Help Desk Using Cisco Unified CCX

Technology Design Guide

June 2017

Contents

Contents | Deployment Details

Preface

Cisco Validated Designs (CVDs) provide the foundation for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Cisco engineers have comprehensively tested and documented each CVD in order to ensure faster, more reliable, and fully predictable deployment.

CVDs include two guide types that provide tested and validated design and deployment details:

- **Technology design guides** provide deployment details, information about validated products and software, and best practices for specific types of technology.
- **Solution design guides** integrate or reference existing CVDs, but also include product features and functionality across Cisco products and may include information about third-party integration.

Both CVD types provide a tested starting point for Cisco partners or customers to begin designing and deploying systems using their own setup and configuration.

Scope

This guide covers the following technology areas and products:

- Unified communications applications, such as IP telephony and contact center
- Telephony call agent
- Cisco Contact center server
- Cisco SocialMiner
- Cisco Finesse Desktop
- Cisco Unified Intelligence Center
- Virtualized servers
- Cisco IP telephones
- Integration of the above with LAN and data center switching infrastructure

For more information, see the "Design Overview" section in this guide.

Proficiency

This guide is for people with technical proficiencies—or equivalent experience in **CCNA Collaboration**—1 to 3 years in designing, installing, and troubleshooting voice and unified communications applications, devices, and networks.

Comments and Questions

If you would like to comment on a guide or ask questions, please email: collab-mm-cvd@external.cisco.com.

Contents | Deployment Details

Disclaimer

The IP address scheme used in this document is for representational purposes only.

Introduction

Historically, the ability to easily add functionality into the telephony environment for corporate help desks has been challenging. Traditional contact center solutions have been difficult to implement because of the additional hardware components required, and the complexity of the software needed to implement the business requirements of the contact center. In addition, it has been very difficult to integrate the contact center with the corporate data systems, due to the lack of availability of common interfaces.

This complexity has typically made the implementation of IP telephony functionality a long and involved process, and the expertise required to install and maintain the system is expensive.

This guide shows you how to reduce the complexity of deploying a contact center by using Cisco Unified Contact Center Express (CCX).

Technology Use Case–IP-based Help Desk

Organizations need a simple multichannel communication system for their employees to contact internal support departments, like Human Resources and Information Technology to provide enhanced user experience, faster problem resolution and real-time communication. Users expect timely responses to their questions and problems. However, it is easy for an issue to go unresolved, forgotten, or simply fall through the cracks if not handled promptly. The information about the user and their particular issue should be collected in real time, so a subject matter expert can help the caller as quickly as possible. Organizations need an easy way to manage their help desk from a central location without replicating costly components at their remote sites.

This design guide provides guidance on the following aspects of deploying Cisco Unified CCX:

- Simplifying deployment and management through a centralized design, while saving on infrastructure components
- Enabling of the Single Sign-On feature and related configuration on Cisco Unified CCX
- Routing of calls over the internal IP network, avoiding the use of expensive dedicated PSTN trunks
- Establishing multiple queues for each department so that agents can be assigned to one or more available queues based on their skills as well as skill levels
- Allowing agents to handle requests via multiple channels of communication like voice, email and web chat, regardless of their physical location
- Demonstrating how Context Service Finesse helps improve agent productivity and customer experience
- Providing live and historical data in easy-to-read reports to assist the help desk in responding to users
- Strategically defining the agent and supervisor desktop layouts to match the needs of the teams and their contact center activities
- Creating customized, detailed reports on key contact center metrics

Contents | Deployment Details

Design Overview

Cisco Unified Contact Center Express (Unified CCX) is an IP-based help desk solution with support for multiple channels of communication. It addresses the small to mid-size contact center market. It is tightly integrated with other Cisco Unified Communications platforms. Design and testing is performed on the suite of Cisco Unified Communications products as part of a complete solution.

Cisco Unified CCX has the features of a large contact center packaged into a single or dual-server deployment. The system scales up to 400 concurrent agents, 42 supervisors, 150 agent groups, and 150 skill groups. A UCCX implementation can be designed to support email, web chat, outbound calling, inbound calling, workforce optimization and reporting.

i	Tech Tip
	The Cisco Business Edition 6000 (BE6000) supports a maximum of 100 concurrent agents. The design and deployment discussed here otherwise apply to a full-fledged Cisco Unified Call Manager deployment.

Solution Details

The CCX help desk solution includes the following components (see Figure 1):

- Cisco Unified CCX for contact center software
- Cisco Unified CM for agent and supervisor phones
- Network Time Protocol (NTP) server for logging consistency
- Domain Name System (DNS) for name-to-IP resolution
- Syslog server for logging events (optional)

Configuration of Cisco Unified CCX is easier than traditional systems because the components communicate over the internal IP network, which helps streamline the procedures. For example, when a phone number is created on Unified CCX to reach a help desk application, no additional configuration is needed in the Cisco Unified Communications Manager (Unified CM). The configuration is sent over the network to Unified CM and the directory number is created. Unified CM is automatically configured to pass calls for the directory number to Unified CCX for further processing.

When a call is placed to the help desk, it is first processed by Cisco Unified CM, which recognizes that the number is destined for the Cisco Unified CCX application server. Unified CCX receives the incoming call and identifies which application script is needed to handle the request based on the extension number that was dialed. The script plays prompts and collects digits as dictated by the steps in the script and, if necessary, uses the information from the caller to select an appropriate agent. If an assigned agent is not available, the call is put into an appropriate queue and a recorded message or music is streamed to the caller. As soon as an agent is available, Unified CCX instructs Unified CM to ring the agent's phone. When

Contents | Deployment Details

the agent picks up, relative call context can be displayed in the agent's desktop application using the Context Services as the call is delivered to the answering agent. This ensures that the agent has the information they need to support the customer.

Cisco SocialMiner checks for new emails or web chats periodically and notifies the Cisco Unified CCX about the new contact. Cisco Unified CCX queues the contact in the appropriate queue. When an agent is available it assigns the email/webchat request. The agent can click the accept button and start responding.

Figure 1. Help Desk using Cisco Unified CCX
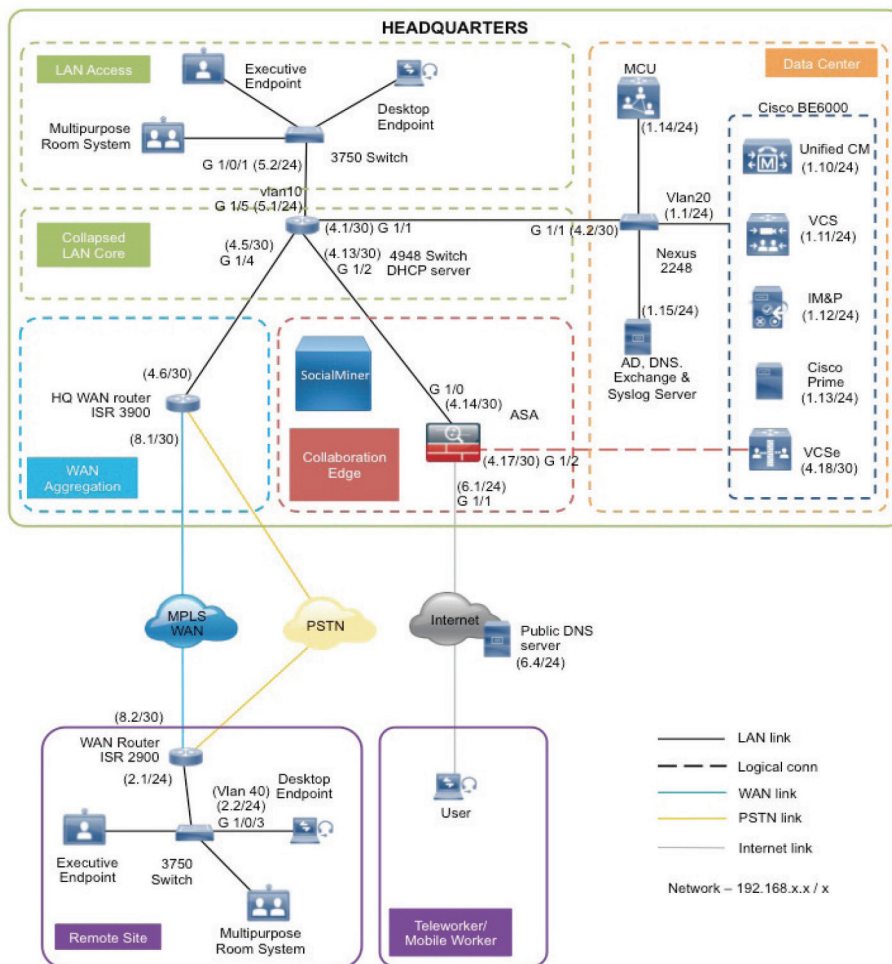
Deployment Details

Cisco Unified CCX runs on the same Linux operating systems as other Unified Communications platforms from Cisco. You install the operating system with the application by using the standard installation DVD or ISO file.

This guide has the following sections

1. Preparing the Platform for Cisco Unified CCX
2. Installing the Cisco Unified CCX
3. Configuring the Helpdesk
4. Configuring the Finesse Desktop
5. Configuring the Cisco Unified Intelligence Reporting

Pre-deployment Checklist

✓	Item
☐	Fill in the Easy Access Configuration Sheet for your reference during the deployment process.
☐	Establish network connectivity for BE6000 server to application and DMZ networks.
☐	Obtain license files from the Cisco licensing system.
☐	Download the Open Virtualization Archive (OVA) file from the Cisco website, here: https://software.cisco.com/download/release.html?mdfid=286279660&softwareid=280840578&os=&rele_ase=10.6%281%29&relind=AVAILABLE&rellifecycle=&reltype=latest&i=!pp
☐	Define the required DNS records on the DNS servers as specified under the Easy access configuration sheet DNS records requirements.
☐	To enable single sign-on feature on Cisco Unified CCX you must already have a configured ADFS server.

Contents | Deployment Details

Easy Access Configuration Sheet

The following table provides you with a place to capture all the information you may need during the configuration of Cisco UCCX-related services. It includes example values used in this CVD, and a column where you can enter your site-specific configuration values.

Table 1. CVD network configuration

Item	CVD Configuration	Site-specific Configuration
	Cisco Unified CCX	Cisco Unified CCX
IPv4 LAN address	10.106.170.160	
IPv4 LAN subnet	255.255.255.0	
IPv4 gateway	10.106.170.129	
System hostname	uccx	
Default DNS servers (Local)	10.106.170.130 (Local DNS)	
Domain name	mmcvd.ciscolabs.com	
NTP servers	10.106.170.130	
Time zone	Asia/Calcutta	
Administrator	Admin	
Password	User123	
Application User	CCXAdmin	
Password	User123	
Security Password	User123	
Organization unit	Cisco System inc	
Location, country		

Contents | Deployment Details

Preparing the Platform for Cisco Unified CCX

PROCESS

1. Configure platform connectivity to the LAN
2. Prepare the server for Cisco Unified CCX

Procedure 1   Configure platform connectivity to the LAN

The Cisco Unified Contact Center Express server can be connected to a Cisco Nexus switch in the data center or a Cisco Catalyst switch in the server room. In both cases, quality-of-service (QoS) policies are added to the ports to maintain voice quality during the setup and completion of calls. Please choose the option that is appropriate for your environment.

Option 1: Connect Cisco Unified CCX to a Nexus 2248 Switch

Step 1. Log in to the Cisco Nexus switch with a user account that has permission to make configuration changes.

Step 2. If there is a previous configuration on the switch port where Cisco Unified CCX is connected, remove the individual commands by issuing a no in front of each one to bring the port back to its default state.

Step 3. Configure the port as an access port, and then apply the QoS policy.

```
Interface Ethernet107/1/18
  description Unified Contact Center Express
  switchport access vlan 148
  spanning-tree port type edge
  service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
```

_i_	Tech Tip
When deploying a dual-homed Cisco Nexus 2248 Switch, you must apply this configuration to both Nexus 2248 devices.	

Contents | Deployment Details

Option 2: Connect Cisco Unified CCX to a Catalyst 3X50 Switch

To ensure that signaling traffic is prioritized appropriately, you must configure the Cisco Catalyst access switch port where Cisco Unified CCX is connected to trust the Differentiated Services Code Point (DSCP) markings. The easiest way to do this is to clear the interface trigger of any previous configuration, and then apply the egress QoS macro that was defined in the access-switch platform configuration. For more information, see the Campus Wired LAN Technology Design Guide.

Step 1. Log in to the Cisco Catalyst switch with a user account that has permission to make configuration changes.

Step 2. Clear the interface's configuration on the switch port where Cisco Unified CCX is connected.

```
default interface GigabitEthernet1/0/18
```

Step 3. Configure the port as an access port, and then apply the Egress QoS policy.

```
interface GigabitEthernet1/0/18
  description Unified Contact Center Express
  switchport access vlan 148
  switchport host
  macro apply EgressQoS
```

Contents | Deployment Details

| Procedure 2 | Prepare the server for Cisco Unified CCX |

The following table describes the scaling options for Cisco Unified CCX.

Table 2. Cisco Unified CCX virtual machine scaling options

	100 agents	300 agents	400 agents
Virtual CPUs	2	2	4
CPU speed	900 MHz	900 MHz	900 MHz
RAM	10 GB	10 GB	16 GB
Hard disk	146 GB (1)	146 GB (2)	146 GB (2)
VMware ESXi	5.0 U1, 5.1, 5.5, 6.0	5.0 U1, 5.1, 5.5, 6.0	5.0 U1, 5.1, 5.5, 6.0
OS support	RHE Linux 6 (64-bit)	RHE Linux 6 (64-bit)	RHE Linux 6 (64-bit)
Total agents	Up to 100	Up to 300	Up to 400

Complete the following steps to deploy an OVA file to define the virtual machine requirements. You use the Open Virtualization Format (OVF) support of VMware to import and deploy the OVA file.

Step 1. In the VMware vSphere client, choose **File > Deploy OVF Template**.

Step 2. Click the **Browse** button next to the file or URL box, find the location of the OVA file that you downloaded from Cisco, and then click **Next**.

Step 3. Verify the information on the OVF Template Details page, and then click **Next**.

Step 4. Read the End User License Agreement, click **Accept**, and then click **Next**.

Step 5. Enter the following information in the Deploy OVF Template wizard, and then click **Finish**.

- On the Name and Location page, in the Name box, enter the virtual machine name CCX1, and then click Next.
- On the Deployment Configuration page, from the menu, choose the Configuration type, and then click Next.
- On the Storage page, choose the location to store the VM files, and then click Next.
- On the Disk Format page, choose Thick Provision Eager Zeroed, and then click Next.
- On the Ready to Complete page, verify the settings, and then click Finish.
- In the message window, click Close.

Contents | Deployment Details

⌒◯◯⌒ Reader Tip

In the Cisco BE6000 deployment, select the 100 agent profile in the OVA template to be deployed.

Source
OVF Template Details
End User License Agreement
Name and Location
Deployment Configuration
Storage
Disk Format
Ready to Complete

When you click Finish, the deployment task will be started.
Deployment settings:

OVF file:	C:\Users\kfleshne\Documents\SBA\2013 1H Feb\06 Help...
Download size:	95.5 KB
Size on disk:	292.0 GB
Name:	CCX1
Folder:	10k
Deployment Configuration:	UCCX 400 Agent
Host/Cluster:	chas2-s3.cisco.local
Datastore:	chas2-s3-local
Disk provisioning:	Thick Provision Eager Zeroed
Network Mapping:	"eth0" to "Servers_1"

☐ Power on after deployment

The virtual machine is created.

Step 6. Click the server name (In this example, **CCX1**), navigate to the Getting Started tab, and then choose **Edit virtual machine settings**.

Step 7. On the Hardware tab, click **CD/DVD Drive 1**, and then select the **Connect at power on** check box.

Step 8. Select **Datastore ISO File**, click **Browse**, and then navigate to the location of the Cisco Unified CCX bootable installation file. After selecting the correct ISO image, click **OK**.

Contents | Deployment Details

Step 9. On the Getting Started tab, choose **Power on the virtual machine**.

Step 10. Click the **Console** tab, and then watch the server boot.

The virtual machine is prepared for installation.

Contents | Deployment Details

Installing Cisco Unified CCX

PROCESS

1. Install the Cisco Unified CCX platform
2. Set up application administration

Procedure 1 . Install the Cisco Unified CCX platform

After the ISO/DVD loads, continue the installation on the server console.

Step 1. On the DVD Found page, perform a media check by selecting **Yes**.

Step 2. If the media check is successful, choose **OK**.

If the media check does not pass, contact the Cisco Technical Assistance Center or your local representative to replace the media, and then repeat this step.

Step 3. On the Product Deployment Selection page, verify the product is Cisco Unified Contact Center Express, and then choose **OK**.

Step 4. On the Proceed with Install page, verify that the version is correct, and then choose **Yes**.
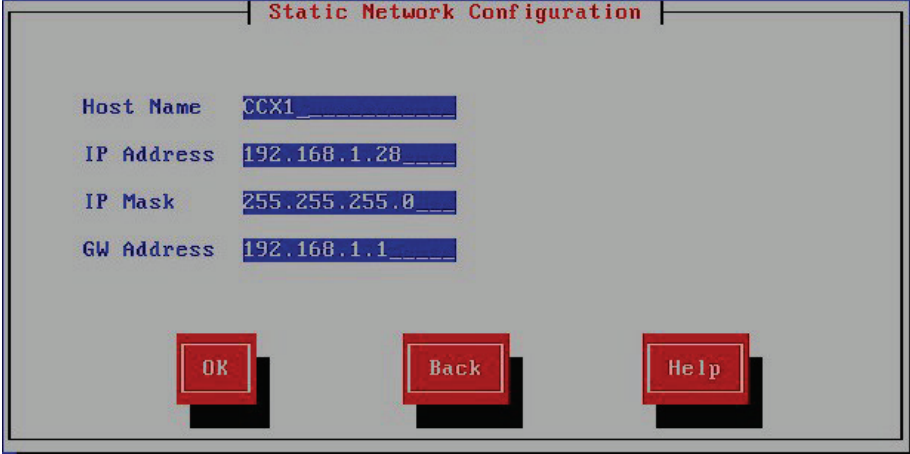
Step 5. On the Platform Installation Wizard page, choose **Proceed**.

Contents | Deployment Details

Step 6. If no upgrade patch exists for the version you are installing, on the Apply Patch page, choose **No**.

If an upgrade patch does exist, on the Apply Patch page, choose **Yes**, and then follow the instructions to complete the process.

Step 7. On the Basic Install page, choose **Continue**.

Step 8. On the Timezone Configuration page, select the correct time zone for the server location, and then choose **OK**.

```
┤ Timezone Configuraton ├
  Choose the correct timezone from the following list:

      America/Jamaica
      America/Juneau
      America/Kentucky/Louisville                    #
      America/Kentucky/Monticello
      America/La_Paz
      America/Lima
      America/Los_Angeles

         OK              Back            Help
```
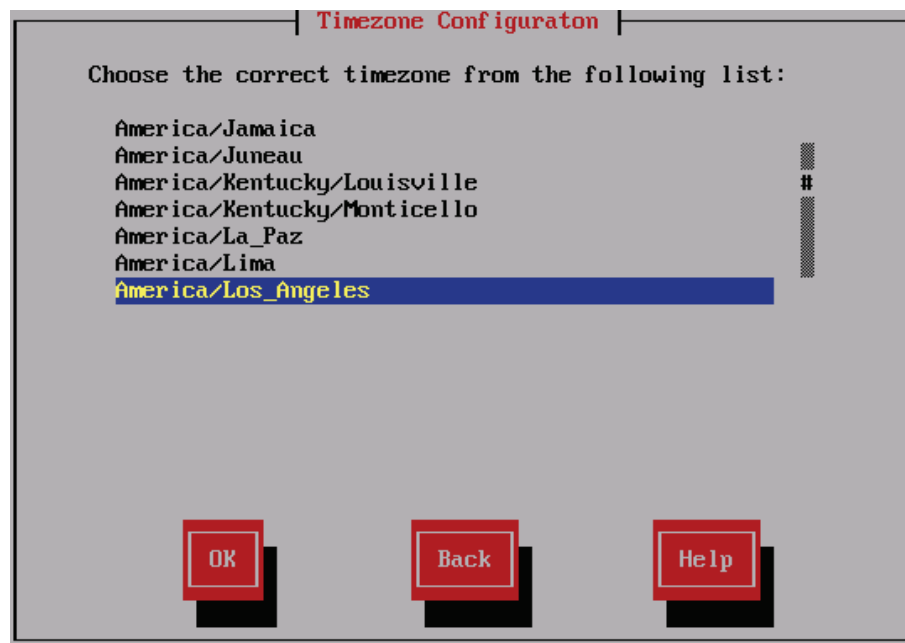
Step 9. On the Auto Negotiation Configuration page, choose **Continue**.

Step 10. On the MTU Configuration page, choose **No**.

Step 11. On the Static Network Configuration page, enter the following information, and then choose **OK**.

- Host Name—**CCX1**
- IP Address—**192.168.1.28**
- IP Mask—**255.255.255.0**
- GW Address—**192.168.1.1**
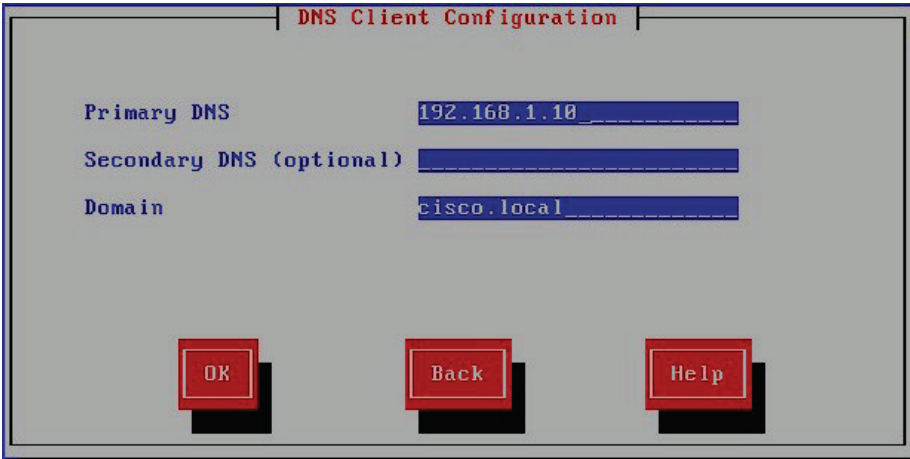
Contents | Deployment Details

Step 12. On the DNS Client Configuration page, enter the following information, and then choose OK.

- Primary DNS—192.168.1.10
- Domain—cisco.local

Step 13. On the Administrator Login Configuration page, enter the following information, and then choose OK.

- Administrator ID—Admin
- Password—[password]
- Confirm Password—[password]

Contents | Deployment Details

```
┤ Administrator Login Configuration ├

    Enter the Platform administration username and password.
    Choose Help for username and password guidelines.

       Administrator ID   Admin_____

       Password           ********_____

       Confirm Password   ********_____




              OK              Back              Help
```

Step 14. On the Certificate Information page, enter the information that will be used to generate security certificates, and then choose **OK**.

- Organization—Cisco Systems, Inc.
- Unit—Unified Communications Group
- Location—San Jose
- State—California
- Country—United States

i	Tech Tip
These fields must match the information submitted to Cisco or the licenses will not be valid.	

Step 15. On the First Node Configuration page, choose **Yes**.

Step 16. On the Network Time Protocol Client Configuration page, enter the following information, and then choose **OK**.

- NTP server 1—**192.168.1.10**

Step 17. On the Security Configuration page, enter the password for server-to-server communication, and then choose **OK**.

i	Tech Tip
These passwords must match the information submitted to Cisco, or the licenses will not be valid.	

Step 18. On the SMTP Host Configuration page, choose No.

Step 19. On the Application User Configuration page, enter the following information, and then choose **OK**.

- Application User Username—CCXAdmin
- Password—[password]
- Confirm Password—[password]

Step 20. On the Platform Configuration Confirmation page, choose **OK**.

The system continues with the rest of the installation process without user input. The system will reboot a few times during installation. The process can take 60 minutes or more, depending on your hardware.

After the software has finished installing, the login prompt appears on the console.

Step 21. From the vSphere client, navigate to the virtual machine's Getting Started tab, and then choose **Edit virtual machine settings**.

Step 22. On the Hardware tab, choose **CD/DVD Drive 1**.

Step 23. Clear Connect at power on, and then click **OK**.

Procedure 2	Set up application administration

After the software is installed, you use the web interface in order to complete the rest of the procedures.

Step 1. With your web browser, access the IP address or hostname of the Cisco Unified CCX server and, in the center of the page, click **Cisco Unified Contact Center Express Administration**.

Step 2. If you receive a warning about the website's security certificate, ignore it and continue to the page.

Step 3. Enter the name and password you entered on the Application User Configuration page in Step 19 of the "Install the Cisco Unified CCX platform" procedure, and then click **Login**.

Step 4. On the Cisco Unified CCX Administrator Setup page, choose **Fresh Install**, and then click **Next**.

Step 5. On the Cisco Unified CM Configuration–Service Provider Configuration page, enter the following information, and then click **Next**.

- Unified CM server IP address—192.168.1.16 (publisher)
- AXL Admin UserName—CUCMAdmin
- Password—[password] (must match the password on Cisco Unified CM).

Step 6. On the License Information page, click Browse, locate the Unified CCX license file received from Cisco, click Open, and then click **Next**.

Contents | Deployment Details

Enter a license or zip file name

License File* [_____] [Browse...]

Step 7. After the license validation is completed, click **Next**.

Step 8. After all of the components are successfully activated, click **Next**.

Status

ⓘ Component(s) successfully Activated.

Component Name	Status
Cisco Monitoring	Activated
Cisco Recording	Activated
Cisco Unified CCX Agent Datastore	Activated
Cisco Unified CCX Config Datastore	Activated
Cisco Unified CCX Engine	Activated
Cisco Unified CCX Historical Datastore	Activated
Cisco Unified CCX Node Manager	Activated
Cisco Unified CCX Repository Datastore	Activated

Step 9. On the Publisher Activation page, click **Next**.

	Datastore Name	Server Name	Status
☑	Cisco Unified CCX Historical Datastore	CCX1	Not Activated
☑	Cisco Unified CCX Agent Datastore	CCX1	Not Activated
☑	Cisco Unified CCX Repository Datastore	CCX1	Not Activated

Step 10. On the Cisco Unified CM Configuration page, in the AXL Service Provider Configuration section, in the **Selected AXL Service Providers** list, choose the Unified CM server **192.168.1.16** (publisher), and then remove it from the list by clicking the right-facing arrow.

Step 11. Under Available AXL Service Providers, select the Unified CM servers **192.168.1.17** (subscriber), and then move them to the **Selected AXL Service Providers** list by clicking the left-facing arrow.

Step 12. In the Cluster Wide Parameters section, it will be pre-populated with the credentials as shown below:

Contents | Deployment Details

Step 13. In the Unified CM Telephony Subsystem–Unified CM Telephony Provider Configuration section, in the **Available CTI Managers** list, choose the Unified CM servers **192.168.1.17**(subscriber), and then move them to the **Selected CTI Managers** list by clicking the left-facing arrow.

Step 14. In the Cluster Wide Parameters section, enter the following information:

- User Prefix–CCX_jtapi
- Password–[password]
- Confirm Password–[password]

Step 15. In the RmCm Subsystem–RmCm Provider Configuration section, in the **Available CTI Managers** list, choose the Unified CM servers **192.168.1.17**(subscriber), and then move them to the **Selected CTI Managers** list by clicking the left-facing arrow.

Step 16. In the Cluster Wide Parameters section, enter the following information, and then click **Next**.

- User Id–CCX_rmjtapi
- Password–[password]
- Confirm Password–[password]

Cisco Unified CCX sends the user information to the Cisco Unified CM server, and the application

users are created automatically.

For historical reporting of the number of HR sessions, use the maximum number of supervisors or administrators who will be running Cisco Unified CCX reports at the same time. For the Recording Count, enter the maximum number of concurrent ad-hoc recording sessions.

The G.711 codec choice requires one of the following choices for calls that do not originate from the same region and location as the Cisco Unified CCX server:

- Transcoders must be configured in Cisco Unified CM and added to the media resource group list at the Cisco Unified CCX site in order to allow contact center calls to and from the remote sites.

- The regions must allow 64 kbps as the maximum audio bit rate between their site and the Cisco Unified CCX site for the contact center calls.

i	Tech Tip
	If either these two options are not completed, contact center calls from remote sites will experience a fast-busy tone when calling the main pilot number for Cisco Unified CCX.

Step 17. On the System Parameters Configuration page, enter the following information, and then click **Next**:

- Number of HR sessions—4

- Recording Count—25

- Number of Outbound seats—100

- Codec—G.711

Number of HR sessions*	4	
Recording Count*	25	(Limit : 84)
Number of Outbound seats*	100	(Maximum limit :100)
Codec	G711 ▼	

Step 18. On the Language Configuration page, enter the language that will be used for default Interactive Voice Response (IVR) prompts, , and then click **Next**.

Contents | Deployment Details

Step 19. On the User Configuration page, select the Cisco Unified CM users who need administrative rights, move them to the Cisco Unified CCX Administrator list by clicking the left-facing arrow, and then click **Finish**.

The initial application administration setup is now complete.

Contents | Deployment Details

Configuring Single Sign-On on Cisco UCCX

<table>
<tr>
<td rowspan="2">PROCESS</td>
<td>1.</td>
<td>Perform the metadata exchange on the IdS and establish trust between the IdP and IdS servers</td>
</tr>
<tr>
<td>2.</td>
<td>Enable Single Sign-On on Cisco UCCX</td>
</tr>
</table>

1.	Perform the metadata exchange on the IdS server and establish trust between the IdP and IdS servers

1. Access IdS server management page using the following URL:
   https://FQDN of UCCX:8553/idsadmin/

2. Log in using the Cisco UCCX application user credentials:
   User– CCXAdmin
   Password –– xxxxxxx

3. Choose **Settings** and click **Download Metadata File**. (This downloaded file should be uploaded on the IdP server.)

Settings   IdS Trust

Download SAML SP Metadata

Begin configuring the trust relationship between the Identity Provider(IdP) and the Identity Server (IdS) by obtaining a SAML SP metadata file from the IdS Server. Use this metadata file to configure trust relationship in Identity Provider (IdP).

Download Metadata File
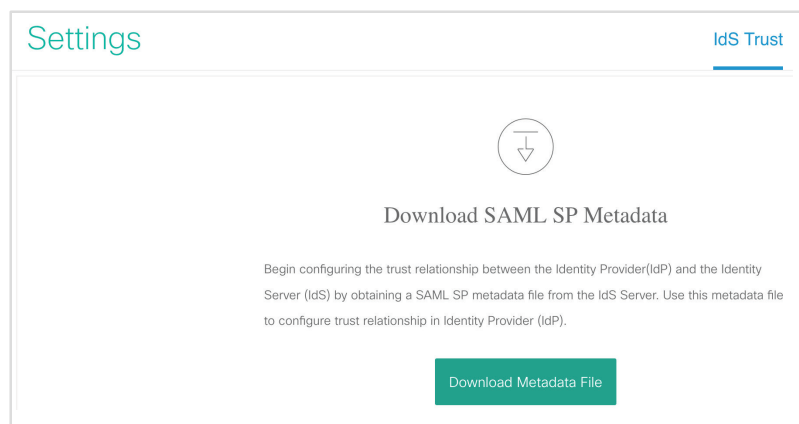
4. Select **Next** and click Upload IdP Metadata to upload the metadata file downloaded from the IdP server.

Contents | Deployment Details

Settings

IdS Trust

IdP Entity Id : http://fs.mmcvd.ciscolabs.com/adfs/services/trust

Upload IdP Metadata

Establish the trust relationship between the Identity Provider (IdP) and the Identity Server (IdS) by obtaining a trust metadata file from the IdP and uploading it here.

Use file browser to upload the file.
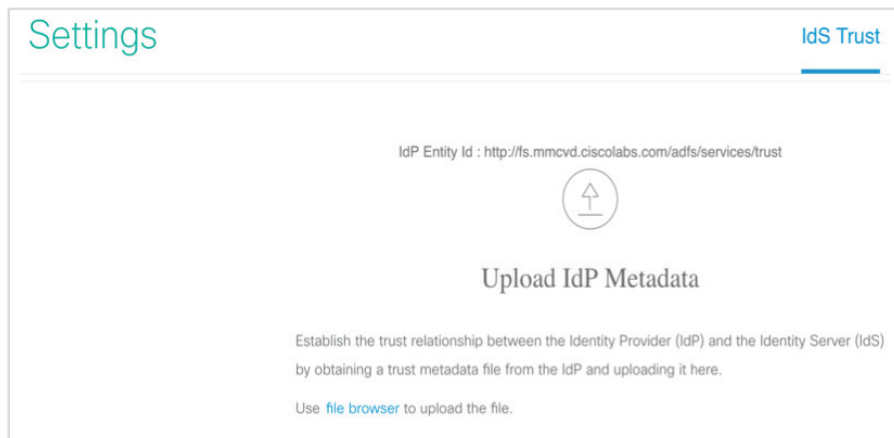
5. The following link provides the steps to upload the IdS server metadata file onto the IdP server and add the appropriate claim rules:

   https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/200612-Configure-the-Identity-Provider-for-UCCX.html – anc10

2.	Enable Single Sign-on Cisco UCCX

1. Access the Cisco UCCX administration page using https://uccx.mmcvd.ciscolabs.com. Enter the administrator credentials:
   User Name – Sudheer
   Password -- XXXXXX

2. Click the System menu and select **Single Sign-On (SSO).**

System | Applications | Subsystems | Wizards | Tools | Help

Server
Cisco Unified CM Configuration
System Parameters
Recording Configuration | red successfully Click here to update Cisco Identity Service configuration
Single Sign-On (SSO)
Custom File Configuration
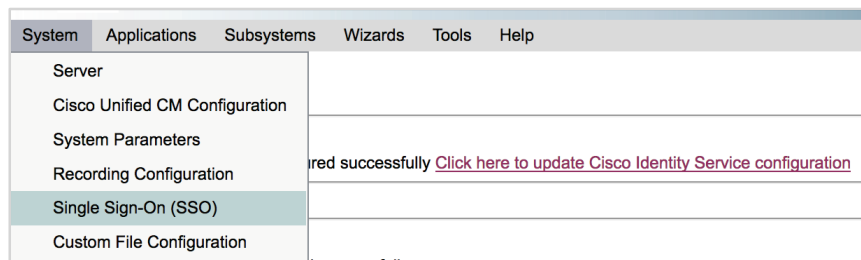
3. Click the **Register** button to register the components to be enabled for Single Sign-On. A green checkmark will appear next to components that are successfully registered.

Contents | Deployment Details

4. Before testing the SSO operation, ensure the following items are configured:

Before proceeding with the SSO Test operation ensure you have:

☑ Configured and Performed LDAP Sync in CUCM.

☑ Assigned administrator rights to one or more enterprise users.

☑ Assigned reporting capability to Cisco Unified CCX Administrator (assigned in Administrator Capability view) and executed CLI command "utils cuic user make-admin CCX\<Admin's User Id>". Use the configured user with administrator rights for the SSO Test operation.

5. In the SSO test panel, click the **Test** button. In the message appears, accept the certificates.

A green checkmark will appear next to components that are successfully tested.

6. In the SSO Status panel, click the **Enable** button to activate Single Sign-On.

A green checkmark will appear next to components that are successfully enabled.

Contents | Deployment Details

# Configuring Context Service on Cisco UCCX

PROCESS

1. Configure Cisco UCCX to register for Context Service

---

1.   Configure Cisco UCCX to register for Context Service

1. Open Cisco UCCX using https://uccx.mmcvd.ciscolabs.com and select the **Cisco Unified Contact Center Express Administration**

Cisco Unified Contact Center Express Tools

- Cisco Unified Contact Center Express Administration
- Cisco Unified Contact Center Express Reporting
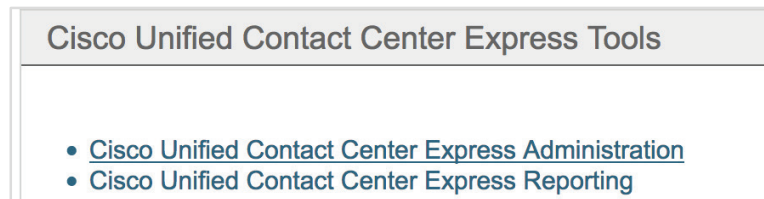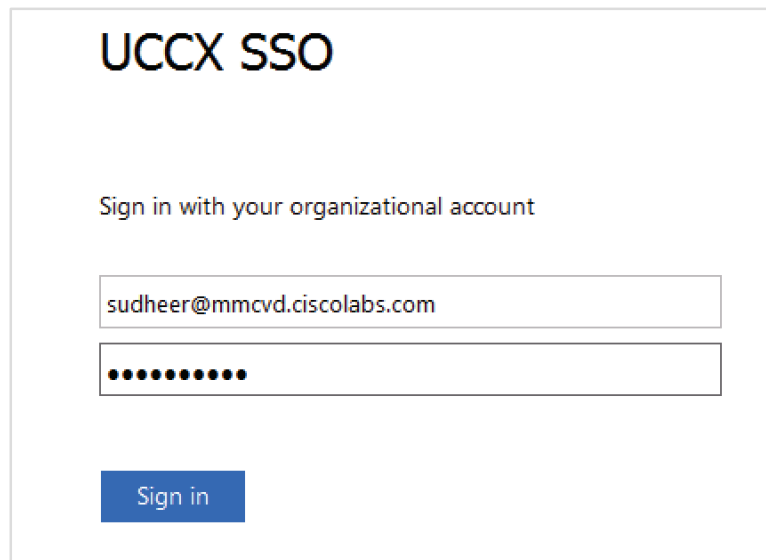
You are redirected to authenticate with the IdP server and will be presented with the UCCX SSO sign-in screen for first time sign-in only.

2. To sign into Cisco UCCX administration, enter the below credentials and click **Sign in**:

Username – sudheer@mmcvd.ciscolab.com
Password – password

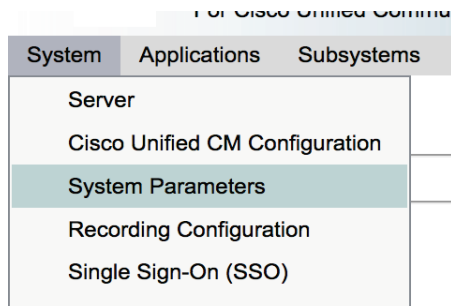Contents | Deployment Details

UCCX SSO

Sign in with your organizational account

sudheer@mmcvd.ciscolabs.com

••••••••••

Sign in

3. Click the System menu and then choose the **System Parameters** menu option.

System	Applications	Subsystems

Server

Cisco Unified CM Configuration

System Parameters

Recording Configuration

Single Sign-On (SSO)

4. Under the Context Service Parameters section, set the following configuration:

- Lab Mode—Enable (For production mode this should be Disabled)

- Request Timeout—5000

- Proxy Type—Http

Context Service Parameters		
Parameter Name	Parameter Value	Suggested Value
Lab Mode*	● Enable ○ Disable	Disable
Request Timeout*	5000 milliseconds(Min:200 Max:5000)	5000 milliseconds
Proxy Type	Http ◊ (http://myproxy.mmcvd.ciscolabs.com:8080)	

5. Under the Proxy Parameters specify:

- Http—myproxy.mmcvd.ciscolabs.com:8080

Contents | Deployment Details

Proxy Parameters

Parameter Name	Parameter Value		
Http	myproxy.mmcvd.ciscolabs.com	: 8080	(Hostname:Port)

6. Click **Update** to save the changes.

Configuring the Help Desk

PROCESS

1. [Create the call control group](#)

2. [Create skills](#)

3. [Assign skills to contact service queues](#)

4. [Associate a phone to an agent user ID](#)

5. [Associate user ID to a phone or profile](#)

6. [Assign skills to resources](#)

7. [Create the supervisors and teams](#)

8. [Create scripts and applications](#)

9. [Add a trigger](#)

10. [Associate Cisco Unified CCX application user](#)

11. [Verify Cisco Unified CCX Engine status](#)

After you configure the application administration for the first time, the next task is to configure the help desk to allow the system to begin taking calls from end users.

1.	Create the call control group

A call control group creates a group of computer telephony integration (CTI) ports on Cisco Unified CM that are used to send calls to Cisco Unified CCX for IVR treatment and queuing. The call stays on the CTI port until it is sent to an agent.

Step 1. Access the IP address or hostname of the Cisco Unified CCX server by using your web browser and then, in the center of the page, click **Cisco Unified Contact Center Express Administration**.

Step 2. Enter the username and password of one of the users you assigned administrative rights in Step 20 of the previous procedure, and then click **Login**.

Contents | Deployment Details

Step 3. Navigate to **Subsystems > Cisco Unified CM Telephony > Call Control Group**, and then click **Add New**.

Step 4. Enter the following information, and then click **Add**.

- Description—Unified CM Telephony Group
- Number of CTI ports—4
- Media Termination Support—No
- Group Type—Inbound
- Device Name Prefix—CTIP
- Starting Directory Number—8009950
- Device Pool—DP_HQ1_1 (default for headquarters location)
- DN Calling Search Space—CSS_Base
- Location—Hub_None
- Partition—PAR_Base

Leave the other fields at their default settings.

2.	Create skills

Create skills for each different type of call you expect to receive in the call center.

Step 1. Navigate to **Subsystems > RmCm > Skills**, and then click **Add New**.

Step 2. On the Skill Name page, enter **IT**, and then click **Save**.

> Skill Name* | IT

Step 3. On the Skills search page, click **Add New**.

Step 4. On the Skill Configuration page, enter **HR (For Human Resources)**, and then click **Save**.

Step 5. Create additional skills, by repeating steps 3 and 4.

3.	Assign skills to contact service queues

Create Contact Service Queues (CSQ) for each skill entered in the previous procedure.

Contents | Deployment Details

i	Tech Tip

The CSQ names created here must exactly match the queue names referenced in the application scripts that are described later in this guide. The example script uses the CSQ names of **IT** and **HR**. Be sure to add these queues to the server.

Step 1. Navigate to **Subsystems > RmCm > Contact Service Queues**, and then click **Add New**.

Step 2. On the first Contact Service Queue Configuration page, enter the following information, and then click **Next**:

- Contact Service Queue Name–IT
- Contact Service Queue Type–Voice
- Automatic Work–Disabled
- Wrapup Time–Disabled
- Resource Pool Selection Model–Resource Skills
- Service Level–5 (seconds)
- Service Level Percentage–70
- Prompt–No Selection

Contents | Deployment Details

Step 3. On the second Contact Service Queue Configuration page, enter the following information, and then click **Add**:

- Resource Selection Criteria—Longest Available
- Select Required Skills—IT
- Minimum Competence—5

Contact Service Queue Name IT

Resource Selection Criteria*	Longest Available ▼
Select Required Skills	HR IT

Add

Skills	Minimum Competence	Delete
IT	5	🗑

Step 4. For each additional skill (such as HR), click **Add New**, and then repeat steps 2 and 3 using the appropriate information.

4.	Associate a phone to an agent user ID

There are two ways to associate agents and supervisors with a phone. You can use extension mobility to allow agents to log in to a Cisco IP phone or you can associate an agent's Cisco Unified CM user ID directly with a phone. Both options can be used for the same Cisco Unified CCX installation. Choose extension mobility if your agents move around from day to day or if you have more than one shift and the same phone will be used by multiple agents. Choose the phone association method if the agents work from the same phone every day.

Step 1. Use your web browser to access the IP address or hostname of the Cisco Unified CM publisher and then, in the center of the page, click **Cisco Unified CM Administration**.

Step 2. Enter the application administrator username and password for Cisco Unified CM, and then click **Login**.

Perform the next several steps only if you are planning to associate agents directly to a phone. If you will use extension mobility exclusively with your agents, you can skip to the next procedure.

Step 3. Navigate to **Device > Phone**, click **Find**, and then click the name of the agent's phone.

Step 4. On the Phone Configuration page, **click line [1]**. This adds the Cisco Unified CCX information for the specific line on the phone.

Step 5. Scroll down to the bottom of the page, and then click **Associate End Users**.

Step 6. On the Find and List Users page, click **Find**, and then choose the agent for this line by selecting the check box next to their name.

Step 7. Click **Add Selected**. You return to the previous page.

Step 8. Repeat steps 3 – 7 for each additional agent and supervisor phone, using each agent's and supervisor's specific information.

5.	Associate user ID to a phone or profile

In this procedure, you associate the agent and supervisor user ID to a phone or extension mobility profile. Please choose one or both of the following options:

- If you are associating agents with phones, follow the steps in Option 1, "Phone Association."
- If your agents will use extension mobility to log in to their phones, follow the steps in Option 2, "Extension mobility association."

Option 1: Phone Association

Step 1. Navigate to **User Management > End User**, and then click **Find**.

Step 2. Select the agent or supervisor from the previous procedure, and then click the user ID.

Step 3. On the End User Configuration page, scroll down to the Device Information section, and then click **Device Association**.

Step 4. On the User Device Association page, click **Find**.

Step 5. Select the check box next to the agent's phone, and then click **Save Selected/Change**s.

Contents | Deployment Details

Step 6. In the upper-right corner of the page, in the **Related Links** list, choose **Back to User**, and then click **Go**.

Step 7. On the End User Configuration page, scroll down to the Extension Mobility section, and then confirm that the **Allow Control of Device from CTI** check box is selected.

Step 8. Scroll down to the Directory Number Associations section, set the IP Contact Center (IPCC) Extension to the phone's directory number from the previous procedure, and then click **Save**.

Step 9. For each additional agent or supervisor using phone association, repeat steps 1 - 8 using their specific information.

Option 2: Extension Mobility Association

Step 1. Navigate to User Management > End User, and then click Find.

Step 2. Select the agent or supervisor, and then click the user ID.

Step 3. On the End User Configuration page, scroll down to the Device Information section, select the agents profile from the Available Profiles: **sudhekum_profile**, and then click the **Down-Arrow** icon to move it into the CTI Controlled Device Profiles.

Step 4. Scroll down to the Extension Mobility section, and then confirm the **Allow Control of Device from CTI** check box is selected.

Step 5. Scroll down to the Directory Number Associations section, set the IPCC Extension to the agent's extension mobility number, and then click Save.

Step 6. For each additional agent or supervisor using extension mobility association, repeat steps 1 – 5, using their specific information.

Contents | Deployment Details

6.	Assign skills to resources

Cisco Unified CM users associated with IPCC extensions appear automatically as resources in Cisco Unified CCX. Using the resource list on the Cisco Unified CCX Administration page, you assign skills to resources, making them available to answer calls in particular Contact Service Queues (CSQs).

Step 1. Use your web browser to access the IP address or hostname of the Cisco Unified CCX server and click **Cisco Unified Contact Center Express Administration**.

Step 2. Enter the name and password of a user with administrative rights to Cisco Unified CCX, and then click **Sign In**.

Step 3. Navigate to **Subsystems > RmCm > Resources**. On the Resources search page, under the **Resource Name**, click a user.

Step 4. On the Resource Configuration page, in the **Unassigned Skills** list, choose the skill(s) that you want to assign, and then move the skill(s) to the **Assigned Skills** list by clicking the left-facing arrow.

Step 5. Select the Competence Level for the resource, and then click **Update**.

Resource Name	Sudheer Kumar
Resource ID	sudheer
IPCC Extension	81004007
Resource Group	-Not Selected-
Automatic Available*	⦿ Enabled ○ Disabled

Assigned Skills		Unassigned Skills
IT(5)	◀ ▶	HR

Competence Level 5 ▾ (1-Beginner, 10-Expert)

Team IT ▾

Step 6. For each additional resource, repeat steps 3 – 5, using the appropriate information for each agent.

Contents | Deployment Details

7.	Create the supervisors and teams

The first step in building a team is to create a *supervisor*. A supervisor has a full view of a team's performance and can monitor the agents by using the Cisco Supervisor Desktop.

Step 1. Navigate to **Tools > User Management > Supervisor Capability View**.

Step 2. On the User Configuration page, in the **Available Users** list, choose the users you want to designate as supervisors, move them to the **Cisco Unified CCX Supervisor** list by clicking the left-facing arrow, and then click **Update**.
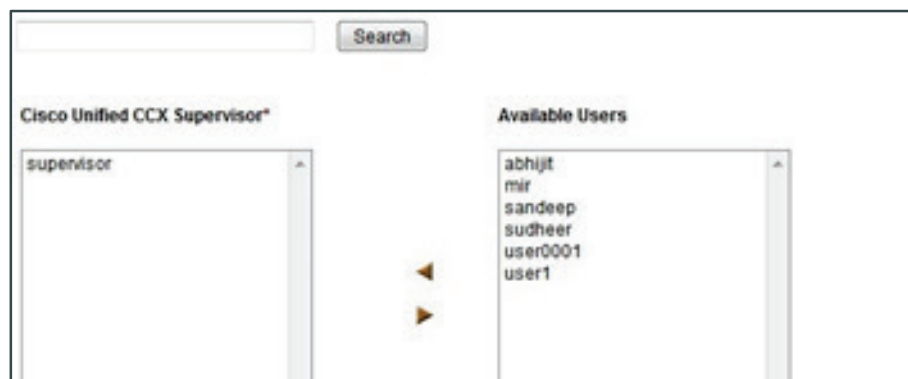
Step 3. Navigate to **Subsystems > RmCm > Teams**, and click **Add New**.

Step 4. On the Team Configuration page, enter the following information, and then click **Save**.

- Team Name—IT
- Primary Supervisor—[Supervisor]
- Assigned Resources—[Agent or supervisor]
- Assigned CSQs—IT

Step 5. For each additional team, repeat steps 3 and 4, using the appropriate information.

Contents | Deployment Details

8.	Create scripts and applications

In this procedure, an externally created script is uploaded to the server to demonstrate how to upload your script and create your site-specific application.
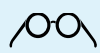
Reader Tip

This guide uses the example script and prompts from a zip file that is included with the document. The script can be used as a template for your help desk application. The zip file can be downloaded from the following URL: http://www.cisco.com/go/cvd/collaboration/

Please use the example script as a template for your scripts.

Step 1. Navigate to **Applications > Script Management**, select the script to upload, and then click **Upload Scripts**.

Step 2. Click **Browse**, find the location of the script (scripts have the file extension .aef), and then click **Upload**.

Step 3. After the script is successfully uploaded, click **Return to Script Management**.

Step 4. Navigate to **Applications > Application Management**, and then click **Add New**.

Step 5. On the Add A New Application page, select **Cisco Script Application**, and then click **Next**.

Step 6. On the Cisco Script Application page, enter the following information, and then click **Add**.

- Name—Help Desk
- ID—[automatic setting] (do not change this value)
- Maximum Number of Sessions—4
- Script—SCRIPT[Helpdesk.aef]
- Description—Help desk for IT and HR
- Enabled—Yes
- Default Script—System Default

Contents | Deployment Details

9.	Add a trigger

The trigger for an application is the phone number the users will dial when they want to speak with someone at the help desk.

Step 1. In the upper-left of the Cisco Script Application page, click **Add New Trigger.**

Step 2. In the **Trigger Type** list, choose **Unified CM Telephony Trigger**, and then click **Next**.

Step 3. On the Cisco Unified CM Telephony Trigger Configuration page, enter the following information:

- Directory Number—8009940 (CTI Route Point that will be automatically created in Cisco Unified CM to direct calls to this application)
- Language—English (United States) [en_US]
- Device Name—InternalHelp
- Description—Trigger for Internal Help Desk
- Call Control Group—Unified CM Telephony Group(1)

Contents | Deployment Details

Step 4. Click **Show More**, enter the following information, and then click **Add**:

- Enabled—Yes
- Maximum Number of Sessions—Default
- Idle Timeout (in ms)—5000
- Override Media Termination—No
- Alerting Name ASCII—Help Desk Pilot
- Device Pool—DP_HQ1_1 (headquarters default)
- Location—Hub_None (headquarters default)
- Partition—PAR_Base (phone default)
- Voice Mail Profile—None
- Calling Search Space—CSS_Base

Leave the rest of the fields at their default settings.

10.	Associate Cisco Unified CCX application user

The next set of steps associate the Cisco Unified CCX application user with the phones, extension mobility profiles, CTI Route Point, and CTI Ports in Cisco Unified CM. Please choose one or both of the following options:

- If you are associating agents and supervisors directly with phones, follow the steps in Option 1, "Phone Association."
- If your agents and supervisors are using extension mobility on their phones, follow the steps in Option 2, "Extension Mobility Association."

Step 1. From a new browser window, access the IP address or hostname of the Cisco Unified CM publisher and then, in the center of the page, click **Cisco Unified CM Administration**.

Step 2. Enter the administrator username and password for Cisco Unified CM, and then click **Login**.

Step 3. Navigate to **User Management > Application User**.

Step 4. On the Application User search page, click **Find**, and then click **CCX_rmjtapi**.

Step 5. On the Application User Configuration page, in the Device Information section, the **Available Devices** list, choose the Unified CCX CTI ports and the Unified CCX CTI route point, and then click the **down-facing arrow.**

Option 1: Phone Association

Step 1. On the Application User Configuration page, under Device Information, in the **Available Devices** list, choose the agent and supervisor phones, and then move them to the **Controlled Devices** list by clicking the **down-facing arrow**.

Step 2. Click **Save**.

Option 2: Extension Mobility Association

Step 1. On the Application User Configuration page, under Device Information, in the **Available Profiles** list, choose the agent and supervisor profiles, and then move them to the **CTI Controlled Device Profiles** list by clicking the **down-facing arrow**.

Step 2. Click **Save**.

11.	Create and upload the prompts

In this procedure, externally created prompts are uploaded to the server to demonstrate how to upload your prompts.
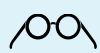
Reader Tip
This guide uses the example script and prompts from a zip file that is included with the document. The prompts can be used as examples for your help desk application. The zip file can be downloaded from the following URL: http://www.cisco.com/go/cvd/collaboration/   Please use the example prompts as templates for your recordings.

Prompts are played to the callers when they are in the application. You must record the prompts as .wav files and save them in a location reachable by the PC accessing Cisco Unified CCX Administration.

Step 1. Navigate to the Cisco Unified CCX Administration main page.

Step 2. Navigate to **Applications > Prompt Management**, and then click the **en_US** folder.

Step 3. After the folder opens, click **Upload Prompts**.

Contents | Deployment Details

Step 4. From the Upload Prompt page, click **Browse**, locate the prompt WAV file, select it, and then click Upload.

Step 5. For each of the prompts, repeat Step 4, and then click **Return to Prompt Management**.

Name	Size	Date Modified	Modified By	Delete	Rename	Refresh
AfterHours.wav	100.13 KB	11/28/2012 09:13:11 AM Pacific Standard Time	kfleshne			
Goodbye.wav	13.26 KB	11/28/2012 09:13:19 AM Pacific Standard Time	kfleshne			
MainMenu.wav	74.51 KB	11/28/2012 09:13:27 AM Pacific Standard Time	kfleshne			
ThankYouHR.wav	53.42 KB	11/28/2012 09:13:34 AM Pacific Standard Time	kfleshne			
ThankYouIT.wav	59.67 KB	11/28/2012 09:13:41 AM Pacific Standard Time	kfleshne			
VeryImportant.wav	57.95 KB	11/28/2012 09:13:47 AM Pacific Standard Time	kfleshne			
Welcome.wav	44.59 KB	11/28/2012 09:13:53 AM Pacific Standard Time	kfleshne			

Step 6. Navigate to **Applications > Application Management**, and then click the application that you created in Procedure 8, "Create scripts and applications."

Step 7. Change the default prompts by selecting the check box next to each one, clicking **Show Prompts**, and then choosing the appropriate file from the list of your own uploaded prompts. After they are all chosen, click **Update**.

i	Tech Tip

Custom prompts must have the following WAV format specifications:

Bit rate: 64 kbps

Audio sample size: 8 bit Channels: 1 (mono) Audio sample rate: 8 kHz

Audio format: CCITT u-Law

Note that the new prompt names must match the variable values listed in the script application or they will not play.

12.	Verify Cisco Unified CCX Engine status

Check the status of the Cisco Unified CCX engine in order to ensure the integration with Cisco Unified CM is working properly and is ready to receive calls.

Step 1. From the **Navigation** menu in the top right, choose **Cisco Unified CCX Serviceability**, and then click Go.

Step 2. Navigate to **Tools > Control Center-Network Services**, and then check the status of the Cisco Unified CCX Engine.

On the Cisco Unified CCX Engine line, the Status should read In Service; if this is the case, the configuration of the server is complete and you can skip ahead to Configuring the Cisco Finesse Desktop. If the Status is Partial Service, continue to the next step to attempt to fix the problem.

Step 3. From the **Navigation** menu in the top right, choose **Cisco Unified CCX Administration**, and then click **Go**.

Step 4. Navigate to **Subsystems > Cisco Unified CM Telephony > Data Synchronization**.

Step 5. Select **Call Control Group(s)**, **Trigger(s)**, and **CM Telephony User(s)**, and then click **Data Resync**.

Step 6. Repeat steps 1 and 2 to recheck if Unified CCX Engine has come into service.

13.	Configuring Web Chat on Unified CCX

/OO\	Reader Tip

Cisco SocialMiner instance should be deployed before configuration of Web Chat. Please refer for the Cisco SocialMiner documentation. Please use the example prompts as templates for your recordings.

Step 1. Navigate to the **Subsystems > Chat and Email > SocialMiner** Configuration. Enter the following details and click the Save button

- IP Address/Host Name—**CCX-SM.cisco.local**
- Username—**ccxsm**
- Password—**[xxxxx]**

Configure SocialMiner

IP Address / Host Name *:	CCX-SM.cisco.local
User Name*:	ccxsm
Password*:	·········

Save   Cancel

Contents | Deployment Details

Step 2. Log into the Cisco Unified OS Administration interface and navigate to **Security > Certificate Management**. Click **Upload Certificate/Certificate Chain** and enter following details

- Certificate Name: tomcat-trust
- Description: SocialMiner
- Upload File: Click the Browse button and select the SocialMiner certificate file to be uploaded.

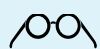**Upload Certificate/Certificate chain**

Certificate Name*	tomcat-trust ▼
Description	SocialMiner
Upload File	Browse... No file selected.

Step 3. Check underUnder the **SocialMiner Sstatus, make sure** the **Feeds** and, **Campaigns** should have the a green tick check mark

SocialMiner Status
- Feeds: ✓
- Campaigns: ✓
- Notifications: ✓

⌒⊙⊙⌒	Reader Tip

The Notifications status will only change to green after having at least 1 Web Chat requests and 1 Email request

---

Step 4. Navigate to the **Subsystems > Chat and Email > Contact Service Queues**

Step 5. Click the **Add New** button to add a new CSQ and specify the following:

- CSQ Name—IT helpdesk
- Resource Selection Criteria—Longest available
- CSQ type—Chat

Step 6. Click **Next** to do the skill association for the newly created CSQ in **step 4**

Contents | Deployment Details

Step 7. Under Skills, select the **IT** from the **Available skills**, click **Add** and then click **Save**.

Skills	
Available	Sel
HR	[Add]

Step 8. Next navigate to **Subsystems>Chat and Email>Teams** menu. In the **Available CSQ's** select the **IT-helpdesk** and click the left arrow to move it to **Assigned CSQs** and click the **Save** button.

14.	Configuring Email on Unified CCX

⌒⌒	Reader Tip

Before configuring the Email, Cisco SocialMiner should be deployed.

The Microsoft Exchange server should also be set up prior to configuration of Email on Unified CCX. Refer the Microsoft knowledge article for installation details

The customer also has option to choose Gmail or O365.

Only secure emails i.e. SMTPS and IMAPS are supported.

Step 1. Navigate to **Subsystems > Chat and Email > Mail Server Configuration,** enter the following information and click the **Save** button:

- Incoming (Secure IMAP)
  - o Host Name—exchange.cisco.local
  - o Port number—993
- Outgoing (Secure SMTP)
  - o Host Name—exchange.cisco.local
  - o Port number—587

Contents | Deployment Details

Incoming (Secure IMAP)
Host Name*: exchange.cisco.local
Port Number*: 993

Outgoing (Secure SMTP)
Host Name*: exchange.cisco.local
Port Number*: 587

Step 2. Navigate to **Subsystems > Chat and Email > SocialMiner** page. Under **SocialMiner Status**, now the **Email Server** should have the green check mark

SocialMiner Status
- Feeds: ✔
- Campaigns: ✔
- Notifications: ✔
- Email Server: ✔

Step 3. Navigate to the **Subsystems > Chat and Email > Contact Service Queues** and click **Add New** button to add a new email CSQ and enter following information

- CSQ Name—IT-email
- Resource selection criteria—Longest available
- CSQ Type—Email

Step 4. Click Next and enter the user credentials for the inbox as below

- Email Username—IT@cisco.local
- Email password—[xxxxxx]
- Folder name—inbox
- iPoll Interval (seconds)—30
- Snapshot age (Minutes) —120

Step 5. Click **Next** to associate the skill for the **IT-email** CSQ. Select **IT** in the **Available Skills** and then click **Save**.

Contents | Deployment Details

Configuring Cisco Finesse Desktop

PROCESS

Finesse Desktop is a feature-rich Web 2.0 browser-based product that offers easy deployment and lower total cost of ownership. Open social technology offers flexibility of customized gadget insertion for other browser-based applications. Finesse offers REST APIs which make it easy to develop customized applications and CRM integrations to meet business requirements.

Procedure 1	Access Cisco Finesse administration

Step 1. Open a supported browser

Step 2. Access the Cisco Finesse administration log in page by entering the following URL.
https://uccx.mmcvd.ciscolabs.com:8445/cfadmin

Step 3. The login screen appears. Enter the following details.

- Username: **Sudheer**
- Password: **[Password]**

Procedure 2	Register for Context Service

Step 1. Under Register with Context Service, click **Register**.

Upon successful registration you should see the following screen:

Procedure 3	Configure Reasons

Step 1. On the Cisco Finesse Administration home page, click the **Reasons** tab.

Step 2. In **Manage Reason codes** (Not Ready gadget), click **New**. A new reason code is created.

Step 3. Create reason codes for other states by repeating steps 1 and 2.

Procedure 4	Configure desktop layout

Step 1. On the Cisco Finesse home page, click the **Manage Desktops** tab.

Step 2. In the Finesse Layout XML gadget, you can design the required layout using the XML constructs.

Step 3. To enable the **Chat and Email** gadget on the Finesse screen, search on the Finesse XML layout text box for "**my-socialminer-server**" and replace it with the actual FQDN of your SocialMiner instance. Also remove the comments.

Procedure 5	Create phonebooks

Step 1. Click the **Phonebooks** tab.

Step 2. In the Manage phonebooks gadget, create new phonebooks by clicking **New**. The phonebook can be assigned to all users or at team level via the **Assign To** list box.

Procedure 6	Configure team resources

Step 1. Click the T**eam Resources** tab.

Step 2. In Manage Team Resources gadget, select the **IT** team for which you want to associate the resources from the list of teams available.

List of Teams

Name	▲	ID
Default		1
IT		2

Step 3. In **Resources for IT**, click the **Desktop Layout** tab, and then associate the desktop layout to this team created above. Likewise, click other available tabs, to associate the Phonebooks, Reason Codes created in above steps.

Procedure 7	Access the Finesse agent desktop

Step 1. Open a supported browser and enter the following URL.
http://uccx.mmcvd.ciscolabs.com:8445/desktop

Step 2. Enter the following details at the log in screen (If SSO is enabled you are automatically redirected to the IdP server to log in for the first time.)

- Username: Sudheer

- Extension: 8140007

After login, the agent home screen appears showing the default Agent CSQ Statistics Report and Agent team summary report gadgets

Contents | Deployment Details

| Procedure 8 | Change agent state from Not Ready to Ready after log in |

Step 1. Under the agent name, click the down arrow, and then choose **Ready** for the state.

Step 2. To enable the agents to accept Email and Chat request on the Finesse screen change the state to **Ready for Chat and Email** using the pull-down arrow as shown below.
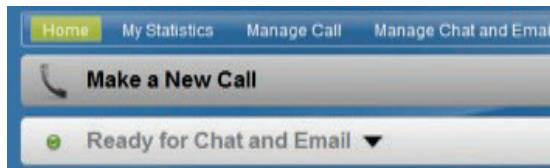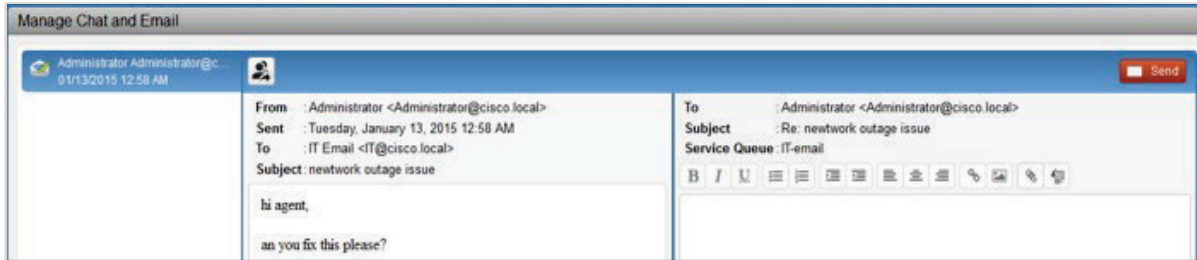

Step 3. Click the **Manage Chat and Email** tab to view/respond to the existing **Email and Chat** requests. For every new request, an agent sees a pop-up message on the Finesse screen. To respond to a query, the agent clicks **Accept**.
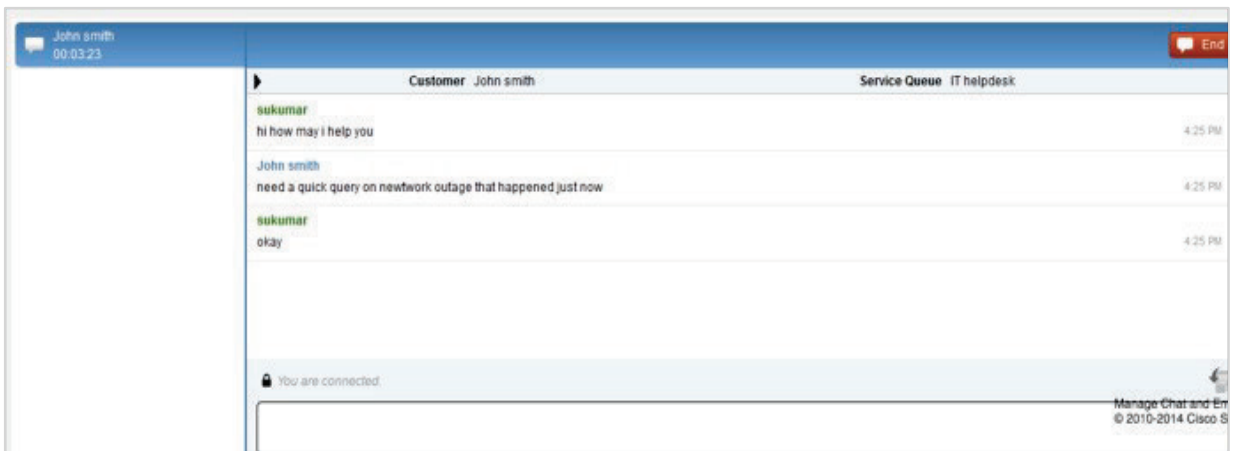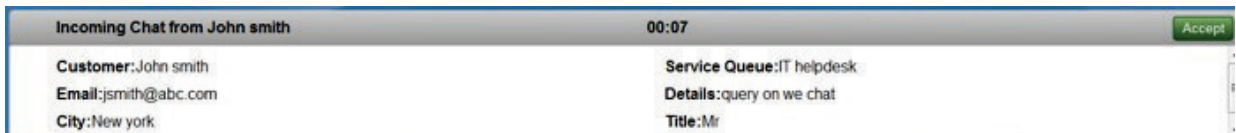
Contents | Deployment Details

Step 4. On a call with the agent, if the customer is registered with the context service, the agent will see the customer's details. The agent can enter and save information.

Procedure 9	Access the Cisco Finesse Supervisor desktop

Step 1. Enter the following URL in a supported browser:
http://uccx.mmcvd.ciscolabs.com:8445/desktop

Step 2. Log in as a supervisor by entering the supervisor extension number.

Contents | Deployment Details

🔍 Reader Tip

By default, the supervisor desktop includes the Manage Team, Team Data, Queue Data, and Manage Customer tabs. Each of these contains default gadgets that provide relevant statistical information using the Unified Intelligence Center.

Step 3. Next, select an agent belonging to the IT team from the Team Performance gadget to perform either a sign-out, forced ready or silent recording on behalf of the agents.

Team Performance				
Start Monitoring Ready Not Ready Sign Out				IT ▾
Agent Name ▲	State		Time in State	Extension
kumar	Ready		00:11:20	81004007
kumar	Ready		00:04:10	81004008

Likewise Click other tabs to view them, if needed.

Procedure 10	Silently monitor and barge-in to existing agent call by supervisor

Step 1. In the Team Performance gadget on the supervisor desktop, click **Start Monitoring**. Now the supervisor can listen to the agent's conversation.

---

i Tech Tip

The agent should be in Talking state for the Monitoring Agent button to be enabled. The supervisor should be in Not Ready state to start the Monitoring Agent. For Silent monitoring to work, BIB on the phone should be enabled.

Team Performance				
Start Monitoring Ready Not Ready Sign Out				IT ▾
Agent Name ▲	State		Time in State	Extension
kumar	Not Ready - lunch		00:00:49	81004007
kumar	Talking		00:00:20	81004008

Step 2. Next, barge-in to an existing agent call, by clicking **Barge-In** in the call control area of the supervisor desktop.

Using Cisco Unified Intelligence Center

PROCESS

1. Start using Cisco Unified Intelligence Center

Cisco Unified CCX users can access reports by using Cisco Unified Intelligence Center and Cisco Finesse. Unified Intelligence Center is a comprehensive, end-to-end reporting solution for Unified CCX which provides access to Historical and Live Data reports.

With Unified Intelligence Center, you can complete the following tasks:

- Generate and view reports.
- Filter data in the reports by setting parameters.
- View help for a report.
- View the report in a new browser.
- Create and view dashboards.
- View permalinks for reports and dashboards, as well as copy this permalink URI and post it onto a webpage for public viewing of reports or dashboards without needing to log into Unified Intelligence Center or have a Finesse desktop.
- Configure thresholds for grid data cells.

Procedure 1	Start using Cisco Unified Intelligence Center

Step 1. Access the Cisco Unified Intelligence Center by going to: https://uccx.mmcvd.ciscolabs.com. Then click **Cisco Unified Contact Center Express Reporting** to access the CUIC home page shown below. (The first time you log in, you will be redirected to the IdP server to enter credentials if SSO is enabled.)

Contents | Deployment Details

Creating and Editing Reports

Procedure 1	Creating sub-folder to store customized reports

i	Tech Tip

To be able to create a folder, the user must be given administrator privileges in the **CUIC** application.

To be able to create report, the user should also have the **report designer** and **report definition designer** access privileges.

Step 1. In the left pane, click the **Report** menu option. The available folders are displayed.
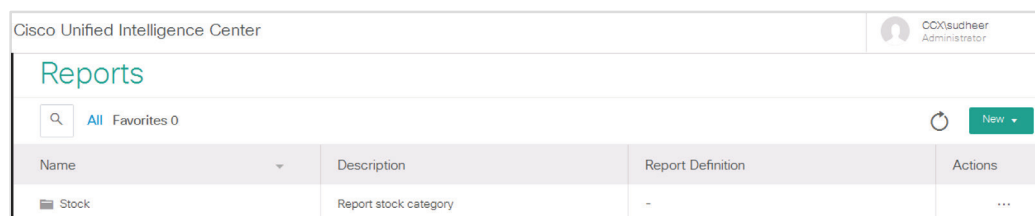
Contents | Deployment Details

Step 2. Navigate to **Report > Stock > Unified CCX Live Data**. On the top-right corner of the screen, click the **New** drop-down menu and select **Folder**. Then create a new folder named **IT HelpDesk Data**.
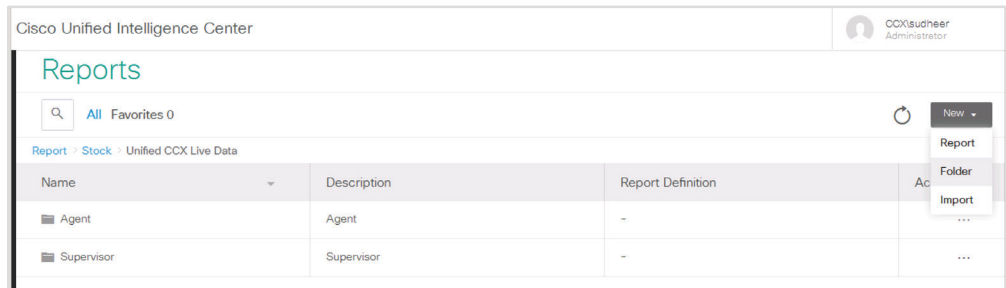
Procedure 2	Create Reports using the Report creation wizard

Step 1. In the newly created folder click the **New** dropdown menu and select the **Report** menu
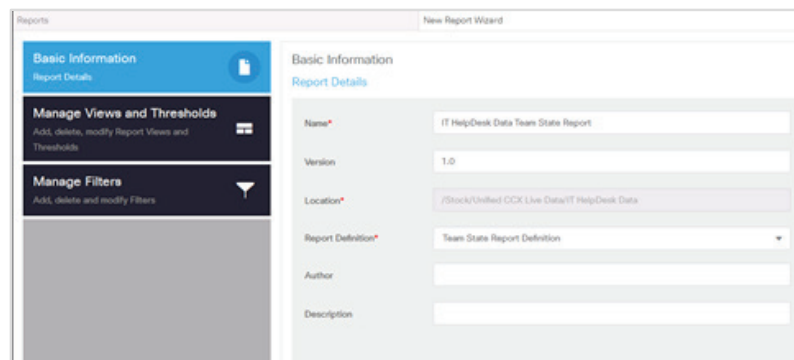
Step 2. Modify Report views and define thresholds if required. This is an optional step
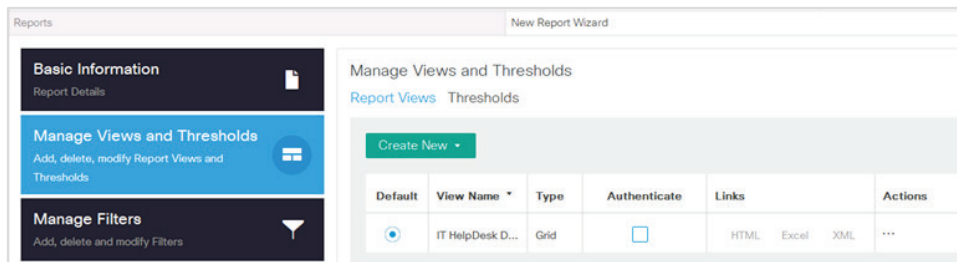
Step 3. Click **Next**, to create filters based on which the Report can be generated
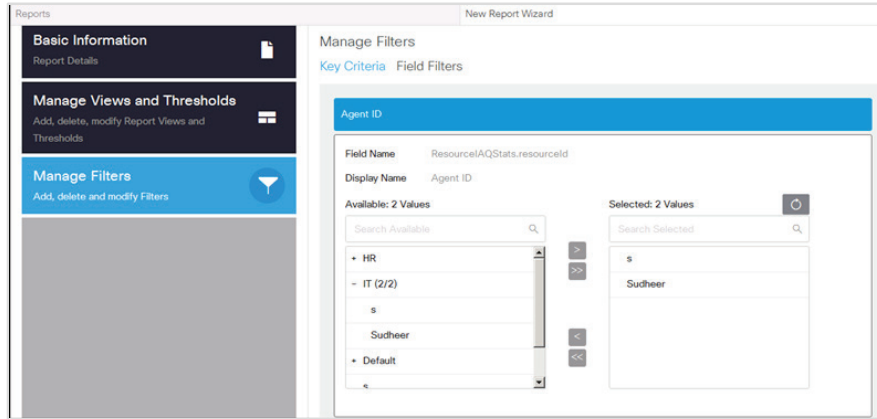
Step 4.   Create other report definitions by repeating above steps 1 – 4.

Procedure 3	Create and view permalinks

Step 1.   Navigate to the newly created Report, right-click under the **Actions** and then click **Permalinks**.
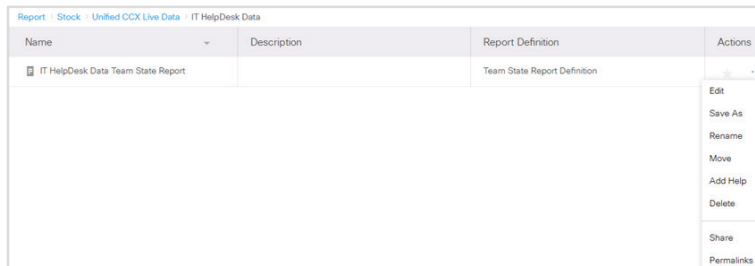
Step 2.   In the Permalinks window, click **HTML** to obtain the permalink as show below.

Contents | Deployment Details
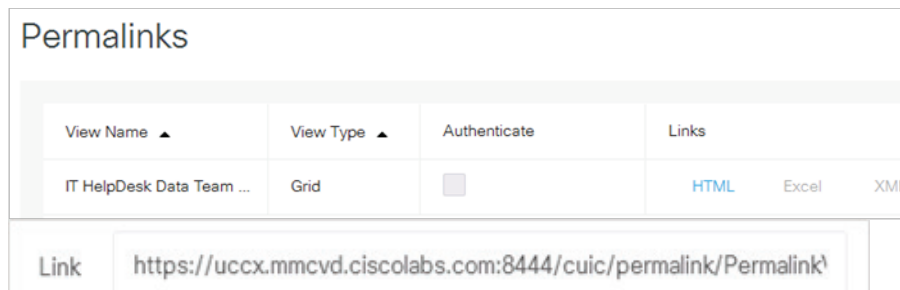
Procedure 4	Generate and view reports

Step 1. Navigate to **Reports > Stock > Unified CCX Live Data > IT HelpDesk Data** and click **IT Helpdesk Data Team State Report** to view the report.

In the top-left corner, you can choose different views of the report if defined. You can generate reports based on filter criteria. The tools icon provides option to edit views and manage thresholds.

⌒OO⌒	Reader Tip
For more information about using Unified Intelligence Center, see the Reporting user guide and the online help available in the Unified Intelligence Center.	

Configuring the Dashboard

PROCESS

1. Create a dashboard
2. Add an item to the dashboard

A *dashboard* is mix of multiple items that you would like shown on a single web page. You can create multiple dashboards, and you can decide if each one is private to certain viewers, or if you want to allow the dashboards to be viewed by others via permission settings.

The following items can be added to any dashboard, and then moved and resized within the dashboard to create the look you want to see within each dashboard:

- Existing reports
- Scheduled reports
- Web page URLs
- Sticky notes
- Custom Widgets

Procedure 1   Create a dashboard

To be able to create a dashboard, you must have the following option enabled for the Users under the **Security > UserList** tab:

- Dashboard Designer

Contents | Deployment Details

Step 1. Move the dashboard drawer to the editing and viewing pallet on the right side of the Unified Intelligence Center display by clicking **Dashboard drawer**, right-click the dashboard folder, and then click **Create Sub-category**.

Step 2. Create Dashboard window, enter the following detail and click **OK**.

• Name: **Helpdesk_dashboard**

Step 3. Assign permissions to the users, and then click **OK**. This example gives all permissions to All Users.

Step 4. For each additional dashboard you want to create, repeat steps 1 - 3.

Procedure 2	Add an item to the dashboard

Step 1. Click **Dashboards**, and then select the dashboard you just created so you can add new items to it.

Contents | Deployment Details
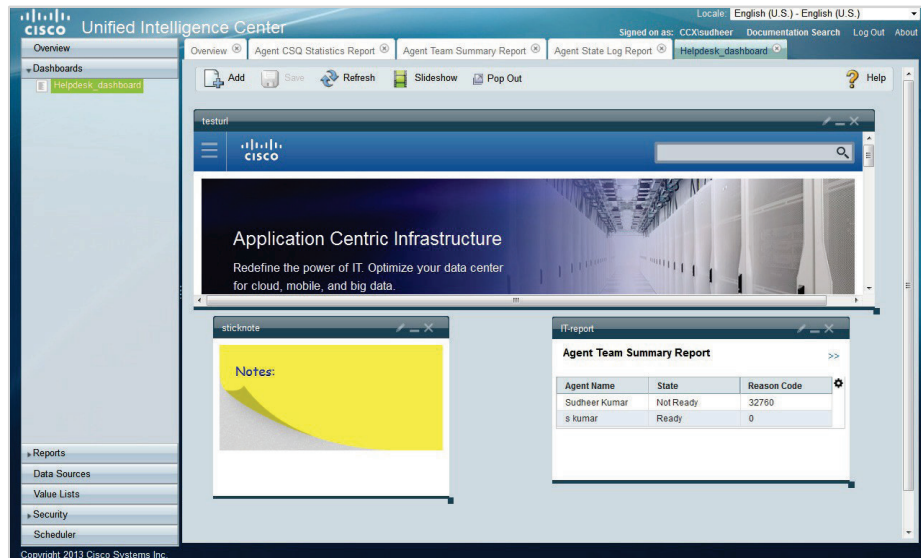
Step 2. Add a new item onto the dashboard by clicking **Add**.

Step 3. In the Dashboard Item settings window, enter the title and the type of item to add.

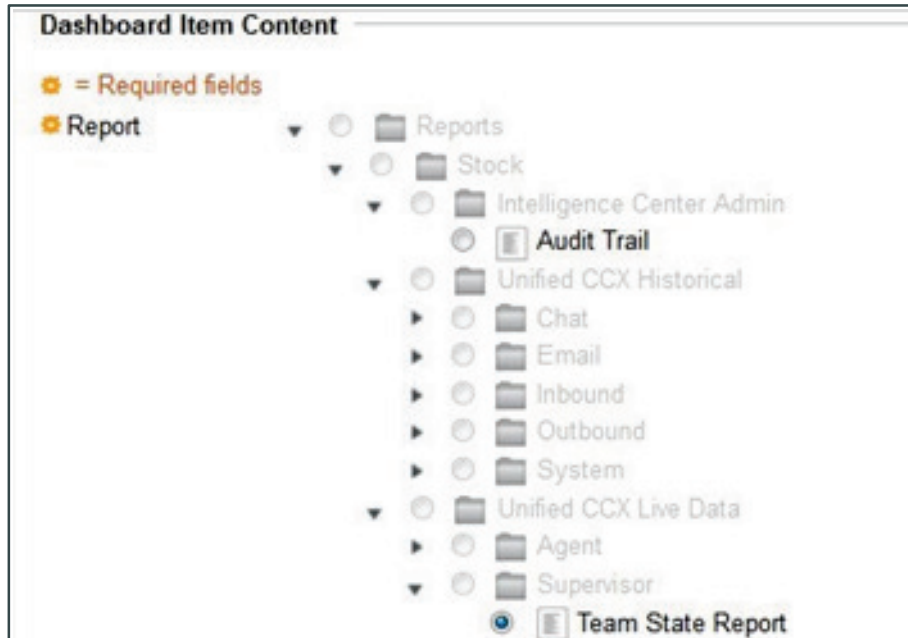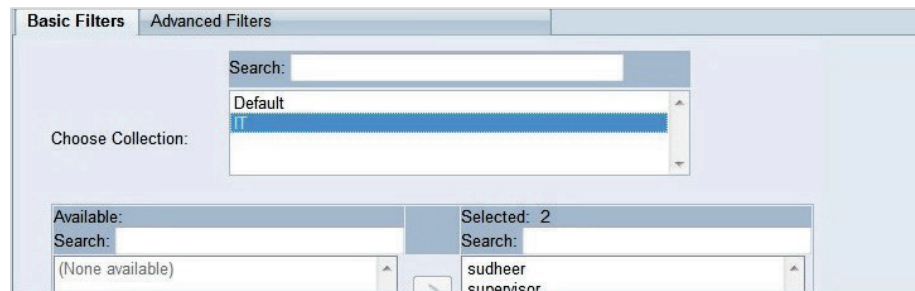**Step 4.** Select the content of the item to be added into the dashboard (Example: Team State Report), and then click **OK**.

Step 5. Select the resource(s) (IT in this example) for which the report needs to be generated, and then click **Run**.

The Report widget is placed into the dashboard, as shown in the following.

Step 6. For each additional item, repeat steps 1 - 5.

Contents | Deployment Details

Appendix A: Product List

Data Center or Server Room

Component	Product Description	Part Numbers	Software
Call Control	Cisco Business Edition 6000 with up to 1000 users	BE6K-ST-BDL-K9	11.5
Contact Center Solution	Cisco Unified Contact Center Express	CCX-11-SYSTEM-K9	11.5
Cisco SocialMiner	Cisco SocialMiner	SocialMiner is included with CCX Premium licenses	11.5

Contents | Deployment Details

Endpoints

Functional Area	Product Description	Part Numbers	Software
Phones	Unified IP Phone 8900 Series	CP-8961-C-K9	11.6
	Unified IP Phone 7800 Series Unified IP Phone 8800 Series	CP-7821-K9 CP-7841-K9 CP-7841-K9	11.6