REVIEW DRAFT - CISCO CONFIDENTIAL

Operations Guide for Cisco Unified Customer Voice Portal, Release 10.0(1)

First Published: December 12, 2013

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

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.

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: http://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)

© 2013 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Preface v

About this document v

Organization v

Related documentation vi

Document conventions vi

Audience vii

Support vii

Documentation feedback vii

CHAPTER 1

Cisco serviceability tools 1

Web services manager 1

Create a WSM user 1

Unified system CLI 2

Access Unified system CLI and its help 3

Unified system CLI: system mode 5

System CLI automated execution 5

System CLI remote execution 6

Help for the system CLI 6

System CLI troubleshooting 7

System CLI commands and parameters 8

Details for specific options 9

Configure Analysis Manager with Unified CVP 10

System CLI commands map to IOS CLI commands 11

CHAPTER 2

Configure Unified CVP logging and event notifications 13

Using syslog 13

Using logs to interpret events 13

REVIEW DRAFT - CISCO CONFIDENTIAL

Editing the log messages XML file 14
Unified CVP event severity levels 15
VoiceXML logs 16
About voiceXML logs 16
Correlate unified CVP/Unified ICME logs with VXML server logs 16
About Unified CVP VXML Server logs 17
About voiceXML application logging 18
About event statistics 19
Infrastructure statistics 20
ICM service call statistics 23
IVR service call statistics 25
SIP service call statistics 28
Gateway statistics 30
Procedure 30
Gateway statistics 31
Trunk utilization reporting 31
RAI information on SIP OPTIONS (CVP server group heartbeats) 32
Unified CVP VXML server statistics 32
Reporting server statistics 34
Unified CVP SNMP-Raise/Clear mappings 35

Preface

- About this document, page v
- Organization, page v
- Related documentation, page vi
- Document conventions, page vi
- Audience, page vii
- Support, page vii
- Documentation feedback, page vii

About this document

The *Operations Guide for Cisco Unified Customer Voice Portal* provides the following information:

- Describes serviceability features on Unified CVP on non-Windows boxes.
- Describes how to configure external events and how to set trace levels and log levels.

Organization

This guide consists of the following chapters:

Table 1: Feature Guide of Cisco Unified Customer Voice Portal Organization

Chapter	Description
Cisco serviceability tools	Describes serviceability features on Unified CVP on non-Windows boxes.
Configure Unified CVP logging and event notifications	Describes how to configure external events and how to set trace levels and log levels.

REVIEW DRAFT - CISCO CONFIDENTIAL

Related documentation

Table 2: Related Documentation for Unified CVP Features

Document Name	Link
Hardware and System Software Specification for Cisco Unified Customer Voice Portal	http://www.cisco.com/en/US/products/sw/custcosw/ps1006/prod_technical_reference_list.html
Cisco Unified Customer Voice Portal Design Guide	http://www.cisco.com/en/us/products/sw/custcosw/ps1006/products_implementation_design_guides_list.html
Configuration Guide for Cisco Unified Customer Voice Portal	http://www.cisco.com/en/US/products/sw/custcosw/ps1006/tsd_products_support_series_home.html
Feature Guide for Cisco Unified Customer Voice Portal	http://www.cisco.com/en/US/products/sw/custcosw/ps1006/tsd_products_support_series_home.html

Document conventions

Convention	Description
boldface font	Boldface font is used to indicate commands, such as user entries, keys, buttons, and folder and submenu names. For example: • Choose **Edit** > **Find**. • Click **Finish**.
italic font	Italic font is used to indicate the following: • Document title. Example: *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal 10.0(1)*. • A syntax value that the user must replace. Example: IF (*condition, true-value, false-value*)
`window font`	Window font, such as Courier, is used for the following: • Text as it appears in code or that the window displays. Example: `<html><title>Cisco Systems,Inc. </title></html>`

REVIEW DRAFT - CISCO CONFIDENTIAL

Convention	Description
< >	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output. • A character string that the user enters but that does not appear on the window such as a password.

Audience

This guide is intended for managers, Unified CVP system managers, Cisco Unified Intelligent Contact Management Enterprise (Unified ICME)/ Cisco Unified Intelligent Management Hosted (Unified ICMH) system managers, VoIP technical experts, and IVR application developers, who are familiar with the following:

- Configuring Cisco Gateways
- Configuring Cisco Unified Communications Manager
- ICM Configuration Manager and ICM Script Editor tools for call center operations and management

Support

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

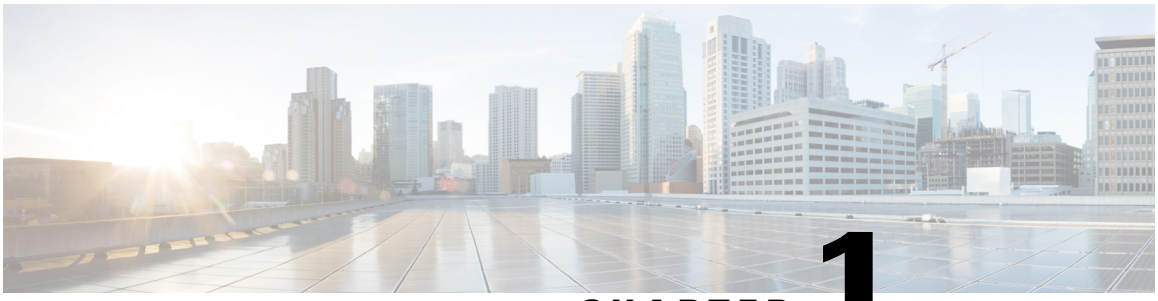
Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Documentation feedback

Provide your comments about this document to:

mailto:ccbu_docfeedback@cisco.com

REVIEW DRAFT - CISCO CONFIDENTIAL



CHAPTER 1

Cisco serviceability tools

This chapter presents an overview of Cisco serviceability tools, including the tools available with Unified CVP solutions running on Windows environments. It also presents the serviceability tools that use the Web Services Manager (WSM).

- Web services manager, page 1
- Unified system CLI, page 2
- Configure Analysis Manager with Unified CVP, page 10
- System CLI commands map to IOS CLI commands, page 11

Web services manager

Unified CVP supports a new service layer called the Web Services Manager (WSM). WSM interacts with various subsystems and infrastructure handlers, consolidates the responses, and publishes an XML result. The Web Services Manager supports HTTPS requests and sends a predefined XML response. WSM is installed on each Unified CVP device and runs automatically as a Windows service. For a device to be managed by WSM, the device must be deployed from the Operations Console.

Note System CLI uses WSM to collect and present the data available to WSM from the various Unified CVP components.

Create a WSM user

When Unified CVP is installed, a new user called wsmadmin is created with the same password as the Operations Console user. You can create and manage additional WSM users using the Operations Console.

When you have devices deployed in the Operations Console, log on to any server where WSM is installed and access the System CLI. See Unified system CLI.

REVIEW DRAFT - CISCO CONFIDENTIAL

Procedure

Step 1 Log into the Unified CVP Operations Console and select **User Management** > **Users**.

Step 2 Click **Add New**.

Step 3 Provide a **Username** and **Password**.

Step 4 Click the **User Groups** tab.

Step 5 In the **Available** panel, highlight **ServiceabilityAdministrationUserGroup**, then click the right arrow to move that group to the **Selected** panel.

Step 6 Click **Save**.

Unified system CLI

Unified CVP supports a new serviceability CLI called Unified System CLI (System CLI). The System CLI lets you collect diagnostic information (health and status) on Unified CVP servers and collect device-specific information from each supported node connected to the Unified CVP server from which you are using System CLI. The System CLI accesses a new web services layer in Unified CVP called the Web Services Manager. You can run System CLI commands on a local server, or a remote server. You can obtain information from all the devices in your CVP system by switching to *system* mode. (Devices must first be configured and deployed in the Operations Console.)

Note To quickly access and use the System CLI, see Access Unified system CLI and its help

Note In addition to the System CLI, which is automatically installed with the Unified CVP installation, you can also obtain a GUI-based client, . This client is called the Analysis Manager, and it is part of Unified CM. For more information on the Analysis Manager, refer to Cisco Unified Communications Analysis Manager User Guide. For instructions specific to configuring Analysis Manager with Unified CVP, Configure Analysis Manager with Unified CVP, on page 10

The System CLI is installed on all CVP servers. You can leverage the WSM and CLI functionality to collect diagnostic details such as server map, version information, licenses, configuration, components, sessions, logs, traces, performance factors, and platform information for each Unified CVP Device, on a component and sub-component level. You can also set or reset debug levels using CLI on a component and sub-component level.

The System CLI provides a local mode and a system mode:

- The local mode accesses data about the devices associated with the server that you are logged into. Local mode is the default mode accessed automatically when you log into the Unified CLI.
- The system mode, accessed by typing the system command at the CLI prompt, provides access to all the devices in your Unified CVP deployment solution. In system mode, the System CLI automatically detects the Operations Console and extracts solution topology based on the devices configured in the Operations Console. Based on options you enter for a given command, System mode can be limited to a certain device group or list of servers.

REVIEW DRAFT - CISCO CONFIDENTIAL

Note Before you can use the system CLI to obtain information about a device, that device must be listed in and deployed by the Operations Console.

The System CLI commands (for example `show all` and `show component`) enable you to view and zip necessary logs or configurations on a specific server, servers, or groups of servers, and store that data on a local disk.

Access Unified system CLI and its help

The Unified System CLI is installed on all Unified CVP Servers. Using the CLI client on a Unified CVP device enables you to connect to the local server or a remote server. You can also connect to servers defined and deployed in the Operations Console when using system mode.

To launch Unified System CLI on any CVP server, log into a Unified CVP server through windows. You can use tools such as VNC or Remote Desktop console.

Note To be able to log in to the System CLI on Unified CVP, the WSM service must be up and running. By default WSM service is always running.

Note The System CLI only provides information on devices that have been configured, saved, and deployed in the Operations Console. If you change the configuration of a device, you must save and deploy the revised configuration before it is available to the System CLI.

Complete the following example session to quickly learn how to use Unified System CLI.

Procedure

Step 1 Launch Unified System CLI.
Select **Start** > **Programs** > **Cisco Unified Customer Voice Portal** > **Unified System CLI**.

A CMD window displays with an Enter Username prompt.

Step 2 Log into the Unified System CLI by entering the default username, **wsmadmin**, or a username and password that you created. See Create a WSM user.
After logging, in you see the following message and prompt:

```
Welcome to the Platform Command Line Interface
admin:
```

Step 3 You can now receive Web Services Manager data from the local machine using the system CLI commands. The following CLI Usage example shows a user issuing the show tech-support command.

```
Enter username[wsmadmin]: wsmadmin

Enter password:

Welcome to the Platform Command Line Interface
```

REVIEW DRAFT - CISCO CONFIDENTIAL

```
admin: show tech-support
Warning: Because running this command can affect system performance,
Cisco recommends that you run the command during off-peak hours.
Do you want to continue? [y/n]: y

Retrieving [version] data from device [localhost] ProductType [cvp] ...
Retrieving [component] data from device [localhost] ProductType [cvp] ...
Retrieving [log] data from device [localhost] ProductType [cvp] ...
Default time range is last 24 hours.
...
Output is saved to "C:\Cisco\CVP\wsm\CLI\download\clioutput0.zip"
```

Note The show tech-support command creates a single zip file in the directory *%CVP_HOME%\wsm\CLI\download*.

Note By default, this command collects the traces for the last 24 hours. Use the **reltime** parameter to change the time period. For example, if you want to pull traces for the last three days, use the following command: show tech-support reltime 3 days.

Step 4 Each System CLI command has a set of **command options**. Each option consists of a keyword and set of values. The following is an example of how to use a command with options.
In this example, the keyword *component* has a value *cvp:CallServer* and the keyword *subcomponent* has a value *cvp:ICM*. The following command tells the System CLI to get the configuration data for component *CallServer* and subcomponent *ICM* in the Unified CVP deployment.

```
admin: show config component cvp:CallServer subcomponent cvp:ICM
Downloading Configuration file: [ICM: icm.properties] ...
ICM.icmGarbageCollectorInterval : 120
ICM.locationDelimeter : --
ICM.icmHeartbeatInterval : 5000
...
ICM.preRoutedCallServiceID : 2
ICM.icmVxmlIdleTimeout : 30
```

Step 5 Almost all commands have a *redirect* option. This option tells the System CLI to redirect the command output to a directory (or a file). If the output is saved in a directory, it is saved in a zip file in that specific directory. The following example saves the zip file to **c:\temp\clioutput.zip**:

```
admin: show version redirect dir c:\temp
```

The output zip file provides a consistent directory structure when you save to a directory. When unzipped, the directory structure enables you to find the required diagnostic data quickly.

If you redirect the output to a file, the information is stored in the form a of "flat" file similar to what you see for the window output. An example of redirecting to a file is:

```
admin: show version redirect file <filename>
```

Step 6 To obtain information from the Web Services Managers that are part of your Unified CVP environment, you can change to *system* mode to issue system-wide commands.
To enable system mode, type *system* at the prompt.

Note See Unified system CLI.

REVIEW DRAFT - CISCO CONFIDENTIAL

Unified system CLI: system mode

Enter the CLI system mode by typing **system** at the command prompt and then execute the commands exactly like the local version of the CLI for interactive mode.

In system mode, the Unified System CLI automatically detects the Operations Console, which acts as a seed device, and extracts the solution topology automatically based on devices configured in the Operations Console. System mode enables the System CLI to iteratively go to each supported box in the background and run the command that was executed by you in system mode.

Note System CLI initialization for the first system mode command execution, or for the **system init** command, may take a few minutes to complete, especially when there are a lot of devices in a Unified CVP solution, or if devices are unreachable, or network timeouts are involved.

Optionally, you can limit the system command to execute only on a certain device group or list of servers.

Device group is automatically populated based on:

- Device type (Unified CVP, Unified ICM, IOS Firewall , Unified CM as an example)
- Device IP/hostname wildcard (LOC-1*, 10.86.129.* as an example for branch office deployments)
- Device pool (defined within the Operations Console)

When the System CLI executes the *system* command, the System CLI queries each device in the list and caches the responses locally during its first time initialization process, or when **system init** is executed. The cache enables the system command to be executed quickly for subsequent sessions.

If an error is reported due to an unreachable destination or incorrect credentials for a specific device during the execution of a system command , then the device is marked OFFLINE in the System CLI cache. Use *system init* to retry this device.

The most common command to receive all information from all the components in a Unified CVP solution deployment is:

```
system show tech-support dtcomponent "ucm:Cisco CallManager|cusp:Cisco Unified SIP Proxy"
```

This command collects everything from all device types except the devices *ucm* and *cusp*. For ucm, it applies the device type filter *Cisco CallManager* and for the device *cusp* it applies the device type filter *Cisco Unified SIP Proxy*.

System CLI automated execution

To automatically execute Unified System CLI commands, create a plain text file with the .bat extension as shown in the example below and replace the <password> as highlighted with the Operations Console password.

```
 REM TECH-SUPPORT-COLLECTION
 echo show tech-support > clicmds.txt
 echo exit >> clicmds.txt
 type clicmds.txt | systemcli.bat inplace nointeractive novalidation user:wsmadmin
passwd:<password>
```

In a batch file, the system command can also be executed by prefixing *system* on any regular command. For example, **system show tech-support**, the entire example is:

```
   REM SYSTEM-TECH-SUPPORT-COLLECTION
```

REVIEW DRAFT - CISCO CONFIDENTIAL

```
   echo system show tech-support > clicmds.txt
   echo exit >> clicmds.txt
   type clicmds.txt | systemcli.bat inplace nointeractive novalidation user:wsmadmin
passwd:<password>
```

The most commonly used command in a Unified CVP solution deployment, to get data from all solution components, is given below:

```
   REM SYSTEM-TECH-SUPPORT-COLLECTION
   echo system show tech-support dtcomponent "ucm:Cisco CallManager\|cusp:Cisco Unified SIP
 Proxy"> clicmds.txt
   echo exit >> clicmds.txt
   type clicmds.txt \| systemcli.bat inplace nointeractive novalidation user:wsmadmin
passwd:<password>
```

This command collects everything from all device types except for the device *ucm* and the device *cusp*. For the ucm device, it applies the device type filter *Cisco CallManager* and for the device cusp, it applies the device type filter *Cisco Unified SIP Proxy*.

Note You can run a Windows scheduled job and collect traces periodically from one or multiple servers using a schedule. See How to Schedule Tasks in Windows XP for information about scheduling a Windows job.

System CLI remote execution

To launch System CLI remotely from your laptop, (or any Windows system), to connect to any Unified CVP server or other solution component box (for example, Unified CM, ICM, IOS, CUSP Server, etc.), complete the following procedure:

1. Install Unified CVP Remote Operations, if no other CVP software is installed.

   For information about only installing the Remote Operations feature of Unified CVP, see Installation and Upgrade Guide for Cisco Unified Customer Voice Portal.

2. In the Operations Console, complete the following steps:

   a. Select **System** > **Web Services** > **Remote Operations Deployment (tab)**.

   b. Enter the IP address, hostname, and description information for the remote device.

   c. Click **Add** to add the device and click **Save & Deploy** to make this device available for remote operations.

3. Start the System CLI on the remote system.

Note You can also run a Windows scheduled job and collect traces periodically from one or multiple servers, using a schedule from a remote system.

Help for the system CLI

The following types of help are available:

- For an overview of the CLI system help, type help at the admin prompt and press enter.

REVIEW DRAFT - CISCO CONFIDENTIAL

admin:**help<enter>**

- For a list of main commands, enter "?" at the admin prompt.

  admin:**?<enter>**

- To obtain the syntax of the command, type a "?" at the end of the current syntax. For example:

  admin: **capture start ?**

  The preceding entry then informs you that there are two options in the syntax: **duration** and **<cr>**

- To obtain detailed help, enter a portion of the command preceded by the word help. For example:

  admin: **help show version**

  That command provides information about additional options both local and system modes.

The following entries show an example of "drilling down" to obtain more detailed help. At the option level, placing *help* in front of the command, provides detailed information, as in the example. Because this command can be used in "local" mode and in "system" mode, the detailed help also gives information about how to limit the command when using system mode.

```
admin: show version ?
Options: redirect
<cr>

show version redirect ?
Options: dir
file
```

The help system displays the actual components for your Cisco Unified product as shown in the following example for Unified CVP using system mode of the System CLI.

```
admin(system):show log component ?
Options:cvp:CallServer
cvp:OAMP
cvp:ORM
cvp:Reporting
cvp:VXMLServer
```

System CLI troubleshooting

The System CLI shows two types of errors:

- Errors from servers (displayed unchanged)
- Errors from the System CLI for which you need to check the log files in the System CLI directory

Sometimes it is necessary to change the System CLI debug level to "debug" to collect more data about a System CLI error.

1. Open CLI\conf\cli_log4j.xml and change the word "info" to "debug".
2. Restart the System CLI to reproduce the error.

See the Doc Wiki troubleshooting page for more CLI troubleshooting information: System CLI troubleshooting tips.

REVIEW DRAFT - CISCO CONFIDENTIAL

System CLI commands and parameters

The Unified System CLI is designed to work across multiple Cisco Unified products. The meanings of some of the parameters for commands such as *show* vary from product to product. An example is the *components* parameter which vary because the components of systems such as Unified CVP and Unified ICM are different.

The CLI online help provides product-specific information for each command's parameters. Type the command and its parameter, followed by the "?" symbol. An example of this mechanism is given in Help for the system CLI.

The following table provides information about the Unified System CLI commands.

Command or Parameter	Description
capture	Sets up, starts, and stops, a network packet capture. Capturing network packets with the System CLI can be performed in either local mode (to run on a single machine), or system mode (to run across several machines simultaneously). The capture start command has an optional duration parameter, while the capture stop command has no parameters. The duration parameter indicates when the capture should stop. If no duration is provided, the capture process stops after one day. The capture command starts the packet capture on a single Unified CVP device or multiple devices. The capture operation defaults to the interface card that is receiving packets and is used for the Unified CVP server socket and IP address binding. The default setting of the capture command will capture the network packets and save the capture information in the Unified CVP logs folder which can be retrieved using the regular CLI trace command.
help	Accesses the online help system overview. Use the "?" character to access command-specific and parameter-specific help. See Help for the system CLI.
exit	Exits the CLI.
show	Accesses, displays and saves (to a file) data about system configuration and operation. See the next table for descriptions of the sub-level show commands.
system	Enter system mode, which provides access to all the devices in your Unified CVP deployment solution. Use the exit command to return to local mode.

The following table describes the variations of the *show* command.

Show Commands	Descriptions
show all	Shows all available information in all sub-categories listed in this table. However, you can still enter qualifying parameters to restrict the information retrieved.
show component	Shows component-specific information. Available components are based on the Cisco Unified product type and can be listed by entering the command: show component ?

REVIEW DRAFT - CISCO CONFIDENTIAL

show config	Displays the application configuration.
show debug	Shows the current debug level.
show devices	Shows a list of the devices in your deployment (system mode only).
show license	Shows license information.
show log	Shows log contents. You can narstrow this command to specific logs.
show perf	Shows system performance statistics.
show platform	Shows platform information.
show sessions	Shows the current active sessions or calls.
show tech-support	Shows information to help tech support in solving issues. This command is equivalent to show all. **Note** When you issue the show tech-support command, the System CLI issues the other show commands needed to provide all of the system information. During the process of executing the other show commands, the System CLI passes component and sub-component parameters to the show trace command, but does not include component and sub-component parameters when it executes commands such as show configuration and show log.
show trace	Shows trace file information.
show version	Shows Unified CVP component version information.

Details for specific options

This section provides detailed information of certain options that require additional explanations.

Results of the *match* Option when Information is Sent to a Directory Instead of a File

You can use the *match* option with the *show trace* and the *show log* commands to send selected output to a directory. This option enables you to specify text that the CLI should match when examining data in text files. The output is then limited to log information that matches the specified criteria. However, because the system cannot perform a text match to include or exclude information in binary files such as .zip files, these files are *included* in your *show* command execution, since they may contain pertinent information.

If you send the output of the *match* selection process to a file instead of a directory, the output only includes the actual text the CLI command would return to the screen.

Comparison of the *component* Option with the*dtcomponent*Option

The *component* limits the output of a command to the results from specific system components.

Using the command **show trace component ucm:CallManager** and the system components shown in the following list, you receive the following information:

- Unified CVP Call Server: No Information Returned
- Unified Call Manager: Information Returned

REVIEW DRAFT - CISCO CONFIDENTIAL

- Unified CM Tomcat Server: No Information Returned

The command **show trace component ucm:CallManager** only returns information from the Call Manager.

The option *dtcomponent* (device type component option) only restricts the information from the given device type, while allowing data to be returned from other device types.

Using the above system and the command **show trace dtcomponent ucm:CallManager** would restrict its *ucm* component output to just the Call Manager, but returns information for other device types. In this example, it returns the following information for the Unified CVP Call Server and the Call Manager, but not the Unified CM Tomcat Server:

- Unified CVP Call Server: **Information Returned**
- Unified Call Manager: **Information Returned**
- Unified CM Tomcat Server: **No Information Returned**

Configure Analysis Manager with Unified CVP

To configure Analysis Manager with Unified CVP, follow this procedure:

Procedure

Step 1 From the **Unified Analysis Manager** menu, choose **Inventory** > **Node**.
The Node window appears.

Step 2 Click **Add** to add a node or select a node from the list. Click **Edit** to edit an existing configuration.
The Add or Edit Node window appears.

Note Fields on this window that are marked with an asterisk (*) are required fields.

Step 3 From the Product Type drop-down list box, select **CVP**.

Step 4 In the IP/Host Name field, enter the host name or the IP address of the Unified CVP OAMP box.

Step 5 In the Transport Protocol field, select the protocol you want to use. Use the default value populated (HTTPS).

Step 6 In the Port Number field, enter the port number of the node you are using.

Note Use the default value populated (8111).

Step 7 Enter the user name as **wsmadmin** and enter the OAMP password. Re-enter the password in the Confirm Password field.

Step 8 In the Description field, you can optionally provide a brief description of the node you are adding.

Step 9 In the Associated Call Record Server and Associated Trace File Server fields, use the drop-down list to select the respective servers you want to use for the node.

Step 10 To add a node to an existing group, check the **Associated Group** check box.

Step 11 If you have a NAT or Terminal Server configuration, use the Advanced button to display the Add Node-Advanced screen. Enter the appropriate information in the Alternate IP/Hostname and Alternate Port fields.

Step 12 Click **Save** to save the node to the list. Click **Cancel** to end the operation without adding the node.

REVIEW DRAFT - CISCO CONFIDENTIAL

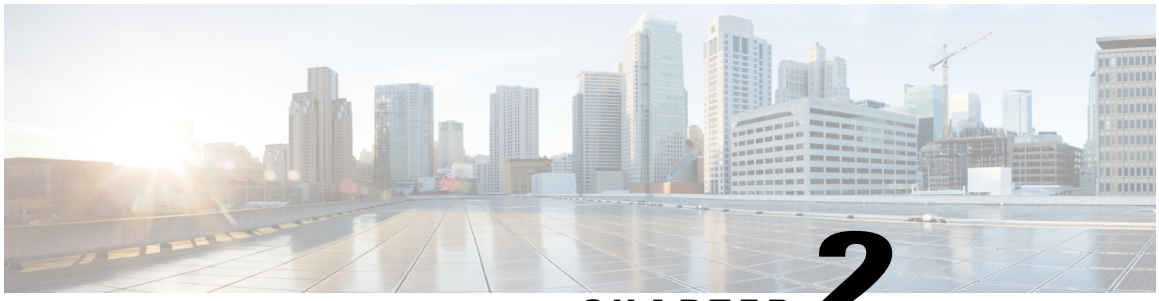
System CLI commands map to IOS CLI commands

The following table maps the System CLI commands to their corresponding IOS CLI commands:

System CLI Commands	IOS CLI Commands
show config	show running-config
show version	show version show clock
show license	show license
show perf	show call resource voice stat show memory statistics show processes cpu history show processes memory sorted show voice dsp group all show voice dsp voice
show debug	show debug
show log	N/A
show sessions	show call active voice compact show voice call status | inc calls show voip rtp connections | inc connect sh sip-ua calls | inc calls
show tech-support	show tech-support <Everything else given above>
show trace	show logging
show platform	show diag sh inventory sh int | inc media type|Ethernet|address sh controllers T1 | inc T1 sh controllers E1 | inc E1
debug	0 no debug all 1 - deb ccsip err

REVIEW DRAFT - CISCO CONFIDENTIAL

	deb cch323 err deb voip app vxml err deb http client err deb mrcp err deb rtsp err deb h225 asn1 err deb h245 asn1 err 2 - debug isdn q931 debug h225 events debug h245 events debug voip ccapi inout debug vtsp events 3 - debug ccsip messages debug h225 q931 debug h225 asn1 debug h245 asn1



CHAPTER 2

Configure Unified CVP logging and event notifications

Unified CVP provides information about component device status and interaction through

- Logs, which are presented in text format and can be viewed using Cisco serviceability tools
- Statistics, which can be viewed using the Unified CVP Operations Console

This chapter also provides information about Unified CVP SNMP-Raise/Clear mappings, and contains the following topics:

- Using syslog, page 13
- Using logs to interpret events, page 13
- VoiceXML logs, page 16
- About event statistics, page 19
- Unified CVP SNMP-Raise/Clear mappings, page 35

Using syslog

Unified CVP allows you to configure the primary and backup syslog servers with the forked primary and forked backup servers. Failover from primary to backup server is not guaranteed. When the primary syslog server goes down (the entire machine, not just the syslog receiver application), Unified CVP relies on the host operating system and the Java Runtime Environment for notification that the destination is not reachable. Because the semantics of this notification do not guarantee delivery, Unified CVP cannot guarantee failover.

Using logs to interpret events

You can use the **CVPLogMessages.xml** file to help interpret events. This file contains all messages (or notifications) on SNMP events and/or through Syslog.

REVIEW DRAFT - CISCO CONFIDENTIAL

Note The **CVPLogMessages.xml** file applies to all Unified CVP Services.

Each event in the **CVPLogMessages.xml** field containing information that must be useful for correcting any problems indicated by the event.

Note Be aware that the <resolution> field might not always contain as much information as the Troubleshooting Guide for Cisco Unified Customer Voice Portal or other Unified CVP documentation, and should be considered with all other resources when troubleshooting a problem.

The sections that follow provide information about editing, uploading, and downloading the CVPLogMessages.xml file from the Operations Console.

Editing the log messages XML file

The log messages XML file, `CVPLogMessages.xml`, defines the severity, destination (SNMP management station or Syslog server) and possible resolution for Unified CVP log messages. This file also identifies an event type identifier and message text identifier for each event. The text for these identifiers is stored in the resource properties file, `CVPLogMessagesRes.properties`.

Each Unified CVP Call Server, VXML Server, and Reporting Server has a log messages XML file and log message file. You can edit the `CVPLogMessages.xml` file on a particular Unified CVP server to customize the severity, destination and possible resolution for each event that the server generates. You can also edit the `CVPLogMessagesRes.properties` file to change the text of the message that is generated when an event occurs on that server.

Use any plain-text editor (one that does not create any markup) or XML editor to edit the `CVPLogMessages.xml` file. Use a resource file editor to edit the `CVPLogMessagesRes.properties` file. If a resource file editor is not available, use a text editor.

Message Element	Possible Values	What it Means
Name	Resource="identifier"	Identifies the event type described in the `CVPLogMessagesRes.properties` file.
Body	Resource="identifier"	Identifies the message text described in the `CVPLogMessagesRes.properties` file.
Severity	0 to 6	Identifies the Unified CVP event severity levels of the event.
SendToSNMP	True or false	Set to true, to send this message, when logged, to an SNMP manager, if one is configured.
SendToSyslog	True or false	Set to true to send this message, when logged, to a Syslog server, if one is configured.

REVIEW DRAFT - CISCO CONFIDENTIAL

Message Element	Possible Values	What it Means
SNMPRaise	True or false	Set to true to identify this message, when logged, as an SNMP raise event, which the SNMP management station uses to initiate a task or automatically take an action. Set to false to identify this message as an SNMP clear when sent to an SNMP management station. An SNMP clear event usually corresponds to an SNMP raise event, indicating that the problem causing the raise has been corrected. An administrator on an SNMP management station can correlate SNMP raise events with SNMP clear events.

Unified CVP event severity levels

The following table describes the available severity levels for Unified CVP events. You can set the severity level for an event by editing the log messages XML file, CVPLogMessages.xml, on the server that generates events. For instructions on editing this file, see Editing the log messages XML file.

Level	Severity	Purpose
EMERGENCY	0	System or service is unusable
ALERT	1	Action must be taken immediately
CRITICAL	2	Critical condition, similar to ALERT, but not necessarily requiring an immediate action
ERROR	3	An error condition that does not necessarily impact the ability of the service to continue to function
WARN	4	A warning about a bad condition, which is not necessarily an error
NOTICE	5	Notification about interesting system-level conditions, which are not errors
INFO	6	Information about internal flows or application or per-request information, not system-wide information

REVIEW DRAFT - CISCO CONFIDENTIAL

VoiceXML logs

About voiceXML logs

VoiceXML logs record Unified CVP system-specific information, such as heartbeat status. By default, VoiceXML logs are stored in the \Cisco\CVP\logs\VXML folder.

The table that follows describes the logs that VoiceXML creates.

Log Type	Log Name	Description
Infrastructure	CVP.<timestamp>.log	Unified CVP logs for the VoiceXML Service: This includes Notice, Info, and Debug logs. With Debug turned on, you can also see Call, Message, and Method trace types of logs.
Error messages	Error.<timestamp>.log	Unified CVP error log: This contains any error that Unified CVP Services and message layer has generated.

Correlate unified CVP/Unified ICME logs with VXML server logs

When using the VXML Server option in the Unified CVP solution, you can correlate Unified CVP/Unified ICME logs with VoiceXML logs. Pass the Call ID to the VXML Server by URL. Building upon the URL used in the previous example, the URL is as follows:
http://10.78.26.28:7000/CVP/Server?application=Chapter1_HelloWorld&callid=XXXXX-XXXXX-XXXXXX-XXXXXX

Note Unified CVP VXML Server (by default) receives callid (which contains the call GUID), _dnis, and _ani as session variables in comprehensive mode even if the variables are not configured as parameters in the ToExtVXML array. If the variables are configured in ToExtVXML then those values are used. These variables are available to VXML applications as session variables, and displayed in the Unified CVP VXML Server log. This change is backwards compatible with the following script. That is, if you have added the following script, you do not change it. However, if you remove this script, you save an estimated 40 bytes of ECC variable space.

The following procedure describes how to configure logging.

Procedure

In the Unified ICME script, use the formula editor to set ToExtVXML[1]. Set the value of ToExtVXML[1] variable to `concatenate("callid=",Call.user.media.id)`

REVIEW DRAFT - CISCO CONFIDENTIAL

Note

- Always include Call ID when sending the call to the Unified CVP VXML Server using the Comprehensive call flow model. The Call ID can also be used in Unified CVP VXML Server (standalone) solutions.
- When you concatenate multiple values, use a comma for the delimiter; for example, concatenate("ICMInfoKeys=",Call.RouterCallKey,"-",Call.RouterCallDay,"-",

  Call.RouterCallKeySequenceNumber).
- See Passing Information to the External VoiceXML.

About Unified CVP VXML Server logs

Unified CVP VXML Server logs record interactions between the Unified CVP VXML Server and the server that hosts the VoiceXML applications. By default, Unified CVP VXML Server logs are stored in the /Cisco/CVP/VXMLServer/logs folder.

The following table describes the logs that Unified CVP VXML Server creates:

Log Type	Log Name	Description
Unified CVP VXML Server Call Log	call_log<timestamp>.txt	Records a single line for every application visit handled by the Unified CVP VXML Server.
Unified CVP VXML Server Call Error Log	error_log<timestamp>.txt	Records errors that occur outside the realm of a particular application.
Unified CVP VXML Server Administration History Log	admin_history<timestamp>.txt	Records information from Unified CVP VXML Server administration scripts.

The Unified CVP VXML Server Call Error Log contains the following error codes:

- Error Code 40 -- System Unavailable

  This is returned if the application server is unavailable (shutdown, network connection disabled, and so forth)
- Error Code 41 -- App Error

  This is returned if some Unified CVP VXML Server-specific error occurs (For example, java exception).
- Error Code 42 -- App Hangup

  This is returned to Unified CVP if the Hang Up element is used without being preceded by a Subdialog_Return element.

  Note If the application is configured correctly, this does not occur.
- Error Code 43 -- Suspended

  This is returned if the Unified CVP VXML Server application is suspended.

REVIEW DRAFT - CISCO CONFIDENTIAL

- Error Code 44 -- No Session Error

  This is returned when an emergency error occurs (for example, an application is called that has not been loaded in the Unified CVP VXML Server application).

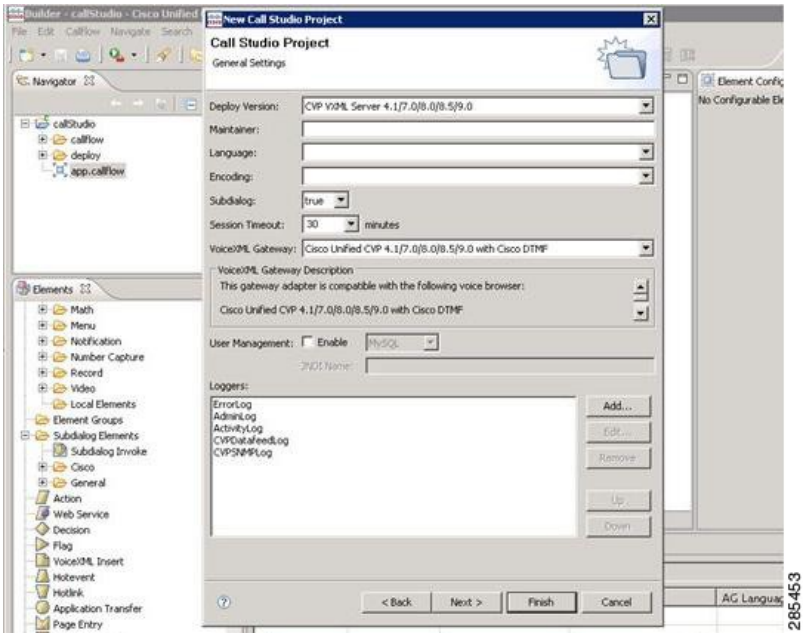
- Error Code 45 -- Bad Fetch

  This is returned when the Unified CVP VXML Server encounters a bad fetch situation. This code is returned when a .wav file or an external grammar file is not found.

About voiceXML application logging

The Unified CVP VXML Server creates several logs for each individual VoiceXML application. By default, these application logs - with the exception of CVPDatafeedLog and CVPSNMPLog - are stored in the /Cisco/CVP/VXMLServer/applications/<NAME of APPLICATION>/logs folder.

Configure these logs using Call Studio:



Note See Element Specifications for Cisco Unified CVP Unified CVP VXML Server and Unified Call Studio for information about configuring loggers.

The following table describes the logs that are created for each application:

Application Logger Type	Log Name	Description
ActivityLog	activity_log<timestamp>.txt **Note** Log files are stored in the ActivityLog directory.	Records all application activity, showing which elements are entered and exited during a call. Default setting: on

REVIEW DRAFT - CISCO CONFIDENTIAL

Application Logger Type	Log Name	Description
ErrorLog	error_log<timestamp>.txt **Note** Log files are stored in the ErrorLog directory.	Records all error messages for the application. Default setting: on
AdminLog	admin_history<timestamp>.txt **Note** Log files are stored in the AdminLog directory.	Records information from application-specific administration scripts. Default setting: on
CVPDatafeedLog	CVPDatafeed.log. **Note** This log is stored in /Cisco/CVP/logs/VXML folder.	Listens for logging events and provides Unified CVP VXML Server and VoiceXML Service data to the Unified CVP Reporting Server. The Unified CVP Reporting Server stores this information in a reporting database so that it is available for later review. One CVPDatafeedLog is created per application. Default setting: on **Note** The VoiceXML Service can be started by adding this logger in the VoiceXML application.
CVPSNMPLog	CVPSNMP.log. **Note** This log is stored in /Cisco/CVP/logs/VXML folder.	Listens for a set of events and sends information about these events to the SNMP log, Syslog, or Unified CVP log. Default setting: on
DebugLog	debug_log<timestamp>.txt. **Note** Log files are stored in the DebugLog directory.	Creates a single file per call that contains all HTTP requests and responses that occurred between a IOS Gateway and Unified CVP VXML Server during the call session. Default setting: off

About event statistics

You can monitor the following statistics through the Operations Console Control Center:

- Device statistics
- Infrastructure statistics
- ICM Service call statistics
- IVR Service call statistics

REVIEW DRAFT - CISCO CONFIDENTIAL

- SIP Service call statistics
- Gateway statistics
- VXML Server statistics
- Reporting Server statistics

Infrastructure statistics

Unified CVP infrastructure statistics include realtime and interval data on the Java Virtual Machine (JVM), threading, and Licensing.

You can access these statistics by choosing Control Center from the System menu and then selecting a device. See the Operations Console topic *Viewing Infrastructure Statistics* for more information.

Access infrastructure statistics either by:

- Selecting **System** > **Control Center**, selecting a device, clicking the Statistics icon in the toolbar, and then selecting the **Infrastructure** tab.
- Selecting a device type from the **Device Management** menu, selecting a device, clicking the Statistics icon in the toolbar, and then selecting the **Infrastructure** tab.

The following table describes Licensing statistics.

Table 3: Licensing Statistics

Statistic	Description
Realtime Statistics	
Port Licenses Available	The number of port licenses available for the processing of new calls. Exactly one port license is used per call, independent of the call's traversal through the individual Call Server services.
Current Port Licenses in Use	The number of port licenses currently in use on the Call Server. One port license is used per call, independent of the call's traversal of the individual Call Server services.
Current Port Licenses State	There are four threshold levels of port license usage: safe, warning, critical and failure. An administrator may set the required percentage of port licenses in use needed to reach a given threshold level, with the exception of the failure level which is reached when the number of ports checked out is equal to the number of licenses ports.
Interval Statistics	
Start Time	The time the system started collecting statistics for the current interval.

REVIEW DRAFT - CISCO CONFIDENTIAL

Statistic	Description
Duration Elapsed	The amount of time that has elapsed since the start time in the current interval.
Interval Duration	The interval at which statistics are collected. The default value is 30 minutes.
Total New Port License Requests	The number of port license checkout requests made in the current interval. For each port license checkout request, this metric is increased by one, regardless of whether if checks out a new port license.
Average License Requests/Minute	The average number of port license checkout requests made per minute in the current interval. This metric is calculated by dividing the port license requests metric by the number of minutes elapsed in the current interval.
Maximum Port Licenses Used	The maximum number of port licenses used during this time interval.
Aggregate Statistics	
Start Time	The time the service started collecting statistics.
Duration Elapsed	The amount of time that has elapsed since the service start time.
Total New Port License Requests	The number of port license checkout requests made since the system was started. For each port license checkout, this metric is increased by one, regardless of whether if checks out a new port license.
Average License Requests /Minute	The average number of port license checkout requests made per minute since the system was started. This metric is calculated by dividing the aggregate port license requests metric by the number of minutes elapsed since the system was started.
Peak Port Licenses Used	The peak number of simultaneous port licenses used since the start of the system. When a port checkout occurs, this metric is set to the current port licenses in use metric if that value is greater than this metric's current peak value.
Total Denied Port License Requests	The number of port license checkout requests that were denied since the start of the system. A port license checkout request is denied if the number of port licenses checked out at the time of the request is equal to the total number of port license available. When a port license checkout is denied, the call does not receive regular treatment (the caller may hear a busy tone or an error message).

REVIEW DRAFT - CISCO CONFIDENTIAL

The following table describes thread pool system statistics. The thread pool is a cache of threads, used by Unified CVP components only, for processing relatively short tasks. Using a thread pool eliminates the waste of resources encountered when rapidly creating and destroying threads for these types of tasks.

Table 4: Thread Pool Realtime Statistics

Statistic	Description
Realtime Statistics	
Idle Threads	The number of idle threads waiting for some work
Running Threads	The number of running thread pool threads currently processing some work.
Core Threads	The number of thread pool threads that will never be destroyed no matter how long they remain idle
Maximum Threads	The maximum number of thread pool threads that will ever exist simultaneously
Peak Threads Used	The peak number of thread pool threads ever simultaneously tasked with some work to process

The following table describes Java Virtual Machine statistics.

Table 5: Java Virtual Machine (JVM) Realtime Statistics

Statistic	Description
Realtime Statistics	
Peak Memory Usage	The greatest amount of memory used by the Java Virtual machine since startup. The number reported is in megabytes and indicates the peak amount of memory ever used simultaneously by this Java Virtual Machine.
Current Memory Usage	The current number of megabytes of memory used by the Java Virtual Machine.
Total Memory	The amount of memory in megabytes available to the Java Virtual Machine. The number indicates how much system memory is available for the Java Virtual Machine.
Available Memory	The amount of available memory in the Java Virtual Machine. The number reported is in megabytes and indicates how much of the current system memory claimed by the Java Virtual Machine is not currently being used.

REVIEW DRAFT - CISCO CONFIDENTIAL

Statistic	Description
Threads in Use	The number of threads currently in use in the Java Virtual Machine. This number includes all of the Unified CVP standalone and thread pool threads, and those threads created by the Web Application Server running within the same JVM.
Peak Threads in Use	The greatest amount of threads used simultaneously in the Java Virtual Machine since startup. The peak number of threads used by thw Java Virtual Machine includes all Unified CVP standalone and thread pool threads, and threads created by the Web Application Server running within the same JVM.
Uptime	The time that the Java Virtual Machine has been running. This time is measured in hh:mm:ss and shows the amount of elapsed time since the Java Virtual Machine process began.

ICM service call statistics

The ICM Service call statistics include data on calls currently being processed by the ICM service, new calls received during a specified interval, and total calls processed since start time.

Access ICM Service statistics either by:

- Selecting **System** > **Control Center**, selecting a CVP Call Server, clicking the **Statistics** icon in the toolbar, and then selecting the **ICM** tab.
- Selecting **Device Management** > **CVP Call Server**, selecting a Call Server, clicking the **Statistics** icon in the toolbar, and then selecting the **ICM** tab.

The following table describes ICM Service call statistics.

Table 6: ICM Service Call Statistics

Statistic	Description
Realtime Statistics	
Active Calls	The current number of calls being serviced by the Unified Intelligent Contact Management (Unified ICM) Server for a Unified CVP Call Server. This value represents the calls currently being serviced by the Unified ICM for the Unified CVP Call Server for follow-on routing to a Contact Center agent.
Active SIP Call Legs	The ICM Server can accept VoIP calls that originate using either the Session Initiation Protocol (SIP). Active SIP Call Legs indicates the number of calls received by the Unified ICM Server from the Unified CVP Call Server using the SIP protocol.

REVIEW DRAFT - CISCO CONFIDENTIAL

Statistic	Description
Active VRU Call Legs	The current number of calls receiving Voice Response Unit (VRU) treatment from the Unified ICM Server. The VRU treatment includes playing pre-recorded messages, asking for Caller Entered Digits (CED) or Speech Recognition Techniques to understand the customer request.
Active ICM Lookup Requests	Calls originating from an external Unified CVP VXML Server need call routing instructions from the Unified ICM Server. Active Lookup Requests indicates the current number of external Unified CVP VXML Server call routing requests sent to the ICM Server.
Active Basic Service Video Calls Offered	The current number of simultaneous basic service video calls being processed by theUnified ICM service where video capability was offered.
Active Basic Service Video Calls Accepted	The current number of simultaneous calls that were accepted as basic service video calls and are being processed by the Unified ICM service.
Interval Statistics	
Start Time	The time at which the current interval began.
Duration Elapsed	The amount of time that has elapsed since the current interval began.
Interval Duration	The time interval at which statistics are collected. The default value is 30 minutes.
New Calls	The number of new calls received by the Unified ICM application for follow-on Voice Response Unit (VRU) treatment and routing to a Contact Center agent during the current interval.
SIP Call Legs	The Unified ICM application accepts VoIP calls that originate from the Session Initiation Protocol (SIP) Protocol. Interval SIP Call Legs is an interval specific snapshot metric indicating the number of calls received by the ICM application from SIP during the current interval.
VRU Call Legs	The number of calls receiving VRU treatment from the Unified ICM application. The VRU treatment includes playing pre-recorded messages, asking for Caller Entered Digits (CED) or speech recognition techniques to understand the customer request during the current interval.
ICM Lookup Requests	Calls originating in an external Unified CVP VXML Server need call routing instructions from the Unified ICM application. Interval Lookup Requests is an interval specific metric indicating the number of external Unified CVP VXML Server call routing requests sent to the Unified ICM application during the current interval.
Basic Service Video Calls Offered	The number of offered basic service video calls processed by the Unified ICM service during the current interval.

REVIEW DRAFT - CISCO CONFIDENTIAL

Statistic	Description
Basic Service Video Calls Accepted	The number of basic service video calls accepted and processed by the Unified ICM service during the current interval.
Aggregate Statistics	
Start Time	The time the service started collecting statistics.
Duration Elapsed	The amount of time that has elapsed since the service start time.
Total Calls	The total number of new calls received by the Unified ICM application for follow-on VRU treatment and routing to a Contact Center agent since system start time.
Total SIP Call Legs	The Unified ICM application can accept VoIP calls that originate from the Session Initiation Protocol (SIP) Protocol. Total SIP Switch Legs is a metric indicating the number of calls received by the ICM application by SIP since system start time.
Total VRU Call Legs	The number of calls that have received VRU treatment from the Unified ICM application since system start time. The VRU treatment includes playing pre-recorded messages, asking for Caller Entered Digits (CED) or Speech Recognition Techniques to understand the customer request.
Total ICM Lookup Requests	Calls originating in an external Unified CVP VXML Server need call routing instructions from the Unified ICM application. Total Lookup Requests is a metric indicating the total number of external Unified CVP VXML Server call routing requests sent to the Unified ICM application since system start time.
Total Basic Service Video Calls Offered	The number of newly offered basic service video calls processed by the Unified ICM service since system start time.
Total Basic Service Video Calls Accepted	The number of new basic service video calls accepted and processed by the Unified ICM service since system start time.

IVR service call statistics

The IVR service call statistics include data on calls currently being processed by the IVR service, new calls received during a specified interval, and total calls processed since the IVR service started.

Access IVR Service statistics either by:

- Selecting **System** > **Control Center**, selecting a Call Server, clicking the **Statistics** icon in the toolbar, and then selecting the **IVR** tab.
- Selecting **Device Management** > **CVP Call Server**, selecting a Call Server, clicking the **Statistics** icon in the toolbar, and then selecting the **IVR** tab.

REVIEW DRAFT - CISCO CONFIDENTIAL

The following table describes the IVR Service call statistics.

Table 7: IVR Service Call Statistics

Statistic	Description
Realtime Call Statistics	
Active Calls	The number of active calls being serviced by the IVR service.
Active HTTP Requests	The number of active HTTP requests being serviced by the IVR service.
Interval Statistics	
Start Time	The time the system starts collecting statistics for the current interval.
Duration Elapsed	The amount of time that has elapsed since the start time in the current interval.
Interval Duration	The interval at which statistics are collected. The default value is 30 minutes.
Peak Active Calls	Maximum number of active calls handled by the IVR service simultaneously.
New Calls	Metric that counts the number of New Call requests received from the IOS Gateway or the CVP H323 Service. A New Call includes the Switch leg of the call and the IVR leg of the call. This metric counts the number of New Call Requests received by the IVR Service.
Calls Finished	Metric that counts the number of Unified CVP Calls that have finished during this interval. A Call, for the purpose of the Call Finished metric, includes both the Switch leg and the IVR leg of the Unified CVP call. When both legs of the call are finished, the *Calls Finished* metric increases.
Average Call Latency	The average amount of time in milliseconds that it takes the IVR Service to process a New Call or Call Result Request.
Maximum Call Latency	The maximum amount of time in milliseconds that it has taken for the IVR Service to process a New Call Request or a Request Instruction Request.
Minimum Call Latency	The minimum amount of time in milliseconds it took for the IVR Service to process a New Call Request or a Request Instruction Request.

REVIEW DRAFT - CISCO CONFIDENTIAL

Statistic	Description
Peak Active HTTP Requests	Active HTTP Requests is a metric that indicates the current number of simultaneous HTTP requests being processed by the IVR Service. Peak Active Requests is a metric that represents the maximum simultaneous HTTP requests being processed by the IVR Service.
Total HTTP Requests	The number of HTTP Requests received from a client by the IVR Service.
Average HTTP Requests/second	The average number of HTTP Requests the IVR Service receives per second.
Peak Active HTTP Requests/second	HTTP Requests per Second is a metric that represents the number of HTTP Requests the IVR Service receives each second from all clients. Peak HTTP Requests per Second is the maximum number of HTTP Requests that were processed by the IVR Service in any given second. This is also known as high water marking.
Aggregate Statistics	
Start Time	The time the service started collecting statistics.
Duration Elapsed	The amount of time that has elapsed since the service start time.
Total New Calls	Metric that counts the number of New Call requests received from the IOS GatewayUsing Unified ICME Warm. A New Call includes the Switch leg of the call and the IVR leg of the call. Total New Calls is a metric that represents the number of new calls received by the IVR Service since system startup.
Peak Active Calls	The maximum number of simultaneous calls processed by the IVR Service since the service started.
Total HTTP Requests	Metric that represents the number of HTTP Requests received from all clients. This metric is the total number of HTTP Requests received by the IVR Service since system startup.
Peak Active HTTP Requests	Peak Active HTTP Requests is a metric that indicates the current number of simultaneous HTTP requests processed by the IVR Service. Maximum number of active HTTP requests processed at the same time since the IVR service started. This is also known as high water marking.
Total Agent Video Pushes	The number of videos pushed by agents since system start time.
Total Agent Initiated Recordings	The number of video recordings by agents since system start time.

REVIEW DRAFT - CISCO CONFIDENTIAL

Statistic	Description
Total Agent VCR Control Invocations	The number of video VCR controls invoked by agents since system start time.

SIP service call statistics

The SIP service call statistics include data on calls currently being processed by the SIP service, new calls received during a specified interval, and total calls processed since the SIP service started.

Access SIP Service statistics either by:

- Selecting **System** > **Control Center**, selecting a Call Server, clicking the **Statistics** icon in the toolbar, and then selecting the **SIP** tab.
- Selecting **Device Management** > **CVP Call Server**, selecting a Call Server, clicking the **Statistics** icon in the toolbar, and then selecting the **SIP** tab.

The following table describes the SIP Service call statistics.

Table 8: SIP Service Call Statistics

Statistic	Description
Realtime Statistics	
Total Call Legs	The number of SIP call legs being handled by the SIP service. A call leg is also known as a SIP dialog. The metric includes incoming, outgoing and ringtone type call legs. For each active call in the SIP service, there is an incoming call leg, and an outgoing call leg to the destination of the transfer label.
Active Basic Service Video Calls Offered	The number of basic service video calls in progress where video capability was offered.
Active Basic Service Video Calls Answered	The number of basic service video calls in progress where video capability was answered.
Interval Statistics	
Start Time	The time the system started collecting statistics.
Duration Elapsed	The amount of time that has elapsed since the start time.
Interval Duration	The interval at which statistics are collected. The default value is 30 minutes.
New Calls	The number of SIP Invite messages received by Unified CVP in the current interval. It includes the failed calls, and calls rejected due to the SIP service being out of service.

REVIEW DRAFT - CISCO CONFIDENTIAL

Statistic	Description
Connects Received	The number of CONNECT messages received by SIP service to perform a call Transfer, in the last statistics aggregation interval. Connects Received includes the regular Unified CVP transfers, and Refer transfers. Any label coming from the ICM service is a CONNECT message, whether it is a label to send to the VRU or a label to transfer to an agent.
Avg Latency Connect to Answer	The period of time between the CONNECT from ICM and when the call is answered. The metric includes the average latency computation for the calls that have been answered in the last statistics aggregation interval.
Failed SIP Transfers (Pre-Dialog)	The number of failed SIP transfers since system start time. When Unified CVP attempts to make a transfer to the first destination of the call, it sends the initial INVITE request to set up the caller with the ICM routed destination label. The metric does not include rejections due to the SIP Service not running. The metric includes failed transfers that were made after a label was returned from the ICM Server in a CONNECT message.
Failed SIP Transfers (Post-Dialog)	The number of failed re-invite requests on either the inbound or outbound legs of the call during the interval. After a SIP dialog is established, re-INVITE messages perform transfers. Re-invite requests can originate from the endpoints or else be initiated by a Unified CVP transfer from the Unified ICME script. This counter includes failures for both kinds of re-invite requests.
Basic Service Video Calls Offered	The number of basic service video calls offered in the current interval.
Basic Service Video Calls Answered	The number of basic service video calls answered in the current interval.
Aggregate Statistics	
Start Time	The time the service started collecting statistics.
Duration Elapsed	The amount of time that has elapsed since the service start time.
Total New Calls	The number of SIP Invite messages received by Unified CVP since system start time. It includes the failed calls, and calls rejected due to the SIP service being out of service.
Connects Received	The number of Connect messages received by SIP service to perform a Unified CVP Transfer, since system start time. Connects Received includes the regular Unified CVP transfers, and Refer transfers. Any label coming from the ICM service is a Connect message, whether it is a label to send to the VRU or a label to transfer to an agent.

REVIEW DRAFT - CISCO CONFIDENTIAL

Statistic	Description
Avg Latency Connect to Answer	The time between the Connect from ICM and when the call is answered. The metric includes the average latency computation for all the calls that have been answered since system start up time.
Failed SIP Transfers (Pre-Dialog)	The total number of failed transfers on the first CVP transfer since system start time. A SIP dialog is established after the first CVP transfer finishes. The metric does not include rejections due to SIP being out of service. The metric includes failed transfers that are after a label is returned from the ICM in a CONNECT message.
Failed SIP Transfers (Post-Dialog)	The number of failed re-invite requests on the inbound or outbound legs of the call since start time. After a SIP dialog is established, re-INVITE messages perform transfers. Re-invite requests can originate from the endpoints or initiated by a Unified CVP transfer from the Unified ICME script. This counter includes failures for re-invite requests.
Total Basic Service Video Calls Offered	The number of basic service video calls offered since system start time.
Total Basic Service Video Calls Answered	The number of basic service video calls answered since system start time.

Gateway statistics

Gateway statistics include the number of active calls, available memory, and CPU utilization.

Procedure

To obtain gateway statistics:

Procedure

Step 1 Choose **System** > **Control Center**.

Step 2 Select the **Device Type** tab in the left pane, then select **Gateways**.
Gateways are listed in the right pane.

Step 3 Select the gateway by clicking on its link under the Hostname column.
the Edit Gateway Configuration window opens.

Step 4 Select the Statistics icon in the toolbar.

REVIEW DRAFT - CISCO CONFIDENTIAL

What to Do Next

See *Administration Guide for Cisco Unified Customer Voice Portal* for device statistics.

Gateway statistics

The following table describes gateway statistics.

Statistic	Description
Active Calls	Number of currently active calls handled by the gateway. For example, Total call-legs: 0 no active calls

Free Memory	Free memory, for example:
	`Processor memory free: 82%`
	`I/O memory free: 79%`

CPU Utilization	CPU utilization, for example: `CPU utilization for five seconds: 3%/3%; one minute: 3%; five minutes: 4%`

Trunk utilization reporting

You can configure IOS gateways to report on truck utilization. The configuration involves two pieces:

- Configuring the Call Server using the Operations Console to request reporting from a given gateway.
- Configuring the gateway to respond to trunk utilization reporting requests.

To configure Unified CVP to provide trunk utilization reporting, complete these steps:

1. In the Operations Console, select: **Device Management** > **Call Server** > **ICM (tab)** > **Advanced Configuration**..
2. Under *Trunk Utilization*, select **Enable Gateway Trunk Reporting**
3. In the same section, associate the gateway(s) that you want to send truck information to the Call Server.
4. Add the following configuration to the gateway configuration:

```
voice class resource-group 1
resource cpu 1-min-avg threshold high 80 low 60
resource ds0
resource dsp
resource mem total-mem
periodic-report interval 30

sip-ua
rai target ipv4:10.86.129.11 resource-group 1
rai target ipv4:10.86.129.24 resource-group 1
```

REVIEW DRAFT - CISCO CONFIDENTIAL

RAI information on SIP OPTIONS (CVP server group heartbeats)

If a resource availability indicator (RAI) is desired on SIP OPTIONS, the option override host setting can be used with server group heartbeating. When one or more Unified CVPs are sending OPTIONS heartbeats to the gateway, RAI trunk utilization information is not normally sent in the 200 OK response, unless an RAI target is configured.

CLI like the following can be added in IOS to have RAI information sent to CVP in the response:

```
sip-ua
rai target dns:cvp.cisco.com resource-group 1
```

Note Trunk Utilization data is only written to the Unified CVP database when RAI OPTIONS are sent from the gateway to Unified CVP targets. When Unified CVP is using server group heartbeats to the gateway, the RAI data in the response is only marks the element as UP or DOWN (overloaded resources) in the server group.

Unified CVP VXML server statistics

The Operations Console displays realtime, interval, and aggregate Unified CVP VXML server statistics.

Access Unified CVP VXML server statistics either by:

- Selecting **System** > **Control Center**, selecting a Unified CVP VXML server, and then clicking the Statistics icon in the toolbar.
- Selecting **Device Management** > **VXML Server** (or Unified CVP VXML server (Standalone)), selecting a Unified CVP VXML server, and then clicking the Statistics icon in the toolbar.

The following table describes the statistics reported by the Unified CVP VXML server.

Table 9: Unified CVP VXML server Statistics

Statistic	Description
Real Time Statistics	
Active Sessions	The number of current sessions being handled by the Unified CVP VXML server.
Active ICM Lookup Requests	The number of current ICM requests being handled by the Unified CVP VXML server.
Interval Statistics	
Start Time	The time when the current interval began.
Duration Elapsed	The time that has elapsed since the start time in the current interval.

REVIEW DRAFT - CISCO CONFIDENTIAL

Statistic	Description
Interval Duration	The interval at which statistics are collected. The default is 30 minutes.
Sessions	The number of sessions in the Unified CVP VXML server.
Reporting Events	The number of events sent to the Reporting Server from the Unified CVP VXML server.
ICM Lookup Requests	The number of requests from the Unified CVP VXML server to the ICM Service.
ICM Lookup Responses	The number of responses to failed and successful ICM Lookup Requests that the ICM Service sends to the Unified CVP VXML server. In the case that multiple response messages are sent back to the Unified CVP VXML server to a single request, this metric increases per response message from the ICM Service.
ICM Lookup Successes	The number of successful requests from the Unified CVP VXML server to the ICM Service in the current interval.
ICM Lookup Failures	The number of requests from the Unified CVP VXML server to the ICM Service in the current interval. This metric increases when an ICM failed message is received or when the Unified CVP VXML server generates the failed message.
Aggregate Statistics	
Start Time	The time when the current interval has begins.
Duration Elapsed	The time since the current interval began.
Total Sessions	The number of sessions in the Unified CVP VXML server since startup.
Total Reporting Events	The number of reporting events sent from the Unified CVP VXML server since startup.
Total ICM Lookup Requests	The number of requests from the Unified CVP VXML server to the ICM Service. For each ICM lookup request (successful or failed), this metric increases by one.
Total ICM Lookup Responses	The number of responses the ICM Service has sent to the Unified CVP VXML server since startup. For each ICM lookup request (successful or failed), this metric increases by one. When multiple response messages are sent back to the Unified CVP VXML server to a single request, this metric increases per response message from the ICM Service.

REVIEW DRAFT - CISCO CONFIDENTIAL

Statistic	Description
Total ICM Lookup Success	The number of requests from the Unified CVP VXML server to the ICM Service since startup. For each ICM lookup request that succeeded, this metric increases one.
Total ICM Lookup Failures	The number of requests from the Unified CVP VXML server to the ICM Service since startup. For each ICM lookup request that failed, this metric increases by one. This metric will increase when an ICM failed message was received or in the case the Unified CVP VXML server generates a failed message.

See the *Administration Guide for Cisco Unified Customer Voice Portal* for Infrastructure Statistics and Device Statistics.

Reporting server statistics

Reporting Server statistics include the total number of events received from the IVR, SIP, and VoiceXML services.

Access Reporting Server statistics either by:

- Selecting **System** > **Control Center**, selecting a Reporting Server, and then clicking the **Statistics** icon in the toolbar.
- Selecting **Device Management** > **CVP Reporting Server**, selecting a Reporting Server, and then clicking the Statistics icon in the toolbar.

The following table describes the Reporting Server statistics.

Table 10: Reporting Server Statistics

Statistic	Description
Interval Statistics	
Start Time	The time the system began collecting statistics.
Duration Elapsed	The amount of time that has elapsed since the start time.
Interval Duration	The interval at which statistics are collected. The default value is 30 minutes.
VXML Events Received	The number of reporting events received from the VoiceXML Service. For each reporting event received from the VoiceXML Service, this metric increases by one.
SIP Events Received	The number of reporting events received from the SIP Service during this interval. For each reporting event received from the SIP Service, this metric increases by one.

REVIEW DRAFT - CISCO CONFIDENTIAL

Statistic	Description
IVR Events Received	The number of reporting events received from the IVR service in the interval. For each reporting event received from the IVR service, this metric increases by one.
Database Writes	The number of writes to the database made by the Reporting server during the interval. For each write, this metric increases one.
Aggregate Statistics	
Start Time	The time the service started collecting statistics.
Duration Elapsed	The amount of time that has elapsed since the service start time.
VXML Events Received	The number of reporting events received from the VoiceXML Service since the service started. For each reporting event received from the VoiceXML Service, this metric increases by one.
SIP Events Received	The number of reporting events received from the SIP Service since the service started. For each reporting event received from the SIP Service, this metric increases by one.
IVR Events Received	The number of reporting events received from the IVR Service since the service started. For each event received, this metric increases by one.
Database Writes	The number of writes to the database made by the Reporting server during since startup. For each write, this metric increases by one.

Unified CVP SNMP-Raise/Clear mappings

The following log messages are SNMP-enabled by default. Administrators can define a unique alarm within their SNMP management station for all SNMP Raise events emitted by a system. These alarms are usually cleared automatically using one or more corresponding SNMP Clear events when the condition is resolved. The tables below list a mapping of Unified CVP SNMP Raise events with their corresponding SNMP Clears.

Note Raises are listed first, with their corresponding clears below them.

Table 11: Messaging Layer

Raise ID	Clear ID	Event Name
7		ADAPTER_INITIALIZATION_FAILURE
	8	ADAPTER_INITIALIZATION_SUCCESS

REVIEW DRAFT - CISCO CONFIDENTIAL

Raise ID	Clear ID	Event Name
9		PLUGIN_INITIALIZATION_FAILURE
	10	PLUGIN_INITIALIZATION_SUCCESS
15		SEND_QUEUE_THRESHOLD_REACHED
	20	SEND_QUEUE_SIZE_CLEAR

Table 12: Infrastructure

Raise ID	Clear ID	Event Name
9005		LICENSING
	1003	[AUDIT] "The system has started up."
9007		PORT_THRESHOLD
	9008	PORT_THRESHOLD
9014		SHUTDOWN
	1003	[AUDIT] "The system has started up."
	1004	[AUDIT] "The system has completely shutdown."
9016		SERVER_SETUP - "CCBUSNMPAgent Server setup failed because XXX"
	9015	SERVER_SETUP - "CCBUSNMPAgent Server setup on port YYY"
1011		HEARTBEATS_STOPPED - "Heartbeats from XXX stopped..."
	1014	RECEIVED_STATE_MSG - "StateManager: Subsystem [XXX] reported change to..."
1012		STATE_MANAGER_STARTUP_FAILURE
	1003	[AUDIT] "The system has started up."
1020		STARTUP
	1003	[AUDIT] "The system has started up."
1024		SERVLET_STARTUP

REVIEW DRAFT - CISCO CONFIDENTIAL

Raise ID	Clear ID	Event Name
	1003	[AUDIT] "The system has started up."
1025		START - "Could not start XXX due to: YYY"
	1003	[AUDIT] "The system has started up."
1033		START - "No Subsystems have been started..."
	1026	START - "All Subsystems have been started."
1035		LICENSE_EXPIRATION
	1003	[AUDIT] "The system has started up."

Table 13: Unified ICME

Raise ID	Clear ID	Event Name
2001		LOGMSG_ICM_SS_MSGBUS_SHUTDOWN
	2003	LOGMSG_ICM_SS_MSGBUS_ACTIVE
2002		LOGMSG_ICM_SS_PIM_SHUTDOWN
	2004	LOGMSG_ICM_SS_PIM_ACTIVE
2005		LOGMSG_ICM_SS_HEARTBEAT_FAILURE
	2012	LOGMSG_ICM_SS_INSERVICE_STATE
2006		LOGMSG_ICM_SS_STATE
	2012	LOGMSG_ICM_SS_INSERVICE_STATE

Table 14: Reporting

Raise ID	Clear ID	Event Name
4005		REPORTING_SS_ERROR_RAISE
	1026	START - "All Subsystems have been started."
4006		REPORTING_DB_PURGE_FAILED
	4007	REPORTING_DB_PURGE_COMPLETED

REVIEW DRAFT - CISCO CONFIDENTIAL

Raise ID	Clear ID	Event Name
4010		REPORTING_DB_BACKUP_FAILED
	4011	REPORTING_DB_BACKUP_COMPLETED
4014		REPORTING_DB_ALERT_MSG
	N/A	Not applicable
4017		REPORTING_DB_STARTING_PURGE
	4007	REPORTING_DB_PURGE_COMPLETED
	4009	REPORTING_DB_EMERGENCY_PURGE_COMPLETED
4018		REPORTING_DB_REMAINDER_DATA
	4019	REPORTING_DB_NO_REMAINDER_DATA

Table 15: IVR

Raise ID	Clear ID	Event Name
3014		VBCLIENT_REMOVED
	3013	VBCLIENT_ADDED
3027		VBCLIENT_SHUT_DOWN
	3026	VBCLIENT_RESTARTED
3021		VBSERVLET_STATE_CHANGED
	3022	VBSERVLET_STATE_IN_SERVICE
3002		STATE_CHANGED
	3001	STATE_CHANGED_IN_SERVICE
3000		SHUTDOWN_NOTICE
	3001	STATE_CHANGED_IN_SERVICE

REVIEW DRAFT - CISCO CONFIDENTIAL

Table 16: SIP

Raise ID	Clear ID	Event Name
5001		SS_STATE; The SIP subsystem changed state to something other than the *in service* state.
	5002	SS_STATE; The SIP subsystem changed state to the *in service* state.

Table 17: VoiceXML

Raise ID	Clear ID	Event Name
6012		VXML_SERVER_APP_SHUTDOWN_ALERT
	6011	VXML_SERVER_APP_STARTUP_CLEAR
6013		VXML_SERVER_APPADMIN_ERROR
	1003	[AUDIT] "The system has started up."
	1004	[AUDIT] "The system has completely shutdown."
6014		VXML_SERVER_SYSTEM_ERROR
	1003	[AUDIT] "The system has started up."
	1004	[AUDIT] "The system has completely shutdown."
6024		VXML_LICENSE_ALERT
	6025	VXML_LICENSE_ALERT_CLEAR

Note VXML_LICENSE_ALERT is raised when the VXML Port license utilization exceeds 90% of the total deployed license ports and the VXML_LICENSE_ALERT_CLEAR is raised when the VXML port license utilization drops below 70% of the total deployed license ports.

REVIEW DRAFT - CISCO CONFIDENTIAL

INDEX

A

application logging, VoiceXML 18

C

call statistics 23, 25, 28
  ICM Service 23
  IVR service 25
  SIP Service 28
CLI (for WSM) 1, 2, 3, 6
  access the CLI 3
  create user 1
  overview 2
  various kinds of help for the CLI 6
configuring 13, 16
  logging 16
  logging and event notifications 13
CVPLogMessages.properties file 14
CVPLogMessages.xml file 14
  editing 14

E

event statistics 19
  viewing 19
events 13, 15, 35
  notifications, configuring 13
  severity levels for 15
  SNMP raise/clear 35
  using logs to interpret 13
exporting Operations Console certificate to a file 10

G

gateway 30
  statistics 30

I

ICM Service 23
  statistics 23
infrastructure statistics 20
  descriptions 20
IVR Service 25
  statistics 25

L

licensing 20
  statistics 20
log messages 14
  CVPLogMessages.xml 14
logging and event notifications, configuring 13
logs 13
  using to interpret events 13
logs, VXML Server 17

O

Operations Console 19
  viewing event statistics 19

R

recording Unified CVP system-specific information 16
Reporting Server 34
  statistics 34
resource properties file 14

S

severity 14, 15
  log messages 14
  of events 15

REVIEW DRAFT - CISCO CONFIDENTIAL

SIP Service call statistics 28
SNMP 35
raise/clear events 35
raise/clear mappings 35
statistics 20, 23, 25, 28, 30, 32, 34
gateway 30
ICM service 23
infrastructure 20
IVR Service 25
licensing 20
Reporting Server 34
SIP Service 28
thread pool 20
VXML Server 32
syslog, using 13
system statistics 20
licensing 20
thread pool 20

T

thread pool statistics 20

U

using 13
logs to interpret events 13
syslog 13

V

VoiceXML application logging 18
VoiceXML logs 16
VXML Server 32
statistics 32
VXML Server logs 16, 17
about 17
correlating Unified CVP/Unified ICME logs 16

W

Web Services Manager 1, 2
create user 1
overview 2