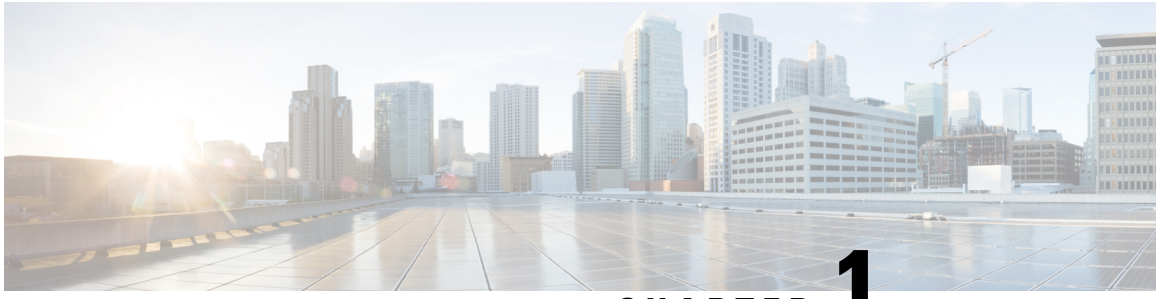
# Cisco Virtualized Voice Browser Administration and Configuration Guide, Release 12.6(1)

**First Published:** 2021-05-14

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

# CONTENTS



CHAPTER 1

# Cisco VVB Introduction

Cisco Virtualized Voice Browser (VVB) is designed to facilitate concurrent multimedia communication processing.

Cisco VVB has the following features:

- Facilitates self-service options such as access to check account information or user-directed call routing by processing user commands through touchtone input or speech-recognition technologies.
- Allows customers to retrieve the required information through voice commands without interacting with an agent, to navigate to the correct department, or to get help from an agent.
- Provides multilingual support for Cisco VVB server prompts for automated speech recognition (ASR) and text-to-speech (TTS) capabilities.
- Provides more comprehensive and effective customer service by efficiently handling call traffic with self-service or fast transfer to the correct agent the first time.



# Cisco VVB Web Interfaces

You can use a web browser to administer Cisco VVB. Cisco VVB provides the following two web interfaces:

- **Cisco VVB Administration**—Use this web interface to configure system parameters, configure subsystems, view real-time reports that include total system activity and application statistics, and so on.
- **Cisco VVBServiceability**—Use this web interface to view alarm and trace definitions for Cisco VVB services, start and stop engine, monitor engine activity, and so on.

**Note**

- If you are using Microsoft Internet Explorer or Mozilla Firefox, ensure that the popup blocker is disabled.
- Multiple Web sessions for same user are not supported.

# Accept Security Certificates

Ensure that the pop-ups are enabled for Cisco VVB Administration.

If you receive a certificate expiry alert, it means that the validity of your CA certificate is about to expire. You can delete the certificate after expiry. If you use any CA to sign your certificates, you must upload the new certificates to ensure your system remains operational. Some CA certificates that are shipped with the platform do not require to be uploaded and can be deleted after expiry. For the complete list of CAs that can be safely deleted after expiry, refer to the *Manage Expired CA Certificates* section in the Cisco Unified Contact Center Express Administration and Operations Guide.

After you enter Cisco VVB Administration URL in your browser, the procedure to add a certificate is as follows:

### Install certificates on Windows operating system:

The procedure to add a certificate varies for each browser. The procedure for each browser is as follows:

**Internet Explorer**

**Note** If you are using a Windows client, signed in as a Windows user, you must run Internet Explorer as an administrator to install the security certificates. In your Start menu, right-click Internet Explorer and select Run as administrator.

Contact your administrator if you do not have the required permissions to install the security certificates.

1. A page appears that states there is a problem with the website's security certificate. Click **Continue to this website (not recommended)** link to open Cisco VVB Administration sign in page. Cisco VVB Administration sign in screen appears with a certificate error in the address bar.
2. Click on the certificate error that appears in the address bar and then click **View Certificates**.
3. In the **Certificate** dialog box, click **Install Certificate** to open the **Certificate Import Wizard**.
4. Select **Current User** to install the certificate for the current user only, or select **Local Machine** to install the certificate for all Windows users.
5. On the **Certificate Import Wizard**, click **Next**.
6. Select **Place all certificates in the following store** and click **Browse**.
7. Select **Trusted Root Certification Authorities** and click **OK**.
8. Click **Next** and then click **Finish**. A **Security Warning** dialog box appears.
9. Click **Yes** to install the certificate. The **Certificate Import** dialog box appears.
10. Click **OK** and close the **Certificate Import** dialog box.
11. Close the browser tab. The accepted certificate link is removed from the **SSL Certificate Not Accepted** dialog box.

Repeat the preceding steps for all the certificate links. After you accept all the certificates, the sign-in process is complete.

**Note** To remove the certificate error from the desktop, you must close and reopen your browser.

**Firefox**

1. On **Your connection is not secure** page, click **Advanced** > **Add Exception**.

   **Note** Ensure that the **Permanently store this exception** box is checked.

2. Click **Confirm Security Exception**.
3. On Cisco VVB Administration sign in page, enter your username and password, and click **Sign In**.
4. In the **SSL Certificate Not Accepted** dialog box, click the certificate link. A browser tab opens for the certificate that you must accept.
5. On the browser tab, click **I Understand the Risks** > **Add Exception**. Ensure that the **Permanently store this exception** box is checked.
6. Click **Confirm Security Exception**. The browser tab closes after you accept the certificate and the accepted certificate link is removed from the **SSL Certificate Not Accepted** dialog box. Close the browser tab if it does not automatically close.

Repeat the preceding steps for all the certificate links. After you accept all the certificates, the sign-in process is complete.

**Chrome and Edge Chromium (Microsoft Edge)**

1. A page appears that states your connection is not private. To open Cisco VVB Administration sign in page,

   In Chrome, click **Advanced** > **Proceed to <Hostname> (unsafe)**.

   In Microsoft Edge, click **Advanced** > **Continue to <Hostname> (unsafe)**.

2. Enter your agent ID or username, password, and extension, and then click **Sign In**.
3. In the **SSL Certificate Not Accepted** dialog box, click the certificate link. A browser tab opens for the certificate that you must accept.
4. On the browser tab,

   In Chrome, click **Advanced** > **Proceed to <Hostname> (unsafe)**.

   In Microsoft Edge, click **Advanced** > **Continue to <Hostname> (unsafe)**.

   The browser tab closes after you accept the certificate and the accepted certificate link is removed from the **SSL Certificate Not Accepted** dialog box. Close the browser tab if it does not automatically close.

   **Note** If you click the certificate link and do not accept it, the certificate link stays enabled in the **SSL Certificate Not Accepted** dialog box. The certificate error appears every time you sign in. The procedure to permanently accept the certificate is as follows.

5. Click on the certificate error that appears in the address bar and then,

   In Chrome, select **Certificate (Invalid)**.

   In Microsoft Edge, select **Certificate (not valid)**.

   The **Certificate** dialog box appears.

6. In the **Details** tab, click **Copy to File**. The **Certificate Export Wizard** appears.
7. Click **Next**.
8. Keep the default selection **DER encoded binary X.509 (.CER)** and click **Next**.
9. Click **Browse** and select the folder in which you want to save the certificate, enter a recognizable file name and click **Save**.
10. Browse to the folder where you have saved the certificate (**.cer** file), right-click on the file, and click **Install Certificate**. The **Certificate Import Wizard** appears.
11. Keep the default selection **Current User** and click **Next**.
12. Select **Place all certificates in the following store** and click **Browse**. The **Select Certificate Store** dialog box appears.
13. Select **Trusted Root Certification Authorities** and click **OK**.
14. Click **Next** and then click **Finish**. A **Security Warning** dialog box appears that asks if you want to install the certificate.
15. Click **Yes**. A **Certificate Import** dialog box that states the import was successful appears.

Close the browser and sign in to Cisco VVB Administration. The security error does not appear in the address bar.

### Install certificates on macOS:

The procedure to download a certificate varies for each browser. The procedure for each browser is as follows:

**Chrome and Edge Chromium (Microsoft Edge)**

1. A warning page appears which states that your connection is not private. To open Cisco VVB Administration sign in page,

   In Chrome, click **Advanced** > **Proceed to <Hostname> (unsafe)**.

   In Microsoft Edge, click **Advanced** > **Continue to <Hostname> (unsafe)**.

2. Click on the certificate error that appears in the address bar and then,

   In Chrome, select **Certificate (Invalid)**.

   In Microsoft Edge, select **Certificate (Not Valid)**.

   A certificate dialog box appears with the certificate details.

3. Drag the **Certificate** icon to the desktop.
4. Double-click the certificate. The **Keychain Access** application opens.
5. In the right pane of Keychains dialog, browse to the certificate, right-click on the certificate, and select **Get Info** from the options that are listed. A dialog appears with more information about the certificate.

6. Expand **Trust**. From the **When using this certificate** drop-down, select **Always Trust**.
7. Close the dialog box that has more information about the certificate. A confirmation dialog box appears.
8. Authenticate the modification of Keychains by providing a password.
9. The certificate is now trusted, and the certificate error does not appear on the address bar.

**Firefox**

1. In your Firefox browser, enter Cisco VVB Administration URL. A warning page appears which states that there is a security risk.
2. Click **Advanced** and then click **View Certificate** link. The **Certificate Viewer** dialog box appears.
3. Click **Details** and then click **Export**. Save the certificate (**.crt** file) in a local folder.

**Note** If **.crt** file option is not available, select **.der** option to save the certificate.

4. From the menu, select **Firefox** > **Preferences**. The **Preferences** page is displayed.
5. In the left pane, select **Privacy & Security**.
6. Scroll to the **Certificates** section and click **View Certificates ...**. The **Certificate Manager** window is displayed.
7. Click **Import** and select the certificate.
8. The certificate is now authorized, and the certificate error does not appear on the address bar.

# Configure System Parameters

The initial system parameter configuration is part of the Setup Wizard procedure (during installation).

The following audio codecs are supported:

- G711A for A-law
- G711U for u-law
- G729

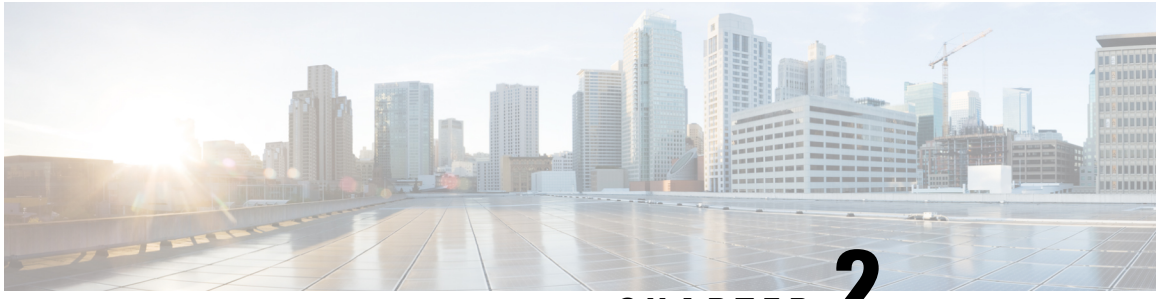
**Note**

- You can change the codec anytime after installation by navigating to **System** > **System Parameters**.
- Only one codec can be configured.
- G711 and G729 audio codecs with a sampling rate of 8K are supported.
- G729 is not supported for ASR and TTS integrations.

# Pre-configured Cisco VVB Applications

The following applications are pre-configured on the Cisco VVB:

| Script | Description | Pre-configured Dial Number |
|---|---|---|
| *CVPComprehensive* | Used for comprehensive calls. | 7777777777* |
| *Ringtone* | Used for playing ringtone and whisper. | 919191* |
| *Error* | Used for playing error tone. | 929292* |
| *VRUComprehensive* | Used for VRU-only calls | Customer can configure the dial number. |



CHAPTER 2

# Cisco VVB Configuration



## Configure Cisco VVB on Unified CVP

For detailed instructions on how to configure Cisco VVB on Unified CVP, see *Administration Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html.

**Note** Cisco VVB does not support clustering. Therefore, you may ignore any message on the Cisco VVB Admin UI/CLI that refers to **cluster**, **publisher**, **subscriber**, etc.

## Configure Cisco VVB Call Flow

Cisco VVB provides the standard list of scripts that require you to configure for the Unified CVP call flow to work. The primary steps are to create application and assign corresponding SIP trigger.

Log in to Cisco VVB Administration Console and follow these tasks:

### Procedure

**Step 1** Create an application to define the call flow through the scripts.

To configure standalone application, see Configure Cisco VVB Settings for Standalone Call Flow Model, on page 8.

To configure comprehensive and ringtone application, see Configure Cisco VVB Settings for Comprehensive Call Flow Model, on page 10.

To configure error application, see Configure Error Application, on page 14.

**Step 2** Create triggers to invoke an application using the incoming directory number.

To configure the trigger, see Configure SIP Triggers, on page 15.

**Step 3** Cisco VVB can play recorded audio prompts and detect DTMF tones. To recognize speech and play text, configure Automatic Speech Recognition (ASR) and Text-To-Speech (TTS).

To configure ASR and TTS, see Configure Speech Servers, on page 17.

**Step 4** Manage prompt files to add custom ringtone for comprehensive call flow or to use custom prompts.

To configure and manage prompts, see Configure Prompt Management , on page 20.

### Related Topics

Configure Cisco VVB Settings for Standalone Call Flow Model, on page 8
Configure Cisco VVB Settings for Comprehensive Call Flow Model, on page 10
Configure Error Application, on page 14
Configure SIP Triggers, on page 15
Configure Speech Servers, on page 17
Configure Prompt Management , on page 20

# Configure Cisco VVB Settings for Standalone Call Flow Model

### Procedure

**Step 1** From Cisco VVB Administration menu bar, choose **Applications** > **Application Management**.

**Step 2** Click the **Add New** icon that is displayed in the toolbar in the upper left corner of the window or the **Add New** button that is displayed at the bottom of the window.

**Step 3** Type the application name in the **Name** field.
The **Maximum Number of Sessions** field is prepopulated based on the OVA profile. You can edit this field.

**Note** This number must not exceed the maximum number of ports supported for Cisco VVB profile. For more information, see *Virtualization for Cisco Virtualized Voice Browser* available at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-virtualized-voice-browser.html.

**Step 4** Select the `SelfService.aef` script from the drop-down list for a standalone application.

The following table describes the parameters:

| Parameter | Description | Default | Base Type |
|---|---|---|---|
| Application Name | Application name that is present on the VXML server. Mandatory field to enter. | "HelloWorld" | Alphanumeric |
| Port | Port on which the VXML server or load balancer is running.<br>**Note** Ports 7000/7443 must be configured for interworking with CVP Release 11.5 and later. For earlier versions of CVP, configure ports 8000/8443. | "7000" | Numeric |
| PrimaryVXMLServer | VXML server or load balancer IP address. | "" | Alphanumeric |
| BackupVXMLServer | VXML server backup server IP address. | "" | Alphanumeric |
| Secured | If enabled, HTTPS is used while fetching VXML application from Unified CVP. By default it is not enabled.<br>**Note** If you have enabled secure communication, then ensure to:<br>**a.** Change the port number in the above field to 7443.<br>**b.** Upload the relevant certificate. To upload certificate, see *Upload certificate or certificate trust list* topic in *Cisco Unified Communications Operating System Administration Guide.*<br>**c.** Restart Tomcat server and Engine from command line. | false | Boolean |

**Step 5** Use the Tab key to automatically populate the **Description** field.

**Step 6** Enable the application by selecting the radio button. You can choose to disable the application to retain the configurations for later use.

**Step 7** Click **Add**.

The Cisco Script Application page refreshes and the **Add New Trigger** hyperlink appears in the left navigation bar. The following message is displayed in the status bar on top:

```
The operation has been executed successfully.
```

**Step 8** Create a trigger using the **Add New Trigger** hyperlink or follow the procedure Configure SIP Triggers, on page 15.

**Related Topics**

Configure SIP Triggers, on page 15

# Configure Cisco VVB Settings for Comprehensive Call Flow Model

This topic provides information about comprehensive and ringtone applications.

**Note** Cisco VVB is prepopulated with comprehensive application (also called bootstrap) and the ringtone application.

To create a custom comprehensive (CVP/VRU comprehensive) or ringtone application, follow the steps:

**Procedure**

**Step 1** From Cisco VVB Administration menu bar, choose **Applications** > **Application Management**.

**Step 2** Click **Add New**.

**Step 3** (Mandatory) Type the application name in the **Name** field.

**Step 4** The **Maximum Number of Sessions** field is prepopulated based on the OVA profile. You can edit this field.

**Note** This number must not exceed the maximum number of ports supported for Cisco VVB profile. For more information, see *Virtualization for Cisco Virtualized Voice Browser* available at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-virtualized-voice-browser.html.

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

The following scripts are provided for comprehensive call flow:

- CVPComprehensive.aef (bootstrap)
- Ringtone.aef

The following table describes the parameters:

| Parameter | Description | Default | Base Type |
|---|---|---|---|
| Secured | If enabled, HTTPS is used while fetching VXML application from Unified CVP. By default, it is not enabled.<br>**Note** If you have enabled secure communication, then ensure to:<br>**a.** Upload the relevant certificate. To upload certificate, see *Upload certificate or certificate trust list* topic in *Cisco Unified Communications Operating System Administration Guide.*<br>**b.** Restart Tomcat server and Engine from command line.<br>If you are using a coresident VXML and Call Server, use CA-signed certificate. | false | Boolean |
| Sigdigit | Enable this parameter to use Significant Digits feature. Enter the number of digits that are used as sigdigit. When Cisco VVB receives the call, the CVP comprehensive service is configured to strip the digits. When the IVR leg of the call is set up, the original label is used on the incoming VoiceXML request. | 0 | Numeric |

**Step 6** Use the Tab key to automatically populate the **Description** field.

**Step 7** Enable the application by selecting the radio button. You can choose to disable the application to retain the configurations for later use.

**Step 8** Click **Add**.

The Cisco Script Application page refreshes and the **Add New Trigger** hyperlink appears in the left navigation bar. The following message is displayed in the status bar on top:

```
The operation has been executed successfully.
```

**Step 9** Create a trigger using the **Add New Trigger** hyperlink or follow the procedure Configure SIP Triggers, on page 15.

**Related Topics**

Configure SIP Triggers, on page 15

# Configure Cisco VVB Settings for VRU-Only Call Flow Model

This topic provides information to create VRU-Only applications.

Use the *VRUComprehensive.aef* script if your CVP implementation needs to support non-reference VRU call flows or VRU-Only call flows. For more details on non-reference call flows, see *Solution Design Guide for Cisco Unified Contact Center Enterprise.*

To support the comprehensive call flow in addition to the non-reference VRU call flows, add relevant options to this script. The *CVPComprehensive* script must not be separately configured to handle a mixed implementation.

To create a VRU-Only application, follow the steps:

**Procedure**

**Step 1** From Cisco VVB Administration menu bar, choose **Applications** > **Application Management**.

**Step 2** Click **Add New**.

**Step 3** (Mandatory) Type the application name in the **Name** field.

**Step 4** The **Maximum Number of Sessions** field is prepopulated based on the OVA profile. You can edit this field.

**Note** This number must not exceed the maximum number of ports supported for Cisco VVB profile. For more information, see *Virtualization for Cisco Virtualized Voice Browser* available at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-virtualized-voice-browser.html.

**Step 5** From the **Script** drop-down list, select the *VRUComprehensive.aef* script.

| Parameter | Description | Default | Base Type |
|---|---|---|---|
| PrimaryVXMLServer | VXML server or load balancer IP address | "" | Alphanumeric |
| BackupVXMLServer | VXML backup server or load balancer IP address | "" | Alphanumeric |
| Port | Port on which VXML server or load balancer is running.<br>**Note** Ports 7000/7443 must be configured for interworking with CVP Release 11.5 and later. | "7000" | Numeric |

| Parameter | Description | Default | Base Type |
|---|---|---|---|
| Secured | If enabled, HTTPS is used while fetching VXML application from Unified CVP. By default, Secured is not enabled.<br>**Note** If you have enabled secure communication, then ensure to:<br>**a.** Change the port number to 7443.<br>**b.** Upload the relevant certificate. To upload certificate, see *Upload certificate or certificate trust list* topic in *Configuration Guide for Cisco Unified Customer Voice Portal.*<br>**c.** Restart Tomcat server and engine from command line.<br>If you are using a co-resident VXML and Call Server, use a CA-signed certificate. | false | Boolean |
| Sigdigit | Enable this parameter to use Significant Digits feature. Enter the number of digits that are used as sigdigit. When Cisco VVB receives a call, the VRU comprehensive service is configured to strip the digits. When the IVR leg of the call is set up, the original label is used on the incoming VoiceXML request. | 0 | Numeric |

**Step 6** Use the Tab key to automatically populate the **Description** field.

**Step 7** Enable the application by selecting the radio button. You can choose to disable the application to retain the configurations for later use.

**Step 8** Click **Add**.

Cisco Script Application page refreshes. The **Add New Trigger** hyperlink appears in the left navigation bar. The following message is displayed in the status bar on top:

```
The operation has been executed successfully.
```

**Step 9** Create a trigger using the **Add New Trigger** hyperlink or follow the procedure Configure SIP Triggers, on page 15.

# Configure Error Application

To create a comprehensive application, follow the steps:

**Procedure**

**Step 1** From Cisco VVB Administration menu bar, choose **Applications** > **Application Management**.

**Step 2** Click **Add New**.

**Step 3** Type the application name in the **Name** field.
The **Maximum Number of Sessions** field is prepopulated based on the OVA profile. You can edit this field.

**Note** This number must not exceed the maximum number of ports supported for Cisco VVB profile. For more information, see *Virtualization for Cisco Virtualized Voice Browser* available at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-virtualized-voice-browser.html.

**Step 4** Select the `Error.aef` script from the drop-down list. This script is used to play error tone.

The following table describes the parameter details:

| Parameter | Default | Base Type |
|---|---|---|
| *CVPErrorPrompt*—Select and associate custom wav file from VVB application.<br>To override system default wav file, upload custom wav file from **Prompt Management** menu.<br>**Note** You can upload custom wav files only for `Error.aef` script. | 92929292 | Numeric |

**Step 5** Use the Tab key to automatically populate the Description field.

**Step 6** Enable the application by selecting the radio button. You can choose to disable the application to retain the configurations for later use.

**Step 7** Click **Add**.

Cisco Script Application page is refreshed and the **Add New Trigger** hyperlink appears in the left navigation bar. The following message is displayed in the status bar on top:

```
The operation has been executed successfully.
```

**Step 8** Create a trigger using the **Add New Trigger** hyperlink or follow the procedure Configure SIP Triggers, on page 15.

**Related Topics**

Configure SIP Triggers, on page 15

# Configure SIP Triggers

An SIP trigger responds to calls that arrive on a specific route point and uses telephony and media resources to complete the call and to invoke the application script.

You must add SIP triggers to invoke Cisco applications in response to incoming contacts.

## Add SIP Trigger

To add an SIP trigger:

**Procedure**

**Step 1** From Cisco VVB Administration menu bar, choose **Subsystems** > **SIP Telephony** > **SIP Triggers**.

**Step 2** Click **Add New** and enter the following fields:

| Field | Description |
|---|---|
| **Directory Information** | |
| Dial Number Pattern | A unique phone number. The value includes digits and optionally includes " * " to mask multiple digits.<br>Examples of **valid** Directory Numbers: 9191*<br>Examples for valid triggers:<br>• 10.919191 where 10. is the same as 101, 102<br>• *12* or 12*23 where *12* is the same as "*" and 12*23 is the same as 12*<br>**Note** The trigger cannot contain only a wildcard character (*). If it contains *, it must also contain numbers.<br>Capital letter "X" can be used as a wildcard, but small letter "x" cannot be used. |
| **Trigger Information** | |
| Application Name | From the drop-down list, choose the application to associate with the trigger. |
| **Advanced Trigger Information** (available only if you click **Show More**) | |
| Enabled | Click a radio button to choose the required option:<br>• **Yes**—Enable the trigger (default)<br>• **No**—Disable the trigger |

| Field | Description |
|---|---|
| Idle Timeout (in ms) | The number of milliseconds (ms) the system waits before rejecting the SIP request for this trigger. |
| Override Media Termination | Click a radio button to choose the required options:<br>**Yes—**Override media termination.<br>**No—**Enable media termination (default).<br>If you select Yes, two panes open:<br>• Selected Dialog Groups — displays the default or selected group.<br>**Note** You must not change the default Selected Dialog Group associated with the application.<br>• Available Dialog Groups — displays the configured dialog. |
| Description | Click the **Tab** key to populate it. |

The new trigger is created and listed on the SIP Trigger page.

# Configure SIP Properties

Cisco VVB does not send 180 Ringing Provisional Response for an incoming SIP INVITE. To enable SIP 180 Ringing Provisional Response:

**Procedure**

**Step 1** From the Cisco VVB Administration menu bar, choose **Subsystems** > **SIP Telephony** > **SIP Properties**.

**Step 2** Select the **Enable** radio button and click **Update**.

# Configure SIP RAI

The Resource Available Indication (RAI) feature supports:

- Monitoring of CPU and memory resources
- Reporting of VVB resource status to an externally configured device

To configure RAI to a server:

**Procedure**

**Step 1** From the Cisco VVB Administration menu bar, choose **Subsystems** > **SIP Telephony** > **SIP RAI**.

**Step 2** On the SIP RAI Configuration page, click **Add New**.

**Step 3** Enter the following fields:

| Field | Default Value / Range | Description |
|---|---|---|
| Server Name | | Hostname or IP address of SIP server. |
| Port | 5060<br>Range: 1 to 65535 | SIP server port number for communication. |
| Interval | 60<br>Range: 30 to 86400 (in seconds) | Interval time to send RAI reports. |

**Step 4** Click **Add** to add a SIP server.

**Step 5** (Optional) To update a server port or interval time, click the server name and update the **Port** and **Interval** fields.

**Step 6** (Optional) To delete a server, click the **Delete** icon present on the SIP RAI List or from the update server page.

# Configure Speech Servers

Cisco VVB supports ASR and TTS through two subsystems:

**ASR**
This subsystem allows users to navigate through a menu of options by speaking instead of pressing keys on a touch-tone telephone.

**TTS**
This subsystem converts plain text into spoken words to provide a user with information, or prompt a user to respond to an action.

**Note** Only G711 codec is supported for ASR and TTS integrations.

## Prepare to Provision ASR/TTS

The customer must perform the following tasks:

- Order ASR and TTS speech servers from Cisco-supported vendors.

**Note** For more information about supported speech servers for Cisco VVB, see the Solutions Compatibility Matrix available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

- Work with the ASR and TTS vendor to size the solutions.
- Provision, install, and configure the ASR and TTS vendor software on a different server (in the same LAN) and not where the Cisco VVB runs.

# Provision ASR Servers

Use the Automatic Speech Recognition Server Configuration web page to specify information about the speech server name and port location.

### Procedure

**Step 1** From the Cisco VVB Administration menu bar, choose **Subsystems** > **Speech Servers** > **ASR Servers**.

| Column | Description |
|---|---|
| Server Name | Hostname or IP address of the ASR server.<br>**Note** ASR server deployment over WAN is not supported in Cisco VVB. Place the ASR server in the same LAN as Cisco VVB. You need to specify the ASR server hostname or IP address that is local with Cisco VVB node while installing the ASR server software in this field. |
| Port | Port number used to connect to a Speech server. |
| Status | Status or state of the server. |

**Step 2** Click the **Add New** button to provision a new ASR Server.

**Step 3** Enter the following fields:

| Field | Description |
|---|---|
| Server Name | Hostname or IP address of the ASR server. |
| Port Number | Port numbers that are used to connect to a Speech server. The default value for MRCPv1 is 4900 and for MRCPv2 is 5060.<br>**Note** If the administrator has configured any other the port value for MRCP/ASR servers, then use the same port value here. Do not use these default values. Whenever the administrator changes from MRCP protocol, ensure ASR server is deleted and re-created with the appropriate port values. |

**Step 4** Click **Add** to apply the changes.

**Step 5** (Optional) Click the **Refresh** button to refresh the status of the server.

# Provision TTS Servers

Use the Text-to-Speech Server Configuration web page to configure the TTS server name and port location.

**Procedure**

**Step 1** From the Cisco VVB Administration menu bar, choose **Subsystems** > **Speech Servers** > **TTS Servers**.

The TTS Server Configuration web page opens displaying a list of previously configured servers, if applicable, with the following information:

| Column | Description |
|---|---|
| Server Name | Hostname or IP address of the TTS server.<br>**Note** TTS server deployment over WAN is not supported in Cisco VVB. In other words, the TTS servers must be in the same LAN as Cisco VVB. Therefore, you need to specify the TTS server hostname or IP address that is local with Cisco VVB node while installing the TTS server software in this field. |
| Port Number | Port number used to connect to a Speech server. |
| Status | Status or state of the server. |

**Step 2** Click the **Add New** button to provision a new TTS Server.

**Step 3** Enter the following fields:

| Field | Description |
|---|---|
| Server Name | Hostname or IP address of the TTS server. |
| Port Number | Port number used to connect to a TTS server. The default value for MRCPv1 is 4900 and for MRCPv2 is 5060.<br>**Note** If the administrator has configured any other the port value for MRCP/TTS servers then use the same port value here, do not use these default values.<br>Whenever the administrator changes from MRCP protocol, ensure TTS server are deleted and recreated with appropriate port values. |

**Step 4** Click **Add** to apply the changes.

**Step 5** (Optional) Click the **Refresh** button to refresh the status of the server.

# Configure Prompt Management

Several system-level prompt files are loaded during Cisco VVB installation. However, any file you create must be available to the Cisco VVB Engine before the Cisco VVB application can use it. Files are made available through the Cisco VVB Repository datastore, where the prompt files are created, stored, and updated.

**Note** Use Prompt Management to store prompt WAV files locally. It helps you avoid any fetch latency while playing the large prompt. You can also use it to override the system default prompts.

## Manage Prompt Files

Many applications make use of prerecorded prompts. These are stored as *.wav* or *.au* files, and are played back to the callers to provide information and elicit caller response.

To access the Prompt Management page:

### Procedure

**Step 1** From Cisco VVBAdministration menu bar, choose **Applications** > **Prompt Management**.

**Step 2** The **Prompt Management** page opens to display the following fields.

| Field | Description |
|---|---|
| Name | Name of the folder. |
| Size | The size of the prompt file in kilobytes (KB).<br>**Note** This column is usually blank on the root page because the items on this page are usually folders.<br>The maximum limit for the uploaded prompt file is 20MB. |
| Date Modified | The date and time when the document was last uploaded or changed along with the time zone. |
| Modified By | The user ID of the person who made these modifications. |
| Delete | To remove the folder and its contents from the repository. |
| Rename | To rename the folder in the repository. |
| Refresh | To refresh the folder in the repository. |
| Create New Folder | To create a new subfolder. |

| Field | Description |
|---|---|
| Upload Prompt | To upload a prompt (.wav/.au) file or prompts packaged in a zip.<br>**Note** The maximum limit for the uploaded prompt file is 20MB. |

# Local Audio Files Stored on VVB

### Local Audio Files Stored on VVB

Local audio files that are uploaded to default prompt folder of VVB can be accessed by setting the audio source path starting with "flash:" in microapps or VXML application. The audio files must be pre-uploaded to default folder.

**Example**: "flash:holdmusic.wav"

If you are creating a custom folder in prompt management and uploading an audio file, then mention the folder name in the URL.

**Example**: flash:/<folder_name>/<file_name>

# Overriding Default Ringtone using CVP

Follow these steps to override default ringtone:

1. Go to **System** > **Dialed Number Pattern**.
2. From the listed patterns, click **Pattern** for which custom ringtone needs to be added.
3. From **Dialed Number Pattern Types**, check the **Enable Custom Ringtone** check box.
4. Specify the custom ringtone filename in the text box.

**Note**

- Custom ringtone cannot be named to ringback.wav.
- The audio file in Cisco VVB and the filename you entered in CVP under DNP is case-sensitive (should be same with .wav extension)

# Configure System Parameters

Use the System Parameters web page to configure system parameters such as port settings and locale settings and to default session timeout.

The parameters in the System Parameters Configuration page are grouped logically into sections with headings. Each parameter has a corresponding suggested or default value on the right side of the page. Where applicable, radio buttons are used to toggle between the parameter options.

Choose **System** > **SystemParameters** from the Cisco VVB Administration menu bar to access the System Parameters Configuration web page.

# Manage System Parameters

On System Parameters page, you can configure basic system settings such as Audio Codec, MRCP version,TLS (SIP), and other parameters.

**Note** This release supports only TLS 1.2. For more information, see *Contact Center Enterprise Solution Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/tsd-products-support-series-home.html.

### Procedure

**Step 1** From Cisco VVB Administration menu bar, choose **System** > **SystemParameters**.

**Step 2** To update, click the **Update** icon in the toolbar or the **Update** button at the bottom of the window.

The System Parameters Configuration web page displays the following fields.

***Table 1: System Parameters Configuration***

| Field | Description |
|---|---|
| **Generic System Parameter** | |
| System Time Zone | The system time zone of Cisco VVB server configured during installation. |
| **Media Parameters** | |
| Codec | G711 and G729 audio codecs with sampling rate 8K are supported.<br>Default: G711U |
| MRCP Version | Select the MRCP version to communicate between Nuance and Cisco VVB.<br>Default: MRCPv2<br>**Note** • The default value for ASR/TTS server port for MRCPv1 is 4900 and for MRCPv2 is 5060. Whenever the administrator changes from MRCP protocol, ensure ASR/TTS server is deleted and re-created with appropriate port values.<br>• ASR-TTS service is not supported using G729 codec; therefore, MRCP is not applicable. |

| Field | Description |
|---|---|
| User Prompts override System Prompts | When enabled, custom recorded prompt files can be uploaded to the appropriate language directory under **Prompt Management**. The custom prompts override the system default prompt files for that language. By default, this feature is disabled.<br>**Note** For overriding the system default prompt files for ringtone application:<br>• Create a new folder named **vb**. Select **Applications** > **Prompt Management** and click **Create New Folder**.<br>• Upload the custom ringtone. Choose **Applications** > **Prompt Management** and click **Upload Prompt**. Upload custom ringtone wav file(named same as **ringback.wav**) under folder **vb**. |
| **Security Parameters** | |
| TLS(SIP) | TLS (SIP) is disabled by default. When enabled, this setting secures SIP signaling on the IVR leg. TLS (SIP) version supported is TLSv1.2, and the default cipher suites are `TLS_RSA_WITH_AES_128_CBC_SHA` and `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`.<br>**Note** Multiple clients connecting to Cisco VVB cannot combine RSA and ECDHE cipher suites. They must use either RSA or ECDHE cipher suites.<br>SSL certificates need to be exchanged between VVB and any SIP endpoint (CVP, Ingress Gateway, and so on.) to talk over TLS. For more details on this configuration, see the *Upgrade Unified CVP > Postupgrade Tasks > Manual Configuration of Unified CVP Properties* section in the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal, Release 12.5(1)* available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html.<br>**Note** Cisco VVB Engine restart is required after a change to this configuration. |
| Supported TLS (SIP) Versions | This allows you to select the version of TLS (SIP). TLS (SIP) version supported is TLSv1.2.<br>When you select a given TLS (SIP) version, Cisco VVB will support SIP TLS requests for this version and the higher supported versions.<br>**Note**<br>• Supported TLS (SIP) Versions is available only if TLS (SIP) is enabled.<br>• Cisco VVB Engine restart is required after a change to this configuration.<br>• The supported TLS (SIP) versions as client or server for securing SIP signaling in the IVR leg can alternatively be specified via the CLI command **set tls server min-version** as documented in the *Cisco Unified Contact Center Express Administration and Operations Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-installation-and-configuration-guides-list.html |

| Field | Description |
|---|---|
| Cipher Configuration | This field defines the ciphers that are supported by Cisco VVB with key size lesser than or equal to 2048 bits.<br>The following ciphers are pre-populated.<br>• `TLS_RSA_WITH_AES_128_CBC_SHA`<br>• `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`<br>**Note** • Cipher configuration is available only if TLS (SIP) is enabled.<br>• You must restart the Cisco VVB engine after modifying the cipher configuration. |
| SRTP | • SRTP is disabled by default. When SRTP is disabled, the media is not encrypted.<br>• When SRTP is enabled, it secures the IVR leg. SRTP uses Crypto-Suite AES_CM_128_HMAC_SHA1_32 for encrypting the media stream.<br>• When **Allow RTP (Mixed mode)** check box is checked, the system accepts both SRTP and RTP call flows. This check box can be checked only when SRTP is enabled.<br>**Note** • SRTP is available only if TLS (SIP) is enabled.<br>• Check the **Allow RTP (Mixed mode)** check box if device is configured to work in the RTP mode and interacts with MRCP ARS-TTS servers.<br>• For more details on mixed mode call flow scenarios, see the *Solution Design Guide for Cisco Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html.<br>• Cisco VVB engine restart is required after a change to this configuration.<br>• SRTP is not supported with VVB XU (Export Unrestricted) software image releases. |
| **System Port Parameter** | |
| RMI Port | The port number used by Cisco VVB to serve Remote Method Invocation (RMI) requests. This field is mandatory.<br>Default: 6999 |

### HTTPS Client TLS Configuration

The supported TLS versions as client for securing HTTPS signaling to fetch the VXML applications from VXML server use the CLI command **set tls client min-version** in *Cisco Unified Contact Center Express*

*Administration and Operations Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html

# IP Address and Hostname Management

This section provides the steps you need to follow whenever there is a change in IP address or hostname for Cisco VVB deployment.

## IP Address Modification

This section describes how to change the IP address.

**Caution** Changing the IP address can interrupt call processing and other system functions. Also, changing the IP address can cause the system to generate certain alarms and alerts such as ServerDown. Because of this potential impact to the system, you must perform IP address changes during a planned maintenance window.

**Note** As a prerequisite ensure that the DNS is reachable and the DNS record exists for the server if DNS is enabled.

### Change IP Address using CLI Commands

#### Before you begin

Use this procedure to change the IP address of Cisco VVB.

#### Procedure

**Step 1** If DNS is enabled, change the DNS record of the server to point to the new IP address.

**Step 2** If you want to change the IP address of the server on the same subnet or a different subnet that requires a new default gateway address, then use either CLI Commands or Cisco Unified Operating System Administration interface.

**Step 3** To change the default gateway, enter the following CLI command: **set network gateway <IP Address>**

**The following is a sample output:**

```
admin: set network gateway 10.10.10.1
     ***   W A R N I N G   ***
This will cause the system to temporarily lose network connectivity
Continue (y/n)?
```

**Caution** Ensure that the server is moved to the new subnet and has access to the default gateway before proceeding to the following sub-step

**Note** Skip this step if you want to change only the IP address of the server.

**Step 4** To change the IP address of the server, enter the following CLI command: **set network ip eth0 <ip_address> <netmask> <default gateway>**

**The following sample output displays:**

```
admin:set network ip eth0 10.10.10.170 255.255.255.0 10.10.10.1
           ***   W A R N I N G   ***
This command will restart system services
=======================================================
 Note: Please verify that the new ip address is unique
       across the cluster and, if DNS services are
       utilized, any DNS configuration is completed
       before proceeding.
=======================================================
Continue (y/n)?
```

Enter **y** and press **Enter** to continue.

**Step 5** Reboot the system using the CLI command **utils system restart**.

## Change IP Address using OS Administration interface

**Procedure**

**Step 1** Log in to the Cisco Unified OS Administration using administrator login.

**Step 2** Go to **Settings** > **IP** > **Ethernet**.

**Step 3** Change the Port (IP Address and Subnet Mask) and Gateway information and click **Save**.

**Step 4** Reboot the system using the CLI command **utils system restart**.

# Hostname Modification

This section describes how to change the hostname.

**Caution** Changing the hostname can interrupt call processing and other system functions. Changing the hostname can also cause the system to generate certain alarms and alerts such as ServerDown. Because of this potential impact to the system, you must perform hostname changes during a planned maintenance window.

**Note** If DNS is enabled, as a prerequisite ensure that the DNS is reachable and the DNS record exists for the server.

## Change Hostname using CLI Commands

**Procedure**

**Step 1** Change the DNS record of the server to point to the new hostname. Ensure that you correctly update both the forward (A) and reverse (PTR) records, and there are no duplicate PTR records.

**Step 2** You can change the hostname of the server either using the CLI (command line interface) command or using Cisco Unified OS Administration interface. To change the hostname using CLI command, go to Step 3 or to change the hostname using Cisco Unified OS Administration interface, go to Step 4.

**Step 3** At the CLI prompt, enter **set network hostname** and press **Enter** key.

**The following is a sample output:**

```
***   W A R N I N G   ***
Do not close this window without first canceling the command.
This command will automatically restart system services.
The command should not be issued during normal operating hours.
=======================================================
Note:
Please verify that the new hostname is a unique name across the cluster and,
if DNS services are utilized, any DNS configuration is completed before proceeding.
=======================================================
Security Warning :
This operation will regenerate all UCCX Certificates including any third party
signed Certificates that have been uploaded.
Enter the hostname::
```

**Step 4** Enter the hostname and press Enter.

**Step 5** Reboot the system using the CLI command **utils system restart**.

## Change Hostname using OS Administration Interface

**Procedure**

**Step 1** Login to the Cisco Unified OS Administration using administrator login.

**Step 2** Go to **Settings** > **IP** > **Ethernet**.

**Step 3** Change the hostname and click **Save**.

**Step 4** Reboot the system using the CLI command **utils system restart**.

# Configure Reporting and Monitoring Services

## Real-Time Monitoring Tool

Cisco VVB system includes software components called *plug-in* to enhance Cisco VVBEngine. You can download Real-Time Monitoring Tool (RTMT) plug-in from the web page.

To access the Plug-in web page, choose **Tools** > **Plug-in** from Cisco VVBAdministration menu bar.

The Plug-in web page contains the following hyperlink:

- **Cisco Unified Real-Time Monitoring Tool for Windows**—Click this hyperlink to install client-side Cisco Unified Serviceability RTMT for Windows. RTMT uses HTTP/HTTPS and TCP to monitor device status, system performance, device discovery, and CTI applications. It also connects directly to devices by using HTTP/HTTPS for troubleshooting system problems. This plug-in is available only for users with administrator capability.

**Note** To download, click the **Download** hyperlink and select **Save File**.

## Real-Time Reporting

**Caution** The Real-Time Reporting (RTR) tool is a Java applet that can generate various reports that provide detailed information about the status of your Cisco VVB system. You use the Application Reporting web page to access the RTR tool.

To access the Application Reporting web page, choose **Tools** > **Real-Time Reporting** from the Cisco VVB Administration menu bar.

**Note** To access RTR tool, ensure to add Cisco VVB IP address under **Exception Site List** in **Java Control Panel** > **Security**. Example IP address entry is as follows: `https://10.10.10.10`.

For more information, see Cisco VVB Real-Time Reports, on page 31.

## Logging

A trace file is a log file that records activity from the Cisco VVB component subsystems and steps. Trace files let you obtain specific, detailed information about the system that can help you troubleshoot problems.

This information is stored in a trace file. To help you control the size of the trace file, you specify the components for which you want to collect information and the level of information that you want to collect.

The Cisco VVB server stores the trace files in the Log directory. You can collect and view trace information using the Real-Time Monitoring Tool (RTMT).

To activate and turn off logging, follow this procedure:

## Engine

### Procedure

**Step 1** From the Cisco VVB Serviceability menu bar, choose **Trace** > **Configuration**.

**Step 2** From the **Select Service** drop-down list box, choose **Engine** and click **Go**.

The debug levels for different Cisco VVB services might vary depending on the selected service. The Cisco VVB-related services are listed in the following table:

| Component Code | Description |
|---|---|
| JASMIN | Java Signaling and Monitoring Interface |
| SIP_STACK | SIP Stack logging |
| SS_SIP | SIP Subsystem |
| SS_VB | Voice Browser Subsystem |
| SS_MRCP_ASR | MRCP ASR Subsystem |
| SS_MRCP_TTS | MRCP TTS Subsystem |

**Note** To enable XDebugging for any of the components, check the appropriate check boxes.

**Step 3** To limit the number and size of the trace files, you can specify the trace output setting using the following two fields. See the following table for description and default values for these two fields:

| Field | Description |
|---|---|
| Maximum No. of Files | The maximum number of trace files to be retained by the system.<br>This field specifies the total number of trace files for a given service. Cisco VVB Serviceability automatically appends a sequence number to the filename to indicate which file it is; for example, Cisco001MADM14.log. When the last file in the sequence is full, the trace data begins writing over the first file. The default value varies by service. |
| Maximum File Size | This field specifies the maximum size of the trace file in kilobytes or megabytes depending on the selected service. The default value varies by service. |

**Step 4** Update the debug level for one or more components for the selected service of Cisco VVB by performing these steps:

**a.** To activate traces for a specific component or logging for a server, select the check box for the service for which you need to enable logging.

**b.** To turn off logging for a server, clear the check box.

**Step 5** Click the **Save** icon that displays in the toolbar in the upper left corner of the window or the **Save** button that displays at the bottom of the window to save your trace parameter configuration. The settings are updated in the system and the trace files are generated as per the saved settings. Click the **Restore Defaults** icon or button to revert to the default settings for the selected service.

**Important** Activate logging only for debugging, and remember to turn off logging after the debugging session is complete.

## Speech Server

### Procedure

**Step 1** From the Cisco VVB Serviceability menu bar, choose **Trace** > **Configuration**.

**Step 2** From the **Select Service** drop-down list box, choose **Speech Server** and click **Go**.

| Component Code | Description |
|---|---|
| SS_SRV | Speech Server |

**Note** To enable XDebugging for any of the components, check the appropriate check boxes.

**Step 3** To limit the size of the Log File directory and the size of trace files, you can specify the trace output setting using the following two fields. See the following table for description and default values for these two fields:

| Field | Description |
|---|---|
| Maximum No. of Files | Maximum number of trace files that is used to calculate total log directory size. |
| Maximum File Size | This field specifies the maximum size of the trace file in kilobytes or megabytes depending on the selected service. The default value varies by service. |

**Step 4** Update the debug level for one or more components for the selected service of Cisco VVB by performing these steps:

**a.** To activate traces for a specific component or logging for a server, select the check box for the service for which you need to enable logging.

**b.** To turn off logging for a server, clear the check box.

**Step 5** Click the **Save** icon that displays in the toolbar in the upper left corner of the window or the **Save** button that displays at the bottom of the window to save your trace parameter configuration. The settings are updated in the system and the trace files are generated as per the saved settings. Click the **Restore Defaults** icon or button to revert to the default settings for the selected service.

**Important** Activate logging only for debugging, and remember to turn off logging after the debugging session is complete.

# Service Management

Installed automatically, network services include services that the system requires to function; for example, system services. Because these services are required for basic functionality, you cannot activate them in the Service Activation window. After the installation of your application, network services start automatically.

To start, stop, or restart Cisco VVB services, follow these steps:

**Procedure**

**Step 1** From the Navigation drop-down list, select **Cisco VVB Serviceability.**

**Note** For freshly installed VVB, **Cisco VVB Serviceability** is accessible only after completing the setup procedure from the VVB Administration page.

**Step 2** Select **Tools** > **Control Center - Network Services**.

**Step 3** Select the **Engine** radio button and click your desired operation button.

The page displays the following information for the network services:

- Name of the network services, their dependent subsystems, managers, or components
- Status of the service (IN SERVICE, PARTIAL SERVICE, or SHUT DOWN; for individual subsystems, the status can be OUT OF SERVICE or NOT CONFIGURED)
- Start Time of the service
- Up Time of the service

# Cisco VVB Real-Time Reports

## Available Cisco VVB Real-Time Reports

Cisco VVB real-time reporting provides real-time reports you can use to monitor Cisco VVB system activity. The following table briefly describes each of these reports.

| Report | Description |
|---|---|
| Application Tasks | Provides information about currently active applications. |
| Application Tasks Summary | Provides a summary of specific application activity. |
| Applications | Provides a list of all applications loaded on the Cisco VVB server. |

| Report | Description |
|---|---|
| Contacts Summary | Provides information for call contacts and total number of contacts. |
| Contacts | Provides information about currently active contacts. |
| Engine Tasks | Provides information about currently active Engine tasks. |
| Sessions | Provides information on all active sessions. |

### Related Topic

Report Menu, on page 35

# Open Real-Time Reports

Real-Time reporting is available from the Cisco VVBAdministration web interface.

Real-Time Reporting requires the Java plug-in. If the Java plug-in is not already installed on the PC on which you are viewing the reports, the Cisco VVB system automatically installs it when you choose **Tools** > **Real Time Reporting Tool**.

**Note**

- Use Mozilla Firefox and Internet Explorer for Real Time Reporting.
- If you are using Mozilla Firefox, you must manually install the correct version of JRE to use real-time reports.

The Application Reporting web page is a stand-alone component of the Cisco VVBAdministration interface. It has its own menu bar, which replaces the Cisco VVBAdministration menu bar.

To open real-time reporting, complete the following steps.

### Procedure

**Step 1** If you are running Real-Time Reporting for the **first time** on this system, log into Cisco VVBAdministration as an **Administrator**.

The system prompts you to download the Java plug-in; follow the prompt instructions.

**Note** After you perform the initial download of the Real-Time Reporting Java plug-in, non-Administrative users can access Real-Time Reporting on this system.

**Step 2** Choose **Tools** > **Real-Time Reporting** from the Cisco VVBAdministration menu bar.

The Application Reporting web page opens in a new window. The real-time reporting tool requires a Java plug-in. If the plug-in is not installed on the machine you are using, the Cisco VVB system prompts you to

accept the automatic installation of the plug-in. If you do not accept the installation, you cannot use real-time reporting.

# Run Reports

Open the real-time reporting tool from the Cisco VVBAdministration web interface to run reports.

To run a real-time report, complete the following steps.

**Procedure**

**Step 1** From the Application Reporting menu bar, choose **Reports**.

**Step 2** From the Reports menu, choose the report to run.

The report opens in the Application Reporting window.

# View Detailed Subreports

You can view more detailed information for selected items in these four reports:

- Application Tasks report
- Contacts report
- Applications report
- Sessions report

To view detailed subreports, complete the following steps.

**Procedure**

**Step 1** Run the Application Tasks, Contacts, Applications, or Sessions report.

**Step 2** Click a line in the report for which you want to view more detailed information. For example, click an email address in the Contacts report.

**Step 3** From the Application Reporting menu bar, choose **Views** and click the subreport that you want to run.

You can also open a subreport by right-clicking the selected item and choosing a subreport.

The subreport opens.

# Print Reports

To facilitate printing, you can open a printable version of a report.

To print a report, complete the following steps.

**Procedure**

**Step 1** Run a report.

**Step 2** From the Application Reporting menu, choose **Tools** > **Open Printable Report**.

A printable version of the report opens in a separate window.

**Step 3** Print the report using your browser print functionality.

# Reset Report Statistics

The Cisco VVB system automatically resets all statistics each day at midnight. You can reset the accumulated statistics manually at any time. Resetting statistics does not reset active statistics, such as active contacts and active tasks.

To reset report statistics, complete the following steps.

**Procedure**

**Step 1** From the Application Reporting menu bar, choose **Tools** > **Reset All Stats**.

The Reset Stats dialog box opens for you to confirm the reset.

**Step 2** Click **Yes**.

Accumulated statistics are reset.

# Set Report Options

You can set the following reporting options:

- Refresh interval
- Number of times that the Cisco VVBAdministration web interface should attempt to reconnect to the Cisco VVB server

To set report options, complete the following steps.

**Procedure**

**Step 1** From the Application Reporting menu bar, choose **Settings** > **Options**.

The Options dialog box opens.

**Step 2** From the Polling Interval drop-down menu, choose the refresh rate in seconds.

**Step 3** From the Server Connect Retry Count drop-down menu, choose the number of times that the Cisco VVBAdministration web interface should attempt to reconnect to the Cisco VVB server.

**Step 4** Click **Apply** to apply the settings.

# Set Report Appearance

You can select from three report appearances:

- Windows, which displays reports in colors based on your Windows settings
- Motif, which displays reports in purple and menu items in brown
- Metal, which displays reports in grey and menu items in black

To set the report appearance:

**Procedure**

Choose **Settings** from the Application Reporting menu bar and click the appearance that you want.

# Application Reporting User Interface

When you choose **Tools** > **Real-Time Reporting** from the Cisco VVBAdministration menu, the Application Reporting tool opens a web page in a new window.

The Application Reporting tool menu bar contains the following options:

- **Report**—Choose this option to display a list of the available top-level real-time reports.
- **Tools**—Choose this option to reset all the statistics and refresh connections.
- **Settings**—Choose this option to set the look and feel of the real-time Reporting client, set the polling (refresh) interval times, and set the amount of times the server will attempt to reconnect.
- **Help**—Choose this option to display system information and to access Cisco VVB online help.

## Report Menu

The Report menu provides access to a variety of top-level reports. It contains the following menu options:

### Contacts Summary Real-Time Report

Use the Contacts Summary report to view specific contact information for call contacts, email contacts, HTTP contacts, and total number of contacts.

To access the Contacts Summary real-time report, choose **Reports** > **Contacts Summary** from the Application Reporting menu bar.

**Note** You display the data on this report as numbers or percentages by clicking the Display Value/Display % toggle button.

The following fields are displayed on the Contacts Summary report.

| Field | Description |
|---|---|
| Active | Active contacts that are currently running. |
| Inbound | Number of inbound contacts since the statistics were last reset. |
| Connected | Number of connected contacts since the statistics were last reset.<br>Provides a total for contacts that are connected to resources. |
| Terminated | Number of terminated contacts since the statistics were last reset. |
| Rejected | Number of rejected contacts since the statistics were last reset. |
| Aborted | Number of aborted contacts since the statistics were last reset. |

## Application Tasks Summary

Use the Application Tasks Summary report to display statistics that summarize the activity of specific applications.

To access the Application Tasks Summary real-time report, choose **Reports** > **Application Tasks Summary** from the Application Reporting menu bar.

The following fields are displayed on the Application Tasks Summary report.

| Field | Description |
|---|---|
| Application Name | Names of the applications that are running or have run. |
| Running | Currently running applications. |
| Completed | Applications that have stopped running. |
| Total | Number of times an application was invoked since the statistics were last reset. |

## Application Tasks Real-Time Report

Use the Application Tasks real-time report to view information about currently active applications.

To access the Application Tasks report, choose **Reports** > **Application Tasks** from the Application Reporting menu bar. The following fields are displayed on the Application Tasks report.

| Field | Description |
|---|---|
| ID | Unique application task ID. |
| Node ID | Unique ID for a server in the cluster.<br>**Note** As Cisco VVB does not support clustering, you can ignore the value. |
| Application | Name of the application. |
| Start Time | Time when the application task started. |

| Field | Description |
|---|---|
| Duration | Length of time that the application has been active. |

**Note** If this report indicates that an application is running for an unusually long time, there may be a problem with the application. The application script may not include error handling that prevents infinite retries if a call is no longer present. If the application does not receive a disconnect signal after a call, the application repeatedly retries to locate the call, and causes the application to run for an unusually long time. To prevent this problem, include the proper error handling in the application script.

## Engine Tasks Real-Time Report

Use the Engine Tasks real-time report to view information about currently active Engine tasks.

To access the Engine Tasks report, choose **Reports** > **Engine Tasks** from the Application Reporting menu bar.

The following fields are displayed on the Engine Tasks report.

| Field | Description |
|---|---|
| ID | Unique identifier of the engine task.<br>If the engine task is the main task running the application and the parent ID is empty, its identifier will match the Application Task Identifier. |
| Parent ID | Unique identifier for the parent of the engine task (if any).<br>**Note** This field is not relevant to Cisco VVB. You can ignore the value. |
| Node ID | Unique identifier for a server in the cluster.<br>**Note** As Cisco VVB does not support clustering, you can ignore the value. |
| Server IP Address | IP address identifying the server in the cluster. |
| Script | Name of the script that is running the task (if the task is running a Cisco VVB script). |
| Start Time | Time that the task started. |
| Duration | Length of time the task has been active. |

## Contacts Report

Use the Contacts real-time report to view information for all the active contacts for all servers.

To access the Contacts report, choose **Reports** > **Contacts** from the Application Reporting menu bar.

You can access detailed information about specific contacts listed on the Contacts web page by performing one of the following procedures:

- Call Contacts Detailed Info Report, on page 38

The following fields are displayed on the Contacts report.

| Field | Description |
|---|---|
| ID | Unique identifier representing a contact. |
| Type | Type of contact: |
| Impl ID | Unique identifier provided by the particular type of contact. |
| Node ID | Unique identifier for a server in the cluster.<br>**Note** As Cisco VVB does not support clustering, you can ignore the value. |
| Start Time | Time stamp when the contact was created. |
| Duration | Length of time that the contact is active. |
| Handled | If True, the contact is handled; if False, the contact is not handled. |
| Aborting | If True, the contact is aborted with a default treatment; if False, the contact is not aborted. |
| Application | Name of the application currently managing the contact. |
| Task | Unique identifier of the application task that is currently responsible for the contact. |
| Session | Unique identifier of the session currently managing the contact (if any). |

**Note** The information displayed is dependent on the type of contact selected. Depending on the type of call, some fields may not be supported and will appear blank.

### *Call Contacts Detailed Info Report*

Use the Call Contacts Detailed Info real-time report to view all information related to the call contact.

To access the Call Contacts Detailed Info report, right-click a specific call contact record on the Contacts report; information for that specific record displays.

The following fields are displayed on the Call Contacts Detailed Info report.

| Field | Description |
|---|---|
| State | Current state of the contact. |
| Inbound | If True, this call was received by the Cisco VVB server; if False, this call was placed as an outbound call by an application. |
| Language | The selected language context of the call. |
| Application ID | Unique identifier of the associated application. |
| Called Number | Called number for this call leg from the perspective of the called party. |
| Dialed Number | Dialed number for this call leg from the perspective of the calling party. |
| Calling Number | Calling number of the originator of this call. |

| Field | Description |
|---|---|
| ANI | Automatic number identification. |
| DNIS | Dialed number identification service. |
| CLID | Caller ID. |
| Arrival Type | Information on how the call contact arrived in the system. |
| Last Redirected Number | Number from which the last call diversion or transfer was invoked. |
| Original Called Number | Originally called number. |
| Original Dialed Number | Originally dialed number. |
| ANI Digits | Automatic Number Identification information indicator digit codes. |
| CED | Entered digits that were gathered by the network before the call was received.<br>**Note** Calls running Unified ICME applications are also reported here. |

## Applications Report

Use the Applications real-time report to view all the applications loaded on the server.

To access the Applications report, choose **Reports** > **Applications** from the Application Reporting menu bar.

The following fields are displayed on the Applications report.

| Field | Description |
|---|---|
| Name | Unique name of the currently loaded application. |
| ID | Application ID. |
| Type | Type of application that is currently running (for example, a Cisco Script Application). |
| Description | Description of the application as entered on the Cisco VVBAdministration web site. |
| Enabled | If True, the application is enabled; if False, the application is disabled. |
| Max. Sessions | Maximum number of simultaneous task instances that can run simultaneously on the Cisco VVB server. |
| Valid | If True, the application is valid; if False, the application is invalid.[1] |

[1] An application is valid if it was successfully loaded and initialized from its configuration. At any time, an application can become invalid if it internally fails to be refreshed.

## Sessions Report

Use the Sessions real-time report to view real-time information on all the active sessions.

To access the Sessions report, choose **Reports** > **Sessions** from the Application Reporting menu bar.

The following fields are displayed on the Sessions report.

| Field | Description |
|---|---|
| ID | Session ID.<br>**Note** This identifier is guaranteed to remain unique for a period of 12 months. |
| Mapping ID | User- or system-defined identifier that maps to this session. |
| Node ID | Unique identifier for a server in the cluster.<br>**Note** As Cisco VVB does not support clustering, you can ignore the value. |
| Parent | Sessions that were created as a result of consult calls propagated in the system. |
| Creation Time | Creation time of the session. |
| State | Current state of the session.<br>**Note** When marked IDLE, the session is subject to being “garbage collected” by the system after a specified period of time. In addition, a session is IN_USE if it still has a contact associated or a child session. |

# Tools Menu

The Tools menu gives you access to the following Application Reporting tools:

- **Reset All Stats**—Choose this option to reset all statistics.
- **Open Printable Report**—Choose this option to get a printable report of all currently active contacts in the system.
- **Refresh Connections**—Choose this option to refresh connections with the Cisco VVB system.

## Reset All Statistics

Use the Reset All Stats option to reset all statistics accumulated since the last time the statistics were reset. It will not reset active statistics, such as active contacts, tasks, and so on.

### Procedure

Choose **Tools** > **Reset All Statistics** from the Application Reporting menu bar.

## Open Printable Report

Use the option to get a printable report of all currently active contacts in the system.

To get a printable report:

#### Procedure

Choose a real-time report from the Report menu option and then **Tools** > **Open Printable Report** from the Application Reporting menu bar.

### Refresh Connections

To refresh connections with the Cisco VVB system:

#### Procedure

Choose **Tools** > **Refresh Connections** from the Application Reporting menu bar.

The Cisco VVB system refreshes all connections.

## Views Menu

The Views menu allows you to access more detailed information for the following reports:

The Views menu contains different options, depending on the report you have chosen. Possible options are:

- **Contacts by Application Task ID**—Choose this option to view contacts according to Application Task ID numbers.
- **Engine Tasks by Application Task ID**—Choose this option to view Engine tasks according to Application Task ID numbers.
- **Detailed Info**—Choose this option to view more detailed information on selected reports.
- **Application Tasks by Application Name**—Choose this option to view application tasks by application name.
- **Contacts by Session ID**—Choose this option to view contacts by session ID.

### Application Tasks

You can obtain reports based on the application task ID associated with application tasks.

#### *Contacts by Application Task ID*

This report displays the same report as the Contact report with the exception that the Contacts by Application Task ID report has been filtered using only the contact currently being managed by the selected application task.

#### *Engine Tasks by Application Task ID*

This report displays the same report as the Engine Task reports except that the Engine Tasks by Application Task ID report has been filtered to display only the engine tasks that are associated with the application task.

### Contacts

When you use the Views options with the Contacts report, the Views menu contains only the Detailed Info option.

The Detailed Info option provides various detailed information, depending on the type of contact selected. For example, if the contact is a call, the Calling Party number, the Called Number, and so on, are displayed for that particular call.

### Applications

When you use the Views options with the Application reports, the Views menu contains only the Application Tasks by Application Name option.

The Application Task By Application Name report displays the same report as the Application Task report except that the Application Task By Application Name report is filtered using only the active application tasks associated with this application.

### Sessions

You can obtain reports based on the session ID associated with a session.

#### *Contacts by Session ID*

This report displays the same report as the Contact report with the exception that the Contacts By Session ID report is filtered using only the contacts associated with the selected session.

#### *Detailed Info*

Detailed info displays the time the session was created and its current state.

## Settings Menu

The Settings menu of the Application Reporting menu bar allows you to adjust various settings of the Real Time Reporting tool.

The Settings menu contains the following menu options:

- **Options**—Choose this option to set the polling (refresh) interval times and to set the amount of times the server will attempt to reconnect and to enable the reset statistics at midnight .
- **Window**—Choose this option to display reports in colors based on your Windows settings.
- **Motif**—Choose this option to display reports in purple and menu items in brown.
- **Metal**—Choose this option to display reports in grey and menu items in black.

### Options Menu

Choose **Settings** and click **Options** to access the Options dialog box. Use the Options dialog box to set the polling (refresh) interval time, set the number of times the server will attempt to reconnect.

The following fields are displayed in the Options dialog box.

| Field | Description |
|---|---|
| Polling Interval | Time between two requests to the server for new statistics by the client. |

| Field | Description |
|---|---|
| Server Connect Retry Count | The number of times that the Cisco VVB Administration web interface should attempt to reconnect to the Cisco VVB server.<br>**Note** If an error occurs, an Error dialog box opens to alert you that the server is not communicating with the web interface. |
| Reset Statistics at Midnight | The statistics data gets cleared at midnight if enabled.<br>**Note** This option is disabled either when client is not connected to the server or report is not selected. To connect to the server, select an option from Report menu. |

Click **Apply** to submit configuration changes.

APPENDIX A

# FIPS Update

You can run the new CLI command `utils fips enable` to enable many FIPS 140-2 like settings in the product. However, this is not certified yet to be compliant. Changes leverage FIPS-compliant libraries of BCFIPS and include them to the security provider list in the JRE, keystore format, ciphers supported, algorithms used, etc.

**Note** If AppDynamics monitoring is enabled, disable it before enabling FIPS mode.

FIPS Update

APPENDIX B

# Internal REST API Endpoints

Following authenticated REST API endpoints are exposed for internal invocation from within the solution. These REST API endpoints are listed for information purposes only, and not intended for external consumption currently. If you have a valid use case to know more, please get in touch with the product team.

```
http://<VVB_HOSTNAME_OR_IP>/adminapi/application
http://<VVB_HOSTNAME_OR_IP>/adminapi/asrServer
http://<VVB_HOSTNAME_OR_IP>/adminapi/ttsServer
http://<VVB_HOSTNAME_OR_IP>/adminapi/sipTrigger
http://<VVB_HOSTNAME_OR_IP>/adminapi/callControlGroup
http://<VVB_HOSTNAME_OR_IP>/adminapi/dialogGroup
http://<VVB_HOSTNAME_OR_IP>/adminapi/systemParam
http://<VVB_HOSTNAME_OR_IP>/adminapi/speechconfig/rest/config
http://<VVB_HOSTNAME_OR_IP>/adminapi/cloudConnect
```