

Cisco Virtualized Voice Browser Release 12.5(1) SU

November 2022

Introduction

You may perform a fresh installation or upgrade to Cisco Virtualized Voice Browser 12.5(1) SU on supported virtual machines from previous version.

This document describes how to download and install the Cisco Virtualized Voice Browser **12.5(1) SU** ISO file.

Upgrade Paths

The following upgrade path is supported from the source system:

Source System	Target System
12.5(1)	12.5(1) SU

Downloading the ISO File

Download the required 12.5(1) SU ISO file from [Software Download Areas – Virtualized Voice Browser 12.5\(1\)](#).

Image Type	ISO
12.5(1) SU	UCSInstall_VVB_12_5_2_UCOS_12.5.2.10000-281.sgn.iso
12.5(1) SU KVM	VVB-12-5-2-ISR4K.ova
12.5(1) SU Export Unrestricted (XU)	UCSInstall_VVB_12_5_2_UCOS_12.5.2.99000-275.sgn.iso
12.5(1) SU Export Unrestricted (XU) KVM	VVB-12-5-2-XU-ISR4K.ova

Installing/ Upgrading to 12.5(1) SU

There are no changes in the install or upgrade process. Before upgrading to 12.5(1) SU, the release key cop file *ucos.keymanagement.v01.cop.sgn* must be applied. Download the mandatory cop from [ucos.keymanagement.v01.cop.sgn](#).

For more information about the VVB installation or upgrade procedure, refer to [Installation and Upgrade Guide for Cisco Virtualized Voice Browser](#).

Note:

- The OVA for 12.5(1) and 12.5(1) SU are same.
- The KVM images are only for installation, upgrade to KVM images is not supported.

Compatibility

There is no change in compatibility and is same as 12.5(1) release. For more information, refer to [Compatibility Matrix](#).

New Features

All the features introduced up to 12.5(1) latest ES release are applicable for 12.5(1) SU release. For more information on the latest ES available for Cisco VVB 12.5(1), refer to the [VVB Engineering Specials](#) page.

CORS Support for Private network access

Cross Origin Resource Sharing (CORS) specification is being altered to add a new request header in preflight requests. More details are provided here <https://wicg.github.io/private-network-access/>. The following commands are used to control private network access in CORS requests.

- *'show vvb http pna-status'* command shows the status of the private network access for CORS. Default value is true.
- *'set vvb http pna-enable'* command enables private network access for CORS requests. This command requires a restart of the Cisco Tomcat service.
- *'set vvb http pna-disable'* command disables private network access for CORS requests. This command requires a restart of the Cisco Tomcat service.

Updated Features

None

Important Notes

After installing Cisco Virtualized Voice Browser 12.5(1) SU, the following software versions are updated:

- Tomcat upgraded from version 7.0.94 to 9.0.37
- Java platform version upgraded from OpenJDK-1.7.0.231 to OpenJDK-1.8.0.262

Note: The previous versions of Tomcat and OpenJDK reached end of life. To address the security vulnerabilities, the Tomcat and Java versions are upgraded.

Deprecated Features

None

Removed and Unsupported Features

None

Third Party Software Impacts

None

Resolved Caveats in Release 12.5(1) SU

All the caveats resolved in 12.5(1) latest ES release are applicable for 12.5(1) SU release. For more information on the latest ES available for Cisco VVB 12.5(1), refer to the [VVB Engineering Specials](#) page.

The following VVB caveats are specifically resolved in VVB 12.5(1) SU:

Table 1: Caveats resolved specifically in 12.5(1) SU

Identifier	Headline
CSCwc02895	VVB vmcore seen due to IPVMS crash.
CSCwa76530	TTS server status
CSCwd21906	Files fetched using data element generate temp files which are never deleted
CSCwb78716	VVB 12.5 - VVB services terminating unexpectedly
CSCwc93693	Impact of Chrome deprecating Private Network Access on VVB