



Provisioning Customers in the Cisco Cloud Connected Audio System

You, the vendor, can provision a customer to use Cisco WebEx Cloud Connected Audio (CCA) in the CCA Portal by completing the following steps:

- [Generating LOA and Documentation for CCA Peering Circuits, page 1](#)
- [Entering Network Peering Information, page 2](#)
- [Entering Telephony Information, page 3](#)
- [Entering Staging Site Information, page 4](#)
- [Entering Production Site Information, page 5](#)

Generating LOA and Documentation for CCA Peering Circuits

- Step 1** In the **Configuration** screen, select the customer for whom you want to start the provisioning.
- Step 2** Select **Circuits and LOA**.
- Step 3** You need to generate the LOA for each peering circuit. The LOA is required to order the circuits from the Service Provider. In order to generate the LOAs, you need to provide the customer's data center and Cisco's data center for each peering circuit.
- a) In the **Peering Connection/Datacenter Information** section, enter the customer's peering location for each circuit.
- b) From the **Cisco System** drop-down, select the cisco peering location from the list of available options.
- Note** To add another peering circuit, select **Add Circuit**.
- Step 4** Select **Generate LOA and Circuit Requirements Document**.
A download dialog box is displayed.
- Step 5** Save the file to your computer. This LOA and circuit requirement document needs to be shared with customer. It should be presented to the customer's Service Provider who provides the peering circuits between the customer's and Cisco's data centers.
-

Once the LOA is generated, the CCA system reserves the IP addresses and settings for the customer and that is populated into the **Network Peering** screen. . When the circuits are installed and Cisco is informed of this, the provisioning of the customer can continue.

Entering Network Peering Information

Network peering information is required for BGP provisioning and to establish layer 3 connectivity between the customer and Cisco. Once completed, this information needs to be submitted to Cisco for approval.

Before You Begin

You must have first generated the Letter Of Agency (LOA) for the customer. By doing so, certain fields in the **Network Peering** screen are pre-populated.

-
- Step 1** To provide the network peering information, do one of the following:
- a) In the **Configuration** screen, select **Network Peering Information** under the customer name.
 - b) In the **Circuits and LOA** screen for the customer, select **Enter Network Peering Info**.
- Step 2** In the **ASN** field, enter the Autonomous System Number (ASN) for the customer.
- Step 3** In the **Technical Contact** field, enter the name of the technical contact for the customer.
- Step 4** In the **Phone** field, enter the phone number of the technical contact for the customer.
- Step 5** In the **Email** field, enter the email address of the technical contact for the customer.
- Step 6** In the **Peering Connection/Datacenter Information** section, the detailed networking information for each peering circuit is required. Each peering circuit requires IP address, prefix, and port number for the customer's peering router as well as for Cisco's peering router. For each customer Peering Connection/Datacenter Information location, do the following:
- a) To change the customer Peering Connection/Datacenter Information location , select **Edit Location**.
 - b) In the **Port#** field, enter the number of the customer port.
- Step 7** In the **Peering IP** field, enter the peering IP.
- Step 8** In the **Prefixes** field, enter the prefixes. To add more prefixes, select **Add Prefixes**.
- Step 9** In the **Circuit Vendor** field, enter the name of the vendor that provided the customer circuit.
- Step 10** In the **Circuit ID** field, enter the ID number of the customer circuit.
- Step 11** When all prefixes are entered, select **Generate IP Traffic Direction**. You can enable or disable the IP Traffic Direction by checking or unchecking the relevant check boxes.
- Step 12** In the **BGP Provisioning** section, do the following:
- a) If you are requesting BFD with BGP, check the check box.
 - b) In the **BFD Interval(ms)** field, enter in milliseconds the interval at which the device sends Bidirectional Forwarding Detection (BFD) hello messages.
 - c) In the **Mix RX(ms)** field, enter in milliseconds the rate that the BFD supported device sends messages to its neighbors.
 - d) In the **Multiplier** field, enter the number of consecutive missed BFD packets before BFD informs upper layer protocol of BFD failure.
 - e) In the **Carrier-Delay Up(ms)** field, enter in milliseconds the interval to wait before signalling an interface has gone down to the routing table.
 - f) In the **Carrier-Delay Down(ms)** field, enter in milliseconds the interval to wait before signalling an interface has come back up again to the routing table.

- g) Check **Apply session password** to ensure a password is required for BGP.
- h) Check **Receive MEDs** to receive a hint to external neighbors about the preferred path into an autonomous system (AS) that has multiple entry points.

Step 13

Do one of the following:

- a) Select **Save as Draft** if you have not fully completed the screen.
- b) Select **Save and Submit** to save the information and submit it to Cisco for approval.

What to Do Next

When the information is submitted to Cisco, the Cisco personnel, such as the CCA Administrator or Cloud Services, do one of the following:

- Select **Approve**, which allows the next stage of provisioning to begin.
- Select **Decline**, which requests more information about the customer's network peering. The Approver can also enter any comments on why the information was declined in the **Approver's Comment** field.

When the Network Peering information is approved, WebEx Cloud Services submits the remedy ticket for the customer. Cloud Connected Audio IT personnel ensure the servers and anything else needed are ready for customer provisioning. When complete, the **Customer Overview** screen displays that the engineer has completed the tasks and the provisioning of the customer can continue. The remedy ticket status is updated on an on-going basis in the CCA Portal as provisioning work is completed .

Entering Telephony Information

You must provide Session Border Controller (SBC), Cisco Unified SIP Proxy (CUSP) and Dialed Number Identification Service (DNIS) information for the customer in this screen.

SBC's control and manage real-time multimedia traffic flows between IP network borders, handling signaling, data, voice, and video traffic.

CUSP is a high-performance, highly available Session Initiation Protocol (SIP) server for centralized routing and SIP signaling normalization.

DNIS determines which telephone number was dialed by a customer .

Step 1

In the **Customer SBC Information** section, enter the SBC information for the customer including the SBC ID number, the data center locations, and the SIP and RTP IP addresses.

Note Provide the SBC information for each of the peering locations. This field is mandatory as every CCA deployment requires the customer to deploy SBCs.

- Step 2** To add another SBC, select **Add SBC**.
- Step 3** In the **Customer CUSP Information** section, enter the CUSP information for the customer including the CUSP ID number, the data center locations, and the SIP IP addresses. This field is optional as not all CCA implementations require CUSP deployment.
- Step 4** To add another CUSP, select **Add CUSP**.
- Step 5** In the **DNIS Information** section, enter the DNIS information for the customer including the DNIS label and the DNIS number .
- Note** DNIS is not the same as the displayed number. DNIS is the number that WebEx SBC receives from customer. A single DNIS can be mapped to multiple conferencing number.
- Step 6** To add another DNIS, select **Add DNIS**.
- Step 7** Select **Save**.
-

Entering Staging Site Information

The Telephony information pre-populates some of the Staging Site information. The rest must be entered manually. Staging sites are used to test the Cisco CCA configuration before configuring CCA on the production site. Also, if updates are rolled out in the future, these existing staging sites can be reused for testing the updates.

-
- Step 1** In the Configuration screen under the customer name, select **Add New Site** next to **Staging Sites**.
- Step 2** In the first field, enter the URL of the staging site.
- Note** You can select **Import Data** to import data from another site. This populates the new site with information from that existing site so you do not need to enter all the information again.
- Step 3** From the **Primary** drop-down, select the Cisco Bridge to use. This information is automatically populated by CCA Portal.
- Step 4** As part of telephony provisioning for a CCA customer, WebEx Cloud Services determine the primary and backup Cisco SBCs. From the **Primary/Backup/Disable** drop-down for each SBC, indicate if the SBC should be the primary device, secondary device or disabled.
- Note** The Day 1 Vendor must configure the ingress and egress call routes for the CCA customer. For both ingress and egress routing there are active, standby or backup routes.
- Step 5** For each SBC and, optionally, each CUSP egress call primary route into the customer, do the following:
- From the **Mode** drop-down for each primary route, indicate if the route should be active, in standby or disabled.
 - From the **Country** drop-down, select the list of countries to which the egress route applies. If the egress route applies to all countries, select **All countries**. There may be CCA configurations where the customer has different egress call routings for a different set of countries.
 - To add another set of primary routes, select **Add Primary Routing**.
 - To remove a set of primary routes, select **X** next to the primary routes.
- Step 6** For each SBC ingress call primary route into Cisco, do the following:
- From the **Customer SBC** drop-down for each primary route, select the customer SBC.
 - From the **Cisco SBC** drop-down for each primary route, select the Cisco SBC.
 - To add another set of primary routes, select **Add Primary Routing**.

d) To remove a set of primary routes, select **X** next to the primary routes.

Step 7 In the **Is Customer buying WebEx audio option in addition to Cloud Connected Audio?**, select **Yes** or **No**.

Note For example, if the customer wants to try only 50% of their calls through CCA they can also buy the WebEx audio option for the remaining 50%.

Step 8 To add phone numbers, select **Add Phone** and do the following:

a) In the **Owned By** field, select the customer or Cisco. This is a required field.

Note The **Cisco** option only appears if the customer has also purchased WebEx PSTN as well as the CCA service. Otherwise, all the numbers belong to the customer.

b) In the **Country** field, select the country from which the phone number originates. This is a required field.

c) Select whether the phone number is toll or toll free.

d) Add the phone number and label.

e) Select the DNIS (calls into WebEx). The DNIS list is pre-populated with the DNIS information entered in the **Customer Telephony Information** section. For every dialled number, a corresponding DNIS must be selected. There must be a DNIS mapping for each dialled number

Step 9 In the Callback Option section, do the following:

a) The **Internal Callback** and **Regular Callback** options are checked by default. Uncheck them if required

b) For **Callback over WebEx PSTN**, select **Yes** or **No**.

c) Enter the **Internal Callback Prefix** for all internal callback calls.

Step 10 Do one of the following:

a) Select **Save as Draft**, if you have not fully completed the screen.

b) Select **Save and Submit**, to save the information and submit it to Cisco for approval.

What to Do Next

When the information is submitted to Cisco, the Cisco personnel, such as the CCA Administrator or Cloud Services, do one of the following:

- Select **Approve**, which allows the next stage of provisioning to begin.
- Select **Decline**, which requests more information about the customer's staging site. The Approver can also enter any comments on why the information was declined in the **Approver's Comment** field.

Entering Production Site Information

The production site information is the exact same as it is for staging sites. Production sites are used when CCA has been tested on the staging sites and is now ready to be used in the organization environment. For details on how to enter the production site details, see [Entering Staging Site Information](#).



Note

In the **Production Site Information** screen, you have the option of adding Secondary Routing as well as Primary Routing.

What to Do Next

When the information is submitted to Cisco, the Cisco personnel, such as the CCA Administrator or Cloud Services, do one of the following:

- Select **Approve**, which allows the next stage of provisioning to begin.
- Select **Decline**, which requests more information about the customer's production site. The Approver can also enter any comments on why the information was declined in the **Approver's Comment** field.

When the production sites are approved and the remedy ticket is created and completed, the customer is completely provisioned and can begin using Cisco Cloud Connected Audio.