



## **Cloud Connected Service Administration Tool User Guide**

**First Published:** July 21, 2014

**Last Modified:** January 13, 2015

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

Text Part Number:

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2014 Cisco Systems, Inc. All rights reserved.



## **CONTENTS**

---

### **CHAPTER 1**

**Overview of Cisco Cloud Connected Service Administration Tool 1**

---

### **CHAPTER 2**

**About the Configuration Overview Screen 3**

---

### **CHAPTER 3**

**Provisioning Customers in the Cisco Cloud Connected Audio System 5**

Generating LOA and Documentation for CCA Peering Circuits 5

Entering Network Peering Information 6

Entering Telephony Information 7

Entering Staging Site Information 8

Entering Production Site Information 9





## CHAPTER

# 1

# Overview of Cisco Cloud Connected Service Administration Tool

---

Cisco WebEx Cloud Connected Audio (CCA) is a fully geographically independent, highly available and scalable audio conferencing solution. It manages the audio conferencing traffic for WebEx conferencing over a direct connection between the customer data center and the Cisco data center.

The Cisco WebEx Cloud Connected Service Administration Tool enables CCA Implementation Vendors and WebEx Cloud Operations to provision CCA service for customers.

### Initial Setup of the CCA Portal

The Cisco WebEx Cloud Connected Service administrator sets up customers in the system, controls what features are available to Cisco WebEx Cloud Connected Services Portal users and determines how they can use these features.

This portal requires an initial setup by the CCA administrator before customers can be provisioned to use Cisco Cloud Connected Audio (CCA). During this initial setup the CCA administrator performs the following tasks:

- Creates policies.
- Creates vendor organizations.
- Creates vendor groups and group members and assigns the policies to these groups.
- After receiving the completed **New CCA Customer Information** form from the vendor via email, creates customer organizations and associates them with one or more vendor groups.
- Creates customer groups and group members and assigns the policies to these groups.

Once this initial set-up is complete you, the vendor, are responsible for implementing CCA service for the customer can use the portal to provision CCA service for the customer. See and [Provisioning Customers in the Cisco Cloud Connected Audio System](#), on page 5.

### How Vendors Provision in the Cisco Cloud Connected Audio System

Before customers can begin to use Cisco WebEx Cloud Connected Audio (CCA) in their organization, they must first be provisioned using the Cisco WebEx Cloud Connected Service Administration Tool.

You, the vendor working on behalf of the customer, must complete the **New CCA Customer Information** form that you received from the CCA Portal Administration team. Once you have provided all the necessary

details about the customer and returned it to [cca-portal-newcust@cisco.com](mailto:cca-portal-newcust@cisco.com) the CCA Portal Administration team creates the customer and sends you a welcome email. From then you can begin to provision the customer.

The workflow for how you provision a customer is as follows:

- The provision workflow cannot start without the customer first installing the required circuit or circuits onsite for their organization. You receive the welcome email that contains a link for generating the Letter Of Agency (LOA) and Circuit Requirements document.
- When you select this link, you are prompted to log into the CCA Portal.
- You must then enter the peering connection/datacenter information and generate the Letter Of Agency (LOA) and Circuit Requirements document. See [Generating LOA and Documentation for CCA Peering Circuits](#).
- When the LOA is generated, the circuit has arrived and is installed onsite, you can now enter the network peering information. This must be submitted to Cisco for approval. See [Entering Network Peering Information](#).
- When the network peering information is approved, you can now enter the customer telephony information. See [Entering Telephony Information](#).
- When the customer's Session Border Controller (SBC), Cisco Unified SIP Proxy (CUSP) and Dialed Number Identification Service (DNIS) information is entered in the **Telephony Information** section, you must add and provide the provisioning information for the staging and production sites. CCA service is first configured and tested on the staging site. When the staging site is verified, the production site is configured. The staging and production sites can be added and submitted for approval at the same time.



---

**Note** The staging and production sites information can be entered at any stage after the LOA and circuit and telephony information are complete. They must be submitted to Cisco for approval. See [Entering Staging Site Information](#) and [Entering Production Site Information](#).

---

- When the production site information is approved, the provisioning for the customer is complete.



## About the Configuration Overview Screen

The **Configuration Overview** screen is the home page of the administration site and provides a list of customers and the stage they are in the provisioning process.

The main stages of provisioning include:

- **Start Provisioning:** CCA provisioning information has not been provided. Start with generating the Letter of Agency (LOA) and providing circuit information.
- **Provisioning in progress:** CCA Provisioning is in progress but all the provisioning information has not yet been provided.
- **Provisioned:** all the CCA provisioning information has been provided and approved and the remedy ticket has been created.

In this screen, you can see at a glance what stage every customer in the system is at. You can also view just one customer's details by selecting the customer name from the drop-down list at the very top left of the screen.

The **View** drop-down at the top of the screen filters the customers by the specific stage they are at in provisioning. For example, to view customers who still need Network Peering information added, select **Network Peering** from the drop-down.

When all customers are displayed in the **Configuration Overview** screen, to view a specific customer details, select the arrow next to the customer name. This displays the details and walks you through, step-by-step, the provisioning of the customer. What stage each step in the provisioning is at is indicated by a colored dot:

- Red indicates the step needs to be completed.
- Yellow indicates the step has been started but is not yet completed. For example, if you are creating production sites, you may be waiting for approval for Cisco before this step is considered complete.
- Green indicates the step is complete and you can move onto the next step.

Blue hyperlinked text in the customer details indicates a link to a screen to enter customer provisioning details. For example, the very first step is indicated by the blue text **Circuits and LOA**. When you select this text, the **Circuits and LOA** screen is opened where you can enter the customer Peering Connection/Datacenter Information and generate a LOA and Circuit Requirements document.





## 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 5](#)
- [Entering Network Peering Information, page 6](#)
- [Entering Telephony Information, page 7](#)
- [Entering Staging Site Information, page 8](#)
- [Entering Production Site Information, page 9](#)

### 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:
- In the **Configuration** screen, select **Network Peering Information** under the customer name.
  - 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:
- To change the customer Peering Connection/Datacenter Information location , select **Edit Location**.
  - 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:
- If you are requesting BFD with BGP, check the check box.
  - In the **BFD Interval(ms)** field, enter in milliseconds the interval at which the device sends Bidirectional Forwarding Detection (BFD) hello messages.
  - In the **Mix RX(ms)** field, enter in milliseconds the rate that the BFD supported device sends messages to its neighbors.
  - In the **Multiplier** field, enter the number of consecutive missed BFD packets before BFD informs upper layer protocol of BFD failure.
  - 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.