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, on page 1
- Configure System Parameters, on page 5
- Pre-configured Cisco VVB Applications, on page 6

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

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.