Configure Core Settings for Device Pools

Device Pools Overview

Device pools provide a common set of configurations for a group of devices. You can assign a device pool to devices such as phones, gateways, trunks and CTI route points. After you create a device pool, you can associate devices so that they inherit the device pool settings, rather than configuring each device individually.

Device pools let you configure devices according to their location, by assigning location-related information such as Date/Time Groups, Regions, and Phone NTP References. You can create as many device pools as you need, typically one per location. However, you can also apply device pools to apply configurations according to a job function (for example, if your company has a call center, you may want to assign call center phones to one device pool and administration office phones to another).

This section covers the steps that are required to set up core settings for device pools, such as:

- Network Time Protocol—Configure Phone NTP References to provide NTP support for SIP devices in the device pool.
- Regions—Manage bandwidth and supported audio codecs for calls to and from certain regions.
- Cisco Unified Communications Manager Groups—Configure call processing redundancy and distributed call processing for your devices.

Network Time Protocol Overview

The Network Time Protocol (NTP) allows network devices such as SIP phones to synchronize their clocks to a network time server or network-capable clock. NTP is critical for ensuring that all network devices have the same time and that the timestamps in audit logs match the network time. Features such as billing and call detail records rely on accurate timestamps across the network. In addition, system administrators need accurate timestamps in audit logs for troubleshooting. This allows them to compare audit logs from different systems and create a reliable timeline and sequence of events for whatever issue they are facing.

During installation, you must set up an NTP server for the Unified Communications Manager publisher node. The subscriber nodes then sync their time from the publisher node.

You can assign up to five NTP servers.

Phone NTP References

- **For SIP Phones**: It is mandatory that you configure Phone NTP References and assign them through the device pool. These references direct the SIP phone to an appropriate NTP server that can provide the network time. If a SIP phone cannot get its date/time from the provisioned "Phone NTP Reference" the phone receives this information when it registers with Unified Communications Manager.
- **For SCCP Phones**: Phone NTP References are not required as SCCP phones obtain their network time from Unified Communications Manager directly through SCCP signaling.

Authenticated NTP

To provide more network security to the NTP portion of your network, you can configure Authenticated NTP. Authenticated NTP is configured on the Cisco Unified Communications Manager publisher node. The subscriber nodes and IM and Presence nodes sync the time from the Unified CM publisher node.

You can choose from the following authentication methods:

- **Authentication through Symmetric Key**: If you choose this option, the devices in your network use a symmetric key to encrypt and authenticate NTP messages. This option is recommended by some vendors, such as RedHat.
- **Authentication through Autokey (PKI-based infrastructure)**: If you choose this option, the devices in your network use the autokey protocol to encrypt and authenticate NTP messages. This method is mandatory for Common Criteria compliance.
- **No Authentication**: If you choose not to configure Authentication through Symmetric Key or Authentication through Autokey methods, NTP messages will not be authenticated.

Regions Overview

Regions provide capacity controls for Unified Communications Manager multi-site deployments where you may need to limit the bandwidth for certain calls. For example, you can use regions to limit the bandwidth for calls that are sent across a WAN link, while maintaining a higher bandwidth for internal calls. You can use regions to limit the bandwidth for audio and video calls by setting the maximum bitrate for intraregional or interregional calls to whatever the region(s) can provide.

Additionally, the system uses regions to set the audio codec priority where you have applications that support specific codecs only. You can configure a prioritized list of supported audio codecs and apply it to calls to and from specific regions.

When you configure the maximum audio bit rate setting in the **Region Configuration** window (or use the service parameter in the **Service Parameter Configuration** window), this setting serves as a filter. When an audio codec is selected for a call, Unified Communications Manager takes the matching codecs from both sides of a call leg, filters out the codecs that exceed the configured maximum audio bit rate, and then picks the preferred codec among the codecs that are remaining in the list.

Unified Communications Manager supports up to 2000 regions.

Supported Audio Codecs

Unified Communications Manager supports video stream encryption and the following audio codecs:

Audio Codec	Description
G.711	The most commonly supported codec, used over the public switched telephone network.
G.722	Wideband codec often used in video conferences. This is always preferred by Unified Communications Manager over G.711, unless G.722 is disabled.
G.722.1	Low complexity wideband codec operating at 24 and 32 kb/s. The audio quality approaches that of G.722 while using, at most, half the bit rate.
G.728	Low bit rate codec that video endpoints support.
G.729	Low bit rate codec with 8 kb/s compression that is supported by Cisco IP Phone 7900, and typically used for calls across a WAN link.
GSM	The global system for mobile communications (GSM) codec. GSM enables the MNET system for GSM wireless handsets to operate with Unified Communications Manager.
L16	Advanced Audio Coding-Low Delay (AAC-LD) is a super-wideband audio codec that provides superior sound quality for voice and music. This codec provides equal or improved sound quality over older codecs, even at lower bit rates.
AAC-LD (mpeg4-generic)	Supported for SIP devices, in particular, Cisco TelePresence systems.
AAC-LD (MP4A-LATM)	Low-overhead MPEG-4 Audio Transport Multiplex (LATM) is a super-wideband audio codec that provides superior sound. Supported for SIP devices including Tandberg and some third-party endpoints. **Note** AAC-LD (mpeg4-generic) and AAC-LD (MPA4-LATM) are not compatible.
Internet Speech Audio Codec (iSAC)	An adaptive wideband audio codec, specially designed to deliver wideband sound quality with low delay in both low and medium bit rate applications.
Internet Low Bit Rate Codec (iLBC)	Provides audio quality between G.711 and G.729 at bit rates of 15.2 and 13.3 kb/s while allowing for graceful speech quality degradation in a lossy network due to independently encoded speech frames. iLBC is supported for SIP, SCCP, H323, and MGCP devices. **Note** H.323 Outbound FastStart does not support the iLBC codec.
Adaptive Multi-Rate (AMR)	The required standard codec for 2.5G/3G wireless networks based on GSM (WDMA, EDGE, GPRS). This codec encodes narrowband (200-3400 Hz) signals at variable bit rates ranging from 4.75 to 12.2 kb/s with toll quality speech starting at 7.4 kb/s. AMR is supported only for SIP devices.

Audio Codec	Description
Adaptive Multi-Rate Wideband (AMR-WB)	Codified as G.722.2, an ITU-T standard speech codec formally known as Wideband, codes speech at about 16 kb/s. This codec is preferred over other narrowband speech codecs such as AMR and G.711 because it provides better speech quality due to a wider speech bandwidth of 50 Hz to 7000 Hz. AMR-WB is supported only for SIP devices.
Opus	Opus codec is an interactive speech and audio codec, specially designed to handle a wide range of interactive audio applications such as voice over IP, video conferencing, in-game chat, and live distributed music performance. This codec scales from narrowband low bit rate to a very high quality bit rate ranging from 6 to 510 kb/s. Opus codec support is enabled by default for all SIP devices. You can reconfigure Opus support via the **Opus Codec Enabled** service parameter (the default setting is **Enabled for All Devices**). You can reconfigure this parameter to disable Opus codec support, or to enable support in non-recording devices only. **Note** Opus has a dependency on the G.722 codec. The **Advertise G.722 Codec** enterprise parameter should also be set to **Enabled** for SIP devices to use Opus.

Cisco Unified CM Groups Overview

A Unified Communications Manager Group is a prioritized list of up to three redundant servers to which devices can register. Each group contains a primary node and up to two backup nodes. The order in which you list the nodes determines their priority with the first node being the primary node, the second being the backup node, and the third being the tertiary node. You can assign a device to a Cisco Unified Communictions Manager Group via the **Device Pool Configuration**.

Unified Communications Manager groups provide two important features for your system:

- Call processing redundancy—When a device registers, it attempts to connect to the primary (first) Unified Communications Manager in the group that is assigned to its device pool. If the primary Unified Communications Manager is not available, the device tries to connect to the first backup node and if that node is unavailable, it tries to connect to the tertiary node. Each device pool has one Unified Communications Manager group that is assigned to it.
- Distributed call processing—You can create multiple device pools and Unified Communications Manager groups to distribute device registrations evenly across multiple Unified Communications Managers.

For most systems, you will assign a single Unified Communications Manager to multiple groups to achieve better load distribution and redundancy.

Call Processing Redundancy

Unified Communications Manager groups provide call preccsing redundancy and recovery:

- Failover—Occurs when the primary Unified Communications Manager in a group fails, and the devices reregister with the backup Unified Communications Manager in that group.

- Fallback—Occurs when a failed primary Unified Communications Manager comes back into service, and the devices in that group reregister with the primary Unified Communications Manager.

Under normal operation, the primary Unified Communications Manager in a group controls call processing for all the registered devices (such as phones and gateways) that are associated with that group.

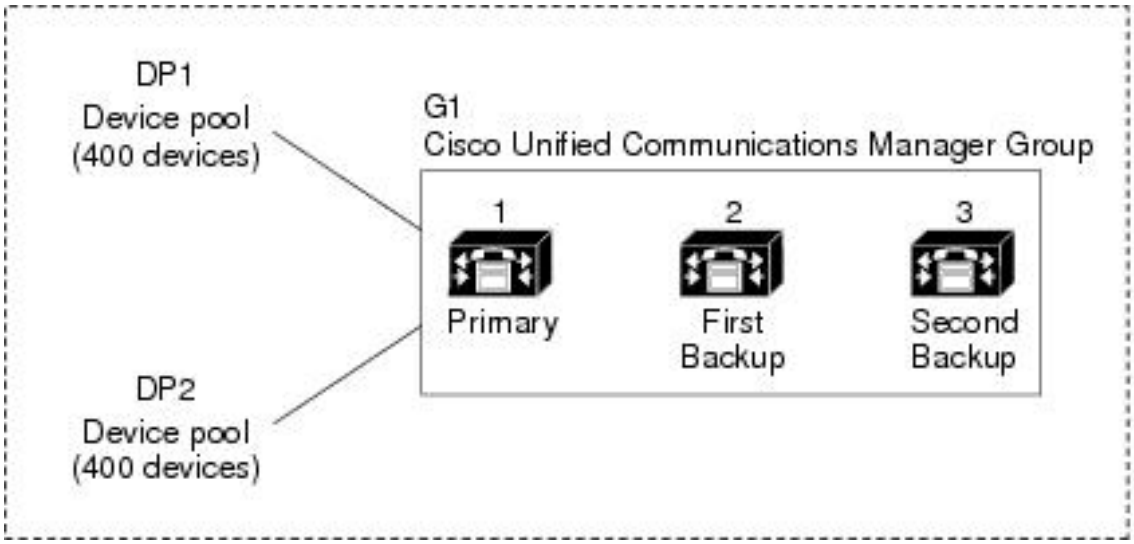
If the primary Unified Communications Manager fails for any reason, the first backup Unified Communications Manager in the group takes control of the devices that were registered with the primary Unified Communications Manager. If you specify a second backup Unified Communications Manager for the group, it takes control of the devices if both the primary and the first backup Unified Communications Managers fail.

When a failed primary Unified Communications Manager comes back into service, it takes control of the group again, and the devices in that group automatically reregister with the primary Unified Communications Manager.

Example

For example, the following figure shows a simple system with three Unified Communications Managers in a single group that is controlling 800 devices.

Figure 1: Unified Communications Manager Group



The figure depicts Unified Communications Manager group G1 that is assigned with two device pools, DP1 and DP2. Unified Communications Manager 1, as the primary Unified Communications Manager in group G1, controls all 800 devices in DP1 and DP2 under normal operation. If Unified Communications Manager 1 fails, control of all 800 devices transfers to Unified Communications Manager 2. If Unified Communications Manager 2 also fails, control of all 800 devices transfers to Unified Communications Manager 3.

The configuration provides call-processing redundancy, but it does not distribute the call-processing load very well among the three Unified Communications Managers in the example. Refer to the following topic for information on how to use Unified Communications Manager groups and device pools to provide distributed call processing within the cluster.

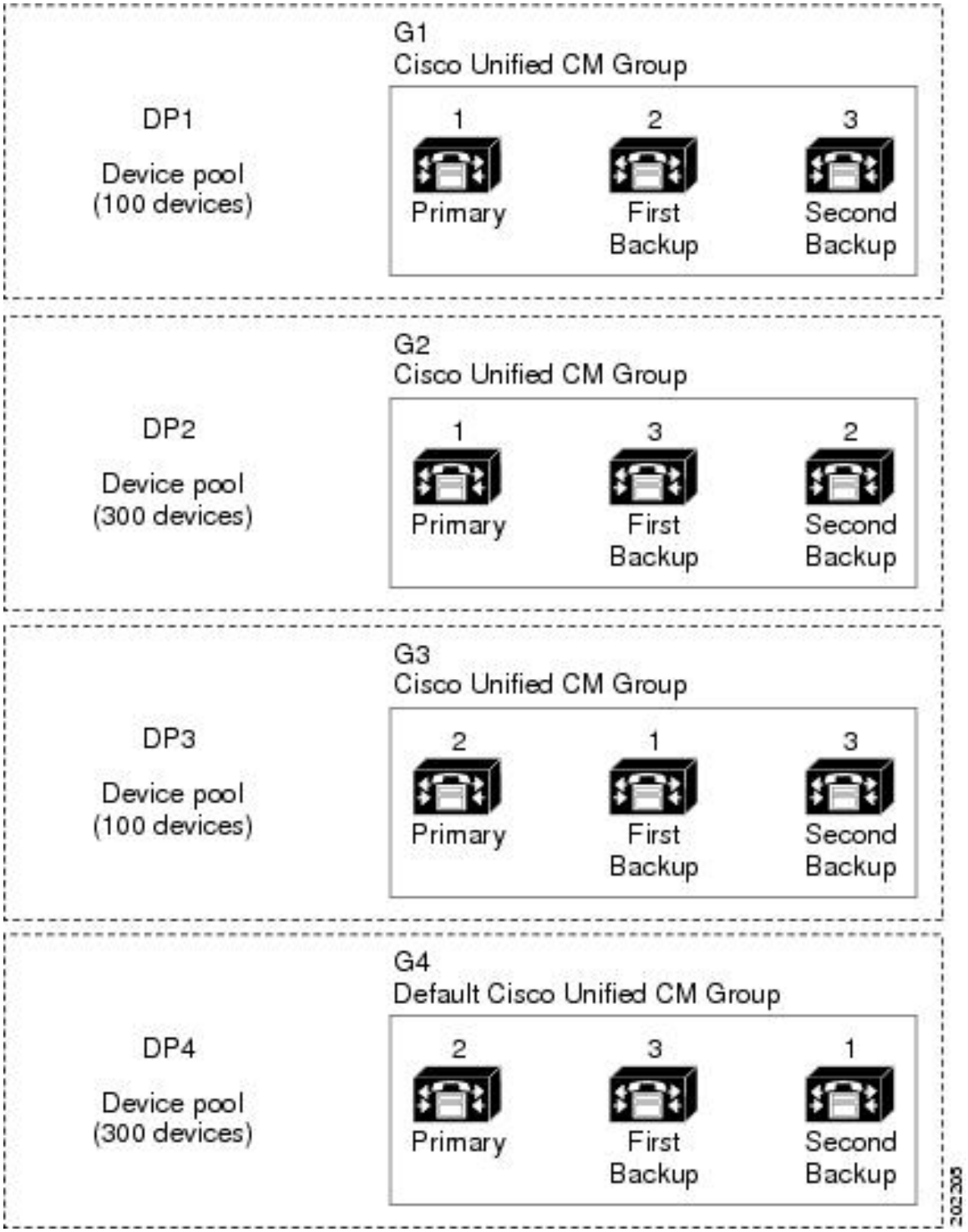
Note Empty Unified Communications Manager groups will not function.

Distributed Call Processing

Unified Communications Manager groups provide both call-processing redundancy and distributed call processing. How you distribute devices, device pools, and Unified Communications Managers among the groups determines the level of redundancy and load balancing in your system.

In most cases, you would want to distribute the devices in a way that prevents the other Unified Communications Managers from becoming overloaded if one Unified Communications Manager in the group fails. The following figure shows one possible way to configure the Unified Communications Manager groups and device pools to achieve both distributed call processing and redundancy for a system of three Unified Communications Managers and 800 devices.

Figure 2: Redundancy Combined with Distributed Call Processing



The previous figure depicts the Unified Communications Manager groups as they are configured and assigned to device pools, so Unified Communications Manager 1 serves as the primary controller in two groups, G1 and G2. If Unified Communications Manager 1 fails, the 100 devices in device pool DP1 reregister with

Unified Communications Manager 2, and the 300 devices in DP2 reregister with Unified Communications Manager 3. Similarly, Unified Communications Manager 2 serves as the primary controller of groups G3 and G4. If Unified Communications Manager 2 fails, the 100 devices in DP3 reregister with Unified Communications Manager 1, and the 300 devices in DP4 reregister with Unified Communications Manager 3. If Unified Communications Manager 1 and Unified Communications Manager 2 both fail, all devices reregister with Unified Communications Manager 3.

Device Pool Prerequisites

Make sure to properly plan out your device pools before you configure them. When configuring device pools and redundant Unified Communications Manager Groups, you will want to provide server redundancy for phones while distributing registrations evenly across your cluster. For additional information that you can use to plan your system, refer to the *Cisco Collaboration System Solution Reference Network Design* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html.

To ensure that Unified Communications Manager includes the latest time zone information, you can install a Cisco Options Package (COP) file that updates the time zone information after you install Unified Communications Manager. After major time zone change events, we will contact you to let you know that you can download the latest COP file at https://software.cisco.com/download/navigator.html.

Change the settings for CMLocal to your local date and time.

Additional Device Pool Configurations

This chapter focuses on core settings such as phone NTP references, regions and call processing redundancy via Unified Communications Manager Groups. However, you can also apply these optional features and components to devices via the device pool configuration:

- Media Resources—Assign media resources such as conference bridges, and music on hold to the devices in your device pool. For more information, see *Media Resources Configuration Task Flow* section of this book.
- Survivable Remote Site Telephony (SRST)—If your deployment uses WAN connections, configure SRST so that in the event of a WAN outage, IP gateways can provide limited call support. For more information, see *Survivable Remote Site Telephony Configuration Task Flow* section in this book.
- Call Routing Information—For information on how to route calls between clusters, see *Call RoutingConfiguration Task Flow* section in this book.
- Device Mobility—Configure Device Mobility groups to allow devices to assume the settings based on their physical location. For more information, see the "Configure Device Mobility" chapter in the *Feature Configuration Guide for Cisco Unified Communications Manager*.

Core Settings for Device Pools Configuration Task Flow

Complete these tasks to set up device pools and apply settings such as Regions, Phone NTP references, and redundancy for the devices that use those device pools.

Procedure

	Command or Action	Purpose
Step 1	Configure the Network Time Protocol, on page 9	Complete the tasks in this task flow to set up NTP on your system. Configure Phone NTP references and apply them to a Date/Time Group that you can assign to a device pool.
Step 2	Configure Region Relationships, on page 15	Complete these tasks to set up Regions for your system. You can create up to 2000 regions and configure customized settings, such as customized audio codec preferences and bitrate restrictions based on what the region can provide.
Step 3	Configure Cisco Unified CM Groups, on page 15	Configure Unified Communications Manager groups for call processing redundancy and load balancing.
Step 4	Configure Device Pools, on page 16	Set up device pools for your system devices. Apply the other core settings that you configured to the device pools in order to apply those settings to the devices that use this device pool.

Configure the Network Time Protocol

Complete these tasks to configure the Network Time Protocol (NTP) for your system. Configure Phone NTP References and apply them to a Date/Time Group which you can then apply to a device pool.

Procedure

	Command or Action	Purpose
Step 1	Add an NTP Server, on page 10	Optional. Use this procedure if you need to add an NTP server. You can add up to five NTP servers. **Note** During system installation, you were required to point Unified Communications Manager to an NTP server. You can use this procedure if you want to add additional NTP servers. Otherwise, you can skip this task.
Step 2	Choose one of these methods to authenticate NTP messages: • Configure NTP Authentication via Symmetric Key, on page 10	Optional. For additional security, configure authenticated NTP. You can configure authentication via either a symmetric key or via autokey. The autokey method is required for Common Criteria compliance.

	Command or Action	Purpose
	• Configure NTP Authentication via Autokey, on page 11	
Step 3	Configure Phone NTP References, on page 11	For SIP phones, it's mandatory that you configure phone NTP references and then apply them via a Date/Time Group and Device Pool.
Step 4	Add a Date/Time Group, on page 12	Define time zones for the various devices that are connected to your system and assign the Phone NTP references that you've set up to the appropriate Date/Time Group.

Note For additional information on CLI commands that you can use to troubleshoot and configure NTP such as the `utils ntp*` set of commands, refer to the *Command Line Interface Reference Guide* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Add an NTP Server

Add an NTP Server to Unified Communications Manager.

Note You can also add an NTP Server in the NTP Server Configuration window of the Cisco Unified OS Administration winodw at **Settings** > **NTP Servers**.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 To confirm that the publisher node can reach the NTP server, run the **utils network ping <ip_address>** where the ip_address represents the address of the NTP server.

Step 3 If the server is reachable, run the `utils ntp server add <ip_address>` to add the server.

Step 4 Restart the NTP service with the `utils ntp restart` command.

Configure NTP Authentication via Symmetric Key

Use this procedure to authenticate NTP messages in your network using a symmetric key.

Note Ensure that you enter the SHA1 Key character by character. Currently, the CLI framework doesn't read the pasted value.

Procedure

Step 1 Log in to the Command Line Interface on the Cisco Unified Communications Manager publisher node.

Step 2 Run the `utils ntp auth symmetric-key status` command to verify the status of the current NTP authentication setting.

Step 3 Do either of the following:

- To enable NTP authentication with a symmetric key, run the `utils ntp auth symmetric-key enable` CLI command.
- To disable NTP authentication with a symmetric key, run the `utils ntp auth symmetric-key disable` CLI command.

Step 4 Follow the prompts to enter the key ID and symmetric key of the NTP server.

Configure NTP Authentication via Autokey

Use this procedure if you want to configure NTP authentication via the PKI-based autokey.

Note If NTP authentication with a symmetric key is enabled, you must disable it before enabling authentication with autokey. To disable NTP authentication with a symmetric key, see Configure NTP Authentication via Symmetric Key, on page 10.

Before you begin

Common Criteria mode must be enabled for you to enable NTP authentication via autokey. For details on enabling Common Criteria mode, see the "FIPS Setup" chapter of the *Security Guide for Cisco Unified Communications Manager*.

Procedure

Step 1 Log into the Command Line Interface.

Step 2 Run the `utils ntp auth auto-key status` command to verify the current NTP authentication setting.

Step 3 Do one of the following:

- To enable NTP authentication run the **utils ntp auth auto-key enable** CLI command.
- To disable NTP authentication, run the **utils ntp auth auto-key disable** CLI command.

Step 4 Enter the number for the NTP server for which you want to enable or disable NTP authentication.

Step 5 If you are enabling authentication, enter the IFF client key. Paste the client key for the NTP server.

Configure Phone NTP References

Use this procedure to configure Phone NTP References, which are mandatory for SIP phones. You can assign the NTP references that you create to a device pool via the Date/Time Group. The reference points the SIP

phone to an appropriate NTP server that can provide the network time. For SCCP phones, this configuration is not required.

Note Unified Communications Manager does not support the multicast and anycast modes. If you choose either of these modes, your system defaults to the directed broadcast mode.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Phone NTP Reference**.

Step 2 Click **Add New**.

Step 3 Enter the NTP server's **IPv4 Address** or **IPv6 Address**, depending on which addressing system your phones use.

Note It is mandatory to enter either IPv4 address or IPv6 address to save the Phone NTP References. If you are deploying both IPv4 phones and IPv6 phones, then provide both the IPv4 address and the IPv6 address for the NTP server.

Step 4 In the **Description** field, enter a description for the phone NTP reference.

Step 5 From the **Mode** drop-down list, choose the mode for the phone NTP reference from the following list of options:

- **Unicast**—If you choose this mode, the phone sends an NTP query packet to that particular NTP server.
- **Directed Broadcast**—If you choose this default NTP mode, the phone accesses date/time information from any NTP server but gives the listed NTP servers (1st = primary, 2nd = secondary) priority.

Note Cisco TelePresence and Cisco Spark device types support Unicast mode only.

Step 6 Click **Save**.

What to do next

Assign the Phone NTP Reference(s) to a Date/Time Group. For details, see Add a Date/Time Group, on page 12

Add a Date/Time Group

Configure Date/Time Groups to define time zones in your system. Assign the Phone NTP references that you configured to the appropriate group. After adding a new date/time group to the database, you can assign it to a device pool to configure the date and time information for all devices in that device pool.

You must reset devices to apply any changes that you make.

Tip For a worldwide distribution of Cisco IP Phones, create a date/time group for each time zones.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Date/Time Group**.

Step 2 Click **Add New**.

Step 3 Assign NTP References to this group:

a) Click **Add Phone NTP References**.

b) In the **Find and List Phone NTP References** popup, click **Find** and select the phone NTP reference(s) that you configured in the previous task.

c) Click **Add Selected**.

d) If you added multiple references, use the up and down arrows to changed the prioritized order. The references at the top have the higher priority.

Step 4 Configure the remaining fields in the **Date/Time Group Configuration** window. See the online help for more information about the fields and their configuration options.

Step 5 Click **Save**.

Configure Regions

Complete the following tasks to configure regions for your device pools. Configure relationships between regions to better manage bandwidth. You can use Regions to control the maximum bit rates for certain types of calls (for example, video calls) and to prioritize specific audio codecs.

Procedure

	Command or Action	Purpose
Step 1	Customize Audio Codec Preferences, on page 13	Optional. Use this procedure if you want to customize priorities for your audio codecs. You may want to do this in order to prioritize specific audio codecs ahead of other codecs. Otherwise, you can assign one of the default audio codec lists to your device pools.
Step 2	Configure Clusterwide Defaults for Regions, on page 14	Configure the clusterwide defaults for Regions. All Regions will use these default settings unless you configure otherwise within the Region Configuration.
Step 3	Configure Region Relationships, on page 15	Set up new regions or edit settings for existing regions. Configure relationships for both interregional and intraregional calls.

Customize Audio Codec Preferences

Use this procedure to customize priorities for your audio codecs. Create a new audio codec preferences list by copying settings from an existing list, and then editing the order of priority within your new list.

Note If you don't need to customize audio codec priorities, you can skip this task. When you configure your device pools, you can assign one of the default audio codec preference lists.

Procedure

Step 1 From Cisco Unified CM Administration choose **System** > **Region Information** > **Audio Codec Preference List**.

Step 2 Click **Add New**.

Step 3 From the **Audio Codec Preference Lists** drop-down list box, select one of the existing audio codec preference lists.
The prioritized list of audio codecs displays for the list that you selected.

Step 4 Click **Copy**. The prioritized list of codecs from the copied list is applied to a newly created list.

Step 5 Edit the **Name** for your new audio codec list. For example, `customizedCodecList`.

Step 6 Edit the **Description**.

Step 7 Use the up and down arrows to move codecs in the prioritized order that appears in the **Codecs in List** list box.

Step 8 Click **Save**.

You must apply the new list to a region and then apply that region to a device pool. All devices in the device pool will use this audio codec preference list.

Configure Clusterwide Defaults for Regions

Use this procedure to configure default settings clusterwide for Regions. These settings apply by default to calls to and from all regions unless you configure region relationships for individual regions within the **Region Configuration** window.

Procedure

Step 1 From Cisco Unified CM Administration choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list, select a Unified Communications Manager node.

Step 3 From the **Service** drop-down list, select the **Cisco CallManager** service.
The **Service Parameter Configuration** window displays.

Step 4 Under **Clusterwide Parameters (System - Location and Region)**, configure any new service parameter settings that you want. For service parameter descriptions, click any of the parameter names to view the help description.

Step 5 Click **Save**.

Configure Region Relationships

Use this procedure to create Regions and to assign custom settings for calls between specific regions. You can edit settings such as preffered audio codecs and maximum bitrates. For example, if you have a region with lower bandwidth capacities than the rest of the network, you may want to edit the maximum session bit rate for video calls to and from the region. You could reset this value to whatever that region can provide.

Note For enhanced scalability, and to ensure that the system uses fewer resources, we recommend that you use the default values from the **Service Parameters Configuration** window wherever possible.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Region Information** > **Regions**.

Step 2 Do either of the following:

- Click **Find** and select a region.
- Click **Add New** ro create a new region.
- Enter a **Name** for the Region. For example, `NewYork`.
- Click **Save**.

The read-only **Region Relationships** area displays any customized settings that you've set up between the selected region and another region.

Step 3 To modify the settings between this region and another region (or the same region for intraregional calls), edit the settings in the **Modify Relationships to other Regions** area:

a) In the **Regions** area, highlight the other region (for intraregional calls, highlight the same region that you are configuring).
b) Edit the settings in the adjacent fields. For help with the fields and their settings, see the online help.
c) Click **Save**.
The new settings now display as a custom rule in the **Region Relationships** area.

Note If you edit a region relationship within one region there is no need to duplicate that configuration in the other region as the settings will update in the other region automatically. For example, let's say that you open Region 1 in the **Region Configuration** window and configure a custom relationship to Region 2. If you were to then open Region 2, you would see the custom relationship displayed in the **Region Relationships** area

Configure Cisco Unified CM Groups

Use this procedure to set up Unified Communications Manager Groups for call processing redundancy, load balancing and failover for the devices in the device pool.

Tip Set up multiple groups and device pools where the primary server is different in each group so as to provide distributed call processing where device registrations are balanced evenly across the cluster nodes.

Note Do not use the default server group because it is not descriptive and can cause confusion.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Cisco Unified CM Group**.

Step 2 Enter a **Name** for the group.

Note Consider identifying the order of the nodes in the name so that you can easily distinguish the group from others. For example, CUCM_PUB-SUB.

Step 3 Check the **Auto-registration Cisco Unified Communications Manager Group** check box if you want this Unified Communications Manager group to be the default Unified Communications Manager group when auto-registration is enabled.

Step 4 From the **Available Cisco Unified Communications Managers** list, choose the nodes that you want to add to this group, and click the down arrow to select them. You can add up to three servers to a group.
The servers in this group appear in the **Selected Cisco Unified Communications Managers** list box. The top server in the list is the primary server

Step 5 Use the arrows beside the **Selected Cisco Unified Communications Managers** list box to change which servers are the primary, and backup servers.

Step 6 Click **Save**.

Configure Device Pools

Set up device pools for your system devices. Apply the other core settings that you configured to the device pools in order to apply those settings to the devices that use this device pool. You can configure multiple device pools to meet your deployment needs.

Before you begin

If you want to assign an SRST configuration, refer to Survivable Remote Site Telephony Configuration Task Flow.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Device Pool**.

Step 2 Do either of the following:

- Click **Add New** to create a new device pool.
- Click **Find** and select an existing device pool.

Step 3 In the **Device Pool Name** field, enter a name for the device pool.

Step 4 From the **Cisco Unified Communications Manager Group** drop-down, select the group that you set up to handle call processing redundancy and load balancing.

Step 5 From the **Date/Time Group** drop-down, select the group that you set up to handle date, time, and phone NTP references for the devices that use this device pool.

Step 6 From the **Region** drop-down list box, select the region that you want to apply to this device pool.

Step 7 From the **Media Resource Group List** drop-down, select a list that contains the media resources that you want to apply to this device pool.

Step 8 Apply SRST settings for this device pool:

a) From the **SRST Reference** drop-down, assign an SRST reference.

b) Assign a value for the **Connection Monitor Duration** field. This This setting defines the time that the phone monitors its connection to Unified Communications Manager before it unregisterring from SRST and reregisterring to Unified Communications Manager.

Step 9 Complete the remaining fields in the **Device Pool Configuration** window. For help with the fields and their settings, see the online help.

Step 10 Click **Save**.

What to do next

Configure multiple device pools according to your deployment requirements.

Basic Device Pool Configuration Fields

Table 1: Basic Device Pool Configuration Fields

Field	Description
Device Pool Name	Enter the name of the new device pool. You can enter up to 50 characters, which include alphanumeric characters, periods (.), hyphens (-), underscores (_), and blank spaces.
Cisco Unified Communications Manager Group	Choose the Cisco Unified Communications Manager group to assign to devices in this device pool. A Cisco Unified Communications Manager group specifies a prioritized list of up to three Unified Communications Manager nodes. The first node in the list serves as the primary node for that group, and the other members of the group serve as backup nodes for redundancy.
Date/Time Group	Choose the date/time group to assign to devices in this device pool. The date/time group specifies the time zone and the display formats for date and time.
Region	Choose the region to assign to devices in this device pool. The region settings specify voice and video codecs that can be used for communications within a region and between other regions.

Call Preservation

The call preservation feature of Unified Communications Manager ensures that an active call does not get interrupted when a Unified Communications Manager fails or when communication fails between the device and the Unified Communications Manager that set up the call.

Unified Communications Manager supports full call preservation for an extended set of Cisco Unified Communications devices. This support includes call preservation between Cisco Unified IP Phones, Media Gateway Control Protocol (MGCP) gateways that support Foreign Exchange Office (FXO) (non-loop-start trunks) and Foreign Exchange Station (FXS) interfaces, and, to a lesser extent, conference bridge, MTP, and transcoding resource devices.

Enable H.323 call preservation by setting the advanced service parameter, Allow Peer to Preserve H.323 Calls, to True.

The following devices and applications support call preservation. If both parties connect through one of the following devices, Unified Communications Manager maintains call preservation:

- Cisco Unified IP Phones
- SIP trunks
- Software conference bridge
- Software MTP
- Hardware conference bridge (Cisco Catalyst 6000 8 Port Voice E1/T1 and Services Module, Cisco Catalyst 4000 Access Gateway Module)
- Transcoder (Cisco Catalyst 6000 8 Port Voice E1/T1 and Services Module, Cisco Catalyst 4000 Access Gateway Module)
- Non-IOS MGCP gateways (Catalyst 6000 24 Port FXS Analog Interface Module, Cisco DT24+, Cisco DE30+, Cisco VG200)
- Cisco IOS H.323 gateways (such as Cisco 2800 series, Cisco 3800 series)
- Cisco IOS MGCP Gateways (Cisco VG200, Catalyst 4000 Access Gateway Module, Cisco 2620, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 3810)
- Cisco VG248 Analog Phone Gateway

The following devices and applications do not support call preservation:

- Annunciator
- H.323 endpoints such as NetMeeting or third-party H.323 endpoints
- CTI applications
- TAPI applications
- JTAPI applications

Call Preservation Scenarios

The below table describes how call preservation is handled in various scenarios.

Table 2: Call Preservation Scenarios

Scenario	Call Preservation Handling
Cisco Unified Communications Manager fails.	A Cisco Unified Communications Manager failure causes the call-processing function for all calls that were set up through the failed Cisco Unified Communications Manager to be lost. Cisco Unified Communications Manager maintains affected active calls until the end user hangs up or until the devices can determine that the media connection has been released. Users cannot invoke any call-processing features for calls that are maintained due to this failure.
Communication failure occurs between Cisco Unified Communications Manager and the device.	When communication fails between a device and the Cisco Unified Communications Manager that controls it, the device recognizes the failure and maintains active connections. The Cisco Unified Communications Manager recognizes the communication failure and clears call-processing entities that are associated with calls in the device where communication was lost. The Cisco Unified Communications Manager still maintain control of the surviving devices that are associated with the affected calls. Cisco Unified Communications Manager maintains affected active calls until the end user hangs up or until the devices can determine that the media connection has been released. Users cannot invoke any call-processing features for calls that are maintained due to this failure. **Note** • If there is a failover, when you bring up the Cisco Unified Communications Manager node within the KeepAlive timer, the phone remains registered to the current node although the call is in preservation mode. This is possible as KeepAliver time is active. • Consider a scenario where the peer is a SIP trunk and a call is established between an IP phone and the SIP trunk. If the phone loses communication with the Cisco Unified Communications Manager, then any media change from the trunk side results in 488 (not acceptable media) response with a cause value 38 (network error) in its reason header.
Device failure (Phone, gateway, conference bridge, transcoder, MTP)	When a device fails, the connections that exist through the device stop streaming media. The active Cisco Unified Communications Manager recognizes the device failure and clears call-processing entities that are associated with calls in the failed device. The Cisco Unified Communications Manager maintain control of the surviving devices that are associated with the affected calls. Cisco Unified Communications Manager maintains the active connections (calls) that are associated with the surviving devices until the surviving end users hang up or until the surviving devices can determine that the media connection has been released.