

Unified CVP and Virtualized Voice Browser TLS and SRTP Security Configuration

First Published: September 6, 2017

Introduction

This page provides configuration information for securing Cisco Unified Customer Voice Portal (Unified CVP) and Cisco Virtualized Voice Browser (Virtualized Voice Browser) by enabling Transport Layer Security (TLS) and Secure Real-Time Transport Protocol (SRTP) security settings.

The intended audience should be able to perform system-level configuration of Cisco Collaboration components and deployments and be familiar with Cisco Collaboration products.

The configuration information is based primarily on system testing performed in the 11.6(1) Packaged CCE test bed during Cisco Collaboration Systems Release 12.0(1).

Design

For information on design considerations and guidelines for deploying Packaged CCE, see: <u>https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html</u>.

Topologies

This section provides information about the Cisco Packaged Contact Center Enterprise deployment. In the test bed, various components were tested, including Unified CVP and Virtualized Voice Browser.



Configuration Task Flow

This section provides the high-level tasks and related information for enabling TLS and SRSTP security of Unified CVP and Virtualized Voice Browser.

Table 1. Unified CVP and Virtualized Voice Browser Configuration Task Flow

	Task
1.	Install Unified CVP Secure Certificate
2.	Install Unified CVP Call Server and VXML Server Certificate
3.	Convert Virtualized Voice Browser to Secure
4.	 Exchange Virtualized Voice Browser Certificate a. Generate and Download CSR b. Submit CSR to CA c. Download CA Cert d. Upload Root Certificates as tomcat-trust e. Upload Identity Certificate as tomcat f. Restart Tomcat

Install Unified CVP Secure Certificate

Use this procedure to install Unified CVP security certificate.

- Step 1 Backup the %CVP_HOME%\conf\security folder.
- Step 2 Open the **security.properties** file to retrieve the .keystore password and copy and paste the value of this property when managing the .keystore.
 - a. Open the %CVP_HOME%\conf\security.properties file.

Note The property file should contain the Security.keystorePW property.

- b. Enter the keystore password after keytool prompts you to enter it.
- c. Copy the value of the Security.keystorePW property and paste it into the command-line window.
- Step 3 Open a command prompt and navigate to the %CVP_HOME%\conf\security folder.
- Step 4 Generate a Certificate Signing Request (CSR) by entering the following command:

```
.....jre\bin\keytool.exe -storepass <keystore pwd> -storetype JCEKS -keystore .keystore -
              certreq -dname CN=<cvp.your.domain> -alias oamp_certificate -file oamp.csr
          Install the root certificate by entering the following command:
Step 5
               ....jre\bin\keytool.exe -storepass <keystore_pwd> -storetype JCEKS -keystore .keystore -
              import -v -trustcacerts -alias root -file ca.cer
Step 6
          Install the CA signed certificate by entering the following command:
               ..\..\jre\bin\keytool.exe -storepass <keystore pwd> -storetype JCEKS -keystore .keystore -
              import -v -trustcacerts -alias oamp certificate -file oamp.cer
Step 7
          Run the following command to check whether the certificate is imported:
               .....jre\bin\keytool.exe -storepass <keystore_pwd> -storetype JCEKS -keystore .keystore -
              list
Step 8
          Restart the Cisco CVP OPSConsoleServer.
```

- a. Choose Start > Control Panel > Administrative ToolsServices.
- b. Right-click the Cisco CVP OPSConsoleServer service and then click Restart.

Install Unified CVP Call Server and VXML Server Certificate

- Step 1 Open the security.properties file to retrieve the .keystore password and copy and paste the value of this property when managing the .keystore.
 - a. Open the %CVP_HOME%\conf\security.properties file, where %CVP_HOME% is the installation directory for Unified CVP. By default, Unified CVP is installed in C:\Cisco\CVP.

Note The property file should contain the Security.keystorePW property.

- b. Enter the keystore password after keytool prompts you to enter it.
- c. Copy the value of the Security.keystorePW property and paste it into the command-line window.

For example, if the %CVP_HOME%\conf\security.properties file contains theSecurity.keystorePW = [3X]}E7@nhMXGy{ou.5AL!+4Ffm868 property line, the password to copy is [3X]}E7@nhMXGy{ou.5AL!+4Ffm868.

Step 2 Back up the %CVP_HOME%\conf\security directory.

- Step 3 Open a command-line prompt window, and change to security configuration directory to cd\cisco\cvp\conf\security.
- Step 4 Create the certificate signing request to use the private key entry for your certificate, Remember:

Enter the keystore password when prompted.

Example:

- Call Server: %CVP_HOME%\jre\bin\keytool.exe -certreq -alias callserver_certificate -storetype JCEKS -keystore .keystore -file callserver_certificate.csr
- VXML Server: %CVP_HOME%\jre\bin\keytool.exe -certreq -alias vxml_certificate -storetype JCEKS -keystore .keystore -file vxml_certificate.csr

A new csr file is created on the file system.

- Step 5 Give the certificate signing request file to a trusted Certificate Authority. They sign it and return one or more trusted certificates.
- Step 6 Install the root certificate by entering the following command:

```
..\..\jre\bin\keytool.exe -storepass <keystore_pwd> -storetype JCEKS -keystore .keystore - import -v -trustcacerts -alias root -file ca.cer
```

Step 7 Import the signed certificate file from your trusted Certificate Authority to the .keystore file, and enter in the keystore password when prompted.

If more than one certificate is delivered, certificates must be imported in order of the chained certificate hierarchy. For example: root, intermediate, signed certificate.

Example:

- Call Server: %CVP_HOME%\jre\bin\keytool.exe -import -v -alias callserver_certificate -storetype JCEKS trustcacerts -keystore .keystore -file signed_callserver_certificate.crt
- VXML Server: %CVP_HOME%\jre\bin\keytool.exe -import -v -alias vxml_certificate -storetype JCEKS -trustcacerts -keystore .file signed_vxml_certificate.crt

Convert Virtualized Voice Browser to Secure

Use this procedure to enable the Virtualized Voice Browser TLS and SRST security settings.

Task

```
Step 1 From the Cisco Virtualized Voice Browser Administration, choose System > System Parameters Configuration.
```

Step 2 To enable In Security Parameters, click the TLS and SRST **Enable** radio buttons.

Cisco Virtualized Voice Browser A × +			
🗲 🛈 🐔 https://10.10.2.16/appadmin/SystemParams?request_type=	sysparams.configure	🖾 🤇 📿 Search	☆自
Cisco Virtualized Voice Browse For Cisco Virtualized Voice Browser	r Administration		Navigation Cisco VVB Admini administ
System Applications Subsystems Tools Help			
System Parameters Configuration			
Update 🔇 Clear			
Status -			
Generic System Parameter			
Parameter Name	Parameter Value	Suggested Value	
System Time Zone	Eastern Standard Time		
Media Parameters			
Parameter Name	Parameter Value	Suggested Value	
Codec	G711U 👻	G711U	
MRCP Version	MRCPv2 -	MRCPv2	
User Prompts override System Prompts	Oisable C Enable	Disable	
Security Parameters			
Parameter Name	Parameter Value	Suggested Value	
TLS	Disable Enable	Disable	
SRTP [Crypto Suite : AES_CM_128_HMAC_SHA1_32]	🔿 Disable 🔍 Enable 👘 Allow Mixed mo	de Disable	
System Port Parameter			
Parameter Name	Parameter Value	Suggested Value	
RMI Port	6999	6999	

Update Clear

Exchange Virtualized Voice Browser Certificate

Use this procedure to make the certificate exchange between Virtualized Voice Browser and the Root Certificate Authority (CA).

Table 2. Exchange Virtualized Voice Browser Certificate Task Flow

	Task
1.	Generate and Download CSR
2.	Submit CSR to CA
3.	Download CA Certificate
4.	Upload Root Certificates as tomcat-trust
5.	Upload Identity Certificate as tomcat
6.	Restart Tomcat

Generate and Download CSR

Step 1 From Cisco Unified Operating System Administration, choose **Security > Certificate Management**.

Step 2 Click Generate CSR.

Step 3 Click **Download CSR**.

Cisco Unified Operating System Administration

300	For Cisco	Unified	Communications Solutions	
-----	-----------	---------	--------------------------	--

Show - Settings	✓ Security ✓ Software Upgrades ✓ Services ✓ Help ✓
Certificate Con	figuration
Regenerate	🛐 Download 🔋 Generate CSR 🔋 Download CSR
Status	ertificate Signing Request Generated
Certificate Set	tings
File Name	tomcat.pem
Certificate Name	e tomcat
Certificate Type	certs
Certificate Grou	p product-cpi
Description	Self-signed certificate generated by system

Submit CSR To CA

- Step 1 In Notepad, open the CSR file previously downloaded and copy the entire contents including the ---BEGIN CERTIFICATE REQUEST--- and ---END CERTIFICATE REQUEST--- lines.
- Step 2 Go to: <u>http://10.8.2.200/certsrv</u>.
- Step 3 Choose **Request a certificate > Advanced Certificate Request**.
- Step 4 From the **Certificate Template** drop-down, choose Tomcat.

Step 5 Paste the Notepad contents into this window and click **Submit**.

Certificate List	imes Microsoft Active Directory Certif $ imes$ +				_	٥
(i) 10.8.2.200/ce	tsrv/certrqxt.asp	C Q Search	☆ 自	Ŧ	Â	◙
Microsoft Active Dire	tory Certificate Services apl-LAX-DC-CA					Ho

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	2q5dhQszH76nTHNMvuiIR9F m21N14BAMms/sElVpHqsZ/v V/6KWcoWpnjSC2G0Aloirt LLM/A9t7ViRn4p4XmzyiJ71 puQF104+TFpVQTT46Nb3B+L END CERTIFICATE RE	RocCl5xOE1QA239HEf rtuFL109S6S20eNVAt hzMfuD/FmcSY3C8EI V/F/0pM4sFH81TFwV zi1PLECqI64k= QUEST >
Certificate Temp	ate:	
	Tomcat	~
Additional Attrib	ites:	
Attributes:		
		Submit >

- Step 6 From the Certificate Issued page, click the **Base 64 encoded** radio button.
- Step 7 Click **Download certificate**, and save the file in desired folder. Note the name of the file. For example: certnew.CER

Certificate List	× Microsoft Active Directory Certifi × +		
(i) 10.8.2.200/cert	srv/certfnsh.asp	C Q. Search	☆
Microsoft Active Direct	tory Certificate Services apl-LAX-DC-CA		
Certificate Issued			
The certificate you re	equested was issued to you.		
	encoded or Base 64 encoded 		
Downloa Downloa	<u>d certificate</u> d certificate chain		

Download CA Certificate

Step 1 The Server Admin must build a complete chain of certificates, so must download the root CA certificate.

Go to: <u>http://10.8.2.200/certsrv</u>.

Choose Download a CA Certificate, Certificate Chain, or CRL.

Click the Base 64 radio button.

Certificate List X Microsoft Active Directory Certif X +	
① 10.8.2.200/certsrv/certcarc.asp	El C Search
Microsoft Active Directory Certificate Services apl-LAX-DC-CA	
Download a CA Certificate, Certificate Chain, or CRL	
To trust certificates issued from this certification authority, install th	is CA certificate.
To download a CA certificate, certificate chain, or CRL, select the	certificate and encoding method.
CA certificate: Current [apl-LAX-DC-CA(1)] Previous [apl-LAX-DC-CA] V	
Encoding method:	
⊙ DER ● Base 64	
Install CA certificate	
Download CA certificate	
Download CA certificate chain	
Download latest delta CRI	

Step 2 Click **Download CA Certificate** and save it to a folder. For example: certnew(1).CER)

Upload Root Certificates as tomcat-trust

Step 1	The VB Server must have all certificates in the chain uploaded, starting at the top (roo	ot).
--------	--	------

۲	Jpload Certificate/Certificate chain - Mozilla Firefox 📃 💻 🗖	x				
🕕 🛈 🖍 https://10.10.2	17/cmplatform/certificateUpload.do					
Upload Certificate	'Certificate chain					
🔄 Upload 🔛 Clos	se	_				
Status (i) Warning: Uploa	ading a cluster-wide certificate will distribute it to all servers in this cluster					
_Upload Certificate	>/Certificate chain	_				
Certificate Purpose'	* tomcat-trust 🗸					
Description(friendly	name)					
Upload File	Browse certnew(1).cer					
Upload Close (i) *- indicates required item.						
<	Ш	>				

Related Documentation

Upload Identity Certificate as Tomcat

Step 1 This is the identity certificate issued by the CA.

Complete the cert chain by specifying .pem root cert. The root certificate you specify here could be the name of the root cert, or the name of some intermediate cert. The purpose is to find the certificate that signed the identity certificate, and use that certificate filename in this root cert field.

🙂 Uploa	d Certificate/Certificate chain - Mozilla Firefox	-		X
🛈 🖗 https://10.10.2.17/cmplatform/certificateUpload.do				
Upload Certificate/Certifica	te chain			
Dipload 🖳 Close				
Status Warning: Uploading a clus	ster-wide certificate will distribute it to all servers in this cluster			
Upload Certificate/Certific	ate chain			
Certificate Purpose*	tomcat 🗸			
Description(friendly name)	Self-signed certificate			
Upload File	Browse certnew.cer			
Upload Close				
(i) *- indicates required iter	n.			
<	III			>

Restart Tomcat

Step 1 admin: utils service restart Cisco Tomcat

When Tomcat comes back up, you can access the CCMAdmin or CCMUser GUI to verify your newly added certificates in use.

Related Documentation

- For related installation and configuration information, see:
 - <u>https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-installation-guides-list.html</u>

Obtaining Documentation and Submitting a Service Request

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see <u>What's New in Cisco Product Documentation</u>.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the <u>What's New in Cisco Product</u> <u>Documentation RSS feed</u>. The RSS feeds are a free service. THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017 Cisco Systems, Inc. All rights reserved.