Call Server Configuration

Configure Call Server

Procedure

Step 1 Log in to the Operations Console and click **Device Management** > **Unified CVP Call Server**.

Step 2 Click **Add New**.

Note To use an existing Call Server as a template for configuring a new Call Server, select a Call Server from the list of available Call Servers, click **Use As Template**, and perform Steps 3 to 5.

Step 3 Click the **General** tab, enter the field values, and click **Next**. See General Settings, on page 2.

The Services you select in the **General** tab appear as tabs.

Step 4 Click the following tabs and modify the default values of fields, if required:

a) ICM. See ICM Service Settings, on page 3.
b) SIP. See SIP Service Settings, on page 6.
c) IVR. See IVR Service Settings, on page 19.
d) Device Pool. See Add or Remove Device From Device Pool, on page 22.
e) Infrastructure. See Infrastructure Service Settings, on page 23.

Step 5 Click **Save & Deploy**.

Note Click **Save** to save the changes on the Operations Console and configure the Call Server later.

Related Topics

General Settings, on page 2
ICM Service Settings, on page 3

Call Server Settings

General Settings

To add or edit a Call Server, click the **General** tab and enter or modify the field values, as listed in the following table:

Table 1: Call Server General Tab Configuration Settings

Property	Description	Default Value	Range	Restart Required
General				
IP Address	The IP address of the Call Server.	None	Valid IP address	No
Hostname [1]	The hostname/IP address of the Call Server.	None	A valid DNS name, which includes the uppercase and lowercase letters, the numbers 0 through 9, and a dash	No
Description	The description of the Call Server.	None	0 to 1024 characters	No
Enable Secure Communication with the Ops Console	Select to enable secure communications between the Operations Console and the Call Server. The device is accessed using SSH and files are transferred using HTTPS. **Note** Enable this option after you configure secure communications.	None	Enabled or Disabled	Yes
Device Version	Lists the Release and Build Number for this device.	Read-only	Read-only	No
Turn On Services				

Property	Description	Default Value	Range	Restart Required
ICM	Enables a Call Server to communicate with an ICM Server. **Note** You must configure an ICM Server before the Call Server can communicate with it.	None	Not applicable	Yes
IVR	The IVR Service creates VXML pages that implement the micro-applications, based on run script instructions received from the ICM Server. The VXML pages are sent to the VXML Gateway to be run.	None	Not applicable	Yes
SIP	Session Initiation Protocol (SIP), RFC 3261, is the primary call control protocol in Unified CVP. The SIP Service uses SIP to communicate with other Unified CVP solution components, such as the SIP Proxy Server, the VXML and Ingress Gateways, and Cisco Unified Communications Manager SIP trunks, and SIP phones. **Note** If you are adding a new Call Server or editing a Call Server and you are using the Call Director or Comprehensive call flow model, configure the SIP service.	None	Not applicable	Yes

[1] If secure communication is being used, ensure that the hostname/IP address specified in the hostname field must match the CN or SAN field value of the TLS certificate being used; or an equivalent mapping of the same exists in DNS or local hosts file. Usage of FQDN (Fully Qualified Domain Name) is also recommended for the same purpose.

ICM Service Settings

Restart the Call Server if you configure the ICM Service on a Call Server for the first time. To configure ICM service settings on a Call Server, on the **ICM** tab, enter or modify the field values, as listed in the following table:

Table 2: ICM Service Configuration Settings

Property	Description	Default Value	Range	Restart Required
General Configuration				
VRU Connection Port	The Port Number on which the Intelligent Call Management (ICM) Service listens for a TCP connection from the ICM PIM.	5000	Any valid TCP/IP connection port	Yes
Maximum Length of DNIS	The maximum length of an incoming Dialed Number Identification Service (DNIS). DNIS is a phone service that identifies the number a caller dialed. Your network dial plan has the information for the maximum length of DNIS. The number of DNIS digits from the PSTN must be less than or equal to the maximum length of DNIS field. For example, if the Gateway dial pattern is 1800******, the value of **Maximum Length of DNIS** field should be 10. **Note** If you are using the Correlation ID method in your ICM script to transfer calls to Unified CVP, the maximum length of DNIS should be the length of the label that is returned from ICM for the VRU leg of the call. When ICM transfers the call, the Correlation ID is appended to the label. Unified CVP then separates the two, assuming that any digits greater than maximum length of DNIS are the Correlation ID. The Correlation ID and label are then passed to ICM.	10	Integer. Valid input for this field is 1 to 99999 characters.	No
Translation Routed DNIS Pool				

Property	Description	Default Value	Range	Restart Required
Add	Enter a single DNIS number for translation routed calls. Validations for DNIS field are: • The DNIS must be a positive integer and can begin with a zero. • The first and the last values for the DNIS range must be of the same length. • You cannot add a DNIS or DNIS range that already exists or overlaps with DNIS or is in the range of a DNIS.	None	Integer up to 32 characters	No
Add a Range	This range is a list of DNIS numbers used for translation of routed calls. Click **Add a Range** and enter the first and the last DNIS numbers in the range in the **to** field. Click **Add DNIS** to add the entered DNIS or DNIS range to the list of Configured DNIS numbers. Select a DNIS or DNIS range in the Configured DNIS box and click **Delete DNIS** to remove it from the list of Configured DNIS numbers. The first and the last values for the DNIS range must be of the same length.	None	Integer up to 32 characters	No
Advanced Configuration				
New Call Service ID	Enter a value that identifies calls to be presented to ICM software as a new call. New Call Service ID calls result in a NEW CALL message being sent to ICM software and the call being treated as a new call, even if it had been prerouted by ICM software.	1	Integer	Yes
Pre-routed Service ID	Enter a value that identifies calls prerouted with either a translation route or correlation ID. Pre-routed Service ID calls result in a REQUEST_INSTRUCTION message being sent to ICM software, which continues to run the script for the call.	2	Integer	Yes
New Call Trunk Group ID	Calls presented to ICM as new calls are sent with New Trunk Group ID as part of the NEW_CALL message to ICM.	100	Integer	Yes

Property	Description	Default Value	Range	Restart Required
Pre-routed Call Trunk Group ID	Calls pre-routed with a Translation Route or correlation ID are sent with Pre-routed Trunk Group ID as part of the REQUEST_INSTRUCTION message to ICM.	200	Integer	Yes
Trunk Utilization				
Enable Gateway Trunk Reporting	Check this check box to enable gateway trunk reporting. **Note** While adding or editing a gateway, you can use the optional field, **Trunk Group ID** to customize the trunk group ID for each gateway.	None	Not applicable	No
Maximum Gateway Ports	The value used for setting the maximum number of ports that a gateway supports in a CVP deployment. This value is be used to calculate the number of ports to report to the Unified ICM Server for each gateway.	700	1 to 1500	Yes
Available	The list of gateways available for trunk reporting.	None	Not applicable	No
Selected	The list of gateways selected for trunk reporting.	All Gateways Selected	Not applicable	No

SIP Service Settings

Restart the Call Server if you configure SIP service settings for the first time. To configure SIP service settings on a Call Server, on the **SIP** tab, enter or modify the field values, as listed in the following table:

Table 3: SIP Service Configuration Settings

Property	Description	Default	Range	Restart Required
Configuration				
Enable Outbound Proxy	If you want to use a Cisco Unified SIP Proxy Server, in the **Enable outbound proxy** field, select **Yes**. Else, select **No**.	No	Yes or No	Yes

Property	Description	Default	Range	Restart Required
Enable Outbound Proxy	If you want to use a Cisco Unified SIP Proxy Server, in the **Enable outbound proxy** field, select **Yes**. Else, select **No**.	Yes	Yes or No	Yes
Use DNS SRV type query	If you want to use DNS SRV for outbound proxy lookup, select **Yes** in the **Use DNS SRV type query** field. Else, select **No**. **Note** If you enable **Resolve SRV records locally**, select **Yes** to ensure that the feature works properly.	Yes	Yes or No	Yes
Resolve SRV records locally	Check the **Resolve SRV records locally** check box to resolve the SRV domain name with a local configuration file instead of a DNS Server.	Enabled	Yes or No	Yes
Outbound proxy Host	If you selected **Enable Outbound Proxy**, from the **Outbound proxy Host** drop-down list, select an Outbound Proxy Server. **Note** An Outbound Proxy Server is a the SIP Proxy Server that is added to the Operations Console.	No	Valid IP address	Yes

Property	Description	Default	Range	Restart Required
Outbound SRV domain name/Server group name (FQDN)	If you use a hostname that is an SRV type record instead of a standard DNS type record, in the **Outbound SRV domain name/Server group name (FQDN)** text box, enter a fully qualified domain name that is configured on the DNS server. Else, the field contains an SRV configuration file. **Example:** Outbound calls made from CVP SIP service are addressed to the URL of *sip:<label>@<srvfqdn>*. A server, such as Redundant Proxy Server, can route calls using this configuration.	None	Follows the same validation rules as hostname, which includes uppercase and lowercase letters, the numbers 0 through 9, and a dash. 0 to 256 character length.	Yes
DN on the Gateway to play the ringtone	Enter the dialed number configured on the gateway to play the ringtone, which is dedicated VoIP dial peer.	9191	Any valid label	No
DN on the Gateway to play the error tone	Enter a dial number pattern that you want to be played for an error tone. To find out which DN is configured on the gateway to play the error tone, run the **sh** command on the gateway and look for the dial peer that matches the incoming dialed number.	9292	Any valid label	No
DN on the Gateway to play the whisper announcement	Enter a dial number pattern that you want to be played for whisper announcement.	9191919100 If location ID exists, then append the location ID to the dial number.	Any valid label	No

Property	Description	Default	Range	Restart Required
Override System Dialed Number Pattern Configuration	For upgraded devices, check the **Override System Dialed Number Pattern Configuration** check box. For new devices, keep this field unchecked.	Unchecked	The default state of the override check box differs depending on the device state: • For new devices, override is disabled (unchecked). New Unified CVP Call Server devices will use configured system-level dialed number patterns by default. • For upgraded devices, override is enabled (checked). Upgraded Unified CVP Call Server devices will use device-level dialed number patterns by default.	No
Local Static Routes				

Property	Description	Default	Range	Restart Required
Static routes for local routing without an outbound proxy - Dialed Number (DN)	In the **Dialed Number (DN)** text box, enter a dialed number. The **Static routes for local routing without an outbound proxy - Dialed Number (DN)** field is used to create a Static Proxy Route Configuration Table. Create static routes if you do not use a SIP Proxy Server. Before adding a local static route, enter a value into both the **Dialed Number (DN)** and **IP Address/Hostname/Server Group Name** fields so that the local static route is complete. Click **Add** to create a proxy route using the DN and the IP address or hostname entered in the **IP Address/Hostname/Server Group Name** fields. The newly created proxy route is added to the list of proxy routes displayed in the box below the **Add** button.	None	Dialed number pattern, destination must be format of NNN.NNN.NNN.NNN or a hostname. See Valid Format for Dialed Numbers, on page 18.	No
IP Address/Hostname/ Server Group Name	Enter an IP address, hostname, or server group name.	None	Valid IP address, hostname, or SRV domain name	No
Advanced Configuration				
General				
Outbound proxy port	Enter a value for port on which the SIP service sends requests to the outbound proxy server.	5060	Any available port number. Valid port numbers are integers between 1 and 65535.	Yes
Outgoing transport type	Select a transport type for outgoing SIP requests. Select **TCP** when reliability is important or packet size is an issue. Select **UDP** in the high availability deployments, because the SIP retry counter and retransmission time settings make the change to a second priority DNS SRV destination occur faster.	TCP	TCP and UDP	Yes

Property	Description	Default	Range	Restart Required
Incoming transport type	The type of transport the SIP Service uses to listen for incoming SIP requests.	UDP+TCP	UDP+TCP	Yes
Time to wait for ICM instructions	The maximum number of milliseconds to wait for ICM to send further instructions.	2000	50 to 5000	No
SIP info tone duration	The maximum number of milliseconds for tone durations sent in when sending Dual Tone Multi-Frequency (DTMF) *8 outpulse digits to the gateway.	100 milliseconds	50 to 2000	No
SIP info comma duration	The maximum number of milliseconds to pause for each comma in the label when sending DTMF to the gateway. **Note** SIP info comma duration is a pause between the *8 and the number. For example, four commas imply four times the value.	100 milliseconds	50 to 2000	No

Property	Description	Default	Range	Restart Required
Generic Type Descriptor (GTD) Parameter Forwarding	Enter a value for passing GTD (UUI) data to ICM in a new call.	UUS	48 characters **Note** • You can extract other parameters in the GTD and send them to ICM. Use commas for multiple values, such as UUS, PRN, GCI. • You can extract any parameter contained in the NSS IAM message.	No

Property	Description	Default	Range	Restart Required
Prepend digits	From the **Prepend digits** drop-down list, select the number of digits that are stripped from the beginning of the incoming Dialed Number (DN) before it is submitted to ICM for the scheduled routing script. **Note** • When Unified ICM returns a label, Unified CVP prepends the stripped digits before initiating the transfer. • If you customized the **Prepend Digits** value manually, in the sip.properties files, set this value in Operations Console after upgrading to ensure that your custom value is not overwritten later. Set the Prepend Digits value and then click **Save & Deploy** to ensure the values of both Operations Console and Call Server devices are in sync.	0	0 to 20 digits	No
UDP Retransmission Count	From the **UDP Retransmission Count** drop-down list, select an option to set the UDP retry count for SIP retries.	3	1 to 6	No

Property	Description	Default	Range	Restart Required
Use Error Refer	Check the **Use Error Refer** check box to enable the SIP Use Error Refer property. Else, keep the check box unchecked.	Checked	Checked or unchecked	No
IOS Gateway Options Dynamic Routing	Check the **IOS Gateway Options Dynamic Routing** check box to identify if resource availability indication on a specific route or service basis is required for real-time routing based on trunk utilization data.	Checked	Checked or unchecked	No
IOS Gateway Options Reporting	Check the **IOS Gateway Options Reporting** check box to identify if trunk utilization reporting and resource availability on a router basis is required after the call is completed.	Checked	Checked or unchecked	No
SIP Header Passing (to ICM)				
Header Name	Specify the SIP header name and click **Add** to add it to the list of SIP headers passed to ICM.	None	210 characters	No
Parameter	This field is optional for list addition.	None	210 characters	No
Dialed Number (DN) patterns				

Property	Description	Default	Range	Restart Required
Patterns for sending calls to the originator - Dialed Number (DN)	Creates a SIP Send Back to Originator Lookup Table. Specify the DN patterns to match for sending the call back to the originating gateway for VXML treatment. For the Unified CVP branch model, use this field to automatically route incoming calls to the Call Server from the gateway back to the originating gateway at the branch. This setting overrides sending the call to the outbound proxy or to any locally configured static routes. It is also limited to calls from the IOS gateway SIP "User Agent" because it checks the User Agent header value of the incoming invite to verify this information. If the label returned from ICM for the transfer matches one of the patterns specified in this field, the call is routed to sip:<label>@<host portion of from header of incoming invite>. Three types of DNs work with Send To Originator: VRU label returned from ICM, Agent label returned from ICM, and Ringtone label. Send To Originator does not work for the error message DN because the inbound error message is played by survivability and the postroute error message is a SIP REFER. (Send To Originator does not work for REFER transfers). **Note** For Send To Originator to work properly, the call must be originated by TDM and have survivability configured on the pots dial peer.	None	24 characters. See Valid Format for Dialed Numbers, on page 18.	No

Property	Description	Default	Range	Restart Required
Patterns for RNA timeout on outbound SIP calls - Dialed Number (DN)	Creates a DN pattern outbound invite timeout using the DN and timeout entered above the **Add** button. Click **Add** to add the newly created DN pattern outbound invite timeout to the list displayed in the box below the **Add** button. Click **Remove** to delete the selected DN pattern outbound invite timeout from the list.	None	24 characters. See Valid Format for Dialed Numbers, on page 18.	No
Timeout	The number of seconds the SIP Service waits for transferee to answer the phone or accept the call. If a selected termination (for either a new or transferred call) returns a connection failure or busy status, or if the target rings for a period of time that exceeds the ring-no-answer (RNA) timeout setting of the Call Server, it cancels the transfer request and sends a transfer failure indication to Unified ICM. This scenario causes a router requery operation. The Unified ICM routing script then recovers control and has the opportunity to select a different target or take other remedial action.	60 seconds	5 to 60	No
Custom ringtone patterns - Dialed Number (DN)	Specify a custom DN pattern. Click **Add** to add the newly created DN pattern to the list displayed in the box below the Add button. To know which DN is configured on the gateway to play ringtone, run the **sh** command on the gateway and look for the dial peer that matches the incoming dialed number.	None	24 characters. See Valid Format for Dialed Numbers, on page 18.	No

Property	Description	Default	Range	Restart Required
Ringtone media file name	The filename of the ringtone to be played for the respective dialed number. You must save the ringtone media file to the VXML Gateway.	None	0 to 256 characters without spaces. Provide the URL for the stream name in the following form: rtsp://<streaming server IP address> /<port>/<foldername>/ <filename>.rm	No
Post Call Survey DNIS Mapping				
Incoming Call Dialed Number (DN)	Click **Add** to add the newly created DN pattern to the list displayed in the box below the Add button. Click Remove to delete the selected DN pattern from the list.	None	Dialed Number pattern, destination (must be in the form of NNN.NNN.NNN.NNN or a hostname). See Valid Format for Dialed Numbers, on page 18.	No
Survey Dialed Number (DN)	Click **Add** to add the newly created DN to the list. Click **Remove** to delete the selected DN from the list.	None	Alphanumeric characters	No

Note

- The **Call Max Threshold** property specifies the simultaneous active calls that are allowed on a CVP Server instance. Requests above this value are rejected with a *503 Server Unavailable* status.

  The default value is -1, which disables the check performed by this property. The expected range of values is 0 to the maximum number of concurrent sessions supported on CVP Servers for a given Unified CVP release. For more information, see the Section, *Sizing for Unified CVP* in the *Solution Design Guide for Cisco Unified Contact Center Enterprise* available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-implementation-design-guides-list.html.

  To change or update this property, you must manually edit the *sip.properties* file in `\Cisco\CVP\conf` folder.

  Property: #Calls Max Threshold

  Value: SIP.CallsMaxThreshold= -1

  To use the **Call Max Threshold** property, install the appropriate ES specified against CSCvf87136 in https://www-author3.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/customer_voice_portal/ES_MR/ES/ccvp_b_ccvp-eng-es-spl.html.

- To add CauseCode property in the excluded list for Unreachable Table (for example: 47) in `\Cisco\CVP\conf` folder:

  SIP.System.ExcludedCauseCodeFromUnreachableTable =

Related Topics

Valid Format for Dialed Numbers, on page 18

Ring No Answer Settings with SIP

If you use the Unified CVP Ring No Answer (RNA) settings in SIP, ensure that the RNA value is lower than the Unified ICME Agent Desk Setting RNA timeout. The range of RNA value is from 5 to 60 seconds; the default value is 15 seconds.

Unified CVP makes a call to the ringtone service on the VXML gateway. This call is followed by sending the call to the Unified Communications Manager trunk for the agent. During this period, an agent has sufficient time to receive the delivered event after being reserved, and also ensures that Unified ICME reporting is correct in terms of handled time and RNA call disposition calls reporting.

Valid Format for Dialed Numbers

Valid dialed number patterns are the same as for the ICM label sizes and limitations, including the following:

- Dialed numbers can be up to 24 characters.
- Use the period (.) or the letter X for single-digit wildcard matching in any combination. Avoid using the letter “T” for wildcard matching.

Note Small letter "x" cannot be used as a wildcard.

- Use the greater than (>), asterisk (*), or exclamation (!) character as a wildcard for zero or more digits at the trailing end of a dialing number.
- The highest precedence of pattern matching is an exact match, followed by the most specific wildcard match. When the number of characters is matched equally by more than one wildcard pattern, precedence is given from top to bottom of the configured DN list.

IVR Service Settings

The IVR service creates VXML documents that are used to implement miroapplications based on Run Script instructions received by the ICM. The VXML pages are sent to the VXML Gateway to be run. The IVR Service can also generate external VXML through the microapplications to engage the Unified CVP VXML Server to generate the VXML documents.

The IVR Service plays a significant role in implementing a failover mechanism. This capability is achieved without Automatic Speech Recognition (ASR)/Text To Speech (TTS) Server and VXML Servers. Up to two of each such server are supported, and the IVR Service orchestrates retries and failover between them.

Note Configure the following servers before you configure the IVR service:

- ICM Server
- Media Server
- ASR/TTS Servers
- VXML Server
- Gateway

To configure IVR settings on a Call Server, on the **IVR** tab, enter or modify the field values, as listed in the following table:

Table 4: IVR Service Settings

Property	Description	Default	Range	Restart Required
CVP H.323 Service Configuration				
Heartbeat timeout	Enter the number of seconds after which the heartbeat times out.	120		
IOS Voice Browser Configuration				
Last Access Timeout (seconds)	Enter the number of seconds the IVR Service waits for a call request from a non-Unified CVP Voice Browser before removing that Voice Browser from its current client list. This value must be greater than or equal to the call timeout.	7320	0 to 2147483647	No

Property	Description	Default	Range	Restart Required
Media Server Timeout	Enter the number of seconds the Gateway should wait to connect to the HTTP Media Server before timing out.	4	0 to 2147483647	No
Media Server Retry Attempts	Maximum number of times the non-Unified CVP Voice Browser, such as IOS Voice Browser, or Unified CVP VXML Server attempts to connect to an HTTP Media Server to retrieve a single prompt. If the Voice Browser or Unified CVP VXML Server fails after the specified number of times, it tries the same number of times to retrieve the media from a backup media server before failing and reporting an error. **Note** The backup media server is defined on the gateway as <mediaserver>-backup.	0	0 to 2147483647	No
ASR/TTS Server Retry Attempts	Maximum number of times the Gateway tries to connect to an ASR/TTS server. If the Gateway fails to connect this many attempts, it tries the same number of times to connect to a backup ASR/TTS server before failing and reporting an error. **Note** The backup ASR and TTS servers are defined on the gateway as asr-<locale>-backup and tts-<locale>-backup.	0	0 to 2147483647	No
IVR Service Timeout	The number of seconds the gateway should wait to connect to the IVR Service before being timed out. This setting controls call results only. The initial NEW_CALL timeout from the Gateway to the IVR Service is controlled through the `fetchtimeout` property within the bootstrap VXML in flash memory on the Gateway.	7	0 to 2147483647	No

Property	Description	Default	Range	Restart Required
IVR Service Retry Attempts	Maximum number of times the gateway tries to connect to the IVR Service before failing and reporting an error. This setting controls call results only. The initial NEW_CALL retry count from the Gateway to the IVR Service is controlled from within the bootstrap VXML in flash memory on the Gateway.	0	0 to 2147483647	No
Use Backup ASR/TTS Servers	Click **Yes** if an ASR/TTS Server is unavailable so that the gateway attempts to connect to the backup ASR/TTS server. Else click **No**.	Yes	Yes or No	No
Use Backup Media Servers	Click **Yes** if the Media Server is unavailable so that the gateway attempts to connect to the backup Media Server. Else click **No**.	Yes	Yes or No	No
Use hostnames for default Media/VXML servers	Click **No** to use IP address VXML Server and Media Server. Click **Yes** to use hostnames instead of IP addresses.	No	Yes or No	No
Use Security For Media Fetches	Click **No** to generate HTTP URLs to Media Servers. Click **Yes** to generate HTTPS URLs to Media Servers. **Note** The default option is available for a client using SIP Service and the Media Server is not set to a URL that explicitly specifies an HTTP/ HTTPS scheme.	No	Yes or No	No
Advanced				

Property	Description	Default	Range	Restart Required
Call timeout	The number of seconds the IVR Service waits for a response from the SIP Service before being timed out. Call-timeout should be longer than the longest prompt, transfer, or digit collection at a Voice Browser. On timeout, the call is canceled without affecting other calls. **Note** Having a longer Call-timeout duration is useful even when calls are being stranded, they are not removed from the IVR service until the timeout.	7200	6 seconds or greater	No
ASR/TTS Use the Same MRCP Server	Click this option if your ASR and TTS Servers are on the same computer. **Note** This option helps to minimize the number of MRCP connections on the ASR/TTS Server.	No	Yes or No	No

Device Pool

A device pool is a logical group of devices. It provides a convenient way to define a set of common characteristics that can be assigned to devices, for example, the region in which the devices are located. You can create device pools and assign devices to the device pools you created.

Every device you create is automatically assigned to a default device pool, which you can never remove from the selected device pool list. The Administrator account is also assigned to the default device pool automatically. Having the administrator account ensures that the administrator can view and manage all devices. You cannot remove the Administrator account from the default device pool.

When you create a user account, you can assign the user to one or more device pools, which allows the user to view the devices in those pools from the Control Center. Subsequently, you can remove the user from any associated device pools, which prevents that user from viewing the pool devices in the Control Center. Removing a user from the default device pool prevents the user from viewing all devices.

Add or Remove Device From Device Pool

Procedure

Step 1 From the **Device Management** menu, select a device to add to the Device Pool.

Example:

To add a Call Server to a device pool, select Unified CVP Call Server from the **Device Management** menu.

A window that lists known devices of the type you selected appears. For example, if you select Call Server, all the known Unified CVP Call Servers are listed.

Step 2 Select a device pool from the **Device Pool** list and click **Edit**.

Step 3 On the **Device Pool** tab:

- In the **Available** list box, select one or multiple devices and click the **Add** arrow. The added devices appear in the **Selected** list box.
- To remove the added devices from the **Selected** box, select them and click the **Remove** arrow. The added devices appear in the **Selected** list box.

Step 4 Click **Save & Deploy**.

Note
- Click **Save** to save the changes in Operations Console and add or remove a device from Device Pool later.
- Some edit-device windows have an **Apply** button instead of **Save**. Click **Apply** to copy the configuration to the device.

Infrastructure Service Settings

The Call Server, Unified CVP VXML Server, and Reporting Server offer one or more services. The Call Server provides SIP, IVR, and ICM call services. The Unified CVP VXML Server provides VXML services, and the Reporting Server provides reporting services. Changes to Infrastructure settings affect all services that use threads, publish statistics, send syslog events, or perform logging and tracing. For example, when you change the **syslog** server setting, the changes are applied to all services that write to syslog.

To configure Infrastructure settings, on the **Infrastructure** tab, enter or modify the field values, as listed in the following table:

Table 5: Infrastructure Service Configuration Settings

Property	Description	Default	Range	Restart Required
Configuration: Thread Management				
Maximum Threads	Enter the maximum number of threads allocated in the thread pool that can be shared by all services running as part of a CVP Web Application.	500	100 to 1000	No
Statistics				

Property	Description	Default	Range	Restart Required
Statistics Aggregation Interval	Enter the duration in minutes during which system and service statistics are published to the log file and SNMP events are sent. After the statistics are published, the counters reset and aggregate data for the next interval. Real-time statistics are generated on-demand and have no intervals. Statistics Publishing Interval is used for attributes, such as the number of calls in last interval, the number of transfers in last interval, and the number of HTTP sessions in last interval. **Note** The interval is different than the real time snapshot statistics (for the number of concurrent calls).	30 minutes	10 to 1440 minutes	No
Log File Properties				
Max Log File Size	Enter the maximum size of a log file in megabytes before a new log file is created. **Note** To increase the log file size, go to C:\Cisco\CVP\conf, open log4j.xml file and update the MaxFileSize value as shown: <param name="MaxFileSize" value="**10000000**"/> Save the file and restart Call Server to deploy the changes.	10 MB	1 through 100 MB	No
Max Log Directory Size	Enter the maximum number of megabytes to allocate for disk storage for log files. **Note** Modifying the value to a setting that is below the default value might cause logs to be rolled over quickly. Consequently, log entries might be lost, which can affect troubleshooting.	20,000 MB	500 to 500000 The log folder size divided by the log file size must be less than 5000.	No
Configuration: Primary Syslog Settings				

Property	Description	Default	Range	Restart Required
Primary Syslog Server	Enter a hostname or IP address of Primary Syslog Server to send syslog events from a CVP Application.	None	Valid IP address or hostname.	No
Primary Syslog Server Port Number	Enter a port number of Primary Syslog Server.	None	Any available port number. Valid port numbers are integers between 1 and 65535.	No
Primary Backup Syslog Server	Enter a hostname or IP address of the Primary Backup Syslog Server to send syslog events from a CVP Application when the Syslog Server is not reachable.	None	Valid IP address or host name.	No
Primary Backup Syslog Server Port Number	Enter a port number of Primary Backup Syslog Server.	None	Any available port number. Valid port numbers are integers between 1 and 65535.	No
Configuration: Secondary Syslog Settings				
Secondary Syslog Server	Enter the hostname or IP address of Secondary Syslog Server to send syslog events from a CVP Application.	None	Valid IP address or hostname.	No
Secondary Syslog Server Port Number	Enter port number of Secondary Syslog Server.	None	Any available port number. Valid port numbers are integers between 1 and 65535.	No
Secondary Backup Syslog Server	Enter hostname or IP address of the Secondary Backup Syslog Server to send syslog events from a CVP Application when the Syslog Server is not reachable.	None	Valid IP address or hostname.	No

Property	Description	Default	Range	Restart Required
Secondary Backup Syslog Server Port Number	Enter the port number of Secondary Backup Syslog Server.	None	Any available port number. Valid port numbers are integers between 1 and 65535.	No
License Thresholds				
Critical Threshold	Percentage of licenses in use required to reach Critical licensing state. See License Thresholds, on page 26.	97%	Positive integer less than or equal to 100 and greater than the Warning threshold.	No
Warning Threshold	Percentage of licenses in use required to reach Warning licensing state. See License Thresholds, on page 26.	94%	Positive integer less than the Critical threshold and greater than the Safe threshold.	No
Safe Threshold	Percentage of licenses in use required to reach Safe licensing state. See License Thresholds, on page 26.	90%	Positive integer less than the Warning threshold and greater than 0.	No

Related Topics

License Thresholds, on page 26

License Thresholds

The three thresholds namely safe, warning, and critical describe the percentage of licenses that must be in use to reach their respective licensing state.

Crossing a threshold does not always mean the state changes. For example, if you have 100 licenses and the Safe, Warning, and Critical license thresholds are set to the defaults of 90%, 94%, and 97%, and 89 licenses are in use, licenses are at a Safe level. When the number of licenses in use reaches 94, the license state changes from Safe to Warning level. If one more license is used, the license state remains at the Warning level. If three licenses, which are no longer in use, are released, 92 licenses remain in use and the license state remains at the Warning level. After the licenses in use return to the previous threshold (90), the state changes from Warning to Safe.

IP Address Modification

This section describes how to change the IP address of Call Server, VXML Server, and the Reporting Server. Follow this sequence for changing the IP Address of the devices:

1. Reporting Server
2. VXML Server
3. Call Server
4. OAMP Server

Procedure

Step 1 Select the device from the Operations Console to change the IP address.

Step 2 From the menu bar of the device, select the device and click **Use As Template**.

Step 3 Assign the new IP address to the device and change the Host Name temporarily, which you will revert in Step 8, and click **Save**.

Note Do not click the **Save and Deploy** option until you have changed the physical server to the new IP address.

Step 4 Delete the device from the Operations Console before changing the IP address of the server.

Step 5 Configure the new IP address on the local server.

Step 6 Go to **C:\Cisco\CVP\bin\UpdateRMIServerIP\updatermiserverip.bat** and double-click the batch file to update the IP address in the windows registry and the wrapper.conf file.

Step 7 From the Operations Console, select the device and change the Host Name to the original one. Click **Save and Deploy** for the device. (Restart the server if network-related message is seen).

Step 8 Restart the server.

Note

a. Make sure to change the configuration of VXML Application, Gateway, VVB, ICM PIM, Proxy, and CUCM to reflect the new Call Server IP address.

b. Associate Reporting Server to the Call Server.

c. Delete the existing Media Server and create a new one with the Call Server IP address and deploy the Media Server.

What to do next

Change the IP address of the OAMP Server.

Graceful Shutdown of Call Server or Reporting Server

As a local administrator, you can use the following procedure to gracefully shut down the Call Server or Reporting Server services from the CLI.

Procedure

Step 1 Log in to the CVP Call Server box.

Step 2 Go to the `%CVP_HOME%\bin\ServiceController` folder.

Step 3 Run the `service-controller.bat` file.

Step 4 Enter the administrator credentials, service name, and IP address details at the prompt:

```
CALLSERVER-HOSTNAME: <Hostname or IP Address of the Call Server
CALLSERVER-USERNAME: <Username of the Call Server>
CALLSERVER-PASSWORD:  <Password of the Call Server
SERVICE-NAME: <Name of the service to shutdown gracefully(callserver for Call
Server/reportingserver for Reporting Server)>
REPORTINGSERVER-HOSTNAME: <IP Address of the Reporting Server>
```

Note

- To shut down the Reporting Server gracefully, ensure that the CVP Call Server is up and running.
- To shut down the Reporting Server gracefully, provide the hostname or IP address of the Call Server and the IP address of its associated Reporting Server in the respective entries.
- If you have specified an IP Address instead of a hostname, then ensure that the IP address is in the CN or SAN fields of the SSL certificate of that host.