Unified CVP Postinstallation

After you install Unified CVP, perform postinstallation tasks to ensure that the all the CVP components are installed successfully. In addition, disable port blocking and address security issues. To beign with, do the following:

1. Go to the `%CVP_HOME%\conf` directory and add the following entry in the *vxml.properties* file:

   ```
   VXML.usagefactor = 1.0
   ```

2. Restart the **WebServicesManager** service.

✎

Note Sometimes after installation, `clean.cvp` file may not be available at `%CVP_HOME%\bin\TAC`. This can happen sporadically but does not impact the functionality of CVP. You can always retrieve this file from the `CVP\Utilities` folder of the CVP iso.

Note
- After installation, go to `C:\Cisco\CVP\conf\orm.properties` file and check if the *orm.oamp.id* parameter has any oamp ID (for example, 495a891e-a64f-4e1b-b80d-26e0dce0e249-2098391835) assigned to it. If so, then delete the ID and restart the **WebServicesManager** service.

- Postinstallation excludes CVP components configuration. For information about CVP component configuration, see the *Configuration Guide for Cisco Unified Customer Voice Portal* available at: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html.

If CVP Server, Operation Console, and Reporting Server have not been installed to the default `C:\Cisco\CVP` path, then update the following files under `<install_path>/conf`:

- **cvpconfigdb.properties:** Update the connection URI so that it matches path of the DB directory
  `ConnectionUrl=jdbc:derby://localhost:1529/<install_path>/OPSConsoleServer/sql/db`

  Example:
  `ConnectionUrl=jdbc:derby://localhost:1529/C:/Cisco/CVP/OPSConsoleServer/sql/db`

- **cvpwsm.properties:** Update CVP_HOME.default.dir as **`CVP_HOME.default.dir = <install_path>`**

  Example: `CVP_HOME.default.dir = C:\\Cisco\\CVP`

- **sip.properties:** Update SIP.Secure.KeyStorePath as **`SIP.Secure.KeyStorePath= <install_path>\\security\\.keystore`**

  Example: `SIP.Secure.KeyStorePath= C:\\Cisco\\CVP\\conf\\security\\.keystore`

This chapter explains the following postinstallation tasks.

- Disable Port Blocking, on page 2
- Security, on page 3
- Initiate Metadata Synchronization for Unified CVP Rest API, on page 3

Disable Port Blocking

If you have installed Unified CVP Server components on a computer that has antivirus software configured to block ports, exclude Unified CVP processes and Tomcat executable files.

Note Exclude the following folders from on-access scanning configuration of the AV program for all Antivirus scans:

`c:\Cisco, c:\Temp, c:\tmp, c:\db, c:\IFMXDATA`

It is the customer's responsibility to deploy the VXML applications after the Antivirus scans. This also applies to the custom `java/jar/class` files deployed in the shared path.

For more information on the Virus Scan guidelines, refer to the following sections of the UCCE documentation:

The Virus Protection section of UCCE Design Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html.

The General Antivirus Guidelines section of the Security Guide for Cisco Unified ICM/Contact Center Enterprise at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html

Security

Depending on your choice of Unified CVP deployment, you may need to address certain security considerations. For information about security, see the *Configuration Guide for Cisco Unified Customer Voice Portal* available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html.

Note If you are concerned about any vulnerability in Microsoft Visual VC++ 2005 Redistributable, then uninstall it from Control Panel. This will not impact the normal operation of the CVP Reporting Sever.

Initiate Metadata Synchronization for Unified CVP Rest API

In the Unified CVP REST API architecture, information of media files on Media Server and VXML applications on a VXML server is saved on a WSM Server as metadata in Derby database. This metadata information is created, updated, and deleted by the REST API calls. There may be situations where the metadata may go out of sync with files on VXML Servers and Media Servers. Examples are addition and deletion of Unified CVP Servers, deployment of apps and media files by a tool other than the REST API, and Unified CVP Media Server or the VXML server upgraded from a version where the REST API was not supported.

A command line tool "metasynch.cmd" is available at `C:\Cisco\CVP\wsm\CLI` to enable synchronization of metadata with the files on VXML Servers and Media Servers. The tool internally uses the Synch up API to perform the synchronization. It takes three arguments- WSM user name, WSM user password, and server type (MEDIA, VXML or VXML_ STANDALONE). Based on the server type information, all servers of the respective server type are synchronized. If the server type argument is not provided, metadata is synchronized with all media servers and VXML servers configured in OAMP.

In case of an upgrade, the media files and VXML applications are present in the Media Servers and VXML Servers but corresponding metadata information is not present in the WSM Server. The absence of metadata information limits a user from using the REST API to access, update, and delete existing media files and VXML applications on the Media Server and the VXML Server.

Synchronize Metadata Files Using Sync-Up Tool

To invoke `metasynch.cmd`, complete the following steps.

Step 1 On the Unified CVP OAMP Server, navigate to the `C:\Cisco\CVP\wsm\CLI` location.

Step 2 Run the **metasynch.cmd** file with following arguments:

- **wsm username**
- **wsm password**

Example:

```
metasynch.cmd wsmusername wsmpassword MEDIA
```

Usage : metasynch [options] username password [servertype]

servertype : MEDIA/VXML/VXML_STANDALONE

options : -help -? print this help message

Note The server type argument should be MEDIA, VXML, or VXML_STANDALONE type. If the server type argument is not provided, the metadata is synched with all the VXML applications on VXML servers and all media files on Media servers. Logs for synch command tool can be found at the following location:

```
C:\Cisco\CVP\wsm\CLI\log\SyncTool.log
```