Install and Configure Optional Cisco Components

SPAN-Based Silent Monitoring

Install SPAN-Based Silent Monitoring

Procedure

Step 1 Mount the Cisco Unified CCE CTI ISO image.

Step 2 Run `setup.exe` file to install SPAN based Silent Monitoring.

Step 3 On the **CTIOS Silent Monitoring Service** page, Click **Yes** to stop CTIOS Silent Monitor process

Step 4 Accept the Software License Agreement, then click **Continue**.

Step 5 Enter the MR patch browse location and click **Next**.

If you do not know the MR patch browser location, leave the filed blank and click **Next**.

Step 6 In the **Choose Destination Location** page, browse to the directory where you want to install, then click **Next**.

Step 7 In the **Cisco CTIOS Silent Monitor - Install Shield Wizard** window:

a) In the **Hostname\IP Address** field, enter the hostname of the silent monitor server.

b) In the **Port** field, enter the port number `42228` on which the Silent Monitor Service listens for incoming connections.

c) Check the **Silent Monitor Server** check box to allow the Silent Monitor Service to monitor multiple Mobile Agents simultaneously.

d) Enter the peer(s) information: Select this if this Silent Monitor Service is part of a cluster of Silent Monitor Services.

Step 8 Click **Next**.

Step 9 On the **CTIOS Silent Monitor** page, do not check the **Enable Security** check box, then click **OK**.

Step 10 Click **Finish**.

SPAN-Based Silent Monitoring Configuration

- Configurations for SPAN from Gateway , on page 2
- Configurations for SPAN from Call Manager, on page 3

Configurations for SPAN from Gateway

This section describes the additional configuration required for Mobile Agent deployment:

1. For Mobile Agents, the voice path crosses the Public Switched Telephone Network (PSTN) and two gateways.

   One gateway control calls from customer phones. The other gateway controls calls from agents, known as agent gateway.

   In a Mobile Agent deployment, the Silent Monitor service uses a SPAN port to receive the voice traffic that passes through the agent gateway. This requires the computer running the Silent Monitor service to have two NIC cards; one to handle communications with clients and another to receive all traffic spanned from the switch.

   For example, if the agent gateway is connected to port 1 and the NIC (on the Silent Monitor Server that receives SPAN traffic) is connected on port 10, use the following commands to configure the SPAN session:

   ```
   monitor session 1 source interface fastEthernet0/1
   ```

   ```
   monitor session 1 destination interface fastEthernet0/10
   ```

2. To deploy Silent Monitoring for the Mobile Agent, there must be two gateways; one gateway for agent traffic and another for caller traffic.

   If you use one gateway for both agent and caller traffic, the voice traffic does not leave or cross the agent gateway and therefore cannot be silently monitored.

   For example, agent-to-agent and consultation calls between Mobile Agents share the same gateway and cannot be silently monitored. Most Mobile Agent deployments only allow silent monitoring for calls between agents and customers.

3. Install Silent Monitor service on the supervisors desktop, but you need not configure Silent Monitor service for the Mobile Agents. You must configure the agent to use one or more Silent Monitor Servers in the CTI OS Server setup program.

4. Agents who are both mobile and regular agents require at least two profiles.

   The profiles for regular agents do not contain any Silent Monitor service information.

   The profiles for Mobile Agents, contains information used to connect to a Silent Monitor Server.

Silent Monitor Service Clusters

If more than one agent gateway is present in the call center and an agent can use either gateway to log in, cluster the Silent Monitor services to support Silent Monitor as follows.

1. Deploy a separate silent monitor server for each gateway.
2. Configure a SPAN port for each silent monitor server as described in the previous section.
3. Run the Silent Monitor server installer to install and configure two Silent Monitor servers as peers.
4. Configure the following to set up a connection profile to instruct the agent desktops to connect to one of the peers:
    a. Check the Enter peers information check box.
    b. Enter the IP address of the other silent monitor service in the Hostname/IP address.

Configurations for SPAN from Call Manager

Use span from Call Manager for small agent contact center only as in this deployment model CUCM software resources are being used .

Before you begin

To Span from CUCM ensure that SM server should be on the same blade as CUCM. Ensure that CUCM uses its own mtp resources ,when the agent is logged into a phone across a gateway.

This requires the computer running the Silent Monitor service to have two NIC cards; one to handle communications with clients and another to receive all traffic spanned from the nexus.

Procedure

Use the following commands to configure the LOCAL SPAN session in nexus :

```
monitor session 1
description LOCAL-SPAN
source interface Vethernet76 both
```

where : Vethernet76 is the interface of CUCM(used for spanning) on the switch.

Cisco Unified SIP Proxy

Install Cisco Unified SIP Proxy

Installation of CUSP

Procedure

Step 1 Download all Cisco Unified SIP Proxy 8.5.7 software files.

Step 2 Copy the files to the FTP server.

Step 3 Starting from router EXEC mode, enter the following:

```
ping <ftp_server_ip_address>
```

Step 4 Enter the following and Install the software:

```
Service-Module 1/0 install url ftp://<ftp_server_ip_address>/cusp-k9.sme.8.5.7.pkg
```

Step 5 Enter **Y** to confirm installation.

Step 6 Enter Cisco Unified SIP Proxy Service Module to monitor and complete the installation.

Example of Installation on a Service Module

```
CUSP#service-nodule SM4/0 inst
CUSP#$ule SM4/0 install url ftp://10.10.10.203/cusp-k9.snc.8.5.7.pkg
Delete the installed Cisco Unified SIP Proxy and proceed with new installation?
[no]:yes
Loading cusp-k9.snc.8.5.7.pkg.install.src !
[OK – 1850/4096 bytes]
cur_cpu: 1862
cur_disk: 953880
cur_nem: 4113488
cur_pkg_name: cusp-k9.sne.8.5.7.pkg
cur_ios_version: 15.2<4>M5,
cur_image_name:c3900e-universalk9-mz
cur_pid: SM-SRE-900-K9
bl_str:
inst_str:
app_str:
key_filename: cusp-k9.sne.8.5.7.key
helper_filename:cusp-helper.sme.8.5.7
Resource check passed…
```

Post Installation Configuration Tool

Run the command: **CUSP#service-module SM 4/0 session** to open the first session.

When you open the first session, the system launches the post installation configuration tool, and asks you if you want to start configuration immediately.

Enter the appropriate response, y or n. If you enter n, the system will halt. If you enter “y”, the system will ask you to confirm, then begin the interactive post installation configuration process.

The following is an example:

```
IMPORTANT::
IMPORTANT:: Welcome to Cisco Systems Service Engine
IMPORTANT:: post installation configuration tool.
IMPORTANT::
IMPORTANT:: This is a one time process which will guide
IMPORTANT:: you through initial setup of your Service Engine.
IMPORTANT:: Once run, this process will have configured
IMPORTANT:: the system for your location.
IMPORTANT::
IMPORTANT:: If you do not wish to continue, the system will be halted
IMPORTANT:: so it can be safely removed from the router.
IMPORTANT::

Do you wish to start configuration now (y,n)? yes
Are you sure (y,n)? yes

IMPORTANT::
IMPORTANT:: A configuration has been found in flash. You can choose
IMPORTANT:: to restore this configuration into the current image.
IMPORTANT::
IMPORTANT:: A stored configuration contains some of the data from a
IMPORTANT:: previous installation, but not as much as a backup.
IMPORTANT::
IMPORTANT:: If you are recovering from a disaster and do not have a
IMPORTANT:: backup, you can restore the saved configuration.
IMPORTANT::
IMPORTANT:: If you choose not to restore the saved configuration, it
IMPORTANT:: will be erased from flash.
IMPORTANT::

Would you like to restore the saved configuration? (y,n) n

Erasing old configuration...done.

IMPORTANT::
IMPORTANT:: The old configuration has been erased.
IMPORTANT:: As soon as you finish configuring the system please use the
IMPORTANT:: "write memory" command to save the new configuration to flash.
IMPORTANT::

Enter Hostname
(my-hostname, or enter to use se-10-50-30-125):
Using se-10-50-30-125 as default

Enter Domain Name
(mydomain.com, or enter to use localdomain): cusp

IMPORTANT:: DNS Configuration:
IMPORTANT::
IMPORTANT:: This allows the entry of hostnames, for example foo.cisco.com, instead
IMPORTANT:: of IP addresses like 1.100.10.205 for application configuration. In order
IMPORTANT:: to set up DNS you must know the IP address of at least one of your
IMPORTANT:: DNS Servers.

Would you like to use DNS (y,n)?y

Enter IP Address of the Primary DNS Server
(IP address): 180.180.180.50
```

```
Found server 180.180.180.50

Enter IP Address of the Secondary DNS Server (other than Primary)
(IP address, or enter to bypass):

E

Enter Fully Qualified Domain Name(FQDN: e.g. myhost.mydomain.com)
or IP address of the Primary NTP server
(FQDN or IP address, or enter for 10.50.30.1): 10.50.10.1
Found server 10.50.10.1

Enter Fully Qualified Domain Name(FQDN: e.g. myhost.mydomain.com)
or IP address of the Secondary NTP Server
(FQDN or IP address, or enter to bypass):

Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa 4) Arctic Ocean 7) Australia 10) Pacific Ocean
2) Americas 5) Asia 8) Europe
3) Antarctica 6) Atlantic Ocean 9) Indian Ocean
#? 2
Please select a country.
1) Anguilla 27) Honduras
2) Antigua & Barbuda 28) Jamaica
3) Argentina 29) Martinique
4) Aruba 30) Mexico
5) Bahamas 31) Montserrat
6) Barbados 32) Netherlands Antilles
7) Belize 33) Nicaragua
8) Bolivia 34) Panama
9) Brazil 35) Paraguay
10) Canada 36) Peru
11) Cayman Islands 37) Puerto Rico
12) Chile 38) St Barthelemy
13) Colombia 39) St Kitts & Nevis
14) Costa Rica 40) St Lucia
15) Cuba 41) St Martin (French part)
16) Dominica 42) St Pierre & Miquelon
17) Dominican Republic 43) St Vincent
18) Ecuador 44) Suriname
19) El Salvador 45) Trinidad & Tobago
20) French Guiana 46) Turks & Caicos Is
21) Greenland 47) United States
22) Grenada 48) Uruguay
23) Guadeloupe 49) Venezuela
24) Guatemala 50) Virgin Islands (UK)
25) Guyana 51) Virgin Islands (US)
26) Haiti
#? 47
Please select one of the following time zone regions.
1) Eastern Time
2) Eastern Time - Michigan - most locations
3) Eastern Time - Kentucky - Louisville area
4) Eastern Time - Kentucky - Wayne County
5) Eastern Time - Indiana - most locations
6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
7) Eastern Time - Indiana - Pulaski County
8) Eastern Time - Indiana - Crawford County
9) Eastern Time - Indiana - Pike County
10) Eastern Time - Indiana - Switzerland County
11) Central Time
12) Central Time - Indiana - Perry County
13) Central Time - Indiana - Starke County
```

```
14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
15) Central Time - North Dakota - Oliver County
16) Central Time - North Dakota - Morton County (except Mandan area)
17) Mountain Time
18) Mountain Time - south Idaho & east Oregon
19) Mountain Time - Navajo
20) Mountain Standard Time - Arizona
21) Pacific Time
22) Alaska Time
23) Alaska Time - Alaska panhandle
24) Alaska Time - Alaska panhandle neck
25) Alaska Time - west Alaska
26) Aleutian Islands
27) Hawaii
#? 21

The following information has been given:
United States
Pacific Time

Therefore TZ='America/Los_Angeles' will be used.
Is the above information OK?
1) Yes
2) No
#? 1

Local time is now: Mon Apr 5 11:20:17 PDT 2010.
Universal Time is now: Mon Apr 5 18:20:17 UTC 2010.
executing app post_install
executing app post_install done
Configuring the system. Please wait...
Changing owners and file permissions.
Tightening file permissions ...
Change owners and permissions complete.
Creating Postgres database .... done.
INIT: Switching to runlevel: 4
INIT: Sending processes the TERM signal
==> Starting CDP
STARTED: cli_server.sh
STARTED: ntp_startup.sh
STARTED: LDAP_startup.sh
STARTED: SQL_startup.sh
STARTED: dwnldr_startup.sh
STARTED: HTTP_startup.sh
STARTED: probe
STARTED: fndn_udins_wrapper
STARTED: superthread_startup.sh
STARTED: /bin/products/umg/umg_startup.sh

Waiting 49 ...

IMPORTANT::
IMPORTANT:: Administrator Account Creation
IMPORTANT::
IMPORTANT:: Create an administrator account.
IMPORTANT:: With this account, you can log in to the
IMPORTANT:: Cisco Unified SIP Proxy
IMPORTANT:: GUI and run the initialization wizard.

IMPORTANT::

Enter administrator user ID:
(user ID): test
tesEnter password for test:
```

```
(password):
Confirm password for test by reentering it:
(password):

SYSTEM ONLINE
cusp-sre-49# show software version
Cisco Unified SIP Proxy version <8.5.7>
Technical Support: http://www.cisco.com/techsupport Copyright <c> 1986-2008 by Cisco
Systems,Inc.
Cusp-src-49# show software packages

Installed Packages:
- Installer <Installer application >  <8.5.7.0>
- Infrastructure <Service Engine Infrastructure> <8.5.7>
- Global <Global manifest > <8.5.7>
- Bootloader <Secondary> <Service Engine Bootloader> <2.1.30>
- Core <Service Engine OS Core > <8.5.7>
- GPL Infrastrucutre <Service Engine GPL Infrastructure > <8.5.7>
```

Obtaining New or Additional Licenses

- Required Information, on page 8
- Using the CLI to Install the Cisco Unified SIP Proxy Release 8.5.7 Licenses, on page 9
- Using the Licensing Portal to Obtain Licenses for Additional Features or Applications, on page 8

Required Information

Collect the following information before you obtain new or additional CSL licenses:

- The SKU for the features that you need. The SKU is used in the ordering process to specify the desired licenses for the Cisco Unified SIP Proxy features that you want.
- The Product ID (PID) and the Serial Number (SN) from the device. Together, these form the unique device identifier (UDI). The UDI is printed on a label located on the back of most Cisco hardware devices or on a label tray visible on the front panel of field-replaceable motherboards. The UDI can also be viewed via software using the show license udi command in privileged EXEC mode.

Using the Licensing Portal to Obtain Licenses for Additional Features or Applications

Note You must have a Cisco.com password to access some of the URLs in the following procedure.

Follow these steps to obtain additional licenses for Cisco Unified SIP Proxy Release 8.5.7 features.

Procedure

Step 1 Go to http://www.cisco.com/web/ordering/root/index.html and choose one of the ordering processes (through partner, Cisco direct, etc.) and order licenses. When you purchase a license, you will receive a product activation key (PAK), which is an alphanumeric string that represents the purchase.

Step 2 To get your license file, return to the **Cisco Product License Registration Portal** at http://www.cisco.com/web/ordering/root/index.html. When prompted, and enter the PAK and the unique device identifier (UDI) of the device where the license will be installed.

Step 3 Download the license file or receive the license file by email.

Step 4 Copy the license file(s) to a FTP or TFTP server.

Using the CLI to Install the Cisco Unified SIP Proxy Release 8.5.7 Licenses

Follow these steps to install the licenses for Cisco Unified SIP Proxy

Procedure

Step 1 Login to the CLI.

Step 2 Enter `license install` *<URL>*, where *<URL>* is the FTP URL that you copied the license in the previous procedure.

Step 3 Verify the license by entering either `show license` or `show software licenses`.

Step 4 Activate the new license by entering `license activate`.

Step 5 Reload the module by entering `reload` and confirming that you really want to reload the module.

Note You cannot remove evaluation licenses.

Configure Cisco Unified SIP Proxy Server

Login to CUSP portal *http://<cusp module IP>/admin/Common/HomePage.do* and configure the Cisco Unified SIP Proxy server, in the following order:

Required Software	Tasks
Configure CUSP	Configure Cisco Unified SIP Proxy, on page 9
Configure Gateway	Configure Gateway, on page 16
Configure Unified CVP	Configure Unified CVP, on page 17
Configure Unified Call Manager though UCDM	Configure Cisco Unified Communications Manager , on page 18

Configure Cisco Unified SIP Proxy

Perform the following procedures to configure Unified SIP Proxy

Sequence	Done?	Tasks	Notes
1		Configure Networks, on page 10	
2		Configure Triggers, on page 10	
3		Configure Server Groups, on page 11	
4		Configure Route Tables, on page 12	

Sequence	Done?	Tasks	Notes
5		Configure Route Policies, on page 13	
6		Configure Route Triggers, on page 13	

For complete configuration details of Cisco Unified SIP Proxy, see Full Configuration for Cisco Unified SIP Proxy, on page 13

Table 1: Example CUSP Deployment Details

Server Name	IP Address	FQDN
CUSP	10.10.10.49	cusp.hcsdc1.icm
CVP	10.10.10.10	cvp.hcsdc1.icm
CUCM	10.10.10.30	ccm.hcsdc1.icm
Gateway	10.10.10.180	gw.hcsdc1.icm

Configure Networks

Procedure

Step 1 Login to CUSP portal.

Step 2 Navigate to **Configure** > **Networks** and click **Add**.

Step 3 Enter a unique name for the Network.

Example:

hcs

Step 4 Choose **Standard** from the **TYPE** drop-down list.

Step 5 Enable the **Allow Outbound Connections**.

Step 6 Click **Add** on the **SIP Listen Points** tab.

Step 7 Choose newly added **Network** and select **SIP Listen Points** tab.

Step 8 Select the IP address of the CUSP, from the **IP address** drop-down list, See Table 1: Example CUSP Deployment Details, on page 10.

Step 9 Keep the default port 5060.

Step 10 Select the **Transport Type** as **TCP** and click **Add**.

Step 11 Repeat the **step 6** to **step 8**, select **Transport Type** as UDP and click **Add**.

Step 12 Disable **SIP Record-Route**, select and disable all the networks for the CVP that includes callflows.

Configure Triggers

Procedure

Step 1 Login to CUSP Portal.

Step 2 Navigate to **Configure** > **Triggers** and click **Add**.

Step 3 Enter a name for the Trigger and click **Add**.

Example:

hcs trigger in

Step 4 Choose the appropriate **Trigger conditions** from the drop-down lists.

Example:

Inbound Network,

Is exactly, and

hcs

Step 5 Click **Add**.

Configure Server Groups

Procedure

Step 1 Login to CUSP portal.

Step 2 Navigate to **Configure** > **Server Groups** > **Groups**.

Step 3 Enter a name (FQDN) for the **Server Group**.

Example:

ccm.hcsdc1.icm

Step 4 Choose **global (default)** from **Load Balancing Scheme** drop-down list.

Step 5 Choose **hcs** from **Network** drop-down list.

Step 6 Check the **Pinging Allowed** check-box.

Step 7 Click **Add**.

Step 8 Select newly added **Server Group** to add the elements for a respective server group.

Step 9 Select **Elements** tab and click **Add**.

Step 10 In **<IP Address>** text-box, enter the IP address of the Server Group, see Table 1: Example CUSP Deployment Details, on page 10.

Step 11 In **Port** text-box, enter the port value.

Step 12 Choose **tcp** from **Transport Type** drop-down list.

Step 13 In **Q-Value** text-box, enter the Q-Value as `1.0`.

Step 14 In **Weight** text-box, enter the weight `10`.

Step 15 Click **Add**.

Step 16 Repeat the above steps to configure cvp, gateway, ccm server groups.

Configure Route Tables

Table 2: Example Route Table

Key	Description	Host / Server Group (FQDN)	Network
4000	Agent Extension	ccm.hcsdc1.icm	hcs
7777	Network VRU label for CVP client	gw.hcsdc1.icm	hcs
8881	Network VRU label for CUCM client	cvp.hcsdc1.icm	hcs
811	Dialed number	cvp.hcsdc1.icm	hcs
912	Post call survey dialed number	cvp.hcsdc1.icm	hcs
9191	Ringtone	gw.hcsdc1.icm	hcs
9292	Error Tone	gw.hcsdc1.icm	hcs
6661111000	Network VRU label for MR client	cvp.hcsdc1.icm	hcs
978	Customer Dialed Number	out.hcsdc1.icm	hcs

Procedure

Step 1 Login to CUSP portal.

Step 2 Navigate to **Configure** > **Route Tables**.

Step 3 Click **Add**.

Step 4 Enter a name for a Route Table, click **Add**.

Example:

hcs

Step 5 Select the **Route Table** to add the rules for a respective route table.

Step 6 Click **Add**.

Step 7 In the **Key** text-box, enter key, see Table 2: Example Route Table, on page 12.

Step 8 Choose a **Destination** from **Route Type** drop-down list.

Step 9 In **Host / Server Group** text-box, enter Hostname (FQDN) / IP address, see Table 1: Example CUSP Deployment Details, on page 10.

Step 10 In **Port** text-box, enter the Port value.

Step 11 Choose an appropriate **Transport Type** from the drop-down list

Step 12 Choose an appropriate **Network** from the drop-down list.

Configure Route Policies

Procedure

Step 1 Login to CUSP portal.

Step 2 Navigate to **Configure** > **Route Policies**.

Step 3 Click **Add**.

Step 4 Enter a name for a Route Policy, click **Add**.

Step 5 Choose a **Name** from the drop-down list.

Step 6 Choose a **Lookup Key Matches** from the drop-down list.

Step 7 Choose the **Lookup Key** from the drop-down lists.

Step 8 Click **Add**.

Configure Route Triggers

Procedure

Step 1 Login to CUSP portal.

Step 2 Navigate to **Configure** > **Route Triggers**.

Step 3 Click **Add**.

Step 4 Choose a **Routing Trigger** from the drop-down list.

Step 5 Choose a **Trigger** from the drop-down list.

Step 6 Click **Add**.

Step 7 Select newly added **Trigger** to add trigger condition.

Step 8 Select the **Trigger Condition** from the drop-down lists.

Step 9 Click **Add**.

Full Configuration for Cisco Unified SIP Proxy

```
cusp(cusp)# show configuration active ver
cusp(cusp)# show configuration active verbose
Building CUSP configuration...
!
server-group sip global-load-balance call-id
server-group sip retry-after 0
server-group sip element-retries udp 2
server-group sip element-retries tls 1
server-group sip element-retries tcp 1
sip dns-srv
 enable
 no naptr
 end dns
!
no sip header-compaction
no sip logging
!
```

```
sip max-forwards 70
sip network hcs standard
 no non-invite-provisional
 allow-connections
 retransmit-count invite-client-transaction 3
 retransmit-count invite-server-transaction 5
 retransmit-count non-invite-client-transaction 3
 retransmit-timer T1 500
 retransmit-timer T2 4000
 retransmit-timer T4 5000
 retransmit-timer TU1 5000
 retransmit-timer TU2 32000
 retransmit-timer clientTn 64000
 retransmit-timer serverTn 64000
 tcp connection-setup-timeout 0
 udp max-datagram-size 1500
 end network
!
sip overload reject retry-after 0
!
no sip peg-counting
!
sip privacy service
sip queue message
 drop-policy head
 low-threshold 80
 size 2000
 thread-count 20
 end queue
!
sip queue radius
 drop-policy head
 low-threshold 80
 size 2000
 thread-count 20
 end queue
!
sip queue request
 drop-policy head
 low-threshold 80
 size 2000
 thread-count 20
 end queue
!
sip queue response
 drop-policy head
 low-threshold 80
 size 2000
 thread-count 20
 end queue
!
sip queue st-callback
 drop-policy head
 low-threshold 80
 size 2000
 thread-count 10
 end queue
!
sip queue timer
 drop-policy none
 low-threshold 80
 size 2500
 thread-count 8
 end queue
```

```
!
sip queue xcl
 drop-policy head
 low-threshold 80
 size 2000
 thread-count 2
 end queue
!
route recursion
!
sip tcp connection-timeout 30
sip tcp max-connections 256
!
no sip tls
!
sip tls connection-setup-timeout 1
!
trigger condition hcs_trigger_in
 sequence 1
  in-network ^\Qhcs\E$
  end sequence
 end trigger condition
!
trigger condition hcs_trigger_out
 sequence 1
  out-network ^\Qhcs\E$
  end sequence
 end trigger condition
!
trigger condition mid-dialog
 sequence 1
  mid-dialog
  end sequence
 end trigger condition
!
accounting
 no enable
 no client-side
 no server-side
 end accounting
!
server-group sip group ccm.hcsdc1.icm hcs
 element ip-address 10.10.10.31 5060 tcp q-value 1.0 weight 10
 element ip-address 10.10.10.131 5060 tcp q-value 1.0 weight 10
 failover-resp-codes 503
 lbtype global
 ping
 end server-group
!
server-group sip group cvp.hcsdc1.icm hcs
 element ip-address 10.10.10.10 5060 tcp q-value 1.0 weight 10
 failover-resp-codes 503
 lbtype global
 ping
 end server-group
!
server-group sip group gw.hcsdc1.icm hcs
 element ip-address 10.10.10.180 5060 tcp q-value 1.0 weight 10
 failover-resp-codes 503
 lbtype global
 ping
 end server-group
!
route table hcs
```

```
 key 4000 target-destination ccm.hcsdc1.icm hcs
 key 77777 target-destination gw.hcsdc1.icm hcs
 key 8881 target-destination cvp.hcsdc1.icm hcs
 key 91100 target-destination cvp.hcsdc1.icm hcs
 end route table
!
policy lookup hcs_policy
 sequence 100 hcs request-uri uri-component user
  rule prefix
  end sequence
 end policy
!
trigger routing sequence 1 by-pass condition mid-dialog
trigger routing sequence 3 policy hcs_policy condition hcs_trigger_out
trigger routing sequence 4 policy hcs_policy condition mid-dialog
trigger routing sequence 5 policy hcs_policy condition hcs_trigger_in
!
server-group sip ping-options hcs 10.10.10.49 4000
 method OPTIONS
 ping-type proactive 5000
 timeout 2000
 end ping
!
server-group sip global-ping
sip cac session-timeout 720
sip cac hcs 10.10.10.10 5060 tcp limit -1
sip cac hcs 10.10.10.131 5060 tcp limit -1
sip cac hcs 10.10.10.180 5060 tcp limit -1
sip cac hcs 10.10.10.31 5060 tcp limit -1
!
no sip cac
!
sip listen hcs tcp 10.10.10.49 5060
sip listen hcs udp 10.10.10.49 5060
!
call-rate-limit 200
!
end
cusp(cusp)#
```

Configure Gateway

- Create a Sip-Server with the CUSP IP, on page 16
- Create a Dial-Peer, on page 16

Create a Sip-Server with the CUSP IP

```
sip-ua
 retry invite 2
 retry bye 1
 timers expires 60000
 timers connect 1000
 sip-server ipv4:10.10.10.49:5060
 reason-header override
```

Create a Dial-Peer

```
dial-peer voice 9110 voip
 description Used for CUSP
 preference 1
 destination-pattern 911T
 session protocol sipv2
 session target sip-server
session transport tcp
voice-class codec 1
dtmf-relay rtp-nte
no vad
```

Configure Unified CVP

- Configure SIP Proxy, on page 17
- Configure SIP Server Groups, on page 17
- Configure Call Server, on page 17

Configure SIP Proxy

Procedure

Step 1 Login to Unified Customer Voice Portal.

Step 2 Navigate to **Device Management** > **SIP Proxy Server**, click **Add New**.

Step 3 Enter the IP Address, Hostname. Select **Cisco Unified SIP Proxy** from **Device Type** drop-down list .

Step 4 Click **Save**.

Configure SIP Server Groups

Procedure

Step 1 Login to Unified Customer Voice Portal.

Step 2 Navigate to **System** > **SIP Server Groups**, click **Add New**.

Step 3 Enter the FQDN name, IP Address, Port, Priority, Weight of CUSP and click **Add**.

Step 4 Click **Save**.

Configure Call Server

Procedure

Step 1 Login to Unified Customer Voice Portal.

Step 2 Navigate to **Device Management** > **Call Server**.

Step 3 Select **Call Server** > **Click Edit** > **Click SIP tab**.

Step 4 Select **Yes** to enable Outbound Proxy Server.

Step 5 Enter **Outbound SRV domain name / Server Group Name (FQDN)**, click **Save and Deploy**.

Note As CUSP provides centralized dialed plan , delete the existing Dialed number patterns.

Configure Cisco Unified Communications Manager

Login to the Unified Communications Domain Manager administration interface and perform the following steps to complete a route configuration toward the Unified CUSP server.

- Add Trunk to CVP, on page 18
- Add Trunk to CUSP, on page 18

Add Trunk to CVP

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer admin.

Step 2 Ensure that hierarchy is set to the node where Unified Communication Manager is configured.

Step 3 Navigate to **SIP Trunks**:

- For provider or reseller administrator **Device Management** > **CUCM** > **SIP Trunks**
- For customer administrator **Device Management** > **Advanced** > **SIP Trunks**

Step 4 Click **Add** to create SIP trunk.

Step 5 Perform the following, In **Device Information** tab:

a) Choose required IP address from **CUCM** drop-down list that you want to add SIP trunk.
b) Enter a unique SIP trunk name in **Device Name** field.
c) Choose **Device Pool** from the drop-down list.
d) Check **Run On All Active Unified CM Nodes** check-box.

Step 6 Goto **SIP Info** tab and perform the following:

a) Click **Add** icon in **Destination** panel.
b) Enter destination IP address of CVP **Address IPv4** field.
c) Change **Port** to 5090.
d) Enter **Sort Order** to prioritize multiple destinations.

Note Lower sort order indicates higher priority.

e) Choose newly added **SIP Trunk Security Profile** from the drop-down list.
f) Choose **sip profile** from the drop-down list.

Repeat this step to add another trunk.

Step 7 Click **Save**.

Add Trunk to CUSP

Procedure

Step 1 Login to Cisco Unified Communication Domain Manager as provider, reseller or customer admin.

Step 2 Ensure that hierarchy is set to the node where Unified Communication Manager is configured.

Step 3 Navigate to **SIP Trunks**:

- For provider or reseller administrator **Device Management** > **CUCM** > **SIP Trunks**
- For customer administrator **Device Management** > **Advanced** > **SIP Trunks**

Step 4 Click **Add** to create SIP trunk.

Step 5 Perform the following, In **Device Information** tab:

a) Choose required IP address from **CUCM** drop-down list that you want to add SIP trunk.
b) Enter a unique SIP trunk name in **Device Name** field.
c) Choose **Device Pool** from the drop-down list.
d) Select **Run On All Active Unified CM Nodes** check-box.

Step 6 Goto **SIP Info** tab and perform the following:

a) Click **Add** icon in **Destination** panel.
b) Enter destination IP address of CUSP in **Address IPv4** field.
c) Change **Port**, if required.
d) Enter **Sort Order** to prioritize multiple destinations.

Note Lower sort order indicates higher priority.

e) Choose newly added **SIP Trunk Security Profile** from the drop-down list.
f) Choose **sip profile** from the drop-down list.

Repeat this step to add another trunk.

Step 7 Click **Save**.

Configure Outbound with Cisco Unified SIP Proxy

- Configure Unified CCE, on page 19
- Configure Gateway, on page 20
- Configure Cisco Unified SIP Proxy for IVR based Campaign, on page 20

Configure Unified CCE

Procedure

Step 1 Select **Start** > **All Programs** > **Cisco Unified CCE Tools** > **Peripheral Gateway Setup**.

Step 2 Click **Add** under **Instance Component**, then click **Outbound Dialer** to add the dialer.

Step 3 On the **Outbound Dialer properties** page, ensure that the **SIP** radio button is selected and then click **Next**.

Step 4 In the **SIP Dialer Name** text box, enter the SIP dialer name exactly as it is configured in the **Dialer Tool** under **Configuration Manager**.

Step 5 In **SIP Server Type**, ensure that **(CUSP)/(CUBE)** is selected.

Step 6 Enter **CUSP IP** in the **SIP Server** text box and click **Next**.

Step 7 In the **Campaign Manager Server** text box, enter **Unified CCE DataserverA /RoggerA side IP** address.

Step 8 Check the **Enable Secured Connection** checkbox to enable secured connection.

Note Before you enable secured connection between the components, ensure to complete the security certificate management process.

For more information, see the *Security Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

Step 9 In the **CTI Server A** text box, enter **A side CTIOS server IP Address**; in the **CTI Server Port A** text box, enter the appropriate port number. The default port is**42027** for non-secured connection and **42030** for secured connection.

Step 10 In the **CTI Server B** text box, enter **B side CTIOS server IP address**; in the **CTI Server Port B** text box, enter the appropriate port number. The default port is**42027** for non-secured connection and **42030** for secured connection.

Step 11 Keep all other fields as **default** and click **Next**. In the following window, click **Next** to complete the install.

Configure Gateway

```
dial-peer voice 811 voip
 description ******To CUCM*****
 destination-pattern 811T
 session protocol sipv2
 session target sip-server
 voice-class codec 1
 voice-class sip rel1xx supported "100rel"
 dtmf-relay rtp-nte h245-signal h245-alphanumeric
 no vad
!

 sip-ua
retry invite  2
retry bye 1
timers expires 60000
timers connect 1000
sip-server dns:out.hcsdc1.icm
reason header override
permit hostname dns:out.hcsdc1.icm
```

Configure Cisco Unified SIP Proxy for IVR based Campaign

Procedure

Step 1 Login to CUSP portal.

Step 2 Navigate to **Configure** > **Route Tables**.

Step 3 Click the existing route table.

Example:

HCS.

Step 4 Select the Route Table to add the rules for a respective route table.

Step 5 Click **Add**.

Step 6 In **Key** text-box, enter key, 8881.

Step 7 Choose **Destination** from **Route Type** drop-down list.

Step 8 In **Host / Server Group** text-box, enter Hostname (FQDN) / IP address of CVP.

Example:

cvp.hcsdc1.icm

Step 9 In **Port** text-box, enter the Port value.

Step 10 Choose an appropriate **Transport Type** from the drop-down list.

Step 11 Choose an appropriate **Network** from the drop-down list.

Note As CUSP provides centralized dial plan management you can directly route the IVR call to CVP.

Avaya PG

Follow the below procedures for 4000 and 12000 agent deployment model:

- Create Golden Template for Avaya PG, on page 21
- Configure Avaya PG, on page 25

Create Golden Template for Avaya PG

Follow this sequence of tasks to create the golden template for Avaya PG. After each task, return to this page to mark the task "done" and continue the sequence:

Sequence	Done?	Tasks	Notes
1		Download `UCCE_12.5_Win2016_vmv13_v1.0`	See Download OVA Files, on page 22.
2		Create the virtual machine for the Unified CCE Avaya PG	Follow the procedure Create Virtual Machines, on page 22.
3		Install Microsoft Windows Server	Follow the procedure Install Microsoft Windows Server, on page 23.
4		Install Antivirus Software	Follow the procedure Install Antivirus Software.
5		Install the Unified Contact Center Enterprise	Follow the procedure Install Unified Contact Center Enterprise, on page 24.
6		Convert the virtual machine to a template.	Follow the procedure Convert the Virtual Machine to a Golden Template, on page 24.

After you create all golden templates, you can run the automation process (Automated Cloning and OS Customization). After you run the automation process, you can configure the Avaya PG server on the destination system. See Configure Avaya PG, on page 25.

Download OVA Files

Open Virtualization Format files (OVAs) are required for golden templates. Cisco HCS for Contact Center uses the OVAs that define the basic structure of the corresponding VMs that are created. The structure definition Includes the CPU, RAM, disk space, reservation for CPU, and reservation for memory.

Note The VMs and software components are optimized for Cisco HCS for Contact Center. You must use the OVAs for Cisco HCS for Contact Center.

Before you begin

You must have a valid service contract associated with your Cisco.com profile

Procedure

Step 1 Go to the *Hosted Collaboration Solution for Contact Center* Download Software page on Cisco.com.

Step 2 Select the required software type.

Step 3 Click **Download** and save the OVA file to your local drive. When you create VMs, select the OVA required for the application.

Create Virtual Machines

Procedure

Step 1 Launch the VMware vSphere client and select **File** > **Deploy OVF Template**.

Step 2 Browse to the location on your local drive, where you have stored the OVA. Click **Open** to select the OVA file, click **Next**.

Step 3 On the **OVF Template Details** page, click **Next**.

Step 4 On the **Name and Location** page, in the **Name** field, enter the name of virtual machine, then click **Next**.

Note Enter a maximum of 32 characters; spaces and special characters are not allowed.

Step 5 On the **Deployment Configuration** page, select the appropriate configuration from the drop-down list, click **Next**.

Step 6 On the **Resource Pool** page, select the required resource pool, then click **Next**.

Note Skip this step if you do not have a resource pool allocated in the host server.

Step 7 On the **Storage** page, select a data store you want to deploy in the new virtual machine, then click **Next**.

Step 8 On the **Disk Format** page, select **Thick provisioned Lazy Zeroed**, then click **Next**.

Note Thin provision format is used for the template creation process, it is not supported for production use.

Step 9 On the **Network Mapping** page, select the appropriate network from the **Destination Network** drop-down list, then click **Next**.

Note For Unified Contact Center Enterprise machines, confirm that **Network Mapping** page is correct:

- Public to Visible Network
- Private to Private Network

Step 10 Click **Finish**.

Install Microsoft Windows Server

Procedure

Step 1 Mount the Microsoft Windows Server ISO image on the virtual machine.

Step 2 Switch on the virtual machine.

Step 3 Enter the **Language**, **Time and Currency Format**, and **Keyboard settings**, then click **Next**.

Step 4 Click **Install Now**.

Step 5 Enter the product activation key, then click **Next**.

Step 6 Select the Windows Server you want to install, then click **Next**.

Step 7 Accept the license agreement, then click **Next**.

Step 8 Select **Custom: Install Windows Only (Advanced)**, select the disk, then click **Next**.
The installation begins.

Step 9 Enter and confirm the administrator password, then click **Finish**.

Step 10 Refer related topics to install the VMware tools.

Step 11 Enable **Remote Desktop Connection**:

a) Select **Start** > **Control Panel** > **System and Security**.
b) Click **Allow remote access** > **OK**.
c) Select **Allow connections from computers running any version of Remote Desktop** and click **Apply**.
d) Click **OK**.

Step 12 Open the **Network and Sharing Center** and select **Ethernet**.

Step 13 In the **Ethernet Status** dialog box, configure the network settings and the Domain Name System (DNS) data:

a) Select **Properties**. Uncheck the **Internet Protocol Version 6 (TCP/IP6)**.
b) Select **Internet Protocol Version 4 (TCP/IPv4)**, then click **Properties**.
c) Select **Use the following IP Address** option.
d) Enter the IP address, Subnet mask, and Default gateway.
e) Select **Use the following DNS Server Address** option.
f) Enter **Preferred DNS Server** address, then click **OK**.

Note All network configurations are overwritten with new settings.

Step 14 Go to **Settings** > **Update & Security** and run Microsoft Windows Update.

Note Edge Chromium (Microsoft Edge) is not installed by default on the Windows server. To install Edge Chromium (Microsoft Edge), see *Microsoft* documentation.

Install Unified Contact Center Enterprise

Procedure

Step 1 Add the virtual machine template into the domain.

Step 2 Mount the Unified Contact Center Enterprise ISO image to the virtual machine.

Step 3 From the `ICM-CCE-CCH` Installer directory, run `setup.exe` and follow the InstallShield procedures.

Step 4 In the **Select the installation method** window, select **Fresh Install**, then click **Next**.

Step 5 In the **Maintenance Release (MR)** window, keep the **Maintenance Release Location** field blank, then click **Next**.

Step 6 In the **Installation Location** window, select the drive `C`, then click **Next**.

Step 7 In the **Ready to Copy Files** window, click **Install**.

Step 8 In the **Installation Complete** window, click **Yes, I want to restart my computer now**, then click **Finish**.

Step 9 Apply the Unified Contact Center Enterprise maintenance release, if applicable.

Step 10 Unmount the Unified Contact Center Enterprise ISO image.

Step 11 Move the virtual machine template back to the workgroup.

Note If the ICM-CCE installer installs JRE on the Windows platform, the system retains only the Cisco approved CA certificates in the java certificate store, and removes all the unapproved certificates.

Convert the Virtual Machine to a Golden Template

Perform this procedure for the golden-template install option.

Note VMware uses the term *Template*. HCS for Contact Center uses the term *Golden Template* for templates consisting of application and operating systems that are used for HCS for Contact Center.

Before you begin

Ensure that the Windows-based template virtual machine is in the WORKGROUP.

Procedure

Step 1 If the VM is not already powered off, from the **VM** menu, select **Power** > **Shut down the guest**.

Step 2 From the VMware vCenter **Inventory** menu, right-click the virtual machine and choose **Template** > **Convert to Template**.

Configure Avaya PG

This section explains the configuration procedures you must perform for the Avaya PG:

Sequence	Done?	Tasks	Notes
1		Configure Network Cards	Follow the procedure Configure Network Cards.
2		Verify the Machine in Domain	Follow the procedure Verify the Machine in Domain.
3		Configure Unified CCE Encryption Utility	Follow the procedure Configure Unified CCE Encryption Utility.
4		Add Avaya PG from Configuration Manager	Follow the procedure Add Avaya PG, on page 25.
5		Setup Avaya PG	Follow the procedure Setup Avaya PG, on page 26.
6		Configure CTI server	Follow the procedure Configure CTI Server.
7		Configure CTI OS server	Follow the procedure Configure CTI OS Server, on page 27.
8		Configure Avaya ACD	Follow the procedure in *ACD Configuration* and *Unified ICM Software Configuration* sections of *Cisco Unified ICM ACD Supplement for Avaya Communication Manager* https://docs.cisco.com/share/page/site/nextgen-edcs/document-details?nodeRef=workspace://SpacesStore/e9288eff-12af-4b91-b9f7-2c28528860cf.
9		Verify Cisco Diagnostic Framework Portico	Follow the procedure Verify Cisco Diagnostic Framework Portico.
10		Cisco SNMP Setup	Follow the procedure Cisco SNMP Setup.

Add Avaya PG

Complete the following procedure to add an Avaya PG using Unified CCE Configuration Manager.

Procedure

Step 1 Login to Unified CCE Admin Workstation server and navigate to **Start** > **Cisco Unified CCE Tools** > **Administration Tools** > **Configuration Manager**.

Step 2 Choose **Tools** > **Explorer Tools** and open **PG Explorer** in **Configuration Manager** window.

Step 3 Click **Add PG** and enter the following values in **Logical Controller** pane.

a) Enter *Avaya_PG_XX* , where XX is the Avaya PG number, in the **Peripheral Name** field.
b) Choose **Avaya (Definity)** in the **Client Type** field .

Step 4 Click **Peripheral** and enter the following values in **Peripheral** tab.

a) Choose **None** in the **Default Desk Settings** field.
b) Check **Enable post routing**.

Step 5 Click **Routing Client** tab and enter a name for Routing client.

Step 6 Click **Save** and **Close** .

Setup Avaya PG

Procedure

Step 1 Choose **Start** > **All Programs** > **Cisco Unified CCE Tools** > **Peripheral Gateway Setup**.

Step 2 Click **Add** in the **Instance Components** pane, and choose **Peripheral Gateway**

Step 3 Select the following in the **Peripheral Gateway Properties** dialog box:

a) Check **Production Mode**.
b) Check **Auto Start System Startup**.
c) Check **Duplexed Peripheral Gateway**.
d) Choose an appropriate PG from PG node Properties ID drop-down list.
e) Select the appropriate side (**Side A** or**Side B**) accordingly.
f) Under Client Type pane, add **Avaya (Definity)** to the selected types.
g) Click **Next**.

Add PIM1 (Avaya PIM)

Procedure

Step 1 Enter the logical controller ID in the **Peripheral Gateway Configuration** pane.

Step 2 Select **EAS-PHD Mode** and check **Using MAPD** check-box in the **Avaya (Definity)ECS Setting** pane.

Step 3 Click **Add**, in the **Peripheral Interface Manager** pane.

Step 4 Select **Avaya(Definity)** and **PIM1**, click **OK**.

Step 5 Check **Enabled** in **Avaya(Definity) ECS PIM Configuration** dialog box.

Step 6 Enter the peripheral name in the **Peripheral Name** field.

Step 7 Enter the peripheral id in the **Peripheral ID** field.

Step 8 Check **CMS Enabled** and enter port number in **Port number to listen on** field, in **Call Management System (CMS) Configuration** pane

Step 9 Check **Host1** as **Enabled** in the **CVLAN/MAPD Configuration** pane.

Step 10 Enter **Hostname** of ASAI link, check configured ASAI link number for **Monitor ASAI** links and **Post-Route ASAI** links

Step 11 Click **OK** and click **Next**.

Step 12 Select the preferred side in the **Device Management Protocol Properties** dialog-box.

Step 13 Click **Next**.

Step 14 Enter the PG Private Interfaces and the PG Public (Visible) Interfaces in the **Peripheral Gateway Network Interfaces** dialog box.

Step 15 Click the QoS button in the private interfaces section for Side A and check the **Enable QoS** check-box and click **OK**.

This step applies only to Side A.

Step 16 Click the QoS button in the public interfaces section for Side A and check the **Enable QoS** check-box and click **OK**.

This step applies only to Side A.

Step 17 Click **Next** and **Finish**.

Note Do not start Unified **ICM/CCNodeManager** until all ICM components are installed.

Configure CTI OS Server

Procedure

Step 1 Mount the CTI OS ISO image or copy the CTI OS installer to the local drive of the Unified CCE machine with an Agent PG..

Step 2 If a maintenance release for CTI OS is available, copy the maintenance release to the local drive .

Step 3 Navigate to **%Home\CTIOS\Installs\CTIOS Server** and run setup.exe. Click **Yes** to the warning that the SNMP service will be stopped and then restarted after the installation completes.

Step 4 Accept the Software License Agreement.

Step 5 Browse to the location for the latest Maintenance Release, if any. Click **Next**.

Step 6 In CTI OS Instance dialog box, click in the CTI OS Instance List pane. In the Add CTI OS Server Instance window, enter your instance name and click **OK**.

Note The CTIOS Instance Name must match with ICM Instance Name, else it will not reflect in the Diagnostics portico.

Step 7 Click **Add** in the CTI OS Server List pane and click **OK**.

Step 8 In the Enter Desktop Drive dialog box, choose drive C and click **OK**.

Step 9 In the CTI Server Information dialog box, enter the IP address of the Unified CCE machines where CTI Server is installed, and enter the ports for Side A (**42027**) and Side B (**43027**).

Step 10 To enable secured connection, click the **Enable Secure Connection** checkbox.

Before establishing secured connection between the components, ensure that the security certificate management process is completed. For more information on secured connections, see *Security Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

Step 11 Click **Next**.

Step 12 In the Peripheral Identifier dialog box, enter the following values and Click **Next** .

a) Enter the peripheral ID of respective PG.
b) Select the peripheral type as **G3** for Avaya PG.
c) Choose **Agent ID** .

Step 13 In the Connect Information dialog box, enter Listen Port `42028` and accept all defaults and then click **Next**.

Step 14 In the Statistics Information dialog box, check **Polling for Agent Statistics at End Call** and then click **Next**.

Step 15 In the IPCC Silent Monitor Type dialog box, set Silent Monitor Type to **CCM Based** and click **Next**.

Step 16 In the Peer CTI OS Server dialog box, configure as follows:

a) Check **Duplex CTIOS Install**.
b) In the Peer CTI OS Server field, set the *hostname/IP address of the other CTIOS Server* in the duplex configuration.
c) In the Port field, enter **42028.**

Step 17 Click **Finish**.

Step 18 In the Cisco CTI OS Server Security dialog box, uncheck **Enable Security**. Click **OK**.

Step 19 In the CTI OS Security dialog box, click **Finish**.

Step 20 When prompted to restart the computer, click **Yes**. If there is a Maintenance Release, its installation begins automatically.

Step 21 Follow all prompts to install the Maintenance Release, if there is one.

Step 22 When the Maintenance Release install completes, click **Finish** and follow the prompts to restart.

Step 23 Access Registry Editor (**Run** > **regedit**).

Step 24 Navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems,Inc.\Ctios\CTIOS_<instance name>\CTIOS1\Server\Agent**.

Step 25 Set **forceLogoutOnSessionClose** to **1**.

Translation Route for Avaya

A translation route is a temporary destination for a call that allows call information to be delivered with the call. Network Blind Transfer is used to return the destination label to the originating CVP routing client.

Configure Unified CCE

- Enable Network Transfer Preferred, on page 29
- Create Service, on page 29

- Configure Translation Route, on page 29
- Configure Script, on page 30

Enable Network Transfer Preferred

Perform the following steps for Avaya, CVP, and CUCM PIMs:

Procedure

Step 1 In Unified CCE Admin Workstation Server, navigate to **Start** > **Cisco Unified CCE Tools** > **Administration Tools** > **Configuration Manager**

Step 2 Select **Tools** > **Explorer Tools** > **PG Explorer**.

Step 3 Select appropriate PG from the list and expand the PG.

Step 4 Select appropriate PIM from the list.

Step 5 Goto **Routing Client** tab, check the **Network Transfer Preferred** check box.

Create Service

Procedure

Step 1 Log in to Unified CCDM portal as a tenant or sub customer.

Step 2 Select **Resource Manager**.

Step 3 Select the folder from the left hand side panel that you want to create service.

Step 4 Select **Service** from **Resource** drop-down list.

Step 5 Enter **Name**.

Step 6 Select appropriate Avaya peripheral from **Peripheral** drop-down list.

Step 7 Select **Advanced** tab, choose **Cisco_Voice** from **Media Routing Domain** drop-down list.

Step 8 Click **Save**.

Configure Translation Route

Procedure

Step 1 In Unified CCE Admin Workstation Server, navigate to **Start** > **Cisco Unified CCE Tools** > **Administration Tools** > **Configuration Manager**.

Step 2 Select **Tools** > **Explorer Tools** > **Translation Route Explorer**.

Step 3 In the **Translation Route** tab:

a) Enter **Name**.
b) From the **Type** drop-down list, select **DNIS**.

Step 4 Click **Add Route**.

Step 5 In the **Route** tab:

a) Enter **Name**.
b) From the **Service** drop-down list, select newly created service.

Step 6 Click **Add Peripheral Target**.

Step 7 In the **Peripheral Target** tab:

a) Enter **DNIS**.

> **Note** DNIS should be same as label.

b) Select **Network Trunk Group** from the drop-down list.

Step 8 Click **Add Label**.

Step 9 In the **Label** tab:

a) Select **Routing Client** from the drop-down list.
b) Enter the **Label**.

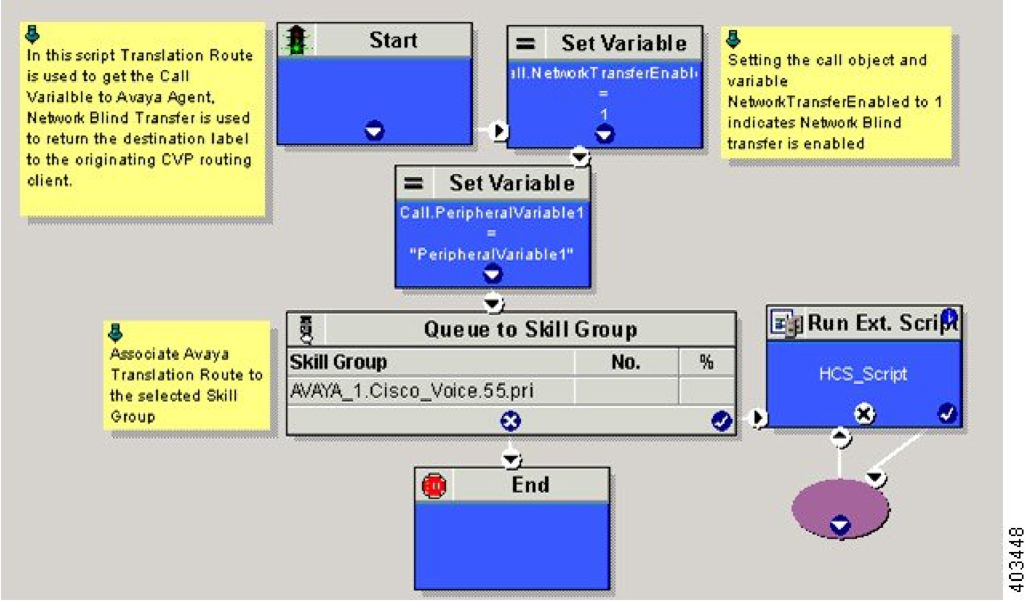
> **Note** Post route VDN should be created as label for the CVP routing client.

Step 10 Click **Save**.

Configure Script

Following illustration explains to configure scripts.

Figure 1: Configure Scripts



In this script Translation Route is used to get the Call Varialble to Avaya Agent, Network Blind Transfer is used to return the destination label to the originating CVP routing client.

Setting the call object and variable NetworkTransferEnabled to 1 indicates Network Blind transfer is enabled

Associate Avaya Translation Route to the selected Skill Group

ıll.NetworkTransferEnabl
=
1

Call.PeripheralVariable1
=
"PeripheralVariable1"

Skill Group	No.	%
AVAYA_1.Cisco_Voice.55.pri		

Cisco Virtualized Voice Browser

Create Golden Template for Cisco Virtualized Voice Browser

Follow this sequence of tasks to create the golden template for Voice Browser. After each task, return to this page to mark the task "done" and continue the sequence:

Sequence	Done?	Tasks	Notes
1		Download `VVB_12.5_vmv13_v2.5.ova`	See Download OVA Files, on page 22.
2		Create the virtual machine for Cisco Virtualized Voice Browser.	Follow the procedure Create Virtual Machines, on page 22.
3		Install Cisco Virtualized Voice Browser.	Follow the procedure for installing VOS applications for golden templates. See Install Voice OS-Based Applications, on page 31.
4		Convert the virtual machine to a Golden Template.	Follow the procedure Convert the Virtual Machine to a Golden Template, on page 24.

After you create all golden templates:

Procedure

Step 1 Run the automation process. See Automated Cloning and OS Customization.

Step 2 Configure Cisco Virtualized Voice Browser. See Configure Cisco Virtualized Voice Browser, on page 33.

Install Voice OS-Based Applications

Use the following procedures to install Voice OS-basedapplications:

- Cisco Virtualized Voice Browser
- Cloud Connect

Procedure

Step 1 Mount the ISO file to the virtual machine and switch on.

Step 2 Follow the Install wizard:

a) On the **Disk found** page, click **OK** to check the media before installation.
b) Click **OK**.
c) On the **Product Deployment Selection** page, select the required product and click **OK**.
d) On the **Proceed with Install** page, click **Yes**.
e) On the **Platform Installation Wizard** page, select the **Skip** option.

   After installation, displays the **Pre-existing Configuration Information** page.

f) Press `Ctrl+Alt` to free your cursor.

Step 3 Shut down the virtual machine.

Step 4 Unmount the ISO image.

Configure Unified CVP

- Add Cisco Virtualized Voice Browser, on page 32
- Associate Dialed Number Pattern, on page 33

Add Cisco Virtualized Voice Browser

Procedure

Step 1 Login CVP operation console.

Step 2 Navigate to **Device Management** > **Gateway** > **Virtualized Voice Browser**.

Step 3 Enter **IP Address** and **Hostname** of Cisco Virtualized Voice Browser.

Step 4 Keep the default trunk option in **Group ID** field.

Step 5 Enter **Username** and **Password**.

Step 6 Enter **Enable Password**.

Step 7 Keep default option in **Port** field.

Step 8 Click **Sign in**.

Step 9 Click **Save**.

Associate Dialed Number Pattern

Procedure

Step 1 Login CVP Operation Console.

Step 2 Select **System** > **Dialed Number Pattern**.

Step 3 Select the **Dialed Number Pattern** from the list that you want to associate.

Step 4 From the **Route to Device** drop-down list, select Cisco Virtualized Voice Browser IP.

Step 5 Click **Save**.

Step 6 Click **Deploy**.

Configure Cisco Virtualized Voice Browser

Access Virtualized VB Administration Web Interface

The web pages of the Virtualized VB Administration web interface allow you to configure and manage the Virtualized VB system and its subsystems.

Use the following procedure to navigate to the server and log in to Vitualized VB Administration web interface.

Procedure

Step 1 Open the Cisco Virtualized Voice Browser Administration Authentication page from a web browser and enter the following case-sensitive URL:*https://<servername>/appadmin*

In this example, replace <*servername*> with the hostname or IP address of the required Virtualized VB server.

Displays Security Alert dialog box.

Step 2 Login **Cisco Virtualized VB Administration** using your credentials.

Note

- If you are accessing Virtualized VB for the first time, enter the Application User credentials that you specified during installation of the Virtualized VB.
- For security purposes, Cisco Virtualized VB Administration logs out after 30 minutes of inactivity.
- Virtalized VB Administration detects web-based cross-site request forgery attacks and rejects malicious client requests. It displays the error message, “The attempted action is not allowed because it violates security policies.”

Step 3 Import the license file and click **Next** to configure.
Displays **Component Activation** page.

Step 4 After all the components status shows **Activated**, click **Next**.
Displays **System Parameters Configuration** page.

Step 5 Choose **codec** from the drop-down list and click **Next**.
Displays **Language Confirmation** page.

Step 6 Choose **Language** from the drop down list and appropriate options.

Step 7 Click **Next**.

Access Virtualized VB Serviceability Web Page

The Vitrualized VB Serviceability is used to view alarm and trace definitions for Virtualized VB services; start and stop the Virtualized VB Engine; monitor Virtualized VB Engine activity and to activate and deactivate services. After you log in to Cisco Virtualized VB Administration web page, you can access Virtualized VB Serviceability:

- From Navigation drop-down list, or
- From Web Browser, enter: *https://<server name or IP address>/uccxservice/*.

Add a SIP Trigger

Follow the below steps to add a SIP trigger:

Procedure

Step 1 Log in to **Cisco Virtualized Voice Browser Administration** page.

Step 2 Select **Subsystems** > **SIP Telephony** > **SIP Triggers**.

Step 3 Click **Add New**.

Step 4 In **Directory Information** tab, enter **Directory Number**.

Step 5 Select **Language** from the drop-down list.

Step 6 Select **Application Name** from the drop-down list.

Step 7 Optional, click **Show More** to associate the trigger for ASR.

Step 8 In **Override Media Termination** field, select **Yes** option.

Step 9 Move required dialog groups between **Select Dialog Groups** and **Available Dialog Groups**.

Step 10 Click **Add** or **Update** to save the changes.

Configure Agent Greeting

- Configure Unified CVP
- Configure Unified CCE, on page 19

Configure Whisper Announcement

Procedure

Step 1 Sign-in to Cisco Virtualized Voice Browser Administration page.

Step 2 Select **Application** > **Application Management**.

Step 3 Ensure that the **ringtone** application is listed and associated with the trigger `919191*`.

What to do next

- Configure Unified CVP
- Configure Unified CCE, on page 19

Configure ASR and TTS

Cisco Virtualized Voice Browser supports ASR and TTS through two subsystems. Follow the procedure to configure ASR and TTS subsystems:

- Configure ASR Subsystem, on page 35
- Configure TTS Subsystem, on page 36

Configure ASR Subsystem

ASR subsystem allows user to choose options through IVR:

Procedure

Step 1 Log in to **Cisco Virtualized Voice Browser Administration** page.

Step 2 Select **Subsystems** > **Speech Servers** > **ASR Servers**

Step 3 Click **Add New**.

Step 4 In **Server Name** field, enter hostname or IP address.

Step 5 Enter **Port Number**.

Step 6 Select **Locales** from the drop-down list and click **Add Language**.

Step 7 Check **Enabled Languages** check-box.

Step 8 Click **Add**.

Configure TTS Subsystem

TTS subsystem converts plain-text (UNICODE) into IVR.

Procedure

Step 1 Log in to **Cisco Virtualized Voice Browser Administration** page.

Step 2 Select **Subsystems** > **Speech Servers** > **TTS Servers**

Step 3 Click **Add New**.

Step 4 In **Server Name** field, enter hostname or IP address.

Step 5 Enter **Port Number**.

Step 6 Select **Locales** from the drop-down list and click **Add Language**.

Step 7 Check **Enabled Languages** check-box.

Step 8 Select **Gender** from the below options:

- Male
- Female
- Neutral

Note Select at least one gender for each enabled language.

Step 9 Click **Add**.

Note Click **Update** to modify the existing configuration.

Configure Courtesy Callback for Cisco VVB

Procedure

Step 1 Log in to **Cisco Virtualized Voice Browser Administration** page.

Step 2 Select **Application** > **Application Management**.

Step 3 Select **Comprehensive** from the list.

Step 4 Ensure **Comprehensive** application is associated with the trigger **777777777***

What to do next

Configure courtesy callback for gateway, Unified CVP, and Unified CCE.

Cloud Connect

Create Golden Template for Cloud Connect

Follow this sequence of tasks to create the golden template for Cloud Connect. After each task, return to this page to mark the task "**done**" and continue the sequence:

Sequence	Done?	Tasks	Notes
1		Download `cloudconnect_12.5_VOS_vmv13_v1.0.ova`	See Download OVA Files, on page 22.
2		Create the virtual machine for Cloud Connect.	Follow the procedure Create Virtual Machines, on page 22.
3		Install Cloud Connect.	Follow the procedure Install Voice OS-Based Applications, on page 31.
4		Convert the virtual machine to a Golden Template.	Follow the procedure Convert the Virtual Machine to a Golden Template, on page 24.

After you create all golden templates, run the automation process. For more information, see Automated Cloning and OS Customization.

Initial Configuration for Cloud Connect

Before adding Cloud Connect to the inventory, you will have to install the certificates from both Cloud Connect publisher and subcriber.

For more information, see the section *Certificates for CCE Web Administration* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Procedure

Step 1 In the Unified CCE Administration, navigate to **Overview** > **Infrastructure Settings**, click **Inventory**.

Step 2 In the Inventory page, click **New** to add the new machine to the System Inventory.

Step 3 In the Add Machine dialog box:

a) Select **Cloud Connect Publisher** from the Type list.
b) Enter Hostname or IP Address of the Cloud Connect Publisher Node.
c) Enter Username and Password for your Cloud Connect cluster Administrator.
d) Click **Save**.

Note When you configure Cloud Connect Publisher, its Cloud Connect Subscriber is added to the Inventory automatically.

Edit Cloud Connect Configuration

Procedure

Step 1 In the Unified CCE Administration, navigate to **Overview** > **Infrastructure Settings**, click **Inventory**.

Step 2 Click the Cloud Connector Publisher device to open the Edit window.

Note If you edit the Cloud Connect Publisher, the Cloud Connect Subscriber associated with the publisher is updated automatically. You cannot edit Cloud Connect Subscriber from the Inventory page.

Step 3 Edit the Username and Password for your Cloud Connect cluster Administrator.

Step 4 Click **Save**.

Monitor Server Status Rules

In CCE deployments, the Unified CCE Administration page displays the total number of alerts for machines with validation rules. Click the alert count to view the list of all alerts for each machine. Upon clicking Alerts for the respective machine, you can view the details of the alerts grouped by the following categories:

Server Status Category	Description	Example Rules
Configuration	Rules for installation and configuration of a component. These rules identify problems with mismatched configuration between components, missing services, and incorrectly configured services.	**Cloud Connect:** The status and alerts will appear only if the Cloud Connect is added to the Inventory. **Note** When the machine status is out of sync, every 10mins auto sync will be triggered to synchronize the machine configuration.
Operation	Rules for the runtime status of a component. These rules identify services and processes that cannot be reached, are not running, or are not in the expected state.	

Delete Cloud Connect Configuration

Procedure

Step 1 Navigate to **Unified CCE Administration** > **Infrastructure Settings** > **Inventory**.

Step 2 Hover over the Cloud Connect Publisher device and click the **x** icon.

Step 3 Click **Yes** to confirm the deletion.

Note If you delete the Cloud Connect Publisher, the Cloud Connect Subscriber associated with the publisher is deleted automatically. You cannot delete Cloud Connect Subscriber from the Inventory page.