Digital Channels Integration Using Webex Connect

Overview

Today's customers want to connect with businesses through any communication channel of their choice. Webex Connect allows the Contact Center business and its customers to interact using digital channels such as email, chat, and SMS.

The Contact Center Enterprise (CCE) solution integrates with Webex Connect to create a seamless omnichannel experience for your customers. This integration helps your customers to interact across voice and digital channels of communication.

Webex Connect offers a rich self-service and bot integration to empower your customers to get answers to some common questions. It provides a unified solution for integrated routing, Agent Desktop, and reporting service. Webex Connect provides a simplified framework that helps partners and customers interact through digital channels.

Prerequisites

The following are the prerequisites for provisioning digital channels for Contact Center Enterprise:

- The following components must be on release 12.6(2) or higher: CCE components (Router, Logger, AW, and PG), Cisco Finesse, Cisco IdS, and Cloud Connect.
- Place an order for Digital service for your customer using Cisco Commerce Workspace (CCW). For more information, see the Cisco Collaboration Flex Contact Center Ordering Guide available at https://www.cisco.com/c/en/us/partners/tools/collaboration-ordering-guides.html.
- If you want your customers to reach you through SMS and if you are provisioning a US phone number for SMS communication, you must first procure a 10 Digit Long Code (10DLC), which is the mandated standard for Application-to-Person (A2P) text messaging. Work with your Account Manager to verify your business and set up your SMS Business account number. After you obtain the number, use it to configure the SMS contact handling. For instructions, see SMS.
- Make sure that you enable the Single Sign-On (SSO) mode for agents who are required to handle digital channel tasks. To enable agents for SSO one at time, use the configuration tools. To enable multiple agents at once for SSO, use the SSO migration tool. For instructions, see the *Migrate Agents and Supervisors to Single Sign-On Accounts* section in the Cisco Unified Contact Center Enterprise Features Guide.
- Tokens created with Cisco IdS are used to authenticate CCE agents with Webex Engage. This necessitates synchronization of the time fields in the tokens between Cisco IdS and Webex Engage cloud services. As a result, the Cisco IdS NTP server configuration must be synchronized, either directly or indirectly, with a public NTP server that supports leap smearing in order for the premise and cloud NTP configurations to be in sync. Furthermore, when used with digital channels, the lifetime of a Cisco IdS token cannot be set to less than 2 hours.

Important considerations

Consider the following before integrating digital channels with CCE using Webex Connect:

- Tasks in the Digital Routing service remain in the service memory only for 15 minutes after the tasks are closed. There is no persistence of closed tasks in the Digital Routing service. This 15-minute interval is a system setting and you cannot modify it.
- The Webhook notification that the Digital Routing service invokes for a closed task contains a disposition code that denotes the reason for the task closure. Using the disposition code in the Close Task, a flow designer can perform different actions as needed in the Webex Connect flow. For example, if a task fails after it has been queued, an error message can be displayed to customers with the option to contact the business via other support channels or schedule a callback, as opposed to a message indicating that the task has been closed due to a system error. For information about disposition codes, see Disposition codes for digital channel interaction, on page 24.

Redaction of sensitive data

This feature redacts or masks all the sensitive data that you send over Webex Connect to ensure PCI compliance. The PCI service scans all your requests for sensitive data, masks the data, and sends it over to the Agent Desktop. The PCI service also scans the agent responses and sends the redacted data, including attachments that do not contain sensitive data, to the end customers.

The following are the supported file types on which the PCI service applies redaction:

Table 1: Supported File Types

Category	File Extension
Document	html, mhtml, mht, odt, pdf, pdfxml, rtf, shtml, xps, xml, xhtml, txt
E-mail	eml, msg
Microsoft	ods, doc, dochtml, docm, docx, docxml, dot, dothtml, dotx, dotm, pot, pothtml, ppthtml, pptmhtml, pptxml, potm, potx, pps, ppam, ppsm, ppsx, pptx, pptm, ppt, pub, pubhtml, pubmhtml, xls, xlshtml, xlthtml, xlt, xlsm, xltx, xltm, xlam, xlsb

Note Any file types that are not listed in the Supported File Types table are automatically dropped in the transmission. If there are any images in the attachments that are sent in the supported file types, the attachments are automatically dropped. For example, if your PDF file includes images, the file is automatically dropped in the transmission, even though PDF is a supported file type.

Workflow for enabling and managing digital channel interactions

As a partner, complete the following tasks to onboard your customer for Hybrid Services and provision the digital channel capabilities:

Note In some rare cases, the customer administrators can also perform the following tasks to provision the digital channel capabilities for their organization.

Note If your customer is already using a Hybrid Service such as CCAI, skip steps 1–6 and directly start with provisioning the digital channel capabilities (step 7 onwards).

Table 2: Initial configurations to enable digital channel capabilities

Step #	Task	Reference
Onboard hybrid services for customers using Control Hub		
Note If your customer is already using a Hybrid Service such as CCAI, skip steps 1 and 2 in this section and directly start with provisioning the digital channel capabilities (step 3).		

Step #	Task	Reference
1	Place an order for Digital service for your customer using Cisco Commerce Workspace (CCW), and your Contact Center subscription starts. Set up hybrid services for your customer.	See the Set up hybrid services for your organization.
2	(Optional) Create a user with Full Admin role to authorize task requests that are sent from Webex Connect to Contact Center Enterprise (CCE) through Cloud Connect.	• Add users manually in Control Hub • Assign organization account roles in Control Hub
3	Provision digital channels for your customer on Control Hub.	See the Provision Webex Connect digital services for your organization.
Integrate CCE and Webex Connect		
Part 1—Cloud Connect Configurations		
4	Install and add the Cloud Connect publisher and subscriber nodes to the inventory for your customer.	See the *Install Cloud Connect* section in the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide.
5	Register Cloud Connect in the Unified CCE Administration portal.	See the *Cloud Connect Integration* section in the Administration Guide for Cisco Unified Contact Center Enterprise.
6	Configure the Media Routing Peripheral Interface Manager (MR PIM) for the Digital Routing service.	See the *Configure Peripheral Gateway Setup* section in the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide
7	Establish secure connections between Cloud Connect and Media Routing Peripheral Gateway (MR PG), and set up the Nginx reverse proxy server certificate for the digital channels interaction.	See the *Certificate Management for Digital Channels Integration* section in the Security Guide for Cisco Unified ICM/Contact Center Enterprise.
Part 2—Reverse Proxy Configurations		
8	Set up and configure reverse proxy server for the digital channel interaction.	See Workflow to configure reverse proxy using automated installer, on page 11.
Part 3—CCE Configurations		

Step #	Task	Reference
9	Create a unique media routing domain (MRD) for each media channel and map it to your media channel if you want granular channel-specific reporting and agent state control. Use the Media Routing Domain List tool to create the MRDs. For Emails and asynchronous social chat channels like SMS, consider a longer **Start Timeout** and **Max Duration** for the Media Routing Domain. You can also map existing MRDs to the Digital Routing media channels. This will avoid having to create new skill groups, precision queues, and scripting logic changes to target the new media channels.	• For instructions about how to create a new MRD, see the online help that is integrated with the Media Routing Domain List tool. • For instructions about how to map the existing MRDs to the Digital Routing media channels, see Set up media channels.
10	Associate the MRDs that you have created for the digital channel integration using Webex Connect to the system-defined application paths. For every agent peripheral gateway, there is a system-defined application path that gets created with a suffix "UQ.Desktop". There is also an associated system-defined application called UQ.Desktop that automatically gets created in the sytem and identifies the Cisco Finesse server as a client to the Agent PG, to control Agent states in MRDs created for digital channels. The first number in the application path identifies the Logical Controller ID of the PG. An example of the system-defined application path is `5000.UQ.Desktop`. **Note** If you create the MRDs through the Unified CCE Administration portal, the MRDs get automatically associated to the system-defined application paths. If you have created the MRDs using the Media Routing Domain List tool under Configuration Manager, you must explicitly associate the MRD with the application path.	See the online help that is integrated with the Application Path List tool

Step #	Task	Reference
11	Create mandatory ECC variables in the Unified CCE Administration portal (**Overview** > **Call Settings** > **Route Settings** > **Expanded Call Variables**). The ECC variables are required to identify the incoming tasks as Digital Routing tasks and the tasks to carry the Webex Engage conversation ID.	• For instructions about how to create ECC variables, see the *Add and Maintain Expanded Call Variables* section in the online help that is integrated with the tool. • For the list of mandatory ECC variables, see the ECC Variables for Digital Routing Tasks, on page 14.
12	Configure digital channel capabilities for your customer in the Unified CCE Administration portal.	See Manage digital channels.
13	Create routing scripts for digital channel interaction.	See the *Example Scripts for Digital Channel Interactions Using Webex Connect* section in the Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise.
14	(Optional) You can configure an Agent Request or Web Callback feature to allow your customers to place a web callback request to the contact center.	See Agent Request or Web Callback using Webex Connect, on page 29.
Part 4—Cisco Finesse Configurations **Note** Ensure that you complete all the prerequisites listed in the *Prerequisites to configure the Manage Digital Channels gadget* section in the Cisco Finesse Administration Guide before you proceed with Finesse configurations to set up the Manage Digital Channels gadget.		
15	Provision Cloud Connect on Cisco Finesse.	See the *Cloud Connect Server Settings* section in the Cisco Finesse Administration Guide.
16	Add the Manage Digital Channels gadget to the Cisco Finesse desktop layout.	See the *Add Manage Digital Channels Gadget* section in the Cisco Finesse Administration Guide.
Part 5—Webex Connect Configurations		
17	Configure node authorizations in Webex Connect to inject new tasks, retrieve a task's details, and close tasks directly on CCE.	See CCE Integration Nodes and Node Authorizations.
18	Configure channel assets for the required media channels such as SMS, Live Chat, and email.	See the following sections: • SMS • Live Chat • Email

Step #	Task	Reference
19	Create flows using the Webex Connect Flow Builder feature for the various digital channels interactions such as SMS, Email, and Live Chat. Use one of the following options to create flows: • Import the Webex Connect CCE Flow Templates - 12.6(2) into the Webex Connect portal and tailor them to your specific needs. • Use a pre-built flow template that is available in the Webex Connect portal and customize it to suit your requirements.	See Flow Configurations.
Part 6—Webex Engage Configurations		
20	Set up the customer chat widget.	See Administration and Setup Guide for Webex Engage with Cisco Contact Center Enterprise.
21	Verify that the agents who are enabled for digital channel interaction are synchronized to Webex Engage.	
Work with Manage Digital Channels gadget		
22	After you complete your initial configurations to enable digital channels interactions, the agents and supervisors can start interacting with customers using the Manage Digital Channels gadget.	See the Cisco Contact Center Enterprise Manage Digital Channels Gadget User Guide.

Step 1 Install and add the Cloud Connect publisher and subscriber nodes to the inventory for your customer. For more information, see the *Install Cloud Connect* section in the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide.

Step 2 Register Cloud Connect in the Unified CCE Administration portal to establish a secure and trusted communication channel between the Cisco Contact Center on-premises deployment and cloud services. For more information, see the *Cloud Connect Integration* section in the Administration Guide for Cisco Unified Contact Center Enterprise.

Step 3 Establish secure connections between the various components such as Cloud Connect, Media Routing Peripheral Gateway (MR PG), Webex Connect, Webex Engage, and Nginx reverse proxy servers for the digital channels interaction. For more information, see the *Certificate Management for Digital Channels Integration* section in the Security Guide for Cisco Unified ICM/Contact Center Enterprise.

Step 4 Provision Cloud Connect on Cisco Finesse. For more information, see the *Cloud Connect Server Settings* section in the Cisco Finesse Administration Guide.

Step 5 After a Contact Center subscription starts, access the **Services Setup** wizard to configure the Contact Center tenant using the Control Hub URL https://admin.webex.com/. For more information, see *Set up hybrid services for your organization*.

Step 6 Provision digital channels for your customer on Control Hub. For more information, see *Provision Webex Connect digital services for your organization*.

Step 7 Create a user with admin privilege to authorize task requests that are sent from Webex Connect to Contact Center Enterprise (CCE) through Cloud Connect. For more information, see Add users manually in Control Hub and Assign organization account roles in Control Hub.

Step 8 In Webex Connect, configure channel assets for each media channels such as SMS, chat, and email. For more information, see Channel Asset Configuration.

Step 9 Configure node authorizations in Webex Connect to inject new tasks, retrieve the task list, and close tasks directly on CCE. For more information, see CCE Task Nodes and Node Authorizations.

Step 10 Create flows using the Webex Connect Flow Builder feature for the various digital channels interactions such as SMS, Email, and Live Chat. You can import the template flows and customize them to suit your requirements. For more information, see *Flow Configuration using Sample Templates*.

Step 11 Create mandatory ECC variables in the Unified CCE Administration portal (**Overview** > **Call Settings** > **Route Settings** > **Expanded Call Variables**). The ECC variables are required to identify the incoming tasks as Digital Routing tasks and the tasks to carry the Webex Engage conversation ID. For instructions about how to create ECC variables, see the *Add and Maintain Expanded Call Variables* section in the online Help that is integrated with the tool. For the list of mandatory ECC variables, see the ECC Variables for Digital Routing Tasks, on page 14.

Step 12 Associate the MRDs that you have created for the digital channel integration using Webex Connect to the `5000.UQ.Desktop` Application path so that the agents can login to the Manage Digital Channels gadget. For instructions, see the online Help that is integrated with the Application Path List tool.

Step 13 Configure digital channel capabilities for your customer in the Unified CCE Administration portal. See Manage digital channels.

Step 14 Create routing scripts for digital channel interaction. For more information, see *Example Scripts for Digital Channel Interactions Using Webex Connect* in the Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise.

Step 15 Add the Manage Digital Channels gadget to the Cisco Finesse desktop layout. See the *Add Manage Digital Channels Gadget* section in the Cisco Finesse Administration Guide.

Step 16 Start interacting with customers using the Manage Digital Channels gadget. See the *Manage Digital Channels Gadget Guide*.

Generate public key certificate using 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.

Note You cannot use a self-signed certificate to provision digital channels in Webex Control Hub.

To generate the public key certificate:

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

Step 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.

Step 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 the signed certificate.

Step 4 Save the contents of the CA provided certificate generated using the CSR in step 3, into a file with extension .pem or .der.

You must upload the certificate in Control Hub when you provision the Digital Channels for an Organiztion. For instructions, see Provision Webex Connect digital services for your organization.

Note You need not upload the CA-signed certificate in the Cisco IdS server.

Regenerate public key certificate using Cisco IdS

To regenerate a public-private key pair:

Before you begin

You need to regenerate the public key certificate when the certificate is compromised, or when the CA-signed certificate or the Cisco IdS certificate expire. Regenerating the certificates for token signing requires all agents to logout and relogin to the Cisco Finesse desktop. Therefore, ensure that you plan for downtime to your Contact Center before you regenerate the public-private key pair that Cisco IdS uses to authenticate agents.

Step 1 Sign in to **Cisco Identity Service Management** using the following URL: https://<*hostname of Cisco IdS server*>*:8553*/cmplatform.

Step 2 From the left navigation pane, choose **Settings** > **Security** > **Keys and Certificates**.

Step 3 In the **Encryption/Signature Key** area, click **Regenerate**.

After you regenerate the new key pair, you must reboot Cisco IdS so that the agents can relogin to their applications. Ensure that a certificate authority signs the regenerated public-private key pair. You must reupload the CA signed certificate to the Control Hub for your agents to resume their tasks in the Manage Digital Channel gadget. For instructions, see Provision Webex Connect digital services for your organization.

Reverse proxy configuration for digital channel interaction

A reverse proxy server is an intermediary server that you must deploy in the Demilitarized Zone (DMZ) in your network. The reverse proxy server forwards task requests and user configuration notifications from Webex Connect and Webex Engage to the Digital Routing and DataConn services respectively, that are

running on the Cloud Connect platform. The task requests such as transfer and close that originate from Cisco Finesse are directly invoked on the Digital Routing service.The reverse proxy configuration enables automatic failover to the stand-by Cloud Connect in case of failures.

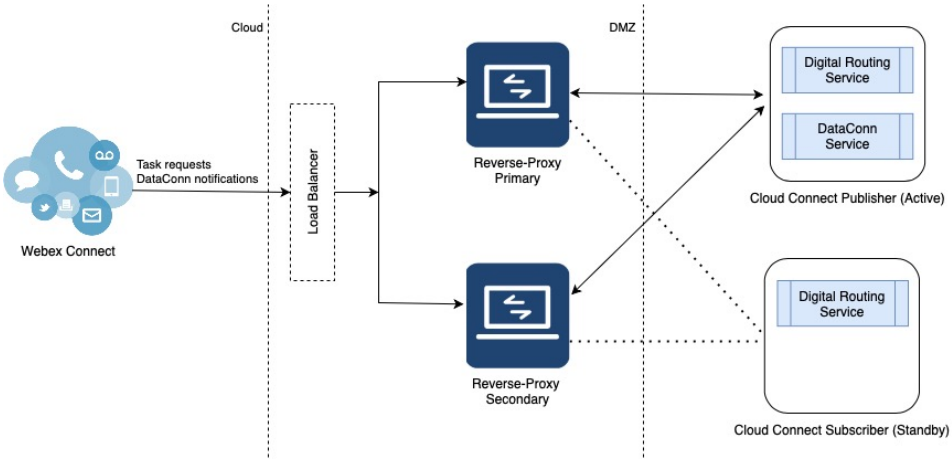
Reverse proxy deployment model

CCE supports the following two deployment models for reverse proxy:

- A pair of reverse proxy servers with physical load balancer.
- A pair of reverse proxy servers with DNS-based load balancer.

Note When using this deployment model with VPN-less Finesse, be sure to set up separate FQDNs for the reverse proxy servers so that Finesse desktop can access the specific reverse proxy IP addresses.

The following diagram depicts the task flow and the reverse proxy deployment model.



The following describes tasks requests and Dataconn flow:

- The Cloud Connect receives task requests from Webex Connect through either a single reverse proxy or a pair of reverse proxy servers deployed in the DMZ network, that is front-ended with a Load Balancer.
- The tasks are sent through reverse proxy only to the active side of Cloud Connect in both the deployment scenarios. That is, when a pair of reverse proxy servers are deployed, both the primary and the secondary reverse proxy servers are connected only to the active side of Cloud Connect.
- The active side of the Digital Routing service can either be on the publisher node or on the subscriber node of Cloud Connect. The following is the behaviour of the Digital Routing service and the DataConn service during failover:
  - The Digital Routing service supports automatic failover and all the task requests are routed through the Digital Routing service on the new active node.
  - The DataConn service runs only on the publisher node and does not failover to the subscriber node. As a result, when there are new users created in CCE, the user configurations are not synchronized in Webex Engage until the DataConn service on the publisher node is up and running.

Note The DataConn service is active only on the Cloud Connect publisher node.

Workflow to configure reverse proxy using automated installer

Complete the following tasks to configure reverse proxy using the automated installer for digital channel interaction:

Note For customers who've opted to set Country of Operation as Canada in Control Hub, you must install the reverse proxy shipped as part of 12.6(2) ES1. This is required to ensure that the traffic originating from the tenants hosted in that data center pass through to Cloud Connect. For a list of mapping between Country of Operation and Data Center, refer to https://help.webex.com/en-us/article/n0p6xa1/Data-Locality-in-Webex-Contact-Center.

Step 1 Install and start the reverse proxy. For instructions, see Reverse Proxy Automated Installer.

Note
- Authentication is not supported at the edge of reverse proxy for all the requests and protocols that are related to digital channel interactions.
- Configuration of mapping file is not required for digital channel interactions.
- Configuration of Finesse is mandatory even if you want to install only Cloud Connect in your setup.

Step 2 Configure the digital channel client hosts.

a) Add the list of trusted digital channel client IP addresses and the corresponding hostnames to the reverse proxy Cloud Connect environment configuration file (cloudconnect.env). Use the variable, **NGX_CLOUDCONNECT_CLIENT_IPS** to add the IP addresses of Webex Connect and Webex Engage to the cloudconnect.env file.

Note
- The reverse proxy considers any requests as valid only if it receives requests from the configured hostnames or IP addresses. For more information about the environment configuration files, see Configure deployment environment configurations.
- All the currently available IP addresses of Webex Connect and Webex Engage are already added in the 'cloudconnect.env' file. Depending on your deployed datacenter, remove any IP addresses that you do not need.

b) Add load balancer or proxy IP addresses. For more information, see Load balancer, WAF, and proxy support for reverse-proxy deployments.

Step 3 Configure the Mutual Transport Layer Security (mTLS) authentication between reverse proxy and Cloud Connect.

a) Add the list of trusted reverse proxy IP addresses and the corresponding hostnames on the publisher and subscriber nodes of Cloud Connect. For details, see Add Proxy IP, on page 12.

b) Configure SSL certificate verification to establish communication between the reverse proxy host and the Digital Routing service. For details, see Configure reverse proxy host verification, on page 13.

Add Proxy IP

You must add the list of trusted reverse proxy IP addresses and the corresponding hostnames on the publisher and subscriber nodes of Cloud Connect. The Cloud Connect nodes consider any requests as valid only if they receive the requests from the configured hostnames or IP addresses. Ensure that the allowed hosts contain only the internal and external FQDN and IP address of the reverse proxy.

Note Do not add the hostname or IP address of the load balancer.

The following is an example of the CLI to add the hosts and IP addresses:

```
admin:utils system reverse-proxy allowed-hosts add 10.78.95.178
Source 10.78.95.178 successfully added
admin:utils system reverse-proxy allowed-hosts add proxy.xyz.com
Source proxy.xyz.com successfully added

Restart Cisco Web Proxy Service for the changes to take effect: utils service restart Cisco
 Web Proxy Service
```

If the added hostname is not resolvable from a component, the following error is displayed:

```
admin:utils system reverse-proxy allowed-hosts add group.facebook

Either IPv4 address or hostname is invalid or is not resolvable. Now validating IPv6 address
 for source group.facebook

Operation failed, please enter valid source(s). Source group.facebook is invalid
```

After adding proxy hosts as trusted hosts through CLI on individual nodes, you must upload proxy server certificates to the Tomcat trust store of the respective components. This is required for proxy authentication to work. Otherwise, the traffic from proxy will be rejected by the components. For information about generating proxy certificates and uploading to the Tomcat trust store, see the *Set up Nginx reverse proxy certificate* and *Generate and Copy CA Certificates of VOS Components* sections in the Security Guide for Cisco Unified ICM/Contact Center Enterprise.

The following is an example of the CLI to view the list of allowed hosts and IP addresses:

```
admin:utils system reverse-proxy allowed-hosts list

Source proxy.xyz.com successfully added list

The following source(s) are configured:

1. 10.78.95.178
2. proxy.xyz.com
3. proxy125.xyz.com
```

The following is an example of the CLI to delete an entry from the list of allowed hosts and IP addresses. This command lists all the configured proxy hosts and IP addresses, and gets user input to delete specific or all proxy hosts and IP addresses.

```
admin:utils system reverse-proxy allowed-hosts delete
Select the reverse-proxy source IP to delete:

 1) 10.78.95.178
 2) proxy.xyz.com
```

```
 3) proxy125.xyz.com
 4) all
 5) quit

Please select an option (1 - 5 or "q" ): 1

Delete operation successful
```

Configure reverse proxy host verification

Reverse proxies are deployed in DMZ and are therefore security sensitive. So, the communication between the proxy and the upstream server that it is proxying, is recommended to be secured to a higher degree. This is achieved by having both the TLS certificates and the copy that is uploaded to the relevant servers be mutually verified. Run the following CLI commands on the publisher and subscriber nodes of Cloud Connect to configure SSL certificate verification for establishing communication between the reverse proxy host and the digital routing service:

utils system reverse-proxy client-auth

This command has the following parameters:

- enable
- disable
- status

By default, the host authentication is enabled.

The following is an example of the CLI to view the status of the host authentication:

```
admin:utils system reverse-proxy client-auth status

SSL certificate verification for connections established from reverse proxy hosts is disabled
```

The following is an example of the CLI to enable the host authentication:

```
admin:utils system reverse-proxy client-auth enable
SSL certificate verification enabled for connections established from reverse proxy hosts

Restart Cisco Web Proxy Service for the changes to take effect:
utils service restart Cisco Web Proxy Service
```

The following is an example of the CLI to disable the host authentication:

```
admin:utils system reverse-proxy client-auth disable
SSL certificate verification disabled for connections established from reverse proxy hosts

Restart Cisco Web Proxy Service for the changes to take effect:
utils service restart Cisco Web Proxy Service
```

Custom reverse proxy configuration

If you choose to not use the reverse proxy installer that Cisco has provided and want to deploy a custom reverse proxy, see Guidelines for Custom Reverse Proxy Deployment.

ECC Variables for Digital Routing Tasks

This section provides the list of ECC Variables that you must configure for the Digital Channel interaction. All ECC variables are of type scalar and they are case-sensitive.

Table 3: ECC Variables

Variable	Table Size	Length	Mandatory / Optional
`user_DR_Primary`	Used to hold the FQDN of either the publisher node or the subscriber node of Cloud Connect. The FQDN denotes the Digital Routing service node that injected the task into CCE.	[1]1 character + the length of the Cloud Connect FQDN.	Mandatory
`user_DR_Backup`	Used to hold the FQDN of either the publisher node or the subscriber node of Cloud Connect. The FQDN denotes the peer node of the Digital Routing service, which can be used as a backup, in case the Primary node is unavailable.	1 character + the length of the Cloud Connect FQDN.	Mandatory
`user_DR_MediaResourceID`	Used to hold the Conversation ID of Webex Engage, which the Webex Connect injects. The Cisco Finesse uses this conversation ID to load the media in the Manage Digital Channels gadget.	16 characters	Mandatory
`user_DR_CustomerName`	Used to display the customer name in the pop-over notification that an agent views when a task is received in the Manage Digital Channels gadget.	Up to a maximum of 210 characters.	Optional

Variable	Table Size	Length	Mandatory / Optional
`user_DR_MediaChannelName`	Used to populate the media channel name for the task, if you configure and add this ECC variable in the **Unified Contact Center Enterprise Management** portal. See the *Define ECC variables* section in the Cisco Unified Contact Center Enterprise Features Guide. This is typically required if you have mapped more than one Digital Routing media channel to the same MRD but still want unique task icons to appear on the agent desktop. For example, in CCE, the system-defined media channels, chat and SMS are both mapped to the same MRD. If there is a 1:1 mapping between the media channel and MRD, the system automatically identifies the icon to be displayed on the desktop based on the media channel with which the task was associated.	8 character	Optional

[1] If there are lengthy FQDNs, the Digital Routing service compresses the FQDN such that it is below 100 characters, and thereby allow ECC variable some space out of the 2000 bytes limit per call / task to be saved by not having to send the long name. In such cases, the variable can be defined as 100 characters long in CCE. The Digital Routing service automatically fills in the first character to indicate whether the following data is compressed or uncompressed. A prefix of 1 denotes compressed data, while a prefix of 0 denotes uncompressed data.

Manage digital channels

Note To access this feature, ensure that you add Cloud Connect to the inventory in the Unified CCE Administration portal and register it.

As an administrator, perform the following configurations in the Unified CCE Administration portal to manage digital channel capabilities for your customers to reach business:

- Set up media channels such as chat, email, social, voice callback, facebook, and whatsapp. See Set up media channels, on page 16.
- Synchronize agents in AW database to Webex Engage database. See Configure User Sync, on page 19.
- Define Expanded Call Context (ECC) variables to assist agents with relevant information. See Define ECC variables.
- Integrate Cloud Connect with Webex Connect using the Open Authorization v2.0 (OAuth v2.0) standard. See Integrate Cloud Connect with Webex Connect.
- Customize the connection parameters between Cloud Connect and MR PG. See Manage connection between Cloud Connect and MR PG, on page 23.

Set up media channels

Contact Center Enterprise (CCE) supports media channels, such as Live Chat, Email, and SMS, with enhanced capabilities. These media channels are mapped to media type and Media Routing Domains (MRDs) for providing granular channel-specific reporting and agent state control. Based on this configuration, Cloud Connect associates the received task request to the appropriate MRD.

MRDs are used to map agents' skill group with the media channels, based on which the agents are assigned a task. You can map multiple media channels to the same MRD. For example, you can map SMS and Chat channels to the same MRD. For more information on MRDs, see the *Media Routing Domains* section in the Configuration Guide for Cisco Unified ICM Enterprise.

Media type is a broad category of media channels and it is different from the media class or MRD in CCE. The Digital Routing service has internal sub-limits and different maximum queue time parameters that it applies for tasks of a certain Media Type as defined by the Queue Settings. The media types are **Chat**, **Email**, **Telephony** (Voice Callback), **Social**, **Facebook**, and **WhatsApp**.

Webex Connect offers support for the pre-provisioned system defined media channels. You can add a custom media channel if one of the many media channels that Webex Connect supports in the future has to be allowed in the CCE system. If not, you can skip adding a Media Channel.

Note System-defined media channels cannot be deleted.

Queue Settings for media channels is used to configure the maximum queue limit and maximum queue time for each media type, individually. For more information on configuring queue settings for media channels, see Configure queue settings.

To set up media channels:

Step 1 In the Unified CCE Administration portal, navigate to **Overview** > **Digital Channels** > **Digital Channel Settings** > **Media Channel**. The list of existing media channels is displayed in a grid. This is the default page.

Step 2 Click **New**. On the **New Media Channel** page, do the following:

a) In the **Name** field, type the name of the media channel.

b) From the **Media Type** drop-down list, select the required media type.

c) In the **Media Routing Domain** field, search and select the MRD that you want to map to the media channel.

Step 3 Click **Save**. The channel is added to the list on the **Digital Channel Settings** page.

When you have created a media channel, you can modify only the **Media Routing Domain** field. If you want to modify any other fields, you must delete the media channel and create afresh. To delete a media channel, hover over the media channel and click the **X** icon.

Configure queue settings

The Digital Routing service maintains a queue for all the incoming tasks. The service accommodates up to a maximum of 100,000 tasks in the queue at any given point in time. Out of these 100,000 tasks, you can configure the maximum number of tasks that can be queued for each media type in the Digital Routing service. The following are the default values in percentage for each media channel:

Media type	Queue setting in %	Description
Email	50%	50,000 tasks can be queued for Email.
Social	40%	40,000 tasks can be queued for SMS.
Voice callback	5%	5,000 tasks can be queued for Voice callbacks.
Chat	5%	5,000 tasks can be queued for live chat.

You can also define the maximum duration for which a task remains in the queue for each media type.

The following are the scenarios in which the Digital Routing service rejects the tasks and sends them back to Webex Connect:

- The number of tasks exceeds the maximum value that is configured for the media channel. For example, consider that the Digital Routing service queue has 50,000 email tasks, which is the maximum queue setting defined for the Email media channel. If Webex Connect further injects email tasks, the Digital Routing service rejects the incoming tasks and sends them back to Webex Connect with an error code of 20286 (MEDIA_TYPE_QUEUE_LIMIT_EXCEEDED). For example, a flow developer can decide to provide appropriate messaging to the end customer and invoke other backend systems to denote queue capacity issues.
- A task exceeds the maximum duration that is defined for the media channel. The Create Task node is successful. There is a Closed webhook event triggered when the task gets auto-closed after exceeding the maximum time in queue, with a specific disposition code set to CD_MAX_DIALOG_LIFETIME_EXCEEDED.

The flow debug logs show the error code returned by the Create Task node API call. For more information about the Create Task node, see Create Task.

To configure the queue settings for the media channels:

Step 1 In the Unified CCE Administration portal, navigate to **Overview > Digital Channels> Digital Channel Settings > Media Channel**.

Step 2 Click **Queue Settings**.

Step 3 Enter the required values in percentage for each media channel.

Note Make sure that the sum of the percentage values configured for all the media channels is 100.

Step 4 Define the duration in days, hours, and minutes for each media channel. This is the maximum duration for which a task that belongs to the specific media channel remains in the queue after which it gets timed out. The default durations are 3 days for Email and Social media channels, and 2 hours for Voice callbacks and Chat media channels.

Step 5 Click **Save**.

Synchronize CCE agents to Webex Engage

For CCE agents to be able to take up the digital channel tasks that are initiated from Webex Connect, the agent configuration details must be synchronized between the AW server and Webex Engage. The DataConn service that is running on the Cloud Connect platform is responsible for synchronizing agent configurations. The default periodic interval for synchronization is 30 minutes. Only the agent records created or updated during the synchronization period will be synchronized with Webex Engage.

The Finesse Desktop SSO login depends on the agent information that is synchronized between AW server and Webex Engage. The agent identity that is used to authenticate the login request, is possible only after this synchronization is complete.

Important considerations for agent synchronization

Consider the following when you synchronize agents between CCE and Webex Engage for the digital channel integration:

- After synchronizing the agents details between CCE and Webex Engage, if you delete an agent in CCE, the agent status in Webex Engage changes to Inactive. However, the agent record is not deleted in Webex Engage.
- The synchronization of agents details is possible only on the publisher node of Cloud Connect. Also, any update to the agent configuration takes effect only when the publisher node is up and running.
- Ensure that you create agents and update the agent configurations in CCE only. Do not create or update agent configurations in Webex Engage.
- Ensure that you always have the agent details synchronized between CCE and Webex Engage for the agents to be able to login to the Manage Digital Channels gadget.
- When you create a new agent in CCE, you must not associate the agent with an existing person record that is already associated with another agent. If you do not select any person record in the **Select Person** drop-down list in the **ICM Configuration Manager** > **Tools** > **Explorer Tools** > **Agent Explorer** tool, a new person record is automatically created for the agent. Also, you must not associate one person record with multiple agents.
- You must not modify the email address of the agent after the agent record and person record are created. If you need to update the email address, contact Cisco Support.

Enable agents for digital channels

To enable agents for digital channel interaction:

Step 1 In the **Configuration Manager**, navigate to **Explorer** > **Agent Explorer** .

Step 2 Click on **Retrieve** button, and select the agent for whom you want to enable the digital channel interaction.

Step 3 Check the **Support Digital Channel** check box to enable the agent for digital channel interaction.

Step 4 Click **Save**.

Note You can perform the above task from the **List Tools**>**Person List** screen as well. For more information about List Tools, see the List Tools Online Help. Click the help button in List Tools to access the Online Help.

Configure SQL user account for digital channels

To configure SQL user account for digital channels:

Step 1 Launch Microsoft SQL Server Management Studio using System Administrator login credentials on the Administration and Data Server.

Step 2 Navigate to **Security** > **Logins**, right-click **Logins** and select **New Logins**.

Step 3 On the General screen:

a) Enter the Login Name.
b) Select **SQL Server authentication**.
c) Enter and confirm the password.
d) Uncheck **Enforce password policy**.

Step 4 In the **Server Roles** page, check the **Public** check box.

Step 5 On the **User Mapping** page, do the following:

a) Check the **Real-time database** check box.
b) In the **Database role membership for** area, check the **db_datareader** check box.

Step 6 Click **OK**.

What to do next

Ensure that you configure SQL User Account on both the primary and secondary AW databases.

Configure User Sync

To synchronize the CCE agents who are configured for digital channel interactions with Webex Connect:

Step 1 In the Unified CCE Administration portal, navigate to **Overview > Digital Channels> Digital Channel Settings > User Sync**.

Note The DataConn service is active only on the publisher node of Cloud Connect. Ensure that the publisher node is accessible for you to view the **User Sync** page.

Step 2 In the **Network Entry Point** field, enter the hostname or FQDN of the load balancer or the reverse proxy server based on your deployment. It is through this network entry point that the Webex Engage sends the response request to the DataConn service for agent synchronization.

For more information about network entry point, see the *Synchronize CCE agents to Webex Engage* section in the Solution Design Guide for Cisco Unified Contact Center Enterprise .

Step 3 In the **AW Database Details** area, complete the following fields to configure the DataConn service for the Primary and the Secondary Server:

a) In the **AW Datasource Host** field, enter the IP address or the host name of the AW server that has the agent configurations.
b) In the **Port** field, enter the SQL port number of the AW database server.
c) In the **Database Name field**, enter the name of the AW database server.
d) In the **Database User ID** and **Password** fields, enter the user ID and password of the SQL user account that you created for digital channels. For more information see the *Configure SQL user account for digital channels* section in the Cisco Unified Contact Center Enterprise Features Guide.

Step 4 Click **Test Connection** to make sure that the DataConn service can read the data from the AW Primary server.

Step 5 Switch on the **Enable Failover** toggle button to enable the failover to the Secondary AW server.

Step 6 To synchronize agents, choose one of the following options:

a. Enable the **Enable Sync** toggle button to automatically synchronize agents in an interval of 30 minutes.

b. Click **Sync Now** to manually synchronize the agents. This option is available only when the **Current Sync Status** field appears as **Scheduled**.

Note If you recreate your AW Database to fix any errors, ensure that you disable User Sync before starting with the recreation process. Enable the User Sync only after the AW Database is created and synchronized with the central controller database.

Step 7 In the **Last sync** field, view the date, time and status of the previous synchronization.

Step 8 In the **Agents Sync Details** field, view the number of agents that are synchronized successfully. The number of agents appears as a clickable link. Click the link to view the list of agent records that have failed to synchronize and the list of agent records that are pending for synchronization. You can choose to refresh the agent records at any given point in time.

Step 9 In the **Current Sync Status** field, you can view one of the following statuses:

a. **No sync is in progress or scheduled**—This status appears when the **Enable Sync** toggle button is off.

b. **Scheduled**—This status appears when the **Enable Sync** toggle button is on.

c. **In Progress**—This status appears when the scheduled sync or manual sync is in progress.

d. **Manual Sync Failed** —This status appears when the manual sync has failed.

e. **Unknown**—When sync status is not available.

Step 10 Click **Save**.

Configure network entry point for agent synchronization using CLI

You must configure the network entry point for the DataConn service that is running on the Cloud Connect platform. It is through this network entry point that the Webex Engage sends the return request in response to the user configuration API request that the DataConn service sent to Webex Engage. For more information, see the *Synchronize CCE agents to Webex Engage* section in the Solution Design Guide for Cisco Unified Contact Center Enterprise .

To configure the host for the network entry point, run the following command on the Cloud Connect console:

```
set cloudconnect dataconn settings
```

The following is the example of the CLI configuration:

```
admin:set cloudconnect dataconn settings
Fetching existing configuration...
Enter the Config details to be saved:
Network Entry Point Host: proxyhost.domain.com
The config details updated successfully.
```

To display the host that is configured for the network entry point, run the following command on the Cloud Connect console:

```
show cloudconnect dataconn settings
```

Field mapping between Webex Engage and CCE

Following table lists the payloads and attributes mapping between Webex Engage and the Contact Center Enterprise (CCE):

Webex Engage fields	CCE fields	Remarks
firstName	Person.FirstName	User's first name will contain only alphanumerics. All special characters from the given name will be removed. If this field is empty, the first name will be the username, which is obtained from the user's email without domain name.
lastName	Person.LastName	User's last name will contain only alphanumerics. All special characters from the family name will be removed. If this field is empty, the last name will be the first character of the username, which is obtained from the user's email without domain name.
aliasId	Person.LoginName	Agent's login name. Single Sign-On (SSO) authentication matches the Person.LoginName from AW database against the UPN or SamAccountName data from Cisco IdP and is used as the user_id in the SSO token. The Person.LoginName information is uploaded as aliasID in Webex Engage database for the purposes of token verification.
emailId	Person.Email	
loginId	Agent.SkillTargetID	Webex Engage uses this mapping to route the agent to the correct interaction.

Webex Engage fields	CCE fields	Remarks
concurrency	Not mapped	The Concurrency value is optional and is set to “99” by default on Webex Engage.
roleType	Fixed to customer_care	This is the fixed user role that is assigned to an agent.
status	Agent.Deleted	If a deleted flag is set in the CCE, the value is inactive.
loginUsingEmail	false	By default, every user on Webex Engage is created with the "loginUsingEmail" value as false.
role	team_agent	This is the fixed role that is assigned to team_agent.

Define ECC variables

The Expanded Call Context (ECC) variables are data that are embedded within the call and are visible to the agent on the Agent Desktop. ECC variables are passed back and forth in ECC payloads. ECC variables assist the agent with relevant information without the customer having to repeat the same information.

To define the ECC variables:

Step 1 In the Unified CCE Administration portal, navigate to **Overview > Digital Channels > Digital Channel Settings > ECC Variable**.

Step 2 On the **ECC Variable** page, click the plus icon (+). The **Add ECC Variable** page appears with existing variables **Name** and **Enabled** details. It excludes the built-in variables.

Step 3 Select the required variable. The **ECC Variable** page displays the newly added ECC variable.

Step 4 Click **Save**.

Integrate Cloud Connect with Webex Connect

You can integrate Cloud Connect with Webex Connect using the Open Authorization v2.0 (OAuth v2.0) standard. You must configure Webex Connect client ID and client secret in the Digital Routing service for the service to gain access to Webex Connect using the access token. This set of client credentials uniquely identifies the Cloud Connect and its permissions to access Webex Connect.

Note The Cloud Connect Management service is active only on the publisher node of Cloud Connect.

To configure client credentials for OAuth v2.0 access token:

Step 1 In the Unified CCE Administration portal, navigate to **Overview** > **Digital Channels** > **Digital Channel Settings** > **Integration**.

Step 2 On the **OAuth2 Authentication Details** page, perform the following steps.

a) In the **Name** field, enter a name for the Cloud Connect integration. This field is editable.
b) In the **Description** field, enter a description of what the client application does.
c) In the **Client Id** and **Client Secret** fields, enter the client id and secret key that you can retrieve from the Webex Connect portal (navigate to **Assets** > **Integrations** > **CCE pre-built integrations** > **Actions** > **Manage**).
d) In the field, enter the password that is provided to you at the time of registration. This is the secret key that was used for generating the token.
e) In the **Token Request URL** field, provide one of the following URLs based on the location of Webex Connect datacenter:

- Ireland—https://keycloak-authservice.imiconnect.io/auth/realms/imiconnect_uk_prod/token
- London—https://keycloak-authservice.imiconnect.eu/auth/realms/imiconnect_ln_prod/token
- Sydney—https://keycloak-authservice.imiconnect.com.au/auth/realms/imiconnect_syd_prod/token
- The United States of America—https://keycloak-authservice-us.imiconnect.io/auth/realms/imiconnect_us_prod/token
- Canada—https://keycloak-authservice.imiconnect.ca/auth/realms/imiconnect_cn_prod/token

f) From the **Method** drop-down list, select the **POST** method for Webex Connect integration.
g) 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**.
h) 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*.
i) (Optional) In the **Header List** section, click **+** icon to add a header name and value and click **Add**. The header name and value are used to pass any additional information that Webex Connect may require for Cloud Connect integration.

Step 3 Click **Save** to save the OAuth2 authentication details.

Step 4 Go to the **Webhook** tab to register the Webhook URL in the Digital Routing service. To fetch the Webhook URL:

a) In the Webex Connect portal, navigate to **Assets** > **Integrations**.
b) In the CCE pre-built integrations row, from the **Actions** column, select **Manage**. The **Manage Integration - Prebuilt Integration** page appears.
c) In the **Inbound Events** section, copy the Webhook URL.

Step 5 Paste the URL in the **Webhook URL** field in the Unified CCE Administration portal (**Overview** > **Digital Channels** > **Digital Channel Settings** > **Integration** > **Webhook**).

Manage connection between Cloud Connect and MR PG

To customize the connection parameters between Cloud Connect and Media Routing Peripheral Gateway (MR PG):

Step 1 In the Unified CCE Administration portal, navigate to **Overview** > **Digital Channels** > **Digital Channel Settings** > **Advanced Settings**.

Step 2 The **Port** is a display-only field and the default value is **38001**. It is through this port that Cloud Connect and MR PG communicates with each other.

Step 3 The **Secured** toggle switch is turned on by default. It is to establish a secured connection between Cloud Connect and MR PG. You can turn-off this toggle switch to disable the secure connection.

Step 4 Click **Save**.

Disposition codes for digital channel interaction

The Webhook notification that the Digital Routing service invokes for a closed task contains a disposition code that denotes the reason for the task closure. Using the disposition code in the Close Task, a flow designer can perform different actions as needed in the Webex Connect flow. For example, if a task fails after it has been queued, an error message can be displayed to customers with the option to contact the business through other support channels or schedule a callback, as opposed to a message indicating that the task has been closed due to a system error.

The following are the list of disposition codes that are available for digital channel interaction:

Table 4: Disposition Codes

Task Disposition	Disposition code value	Description
Normal End	CD_NORMAL_END_TASK	The task ended normally.
Transfer	CD_TASK_TRANSFER	This indicates the disposition when an agent initiates a task transfer using the Finesse desktop. The transfer operation triggers a Webhook notification to Webex Connect which would trigger another NEW task with the same TaskID using the Transferred workflow.

Task Disposition	Disposition code value	Description
Transfer	CD_TASK_TRANSFERRED_ON_AGENT_LOGOUT	This occurs when Finesse server detects an Agent logout, or when the Agent closes the desktop while still having digital channel tasks that aren't completed or Closed yet. The Finesse server initiates a transfer of the task to the same script selector that routed the original task to the Agent.
Transfer	CD_RING_NO_ANSWER	This indicates that the task timed out while waiting to be accepted by an Agent. Finesse invokes the TaskAction API with the Operation Code "Routed-Transfer" to redirect the task to another agent.
Transfer	CD_TASK_TRANSFER_TIMEOUT	The Digital Routing service sends a TRANSFERRED Webhook notification and waits for a maximum of 15 seconds for Webex Connect to complete its side of the processing, and for a create task request to be resubmitted from Webex Connect with the same TaskID. If Webex Connect fails to reinject the task into the Digital Routing service, then the Digital Routing service marks the task as Closed with this disposition code.

Task Disposition	Disposition code value	Description
Task Lifetime Exceeded	CD_MAX_DIALOG_LIFETIME_EXCEEDED	The task ended because it exceeded the maximum task duration defined for the Media Routing Domain (MRD).
Customer Abandoned	CD_TASK_CUSTOMER_ABANDON	The disposition code is sent from Webex Connect when the task was abandoned by the customer before an agent was assigned to the task.
Customer Abandoned	CD_TASK_ABANDONED_WHILE_OFFERED	The customer cancelled the task before the agent began working on the task. In this task disposition, the agent has viewed the offered task, but the dialog was deleted before the agent accepted the task.
Other	UNKNOWN	The reason for the task termination is unknown.
Other	CD_TASK_INVALID_MEDIA_RESOURCE_ID	The task gets closed by Finesse when the media can’t be loaded in the Webex Engage widget. This depends on a mandatory ECC variable that is used by CCE to relay the Webex Engage ConversationID to Finesse desktop. This is to ensure that the media can be loaded in the widget, once the Agent selects the task.

Task Disposition	Disposition code value	Description
Other	CD_TASK_ENDED_DURING_APP_INIT	This indicates that the task was in progress when the connection between the CTI server and Finesse went down, and the task ended before the connection was reinitialized. When the connection was reinitialized, the Agent PG ended the task.
Failed Task Submission	CD_TASK_FAILED_SENDING_MR_REQUEST	This indicates that the task could not be sent to the MR PG owing to an error. The task is automatically marked as Closed with this disposition code.
Failed Task Submission	CD_FAILED_CREATING_NEW_TASK_EXECUTOR	Internal error in the Digital Routing service while processing a new task request. Such tasks get automatically closed with this disposition code.
Failure	CD_FAILED_INVALID_NEW_TASK_MESSAGE	The task failed as the new task message was invalid.
Failure	CD_FAILED_MEDIA_ROUTING_DISABLED	The task failed as the ICM media routing was disabled.
Failure	CD_FAILED_NO_SCRIPT	The task failed as there was no script to run.
Failure	CD_FAILED_INVALID_MRD_ID	The task failed as a result of invalid Media Routing Domain ID.
Failure	CD_FAILED_ICM_TIMEOUT	The task failed as a result of ICM timeout.

Task Disposition	Disposition code value	Description
Failure	CD_FAILED_INVALID_SCRIPT_SELECTOR	The task failed as a result of invalid dialed number or script selector.
Failure	CD_FAILED_NO_TARGET	The task failed because there was no agent available to be assigned for the task.
Failure	CD_FAILED_ROUTER_RELEASED_TASK	This disposition code is as a result of a Release Node being used in the CCE routing script to terminate the task purposely.
Failure	CD_FAILED_UNKNOWN_ROUTING_PROBLEM	The task failed as a result of unknown routing problem.
Failure	CD_FAILED_DUPLICATE_NEW_TASK_REQUEST	The task failed as it was a duplicate new task request.
Failure	CD_FAILED_UNSUPPORTED_SERVICE_REQUESTED	The task failed as the service requested was unsupported.
Failure	CD_FAILED_AGENT_NOT_MEMBER_OF_QUEUE	The task failed as agent not a member of the specified skill group of the precision queue.
Failure	CD_FAILED_INVALID_QUEUE_TYPE_OR_ID	The task failed as the specified Queue Type or ID. was invalid.
Failure	CD_FAILED_INVALID_DIALOG_ID	The task failed as the dialog ID was invalid.
Failure	CD_FAILED_INVALID_AGENT_ID	The task failed as a result of invalid agent ID.
Failure	CD_FAILED_AGENT_OVER_TASK_LIMIT	The task failed as the agent exceeded the task limit.

Task Disposition	Disposition code value	Description
Failure	CD_FAILED_UNSUPPORTED_AGENT_PERIPHERAL_GATEWAY	The task failed as it was unsupported by the agent peripheral gateway for the service request.
Failure	CD_FAILED_INVALID_AGENT_STATE	The task failed as the agent state was invalid.
Failure	CD_FAILED_INVALID_QUEUE_FOR_MRD	The task failed as a result of invalid queue for Media Routing Domain.
Failure	CD_FAILED_NO_PICK_PULL_NODE	The task failed as no pick pull node available.
Failure	CD_FAILED_AGENT_NOT_READY	The task failed as a result of agent not ready.
Failure	CD_FAILED_UNKNOWN	The session failed for unknown reason.
Failure	CD_FAILED_SESSION_ABANDON	The session failed as it was abandoned.
Failure	CD_FAILED_COMM_FAILURE_ROUTER_AND_PG	The communication failed as a result of router and PG failure.

Agent Request or Web Callback using Webex Connect

The Agent Request or Web Callback feature allows a customer to initiate a request on the web that results in a call from an agent. Use the Webex Connect platform to allow your customers to place a Web Callback request to the contact center. The customer needs to fill out a form with the preferred phone number to receive a callback as soon as an agent is available. Use this feature to switch between media channels when the wait time is more on a channel. For example, if the Live Chat media channel is experiencing an extended wait time, you can offer your customers an option to receive a voice callback from the contact center instead of the customer waiting in the Live Chat channel. The Webex Connect platform provides you the ability to route the web callback requests towards Contact Center Enterprise along with call variables and ECC variables that can carry customer-specific task context.

When CCE receives an agent request or a web callback request, it performs the following tasks:

- Processes the callback request.
- Routes the callback request to an agent and places a call from the agent's phone to the customer.

- Notifies the Webex Connect platform through a Closed Webhook notification that the agent has been selected.

The callback request is automatically closed from the Digital Routing service.

Agent Request Scenarios

1. From the web, the customer requests to speak to an agent.
2. The customer receives feedback that the request is accepted.
3. The customer receives feedback that the call is queued and the estimated wait time.
4. The customer receives feedback that a call is on its way.
5. The agent's phone places an outbound call.
6. The agent is presented with call context.

If	Then
The customer is available	The customer receives and answers the call, and speaks to the agent.
The customer is busy when the callback occurs	The agent receives a busy tone.
The customer does not answer when the callback occurs	The agent hears ringing.
The customer cancels the callback before an agent is selected	There is no impact on the agent.

Configure Web Callback

To configure a Web Callback request:

Table 5: Web Callback Configurations

Step #	Configure	Where	Configuration Details	Reference
1	Network VRU	**Configuration Manager** > **Network VRU Explorer** tool	Create a **Type 2** Network VRU to queue voice callback tasks if an agent is not available to handle them.	For instructions about how to create a Network VRU, see the online help that is integrated with the Network VRU Explorer tool.

Step #	Configure	Where	Configuration Details	Reference
2	Network VRU script	**Configuration Manager** > **Network VRU Script List** tool	Add a Network VRU script that references the Network VRU that you created in step 1. Use the script for estimated wait time.	For instructions about how to create a Network VRU script, see the online help that is integrated with the Network VRU Script List tool.
3	Call Type	**Configuration Manager** > **Call Type List** tool	Create a call type to handle calls from an agent request voice callback.	For instructions about how to create a Call Type, see the online help that is integrated with the Call Type List tool.
4	Dialed Number / Script Selector	**Configuration Manager** > **Dialed Number/Script Selector List** tool	**1.** Create a Script Selector corresponding to the Media Routing peripheral routing client that is used to integrate with Cloud Connect's Digital Routing service. **Note** The Webex Connect platform uses this script selector to request agents for voice callback. The script selector configured here must be the same as the one entered in the Webex Connect Platform. **2.** On the **Attributes** tab, from the **Media Routing Domain** drop-down list, select **Cisco_Voice** **3.** On the **Dialed Number Mapping** tab, map the script selector to the Call Type that you created in step 3.	For instructions about how to create a Script Selector, see the online help that is integrated with the Dialed Number/Script Selector List tool.

Step #	Configure	Where	Configuration Details	Reference
5	Routing script	**Script Editor**	Create a routing script and schedule it for the Call Type that you created in step 3.	See the following sections in the Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise: • For instructions, see the *Create Routing Script* and *Schedule Routing Script* sections. • For a script example, see the *Example Digital Channel Interactions Using Webex Connect*.
6	ECC Variables	**Configuration Manager** > **Expanded Call Variable List** tool	Add one or more ECC variables for the callback request. **Note** Arrays are not supported with the Web Callback feature. The CCE solutions support the Latin 1 character set only for Expanded Call Context variables and Call variables.	For instructions about how to create a ECC Variable, see the online help that is integrated with the Expanded Call Variable List tool.
7	A representative flow using CCE Create Task node	**Webex Connect** > **CCE Create Task**	In the **Media Type** and **Media Channel** fields, select **Web Callback**.	For more information, see Create Task.

In the Unified CCE Administration portal, navigate to **Overview** > **Digital Channels** > **Digital Channel Settings** > **Media Channel**. You will see that the "Voice" media channel that has the **Media Type** field set as **Telephony** is associated with the "Cisco_Voice" MRD. For more information, see Set up media channels, on page 16.

In the **Queue Settings** page, ensure that you have the right number of Web Callback requests (which by default is 5000 tasks) that you want to retain in the Digital Routing queue. For more information, see Configure queue settings, on page 17.

Agent Targeting Rule for Web Callback

In addition to the above configurations, ensure that the Agent Targeting rule for the Agent Peripheral also applies to the MR PG routing client, which is required for the Digital Routing service, without which voice calls cannot be routed.

Reporting

Webex Connect reporting

You can view reports related to digital channel information from within the Webex Connect tenant. For more information, see Reports.

View and download the following reports from Webex Connect:

- Count of inbound messages at a channel level
- Count of outbound messages to customers at a channel level
- Flow of tasks counts
- Other standard dashboard reports

Digital Routing reporting

The Cisco Unified Intelligence Center reports include data for voice calls and Digital Routing tasks.

For more information about multichannel reporting data, see the Cisco Unified Contact Center Enterprise Reporting User Guide.

The Digital Routing media channels are mapped to MRDs and the Unified Intelligence Center reports can be filtered based on these mapped MRDs. Use the following All Fields and Live Data report templates to view the summary reports for each digital channel:

- Agent Real Time
- Agent Skill Group Real Time
- Peripheral Skill Group Real Time All Fields
- Precision Queue Real Time All Fields
- Agent Precision Queue Historical All Fields
- Agent Skill Group Historical All Fields
- Peripheral Skill Group Historical All Fields
- Precision Queue Abandon Answer Distribution Historical

- Precision Queue Interval All Fields
- Skill Group Abandon-Answer Distribution Historical
- Precision Queue - Live Data
- Skill Group - Live Data

Digital Routing task-level reporting

The task-level reporting is not available in Cloud Connect. Tasks in the Digital Routing service remain in the service memory only for 15 minutes after the tasks are closed. There is no persistence of closed tasks in the Digital Routing service. This 15-minute interval is a system setting and you cannot modify it.

The individual tasks that are escalated to CCE can be queried using the Route_Call_Detail (RCD) and Termination_Call_Detail (TCD). For more information see the *All Tables* chapter in the Database Schema Handbook for Cisco Unified ICM/Contact Center Enterprise.