Webex Contact Center Enterprise digital channels implementation and troubleshooting powered by Webex Connect

LTRCCT-2003

Speakers: Joshua Raja / Robert W. Rogier

Learning Objectives

Upon completion of this lab, you will be able to:

- Know where Cloud Connect is added to Control Hub
- Know where the SSO Certificate is uploaded.
- Identify the two required authorizations for Webex Connect
- Know how to add these to CCE Admin

Scenario

This lab is designed to introduce the audience to the digital channels (Webex Connect) platform, its architecture, and its provisioning. In addition, this lab will provide the instructions to verify if Webex Connect has been provisioned successfully.

Task 1: Review Cloud Connect in Control Hub

Lab Objective

This first task does not have any user steps. It is simply to review the configuration as this would be required in a customer system.

Prerequisite

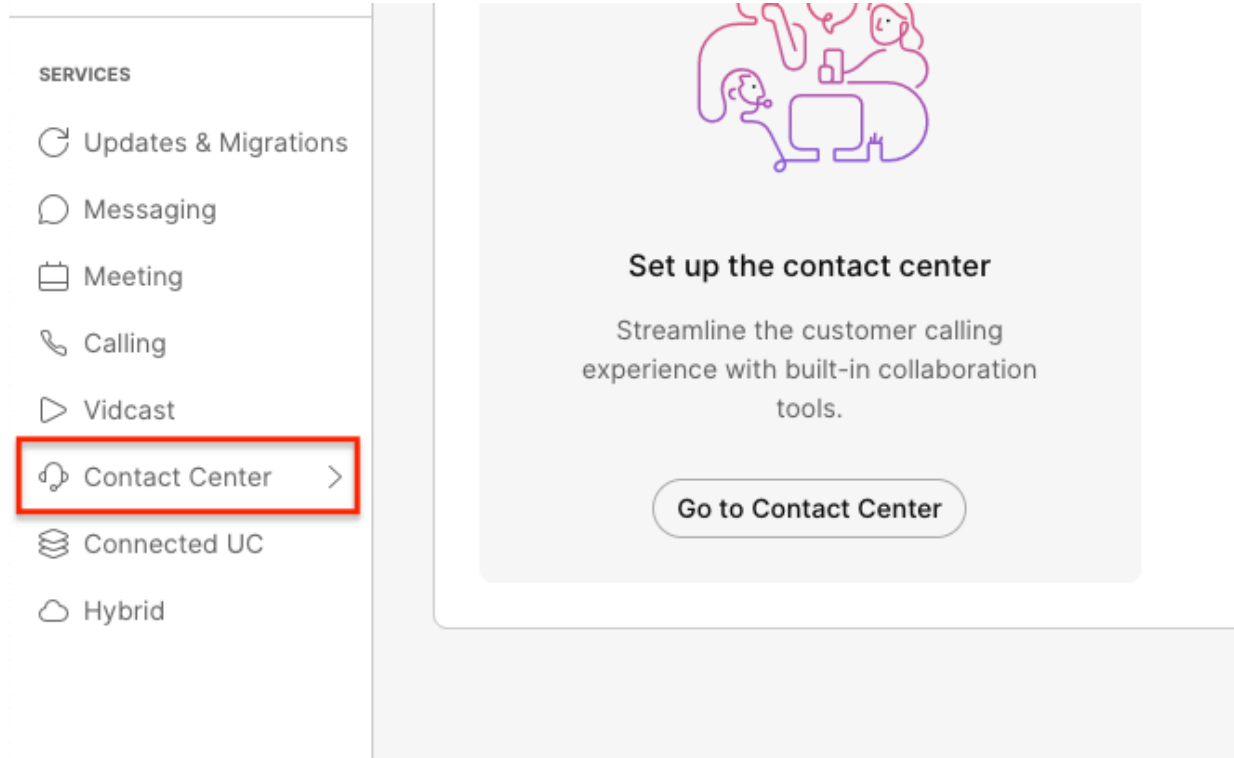Admin credentials to log in to Control Hub.

Quick Links

Control Hub: https://admin.webex.com

Webex Connect Tenant: See *Seat Credentials* document

Step 1: Log in to Control Hub

Open a Web Browser to the Control Hub URL (https://admin.webex.com). Reference the Credentials Document for the credentials for your seat.

Under **Services** select **Contact Center**

Once you have selected this, select the Cloud Connect menu.
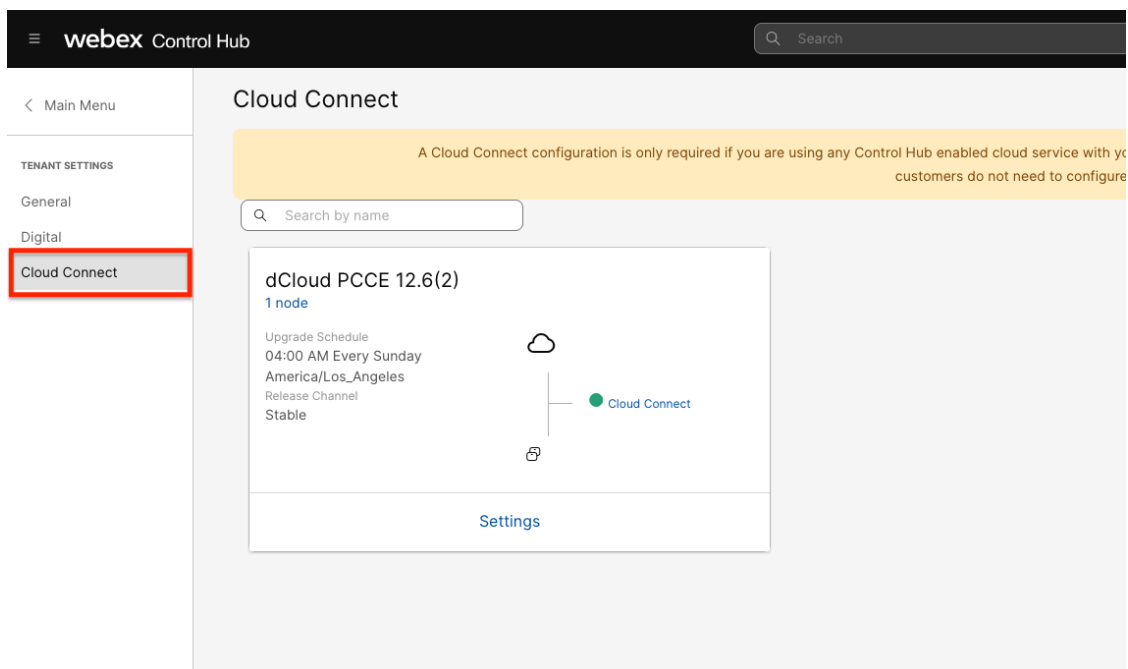
Please do not make any changes in this section as this can break other labs.

Step 2: Obtain Public key certificate from Cisco IdS

The Manage Digital Channel gadget authenticates with Webex Engage in the Single Sign-On (SSO) mode, through tokens generated using public key cryptography. Use a secret private key to sign the tokens after which you can verify the tokens using a freely distributed public key certificate. Cisco Identity Service (IdS) generates the public and private keys that you can use to sign and verify the token. Cisco IdS exposes the CLI or REST interfaces to fetch the public key certificate for verifying the token. A public certificate authority (CA) must sign this public key certificate. You must then upload the CA signed public key certificate in Control Hub to authenticate and enable communication between Webex Engage and the Manage Digital Channel gadget.

1. Log in to the Cisco IdS server's command line interface using the SSH administrator credentials.

2. Run the following CLI command to generate the Certificate Signing Request (CSR) that can be used to obtain a CA signed certificate:

show ids token csr – Displays the CSR corresponding to the public key that is used to validate the tokens.

3. Copy the entire CSR including the header and footer (-----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST----) from the Cisco IdS console and upload the same to the CA provided interface for generating a signed certificate.

4. Save the contents of the CA provided certificate generated using the CSR in step 3 into a file with extension of either .pem or .der. For Windows CA, this means you must choose base-64 encoding when you download the certificate.

You must upload the certificate in Control Hub when you provision the Digital Channels for an Organization.
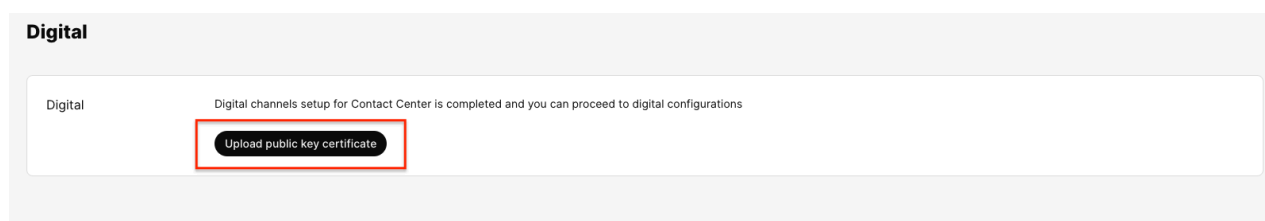
Note: You do not need to upload the CA-signed certificate in the Cisco IdS server
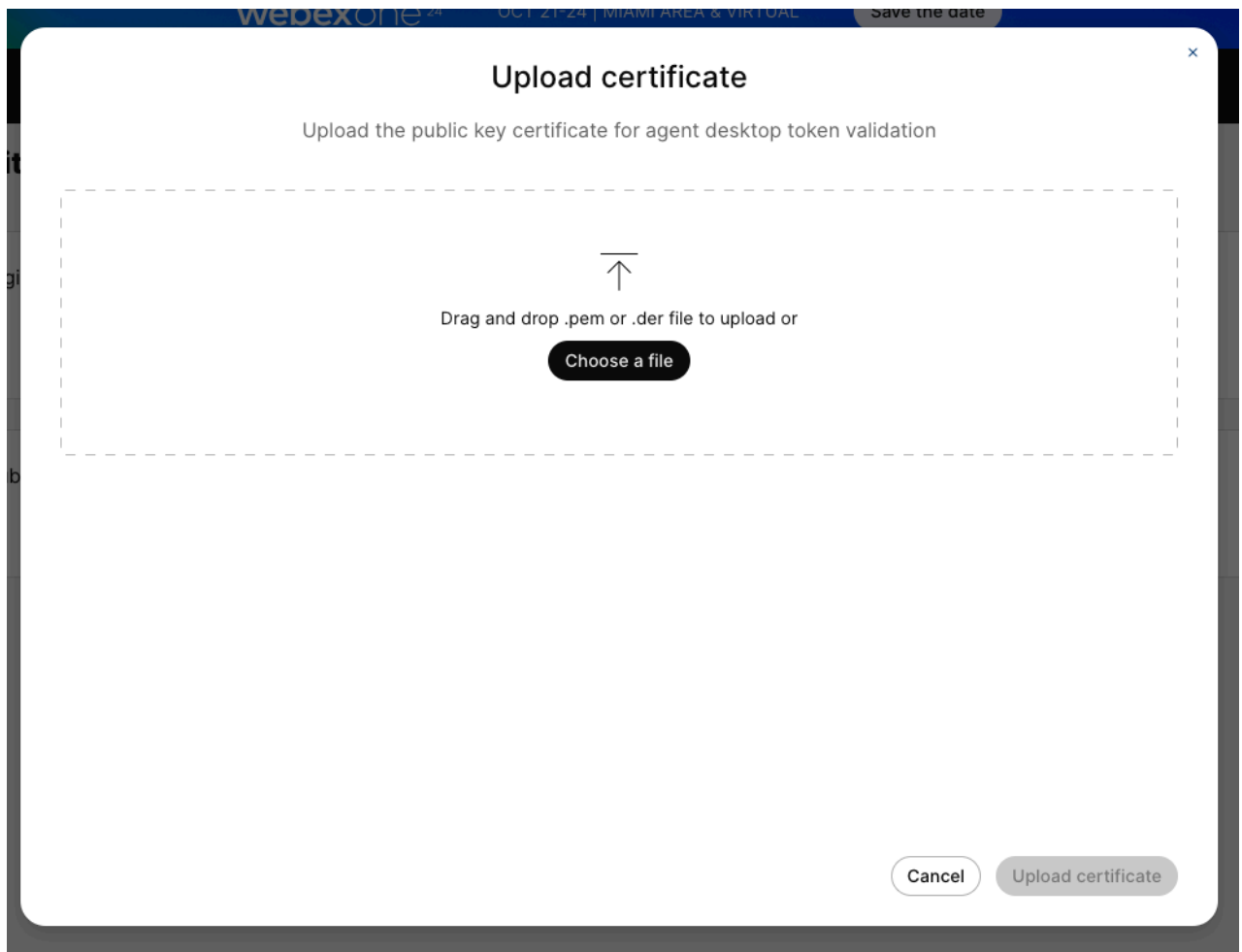
Step 3: Upload the certificate to Control Hub

1. Select the **Digital** menu in Control Hub.
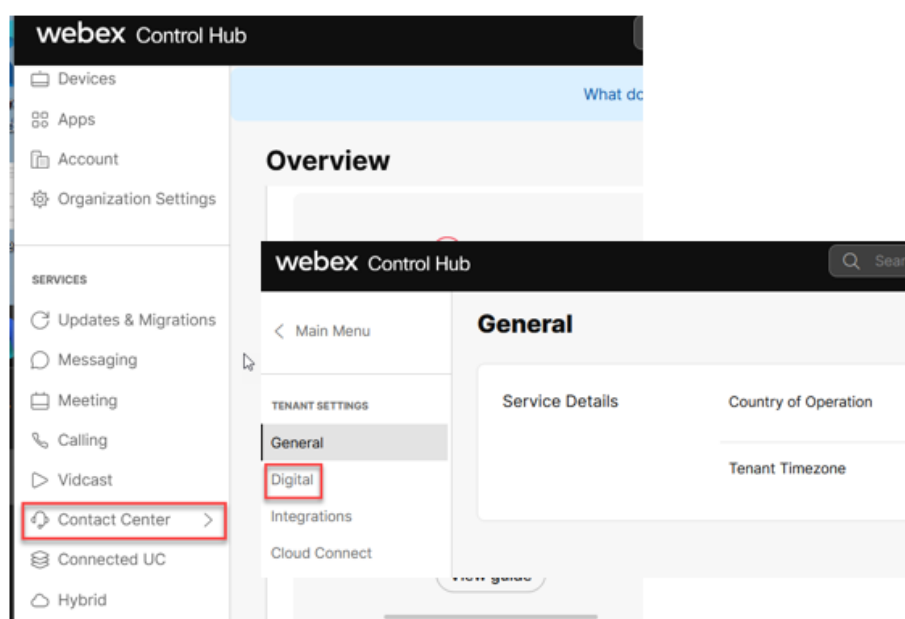
2. Select the **Edit** button to upload the certificate, then either drag-and-drop the signed certificate or select the **Choose a file** button. Once this is done, select the **Upload Certificate** button at the bottom of the page.

Upload certificate

Upload the public key certificate for agent desktop token validation

⬆

Drag and drop .pem or .der file to upload or

Choose a file

Cancel   Upload certificate

3. Wait a few moments for the automated provisioning process to complete.

Once this is done, users will be able to log in to the Engage gadget in Finesse.

Task 2: Configure the OAuth integration

This section shows how to configure CCE so that the outbound API calls to Webex Connect are successful. You will complete all the steps in this lab. We recommend that you log in to the dCloud jump box using one browser window, then use a second browser window to access Control Hub and Webex Connect. There is nothing in these labs that will require you to access both the CCE Admin and Control Hub/Connect in the same browser session.

Step 1: Log in to Webex Connect

Locate the URL for the Webex Connect tenant in the *Credentials* document. Open a web browser and enter the URL. Log in with the username and password documented.
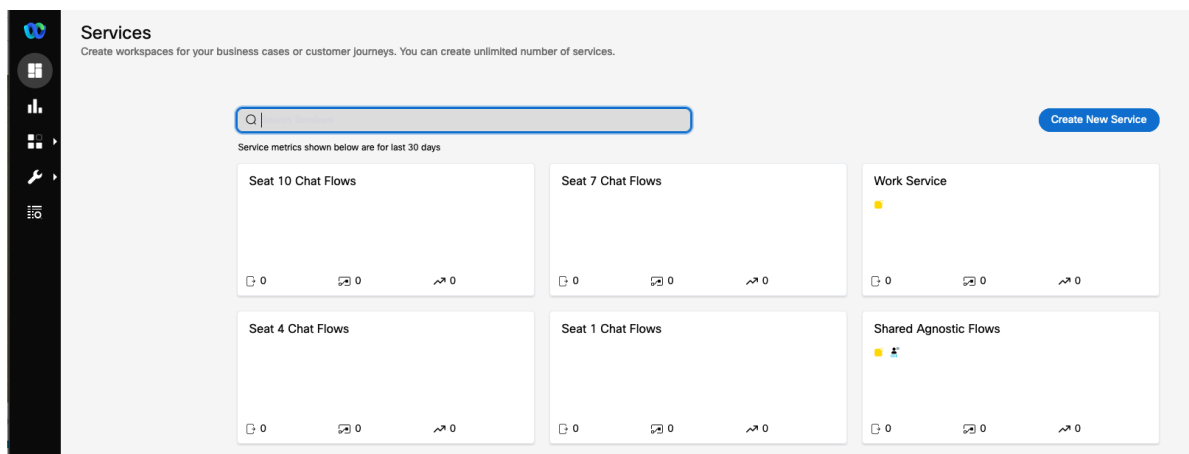
Step 2. Navigate to Assets > Integrations

Select the Assets menu, then select the Integrations sub-menu.
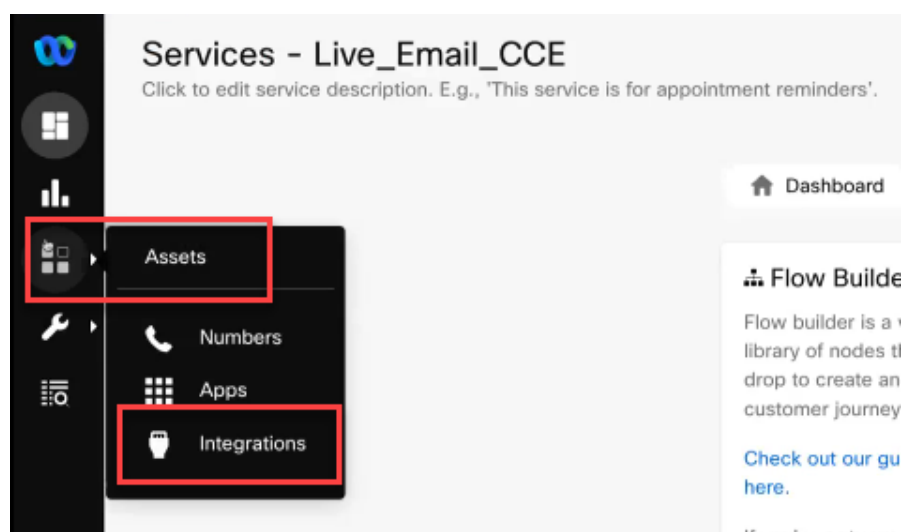
Step 3. Find the CCE Authorization

Select Pre-built Integrations under the Integration Type. In this list, you will see the Webex CC Engage authorization as well as the CCE Authorization.
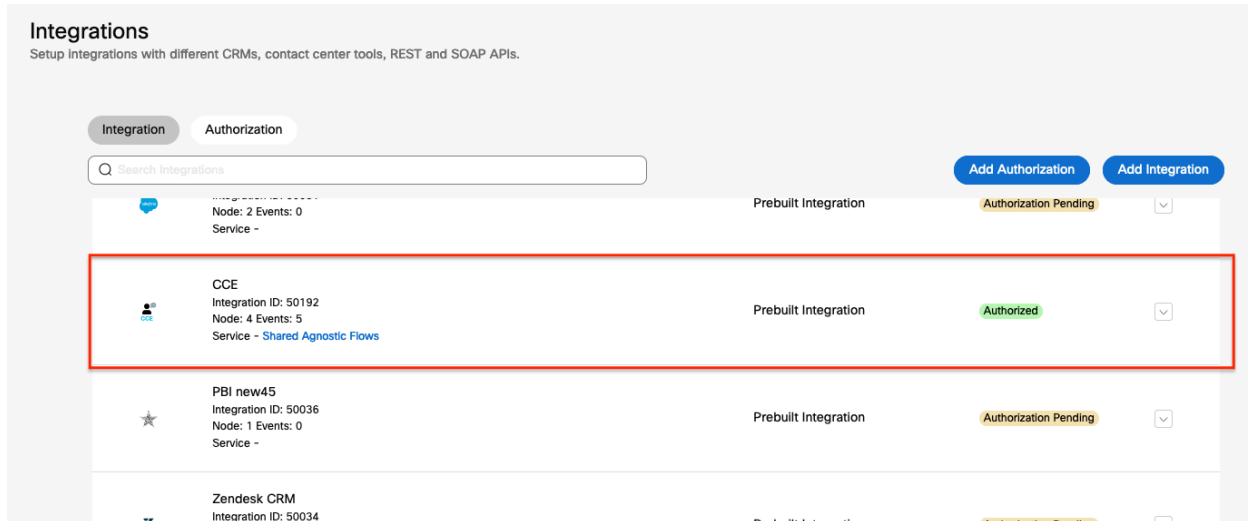
Select the drop-down at the far right, then select View.
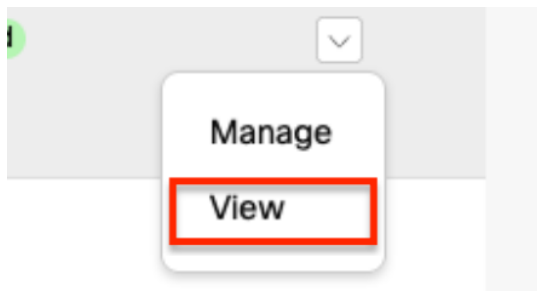
You will need the information in the Integration Details page to do the next step.

Step 4. Log in to CCE Admin

In your assigned dCloud session, ensure that you are logged into CCE Administration. Select the Digital Channels card, then select Digital Channels Settings. In this app, select the Integration tab.

Step 5. Configure the OAuth2 and Webhook settings

In this section, we will configure all the items required to authenticate the API calls.

1. Provide a descriptive name for this configuration.

2. Copy the Client Id, Client Secret, and Token Request URL from Webex Connect. Use the image below to see how to complete this. Select the copy icon in the greyed-out boxes to copy the clear-text version of the text.

The Token Request URL is specified in the Features Guide and depends on which datacenter the Connect tenant exists in. For this lab, all tenants are in the Ireland datacenter so the Token Request URL is, https://keycloak-authservice.imiconnect.io/auth/realms/imiconnect_uk_prod/token

Set the Method to POST.

From the Content Type drop-down list, select a media content type. This determines the response format. The available options are application/json, application/xml, and application/x-www-form-urlencoded. For Webex Connect integration, select application/x-www-form-urlencoded.

In the Access Token JSON path, enter the path in the JSON response to fetch the value of the access token. For the Webex Connect integration, enter *access_token*.

Step 3. Configure the Webhook URL. Copy this from your tenant to the location shown in the image below.

Step 4. Select Save at the bottom of the CCE Admin screen to commit the changes to configuration.

You have completed this portion of the lab.