tras la correcta configuración de los detalles de los artefactos, estos se descargan localmente en el servidor de Cloud Connect a las 02:00 a.m., hora del servidor.

Las operaciones de orquestación, como la instalación de parches, la reversión o la actualización, solo se pueden realizar después de descargar los artefactos.

Si los artefactos tienen que descargarse inmediatamente después de los pasos de configuración, el servidor de Cloud Connect se puede reiniciar y la descarga comienza 10 minutos después del reinicio.

El uso de los comandos CLI relacionados con la orquestación se bloquean cuando se inicia la descarga y esta duración depende del número de artefactos que se van a descargar.

Nota: si el servidor de Cloud Connect requiere un proxy para acceder a Internet, se debe instalar ES3 o superior. Consulte la Guía de instalación y actualización de UCCE para obtener más información sobre la configuración de proxy.

Paso 3. Nodos VOS integrados a nodo de control de orquestación

Requisitos previos:

- Asegúrese de que se cumplen todos los requisitos de la versión del sistema.
- Importe los certificados del clúster de Cloud Connect (Pub y Sub) en tomcat-trust en todos los servidores VOS de destino (tomcat para autofirmado y root/intermedio para CA-firmado)

Para incorporar cada sistema Finesse, CUIC, VVB, IDS y LD a un servidor de Cloud Connect, ejecute el comando, **utils system onboard begin** desde el nodo de editor del clúster VOS respectivo, como se muestra en la imagen.

```
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. Proporcione el FQDN del nodo del editor de Cloud Connect.
 2. Proporcione el nombre de usuario de la aplicación para el servidor de Cloud Connect.
 3. Proporcione la contraseña de usuario de la aplicación para el servidor de Cloud Connect.
- El nodo de editor del servidor de Cloud Connect debe estar en línea cuando el inicio incorporado se ejecuta desde el nodo VOS.

- Cuando el inicio incorporado se ejecuta desde el nodo VOS, se debe utilizar el FQDN del servidor editor de Cloud Connect.
- El comando **utils system onboard begin** se debe ejecutar en todos los VOS Publishers (Finesse, CUIC, LD, IdS, todos los VVB)

Nota: si el sistema (clúster) se incorpora al servidor de Cloud Connect con un error parcial, compruebe el motivo del error y corríjalo. A continuación, ejecute el comando **utils system onboard update** en lugar del comando **utils system onboard begin**.

Nota: La incorporación solo se permite cuando los nodos de editor y suscriptor del servidor de Cloud Connect son accesibles.

Nota: Si el servidor de Cloud Connect está dañado y se vuelve a implementar con una instalación nueva, el administrador tiene que ejecutar **utils system onboard remove** del nodo VOS y luego ejecutar **utils system onboard begin** para incorporar los nodos VOS nuevamente.

Nota: para verificar/encontrar el nombre de usuario de la aplicación de Cloud Connect Servers, ejecute el comando **run sql select * from application user** en la CLI de Cloud Connect Servers.

Paso 4: Incorporación de nodos de Windows al nodo de control de orquestación

El proceso integrado ayuda a establecer una conexión sin contraseña entre el nodo de Cloud Connect y los nodos de Windows. Para incorporar los nodos basados en Windows al nodo de control de orquestación, siga estos pasos:

Configure la clave pública SSH en los nodos de Windows:

- a. Navegue hasta `%Users%\<logonUser>\.ssh\` y cree un archivo **authorized_keys**, si no existe. (El tipo de extensión `authorized_keys` es `File` y no se puede modificar)

Nota: el usuario no debe eliminarse del sistema y debe ser un usuario de dominio con privilegios de administrador de dominio o de administración local.

- b. Abra el navegador e introduzca la **URL del editor de Cloud Connect:**
`https://<CloudConnectIP>:8445/Inventory/ControlNode/Key`

- c. Proporcione las credenciales de usuario de la aplicación Cloud Connect. Una vez que la autenticación es satisfactoria, una respuesta de la API REST obtiene la clave SSH pública de conexión a la nube.

- d. Copie este valor de clave pública en el archivo `authorized_keys` en `%Users%\<logonUser>\.ssh\`.

Se muestra un ejemplo del resultado de la URL. En la salida, copie solamente la parte que comienza con **ssh-rsa** y termina con **root@localhost** en el archivo `authorized_keys`.

```
{"category": "PUBLISHER", "hostName": "cc125clouda.uclabservices.com", "publicKey": "ssh-rsa AAAAB3NzaC1y
```

Se muestra el archivo `authorized_keys` para el ejemplo.

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

e. Repita los pasos b, c y d para obtener la clave pública del suscriptor de Cloud Connect (si la conexión a la nube está configurada como HA).

Nota: las claves públicas de editor y suscriptor de Cloud Connect deben copiarse en un único archivo `authorized_keys`. Las entradas de editor y suscriptor deben estar en líneas separadas y no deben utilizar espacios adicionales, comas ni caracteres especiales al final de la línea.

f. Reinicie los servicios de OpenSSH:

- **Servidor SSH de OpenSSH**
- **Agente de autenticación OpenSSH**

Solucione el problema de inicio de sesión SSH con estos pasos:

- Navegue hasta `C:\ProgramData\ssh` y abra el archivo `sshd_config` en un editor de texto.
- Localice la sección de este archivo que comienza por `# Logging`
- Quite los comentarios de las líneas `SyslogFacility` y `LogLevel`.
- Cambie `SyslogFacility` a `LOCAL0` y `LogLevel` a `DEBUG`, como se muestra en el ejemplo

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

e. Guarde el archivo `sshd_config` y reinicie el servicio **OpenSSH SSH Server**.

f. El archivo de registro se escribe en `C:\ProgramData\ssh\logs\sshd.log`

Paso 5: Actualice el archivo `Inventory.conf`

1. Ejecute el comando, `utils system Inventory export` para cargar el inventario en un servidor SFTP como se muestra en la imagen.


```
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. Proporcione la dirección IP o FQDN de un servidor SFTP.
- b. Proporcione el nombre de usuario que tiene acceso de lectura y escritura al servidor SFTP.
- c. Proporcione la contraseña para el usuario.
- d. Proporcione el directorio para escribir el archivo de inventario en formato UNIX/Linux.

Ejemplo: /voice/ipcc/Enterprise/Orchestration

2. Edite el inventario para incluir los componentes VOS y Windows.

- La sintaxis, la alineación y la sangría deben ser exactamente iguales que en el archivo de inventario.
- Los extremos de línea CRLF deben ser de estilo UNIX. Por lo tanto, se puede utilizar un editor basado en Linux o en Mac OS para crear el archivo de inventario de Windows. También se puede utilizar un programa como Notepad++.
- Los nombres de los componentes, como CVPREPORTING, ROgger, PG, etc., deben ir en mayúsculas.

Nota: El archivo Inventory.conf es sensible a las sangrías; consulte/utilice imágenes y ejemplos de archivos de configuración

Los archivos de ejemplo que muestran el formato correcto se pueden descargar aquí:

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

El ejemplo del servidor VOS se muestra en la imagen:

```

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"

```

El ejemplo de Windows Server se muestra en la imagen:

```

Windows:
CVFGAMP: {}
CVFREPORTING: {}
CVFSEVER:
  CVFCALLSERVER:
    hosts:
      - name: "125cvcp1"
        side: "A"
        user: "administrator@domain.local"
      - name: "125cvcp2"
        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: {}
PGI:
  PGI:
    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. Edite las cadenas en el archivo de inventario, según sea necesario.

deploymentName: introduzca un nombre único para la implementación.

- Este nombre aparece en la línea del asunto de la notificación de correo electrónico. Si no se configura, la línea de asunto de la notificación de correo electrónico contiene sólo el tipo de procedimiento y el

estado general.

deploymentType: Este campo se utiliza para comprobar la compatibilidad en los procedimientos de actualización, reversión o reenvío de switch.

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

Los tipos de implementación admitidos son:

- UCCE-2000-Agents
- UCCE-4000-Agents
- PCCE-2000-Agents
- PCCE-4000-Agents
- HCS-CC-2000-Agents
- HCS-CC-4000-Agents

Nota: Revise estas notas sobre los tipos de implementación admitidos.

No se admite la orquestación para los modelos de implementación de agentes 12000, 24000 y 26000.

El modelo de implementación de HCS-SCC (centro de contacto pequeño) no es compatible actualmente con la orquestación.

Asegúrese de que los valores introducidos en este campo se ajustan al formato de lista de tipos de implementación admitido. El tipo de implementación distingue entre mayúsculas y minúsculas.

Nota: El administrador puede actualizar o editar los valores por defecto, si es necesario, en función de su tipo de implementación y nombre de implementación preferido.

4. Ejecute el comando **utils system Inventory import** en el nodo del editor de Cloud Connect para importar el inventario actualizado del servidor SFTP, como se muestra en la imagen.

```
admin:  
admin:utils system inventory import  
You can import an inventory from SFTP server location. Enter the details of the SFTP server  
SFTP Server:10.128.1.1:1:1:1  
SFTP User:joanaj  
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  
admin:
```

- Proporcione la dirección IP o FQDN de un servidor SFTP.
- Proporcione el nombre de usuario que tiene acceso de lectura y escritura al servidor SFTP.
- Proporcione la contraseña para el usuario.
- Proporcione el directorio para escribir el archivo de inventario en formato UNIX/Linux.

Ejemplo: /voice/ipcc/Enterprise/Orchestration

e. Responda "sí" para permitir que el nuevo archivo de inventario reemplace el inventario actual.

Paso 6: Validar nodos incorporados para la orquestación

Para validar que los nodos de VOS y Windows se han incorporado correctamente, y para comprobar si la característica de orquestación está lista para utilizarse, ejecute el comando **utils deployment test-connection** como se muestra en la imagen.

```
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:
```

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).