



## **Cisco Remote Silent Monitoring Installation and Administration Guide**

Release 9.0(1)

**October 12, 2012**

### **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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0809R)

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

*Cisco Remote Silent Monitoring Installation and Administration Guide*

© 2012 Cisco Systems, Inc. All rights reserved.

# C O N T E N T S

---

## CHAPTER 1

<b>System Overview</b>	1-1
RSM Overview	1-1
Call Flow	1-2
RSM Services	1-3
VLEngine	1-3
PhoneSim	1-3
Application Connectivity	1-4
RSM VLAN Configuration	1-4
Multi-site Deployment	1-6

---

## CHAPTER 2

<b>System Requirements</b>	2-1
Cisco Hardware and Software Requirements	2-1

---

## CHAPTER 3

<b>Pre-Installation Tasks</b>	3-1
Base System Provisioning	3-2
JTAPI Client Libraries Installation	3-3
Unified CM Services Enablement	3-3
Simulated Phones Configuration	3-3
Simphone Device Dependencies	3-4
Simphone Device Creation	3-6
Line DN to Simphone Device Association	3-7
Simphone BAT Tool Usage	3-8
Login Pool Simphone Setup	3-10

- RSM User Group Creation 3-11
- RSM Application User Creation 3-12
- Agent Phone Device Setup 3-13
- Supervisor Login Account Creation 3-13

---

CHAPTER 4

**Installation 4-1**

- Patch Installation 4-1
- RSM Server Installation 4-2
- Configuration Manager 4-2
  - Configuration Settings 4-3
- VLEngine and PhoneSim Services 4-6
- Directory Structure 4-7
- Port Numbers Used 4-8
- Environment Variables 4-8
- Security Settings 4-9
  - Host Level Security 4-9
  - Network Level Security 4-10

---

CHAPTER 5

**VRU Configuration 5-1**

- IP IVR Integration 5-2
  - Upload RSM Prompts 5-3
  - IP IVR Integration (non-Unified ICME) 5-4
  - IP IVR Integration (Unified ICME) 5-5
- CVP Integration 5-6
  - Upload RSM Prompts 5-6
  - CVP Call Flow Integration 5-7
  - Call Flow Deployment 5-8
  - Call Flow Troubleshooting 5-9

VXML Gateway Setup Notes 5-10

Disabling Supervisor Team Structure or User Authentication 5-11

---

**CHAPTER 6****RSM Services 6-1**

RSM Enable, Check, Restart 6-1

Removing RSM 6-2

IP IVR Removal 6-2

CVP Removal 6-3

RSM Application Removal 6-4

Unified ICME Removal 6-4

Unified CM Removal 6-5

---

**CHAPTER 7****Troubleshooting 7-1**

Log Files 7-1

General Call Flow Issues 7-2

VLEngine Runtime Issues 7-9

PhoneSim Runtime Issues 7-14

PhoneSim Log File Error Messages 7-15

Fatal Error Messages 7-22

---

**APPENDIX A****API Extensions A-1**

JSP Suffix A-1

VLEngine HTTP API A-2

checkUserCredentials.jsp A-2

canMonitorAgentID.jsp A-3

getCallToMonitor.jsp A-4

getConvoInfo.jsp A-6

getAgentList.jsp A-7

proxyMonitorAgentForVRU.jsp A-9

- determineAgentCluster A-10
- initiateMonitorAgent A-12
- testEngineServlet.jsp A-13
- PhoneSim HTTP API A-13
  - monitorAgent.jsp A-13

---

**APPENDIX B**

**Registry Keys B-1**

- Changing RSM Registry Keys B-2
- General Registry Keys B-3
  - Version B-3
  - NumClusterConfigs B-3
  - MaxNumRequests B-3
  - ProblemCallMinHolds B-4
  - ProblemCallMinDuration B-4
  - MaxStaleCallDuration B-4
  - SMTP\_HostName B-5
  - SMTP\_Port B-5
  - SMTP\_SenderEmailAddress B-5
  - SMTP\_ReceiverEmailAddress1 B-6
  - SMTP\_ReceiverEmailAddress2 B-6
  - SMTP\_ReceiverEmailAddress3 B-6
  - SMTP\_ReceiverEmailAddress4 B-7
  - VLEngine\_LogLevel B-7
  - PhoneSim\_LogLevel B-7
  - VLEngine\_HostDataIP B-8
  - VLEngine\_HTTPListenPort B-8
  - PhoneSim\_HTTPListenPort B-8
  - PhoneSim\_AudioEncoding B-9
  - PhoneSim\_DoHTTPChunkedTransfers B-9
  - PhoneSim\_AudioBufferLenToVRU B-9

PhoneSim_HostDataIP	B-10
CTIOS_TraceMask	B-10
CTIOS_AgentModeTraceMask	B-11
VLEngine_PassPrefix	B-11
Cluster Configuration Registry Keys	B-12
ClusterN_Name	B-12
ClusterN_MaxNumRequests	B-13
ClusterN_PeripheralID	B-13
ClusterN_JTAPI_UserName	B-13
ClusterN_JTAPI_Password	B-14
ClusterN_NumSimPhonesUsedForCTIOSAgentLogins	B-14
ClusterN_PhoneSim_StartMACRange	B-14
ClusterN_PhoneSim_StartLineNumRange	B-15
ClusterN_PhoneSim_SIPTransport	B-15
ClusterN_PhoneSim_CM1_HostName	B-15
ClusterN_PhoneSim_CM1_Port	B-16
ClusterN_PhoneSim_CM2_HostName	B-16
ClusterN_PhoneSim_CM2_Port	B-16
ClusterN_VLEngine_CM1_HostName	B-17
ClusterN_VLEngine_CM2_HostName	B-17
ClusterN_VLEngine_CTIOS1_HostName	B-17
ClusterN_VLEngine_CTIOS1_Port	B-18
ClusterN_VLEngine_CTIOS2_HostName	B-18
ClusterN_VLEngine_CTIOS2_Port	B-18
ClusterN_VLEngine_CTIOS21_HostName	B-19
ClusterN_VLEngine_CTIOS21_Port	B-19
ClusterN_VLEngine_CTIOS22_HostName	B-19
ClusterN_VLEngine_CTIOS22_Port	B-20
ClusterN_VLEngine_CTIOS31_HostName	B-20
ClusterN_VLEngine_CTIOS31_Port	B-20

ClusterN\_VLEngine\_CTIOS32\_HostName **B-21**  
ClusterN\_VLEngine\_CTIOS32\_Port **B-21**  
ClusterN\_VLEngine\_CTIOS41\_HostName **B-21**  
ClusterN\_VLEngine\_CTIOS41\_Port **B-22**  
ClusterN\_VLEngine\_CTIOS42\_HostName **B-22**  
ClusterN\_VLEngine\_CTIOS42\_Port **B-22**



# Preface

---

## Purpose

This document provides complete installation, configuration, and administration information for Cisco Remote Silent Monitoring, an advanced telephony application which allows for real-time, phone-based monitoring of agents in the Cisco Unified Communications Manager (Unified CM) environment.

## Audience

This document is intended to be read and used by system administrators who are proficient with Cisco's Unified Communications Manager, Unified CCE, CVP, and IP IVR, and who possess basic to intermediate administration and installation capabilities.

# Organization

The chapters in this guide are organized as follows:

<b>Chapter</b>	<b>Description</b>
<a href="#">Chapter 1. "System Overview"</a>	Provides an overview of RSM, from both a user and technical call flow level.
<a href="#">Chapter 2. "System Requirements"</a>	Lists the hardware and software system requirements for RSM installation.
<a href="#">Chapter 3. "Pre-Installation Tasks"</a>	Describes tasks that must be performed to target servers and Cisco environment before installation.
<a href="#">Chapter 4. "Installation"</a>	Describes how to install RSM from the installation CD. Security recommendations are also provided.
<a href="#">Chapter 5. "VRU Configuration"</a>	Describes RSM integration in both IP IVR and CVP VRU environments.
<a href="#">Chapter 6. "RSM Services"</a>	Describes how to enable, check, and restart the two RSM services, VLEngine and PhoneSim, as well as how to remove RSM.
<a href="#">Chapter 7. "Troubleshooting"</a>	Lists log files and describes case scenarios for troubleshooting issues.
<a href="#">Appendix A. "API Extensions"</a>	Lists APIs used by the VLEngine and PhoneSim.
<a href="#">Appendix B. "Registry Keys"</a>	Lists RSM configuration parameters, as stored in the Windows registry.

# Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

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

## Field Alerts and Field Notices

Note that Cisco products may be modified or key processes may be determined important. These are announced through use of the Cisco Field Alert and Cisco Field Notice mechanisms. You can register to receive Field Alerts and Field Notices through the Product Alert Tool on Cisco.com. This tool enables you to create a profile to receive announcements by selecting all products of interest.

Log into [www.cisco.com](http://www.cisco.com); then access the tool at:

<http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

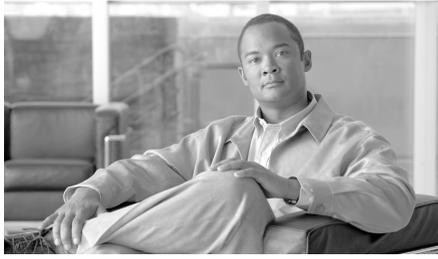
## Documentation Feedback

You can provide comments about this document by sending email to the following address:

[ccbu\\_docfeedback@cisco.com](mailto:ccbu_docfeedback@cisco.com)

We appreciate your comments.





# CHAPTER 1

## System Overview

---

This chapter describes the Remote Silent Monitoring (RSM) system from both a user-level and a technical call flow overview....

The following acronyms are used in this document:

- VRU—Voice Response Unit
- IVR—Interactive Voice Response
- CVP—Customer Voice Portal
- CTI OS—Computer Telephony Integration Object Server
- JTAPI—Java Telephony Application Programming Interface

## RSM Overview

The RSM application allows for real-time phone-based monitoring of agents in Cisco's Unified Contact Center Enterprise (Unified CCE) environment. The RSM platform is installed on a Windows operating system as a single server instance, and a separate call flow script is hosted on an IP IVR or CVP (VRU) platform.

When a supervisor dials into the VRU node via a VoIP or a plain old telephone service (POTS) phone:

- The incoming call is routed to the call flow script;
- The script requests services and data from the RSM server, as per the caller's input to system prompts;
- The script parses a response and provides data and voice stream to the caller.

RSM's system prompts allow for the selection of random, newest, or problem call monitoring modes. Callers can also select the specific agents they want to monitor based on the Agent ID (or Peripheral ID) of the agent, or they can select from a list of currently active agents.

## Call Flow

Call flow is distributed in the system via IP IVR and CVP scripts. These scripts provide core system functionality, and may be modified to better support specific system requirements.

**Note**

---

CRS Editor may be used to edit the IP IVR call flow script, and CVP Unified Call Studio may be used to edit the CVP call flow script.

---

Standard call flow script functionality is executed in the following manner:

- A caller dials in and is prompted to login to the system by entering their supervisor account agent ID and numeric password.
- The CTIOS API authenticates the login input, rejecting the attempt if the data is invalid. (The call flow script can use a different authentication back-end, or remove authentication altogether, as detailed in Chapter 5, VRU Integration.)
- Once logged in, the caller can request to listen to a specific agent on a real-time call.
- The Unified Communications Manager parses the request and instructs RSM to contact the agent's phone.
- RSM contacts the appropriate Unified Communications Manager via JTAPI.
- A simulated supervisor phone (a.k.a., simphone) on RSM calls the agent's phone, patches in, and streams the voice data back to the caller through the VRU node, in real-time one-way listening mode.

**Note**

---

If data is already being streamed to another caller for the selected agent, that same data stream is used, in lieu of creating a second data stream. Data is streamed only for agents currently being monitored.

---

# RSM Services

The RSM server runs two application instances, VLEngine and PhoneSim, which together provide RSM services to callers.

The VLEngine tracks the environment state and handles most of the requests from the call flow script (i.e., login authentication, agent listing, permissions required to monitor a call). The PhoneSim service manages the simulated phones.

## VLEngine

VLEngine runs on the Tomcat application server software, which provides servlet hosting. So, when a supervisor who is dialed into RSM interacts with the system, the call flow script makes HTTP requests for dynamic content from VLEngine servlets and then parses the appropriate output. Requests for static content, such as audio prompts, are also made to the VLEngine in certain cases (e.g., for the CVP VXML script, and for some parts of the IP IVR script through the use of its VXML VoiceBrowser step).

VLEngine monitors all Unified CCE events via CTI OS, keeping dynamic, real-time track of those agents currently handling calls, as well as the skillgroup membership of those agents. So, for example, if an agent was previously not on a call when the caller first dialed in, but is now handling a call, that agent's status is updated so they can now be monitored.



---

**Note**

The Apache Tomcat server bundled with RSM has been modified for optimum security; as such, no additional configuration must need be made to Tomcat.

---

## PhoneSim

PhoneSim device entries look and act exactly like hardware VoIP phones in the Unified Communications Manager environment; however, they are actually managed and controlled by the RSM server, mimicking a supervisor's VoIP phone, and providing supervisor dial-in functionality.

So, when a supervisor inputs a request through RSM to monitor an agent, the system infers that it is streaming the monitored agent's call data directly to the supervisor's VoIP phone. In reality, the call is streamed to the PhoneSim service, which proxies it to the VRU node for playback to the dialed-in supervisor.

**Note**

---

PhoneSim is a standalone service and, as such, is not installed as a component of a larger application server (e.g., Tomcat). It includes its own simple HTTP server for handling an HTTP API call to start the monitoring of an agent.

---

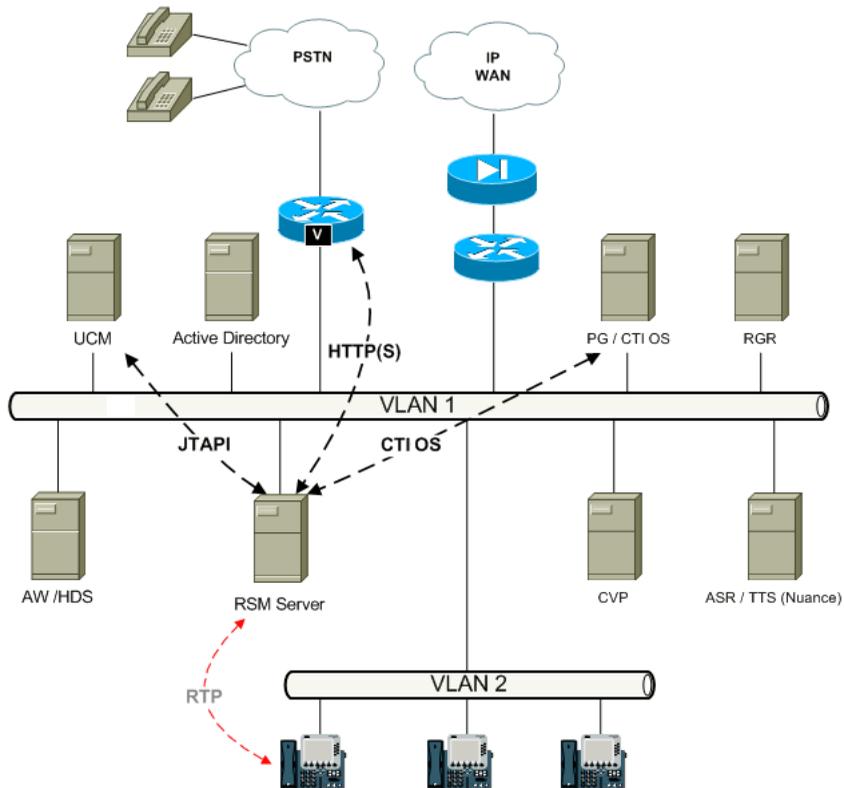
## Application Connectivity

The following diagrams illustrate the various configurations and connections that RSM has with the other contact center components.

### RSM VLAN Configuration

Figure 1-1 on page 1-5 illustrates the basic network connectivity of the RSM server across a typical VLAN network. The diagram illustrates the various protocol interfaces between RSM and the rest of the system, as described.

Figure 1-1 RSM VLAN Configuration



**HTTP(S)**—Carrier protocol for requests into RSM, in standard URL form:

- <http://rsmserver:8080/vlengine/checkUserCredentials?supervisorID=1101&pin=1234&outputFormat=plain>
- <http://rsmserver:8080/vlengine/canMonitorAgentID?supervisorID=1101&agentID=1001&outputFormat=vxml>

As can be deduced, the first request is for the **checkUserCredentials** API call, the second is for the **canMonitorAgentID** call. Request parameters are passed via the GET method, and the HTTP response is either plain text or encapsulated in VoiceXML (as per the API call and outputFormat parameter, if applicable).

**CTI OS**—The RSM server makes several connections to CTI OS. One is a monitor mode connection, which receives platform events. The other connections are agent mode connections used to retrieve the list of agents on the supervisor's team, and to authenticate supervisor logins when standard authentication is utilized.

**JTAPI**—Requests to monitor phones are made via JTAPI. This requires a JTAPI application user to be defined on each Unified Communications Manager cluster, and associate it with all agent phones.

**RTP**—When a dialed-in supervisor monitors an agent, there is a monitoring call-in-progress from the built-in bridge (BiB) of the agent's phone to the RSM server. Signaling data for the call is routed through the Unified Communications Manager similar to any other call, and RTP traffic flows between the agent's phone and the RSM server.

**Note**

---

ODBC-ODBC (SQL Database) connectivity is currently not deployed for use with RSM. Data retrieval from a Cisco Unified Intelligent Contact Management Enterprise (Unified ICME) database is therefore unavailable.

---

## Multi-site Deployment

Figures 1-2 through 1-4 illustrate the network connectivity required for a multi-site deployment of two RSM servers in a Unified ICME environment, connected via a central private WAN.

The example organization has a centralized datacenter in Atlanta, with PSTN gateways into three international cities, London, Austin, and Mumbai.

**Note**

---

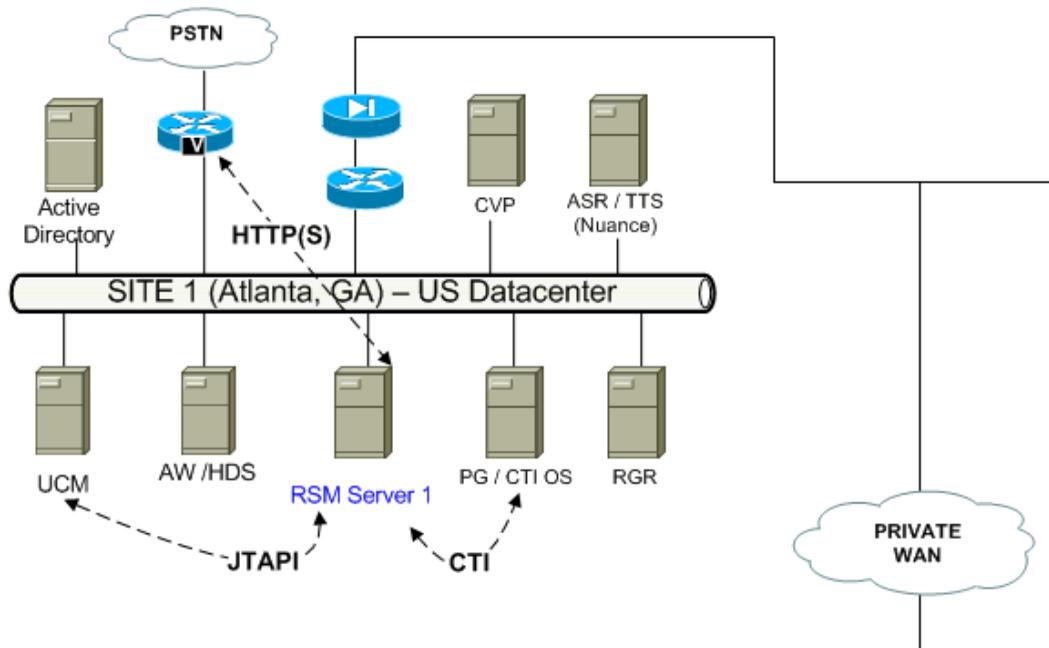
The model shown is for illustrative purposes only and is more complex than a typical RSM deployment.

---

As shown in Figure 1-2, the RSM server at the Atlanta datacenter handles monitoring requests from U.S.-based PSTN callers and personnel.

A single Active Directory server cluster serves as an LDAP directory service at the Atlanta datacenter.

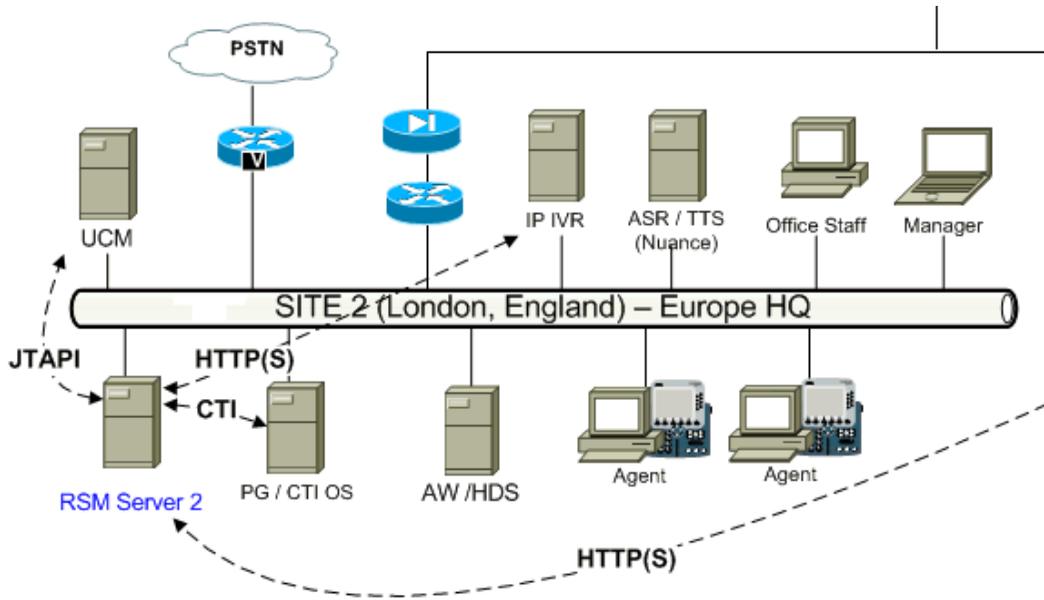
*Figure 1-2 RSM Configuration, Datacenter Site*



As Figure 1-3 illustrates, the London-based RSM server handles monitoring requests from both UK- and India-based PSTN points, as well as London personnel.

The CVP servers in Atlanta and London both handle IVR requests.

*Figure 1-3 RSM Configuration, London Site*

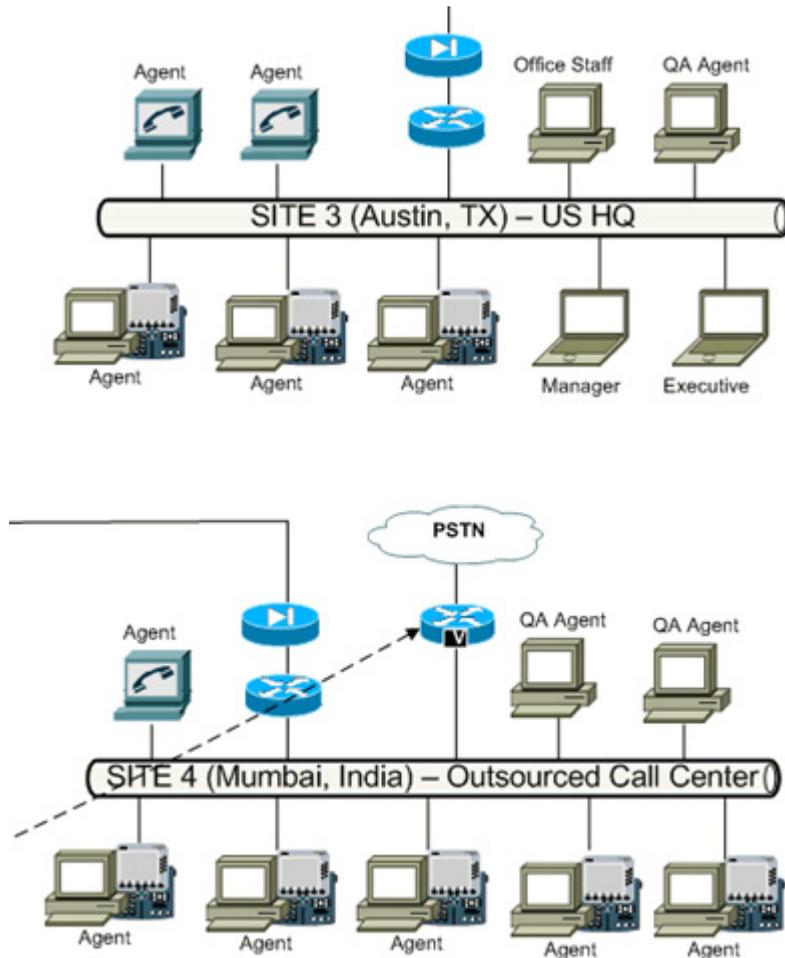


Each RSM server can be connected to both CTI OS servers in the organization (i.e., Atlanta, London) so that agent state across the entire organization can be tracked from both servers.

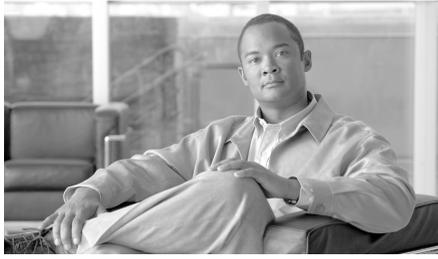
Failover in the U.S. is from RSM server 1 to RSM server 2, and from RSM server 2 to RSM server 1 for London and Mumbai.

The Mumbai site handles IVR requests as a VXML-based voice browser, as shown in Figure 1-4.

*Figure 1-4 RSM Configuration, Austin and Mumbai Sites*







## CHAPTER 2

# System Requirements

---

System requirements for RSM can be found in the Hardware and System Software Specification (Bill of Materials), Cisco Unified ICM/Unified CC Enterprise & Hosted Editions document for Unified CCE Release 7.2(x), 7.5(x), 8.0(x), or 8.5(x) located at

[http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html)

## Cisco Hardware and Software Requirements

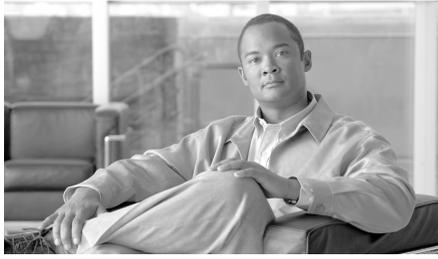
In addition to the RSM requirements, ensure that the specifications for Cisco's Unified Communications Manager (Unified CM) and Unified CCE are also met before installing RSM. Refer to the Hardware and System Software Specification (Bill of Materials), Cisco Unified ICM/Unified CC Enterprise & Hosted Editions document for Unified CCE Release 7.2(x), 7.5(x), 8.0(x), or 8.5(x) located at

[http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html)

To determine which applications are compatible with Unified CM, refer to the Cisco Unified Contact Center Enterprise (Unified CCE) Software Compatibility Guide, accessible from

[http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products\\_device\\_support\\_tables\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_device_support_tables_list.html)





## CHAPTER 3

# Pre-Installation Tasks

---

This chapter describes the modifications that must be made to the Cisco environment before RSM installation, specifically:

- Base system provisioning
- JTAPI client libraries installation
- Unified CM services enabling
- Simulated phones configuration
- Login pool simphone setup
- RSM user group creation
- RSM application user creation
- Supervisor login account creation

# Base System Provisioning

RSM base OS installation is similar to a Peripheral Gateway (PG) installation. However, no persistent static routes to the router and logger need be entered, and any firewall setup must be done manually, as the Cisco Firewall Configuration Utility (CiscoICMfwConfig) does not currently support RSM.

If Windows firewall is used, ensure that the ports used by the VRU to communicate with RSM's VLEngine (8080/TCP) and PhoneSim (29001/TCP) are unblocked. (Refer to the “Security Settings” topic in Chapter 4, Installation, for more information.)

For complete staging information, refer to *Staging Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*, for release 8.x, located at

[http://www.cisco.com/en/US/products/sw/custcosw/ps1844/prod\\_technical\\_reference\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1844/prod_technical_reference_list.html)

When provisioning the RSM server, ensure that the following guidelines are observed for the base system:

- Partition the hard drive as a single C: NTFS partition.
- Install RSM on its own dedicated server. Collocation of any other ICME component (or anything else) on the RSM server is not supported.
- Use Cisco approved anti-virus software (refer to Chapter 2, Cisco Hardware and Software Requirements, for BOM information). Note that all anti-virus software supported by Unified ICME is also supported by RSM.
- Run Microsoft's Baseline Security Analyzer (MBSA) on the server to view possible security improvements.
- Install Cisco Security Agent (CSA) for ICM on the server.
- Do not enable Windows automatic updates on the system, as the patch upgrade procedure for the RSM server must mirror those used for the Unified CCE and Cisco Unified ICME servers.

For additional guidelines on the base operating system, as well as services installation and configuration, refer to the *Security Best Practices Guide for ICM and IPCC Enterprise & Hosted Editions*, located at

[http://www.cisco.com/en/US/products/sw/custcosw/ps1844/prod\\_technical\\_reference\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1844/prod_technical_reference_list.html)

# JTAPI Client Libraries Installation

To install the JTAPI client libraries required to run RSM:

- 
- Step 1** Navigate to the Unified CM Administration web page.
  - Step 2** Log in using the admin ID and password
  - Step 3** Navigate to **Application > Plug-Ins**.
  - Step 4** Click **Find**.
  - Step 5** Click **Cisco JTAPI 32-bit client for Windows**.
  - Step 6** Run this file, installing the libraries to their default locations.

# Unified CM Services Enablement

Several Cisco-based services must be enabled for each Unified CM cluster used by RSM, as follows:

- 
- Step 1** Log into the Serviceability Area of the Unified CM cluster.
  - Step 2** Click **Tools > Service Activation**.
  - Step 3** Enable the following services for each server in the cluster:
    - Cisco CTIManager
  - Step 4** Repeat steps 1 through 3 for each cluster, as required.

# Simulated Phones Configuration

Before installing RSM, you must determine how many simulated phones (a.k.a., simphones) to assign to each Unified CM cluster. Each cluster must have simphones greater than or equal to the maximum number of agents that will be simultaneously monitored through RSM for the cluster.

In this section, you will:

- Configure the simphone device dependencies, creating a Unified CM group, RSM region, device pool, route partition, and calling search space;

- Create the simphone devices and assign MAC addresses;
- Add line DNs to the simphone devices.

The procedures describe how to create one simphone and its associated line DN. Additional simphones can be created by using Unified CM's super copy feature or by creating a batch file.

**Note**

---

You must be logged into the Admin interface of a Unified CM cluster before you can configure your simphones as described below.

---

## Simphone Device Dependencies

### To create a Unified CM group:

- 
- Step 1** Navigate to **System > Cisco Unified CM Groups**.
  - Step 2** Click **Add New**.
  - Step 3** Enter **RSMSimPhone** for the UCM group name, adding prefix or suffix naming conventions, if required (e.g., w\_RSMSimPhone\_3 for Western region three).
  - Step 4** Assign the necessary Call Managers to the group. If you have more than one Call Manager in the cluster, select the subscribers to be part of the group but do not select the publisher.
  - Step 5** Click **Save**.

### To create a simphone region:

- 
- Step 1** Navigate to **System > Region**.
  - Step 2** Click **Add New**.
  - Step 3** Enter **RSMSimPhone** for the region name, adding prefix or suffix naming conventions, if required.
  - Step 4** Click **Save**.
  - Step 5** Add relationships with agent phones to the regions in your environment. Note that calls between simphones and agent phones must use the G.711 codec.
  - Step 6** Click **Save**.

### To create a simphone device pool:

- 
- Step 1** Navigate to **System > Device Pool**.
  - Step 2** Click **Add New**.
  - Step 3** Enter **RSMSimPhone** for the device pool name, adding prefix or suffix naming conventions, if required.
  - Step 4** Select **RSMSimPhone** region from the **Roaming Sensitive Settings > Region** pull-down menu.
  - Step 5** Select the **RSMSimPhone CallManager** group from the **Device Pool Settings > Cisco Unified Communications Manager Group** pull-down menu.
  - Step 6** Enter the remaining parameters, as per your configuration (e.g., date/time group, user locale, etc.)
  - Step 7** Click **Save**.

### To create a simphone route partition:

- 
- Step 1** Navigate to **Call Routing > Class of Control > Partition**.
  - Step 2** Click **Add New**.
  - Step 3** Enter **RSMSimPhone** in the text box, adding prefix or suffix naming conventions, if required.
  - Step 4** Click **Save**.

### To create a simphone calling search space:

- 
- Step 1** Navigate to **Call Routing > Class of Control > Calling Search Space**.
  - Step 2** Click **Add New**.
  - Step 3** Enter **RSMSimPhone** for the calling search space name, adding prefix or suffix naming conventions, if required.
  - Step 4** Select the route partition containing the agent phones that RSM will monitor from the **Available Partitions** selection box, and move them to the **Selected Partitions** selection box.
  - Step 5** Click **Save**.

## Simphone Device Creation

The MAC addresses you assign to your simphones must be part of a reserved range, i.e., they cannot be used by hardware devices, such as network interface cards (NICs).

The following procedures describe how to create simphone devices and add DN lines to them. You can also use Unified CM's BAT tool to automatically perform these tasks, if desired.

A MAC address of 00005E000001 (hexadecimal) is assigned for the first simphone, and subsequent simphones increment from this value (00005E000002, 00005E000003, etc.). You may need to assign a different range of addresses if this range is currently being used. Any MAC address below 00005E is acceptable to use as the device name for a RSM simphone.



---

**Note**

Note that the address is in hexadecimal format; hence, the tenth phone address must be 00005E00000A, not 00005E000010.

---

So, if there are two RSM servers, the first server can use a range of 00005E000001 through 00005E000050, and the second server can use a range of 00005E000101 through 00005E000150, or 00005E110001 through 00005E110020, and so on.

### To create simphone devices:

- 
- Step 1** Navigate to **Device > Phone**.
  - Step 2** Click **Add New** to create a new phone device.
  - Step 3** Select **Cisco 7941** for the phone type, then click **Next**.
  - Step 4** Choose **SIP** for the device protocol, then click **Next**.
  - Step 5** The Phone Configuration page appears. Enter **00005E000001** for the MAC address.

- Step 6** Enter the parameters as listed in Table 3-1. Click **Save**. The simphone device is created. Parameters not listed may be left to their default settings.

*Table 3-1 Simphone Device Parameters*

Parameter	Setting
Device Pool	RSMSimPhone
Phone Button Template	Standard 7941 SIP
Location	As per environment
Built-in Bridge	Off
Phone Personalization	Disabled
Allow Device Control through CTI	Yes
Presence Group	Standard
Device Security Profile	Cisco 7941 Standard Non-Secure SIP
SIP Profile	Standard
Maximum Calls	2 (two)
Busy Trigger	1 (one)



**Note**

Note: Since RSM SimPhones are not created with any specific MRGL, they default to the system default Annunciator. So, whenever a call is being monitored using a simphone, the call going on hold will result in default Annunciator music of beep tones. Since RSM does not support G.729, make sure the region for the default Annunciator is G.711

## Line DN to Simphone Device Association

Each simphone device must have a line directory number (DN) created for it. In this procedure, a DN of 5040 is assigned to the first simphone device. Subsequent lines must have a range that is incrementally sequential (e.g., 5041, 5042) and not used by another device.

### To add a line DN to a simphone device:

- Step 1** Click the **Line [1] - Add a new DN** link in the **Association Information** panel.
- Step 2** Enter the parameters as listed in Table 3-2. Parameters marked with an asterisk (\*) are optional; those not listed may be left to their default settings.
- Step 3** Click **Save**. Your first simphone and its associated line DN is now configured.

*Table 3-2 Line DN Parameters*

<b>Parameter</b>	<b>Setting</b>
Directory Number	5040
Route Partition	RSMSimPhone
CTI Control	Yes
Voice Mail Profile	No voicemail
Calling Search Space	RSMSimPhone
Presence Group	Standard Presence group
User Hold MOH Audio Source *	1-SampleAudioSource
Network Hold MOH Audio Source *	1-SampleAudioSource
Line1 on Device <MAC ADDR> Monitoring Calling Search Space (CSS)	RSM SimPhone

## Simphone BAT Tool Usage

Unified CM's BAT tool can be used to automatically create and add line DNs to your simphone devices, in lieu of the procedures above. This is a solid approach to consider if the number of simphones you need to create is large.

To do this, you must first import the comma-separated template (from either the RSM installation CD or installed instance of RSM), and then edit it, as applicable, in a spreadsheet application such as Microsoft Excel.

**To use the simphone BAT tool:**

- 
- Step 1** Import the **rsmsimphones.csv** spreadsheet template file from either the RSM installation CD (located in the **extras** directory), or from the installed instance of RSM (located in the C:\CiscoRSM\Extras directory).
  - Step 2** Open the file in a spreadsheet application, then add or remove rows in the file to match the number of simphone devices you need to create (default rows = 75).
  - Step 3** If adding new rows, be sure to modify the data in the **Device Name** and **Directory Number 1** columns to increment sequentially from the previous row in the list for the columns (e.g., 00005E000001, 00005E000002, 00005E000003, etc., for the simphone MAC addresses, and 5040, 5041, 5042, etc., for the line DNs).
  - Step 4** Verify that the **Device Pool**, **Partition 1**, **Line CSS 1** and **Monitoring Calling Search Space 1** settings are correct for your environment (refer to Tables 3-1 and 3-2, above). Note that no changes are required if you entered **RSMSimPhone** for the Simphone Device Pool, Partition, and CSS settings during your simphone configuration.
  - Step 5** Navigate to **Bulk Administration > Upload/Download Files**.
  - Step 6** Click **Add New**.
  - Step 7** Click **Browse** and navigate to the **rsmsimphones.csv** file, previously downloaded and modified.
  - Step 8** Choose **Phones** from the **Select The Target** pull-down menu.
  - Step 9** Select **Insert Phones - All Details** from the **Select Transaction Type** pull-down menu.
  - Step 10** Click **Save**. The file is uploaded to the system.
  - Step 11** Navigate to **Bulk Administration > Phones > Insert Phones**.
  - Step 12** Select **Insert Phones All Details**, and then select **rsmsimphones.csv** from the **File Name** pull-down menu.
  - Step 13** Enter **Insert RSMSimPhones** for the Job Description, and then select **Run Immediately**.
  - Step 14** Click **Submit**. The file is imported into the system.
  - Step 15** Navigate to **Bulk Administration > Job Scheduler**.

- Step 16** Enter **Insert RSMSimPhones** in the Find Jobs text box. Ensure that **Description** is selected in the left pull-down menu, and that **begins with** is selected for the right pull-down menu.
- Step 17** Click **Find**. The Insert RSMSimPhones job is now listed. Verify that the job status is either **Processing** or **Completed**.
- Step 18** Once the job status is completed, review the phones you created by navigating to **Device > Phones**.
- Step 19** Enter **SEP00005E** in the Find Phone textbox, then click **Find**.
- Step 20** The simphone devices you created appear in the returned results.

## Login Pool Simphone Setup

The first five simphone devices created for each cluster are automatically assigned to the VLEngine login pool. The login pool performs a test login to CTI OS when a caller is authenticated by RSM, to support the VLEngine authentication mechanism.

Since CTI OS logins are performed on these simphone devices, they must be associated with the pguser account on each Unified CM cluster. They must also have Cisco Unified ICME device targets created for them, as described below.



### Note

---

Device target creation is required only for Unified CCE. You do not need to create device targets if you are using Cisco Unified System Contact Center Enterprise (Unified SCCE) or if the Cisco UCCE PG type is IPCC.

---

### To associate a pguser:

- 
- Step 1** Navigate to **User Management > Application User**.
  - Step 2** Click **Find** to display all application users. Locate then click the pguser account for your cluster.
  - Step 3** Select the first five simphone devices in the **Device Information > Available Devices** listbox.
  - Step 4** Click the down arrow above the box to move the devices to the **Controlled Devices** listbox. Click **Save**.

### To create a Unified ICME device target:

- 
- Step 1** From the Admin Workstation (AW), click **Start > All Programs > ICM Admin Workstation > Configuration Manager**.
  - Step 2** Expand **Tools**, then expand **Explorer Tools**. Double-click **Device Target Explorer**.
  - Step 3** Click **Retrieve** to return a list of all existing device targets in the environment.
  - Step 4** Click **(1) Add Device target**. A blank **Device Target** section appears in the right side of the Device Target Explorer window.
  - Step 5** Enter the DN (i.e., extension number) of the first simphone line, in both the **Name** field and the **Global address** field.
  - Step 6** Enter **/devtype CiscoPhone /dn xxxx** in the **Configuration parameters** field, where xxxx is the DN value entered in step 5.
  - Step 7** Click **Save**. Repeat steps 5 and 6 for the remaining simphones in the VLEngine login pool. If the number of simphones associated with a cluster is less than five, you must modify the cluster's **NumSimPhonesUsedForCTIOSAgentLogins** RSM configuration parameter to reflect that number (default value is five.)

**Note**

---

Refer to Appendix B, Registry Keys, for information on how to modify RSM configuration parameters.

---

## RSM User Group Creation

A RSM user group must be created for each cluster used by RSM. This provides the user with the necessary system permissions that would otherwise be available only to the CCM Super Administrator.

### To add a RSM user group to a cluster:

- 
- Step 1** Navigate to **User Management > User Group**.
  - Step 2** Click **Add New**.
  - Step 3** Enter **Remote Silent Monitoring** in the Name field, then click **Save**.

- Step 4** Navigate to **User Management > User Group**.
- Step 5** Click **Find** to display all user groups.
- Step 6** Click the **i** icon in the **Roles** column for the Remote Silent Monitoring group.
- Step 7** Click **Assign Role to Group**. A new window appears.
- Step 8** Click **Find** to display all group roles.
- Step 9** Select the following roles:
  - Standard CTI Allow Call Monitoring
  - Standard CTI Allow Control of All Devices
  - Standard CTI Enabled
- Step 10** Click **Add Selected**. The User Group Configuration page reappears.
- Step 11** Click **Save**.

## RSM Application User Creation

An application user named **rsmuser** must be created on each Call Manager cluster for RSM. This user derives its permissions from the user group previously created. The **rsmuser** must be associated with all simphones in the cluster (with the exception of simphones in the login pool). It must also be associated with all agent phones that RSM can monitor.

Simphones in the login pool (i.e., the first five simphone devices) must be associated with the cluster's **pguser**, while all other simphones not in the login pool are associated with the RSM application user.




---

**Note** Whenever a new non-login pool simphone or agent device is created, it must be associated with the RSM user.

---

### To add a RSM application user to a cluster:

- 
- Step 1** Navigate to **User Management > Application User**.
  - Step 2** Click **Add New** to create a new application user.
  - Step 3** Enter **rsmuser** for the user ID.

- Step 4** Enter a password. Ensure that the password is alphanumeric and does not contain any special characters.
- Step 5** Associate the user with all simphone devices in the cluster (except for the login pool devices) by selecting those devices in the **Available Devices** section and moving them to the **Controlled Devices** section.
- Step 6** Associate all agent phone devices to be monitored through RSM.
- Step 7** From the Permissions Information window, click **Add to User Group**, and then add the user to the Remote Silent Monitoring group, as previously created.
- Step 8** Click **Save**. The user is now associated with the devices and user group.

## Agent Phone Device Setup

When configuring an agent phone device to be monitored by RSM, ensure the following:

- Edit the device via the Cisco Unified CM Administration interface and enable the Built-In Bridge setting.
- Associate the device with the rsmuser, similar to the way it is associated with the pguser.

## Supervisor Login Account Creation

You must create a new account for each supervisor who will be using RSM, as per your current CTI OS supervisor/agent accounts.

If CTI OS authentication is used, separate supervisor agent accounts must be created in the Unified CCE environment, to allow dialed-in supervisors to log into the system.



### Note

RSM requires numeric supervisor accounts so users can log in via the telephone. However, ICME supervisor agent accounts are also Active Directory user accounts, and there may be an Active Directory security policy that prevents numeric-only accounts. To resolve this issue, refer to Appendix B, Registry Keys, for information on how to modify the VLEngine\_PassPrefix parameter.

**To create a supervisor login account:**

- 
- Step 1** From the Admin Workstation (AW), click **Start > All Programs > ICM Admin Workstation > Configuration Manager**.
- Step 2** Expand **Tools > Explorer Tools**.
- Step 3** Double-click **Agent Explorer**.
- Step 4** Click **Retrieve** to return a list of all existing agents in the environment.
- Step 5** Click **(1) Add Agent**. A blank agent section appears in the right side of the **Agent Explorer** window.
- Step 6** Click the **Agent** tab and enter the following:
- First name** and **Last name** of the supervisor;
  - Numeric **Password** of any length;
  - Value for **AgentID (Peripheral number)**, as per the supervisor's login ID;
  - Select the **Login Enabled** checkbox.
- Step 7** Click the **Supervisor** tab and enter the following:
- Select the **Supervisor Agent** checkbox;
  - Select a **Domain name** as per the environment;
  - Login ID**;
  - Password**.
- Step 8** Click **Save**.
- Step 9** Add the supervisor to a team via the ICM Configuration Manager Agent Team List tool. If the supervisor is not added to a team, they will not be able to log in.

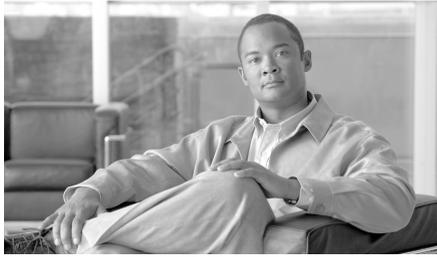
**Note**

---

RSM uses Cisco's Java-based CTI OS access library, and security must be disabled on all CTI OS servers that it is configured to use. For more information, refer to the *CTI OS System Manager's Guide* for your Unified CCE release, located at:

[http://www.cisco.com/en/US/products/sw/custcosw/ps14/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps14/prod_installation_guides_list.html)

---



# CHAPTER 4

## Installation

---

This chapter describes how to install the RSM server from the installation CD. Information on environment variables, installed directory structure, ports used, and security settings is also provided.

The installer automatically enables the VLEngine and PhoneSim services to run at startup. Refer to Chapter 6, RSM Services, for information on how to enable, check, and restart these services.

An RSM release can be either a patch release or a full RSM server installation. Refer to the Cisco Remote Silent Monitoring Release Notes for your release to determine release instructions to follow and to see supported base install versions.



### Note

---

Before you install RSM, you must first perform the pre-installation tasks, as described in Chapter 3.

---

## Patch Installation

The patch installer does not support a full installation of RSM. It includes only those specific files and configurations that need to be updated or created for the patch. The patch installer is available from [www.cisco.com](http://www.cisco.com).



### Caution

---

During patch installation, the VLEngine and PhoneSim services are stopped then re-started once installation is complete. All monitoring sessions in progress are terminated and no new sessions can be initiated until installation is complete

---

During installation, the patch installer will check the product version registry key to ensure that the base RSM installation is present on the server, and will then update the key to reflect the patch version. The patch installer creates a backup directory for all previous files, at `C:\CiscoRSM\Backup_<prior version>`, to facilitate rollback by the patch uninstaller, if required.

## RSM Server Installation

The installer program installs the RSM application files, and the following dependencies:

- Apache Tomcat application server
- Java Service Wrapper



### Note

---

You must disable Cisco Security Agent (CSA) before installing RSM, and then enable it once installation is complete. Refer to the *Installing Cisco Security Agent for Cisco Unified Communications Manager* document for your Unified CM release, located at [http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html)

---

### To install RSM on a Windows Server 2003 or 2008:

- 
- Step 1** Partition your C: drive for 50G (minimum), in NTFS format.
  - Step 2** Insert the RSM CD, navigate to the CD root, and run **setup.exe**.
  - Step 3** The RSM Setup Program starts. Follow the onscreen instructions to install RSM to the `C:\CiscoRSM` directory.

## Configuration Manager

Once the installation is complete, the RSM Configuration Manager utility is launched. This utility is used to set the configuration settings for RSM, as stored in the Windows Registry.

**Note**

Refer to Appendix B, Registry Keys, for information on how to modify these settings manually.

## Configuration Settings

### Mail Server settings

- **Send Email Alerts**—Check this box and fill in the text fields to allow PhoneSim and VLEngine to send email alerts when an error occurs.

### Miscellaneous Configuration settings

- **Problem Call Min Duration**—Call is classified as a problem if it exceeds specified minimum seconds. (Registry key: ProblemCallMinDuration)
- **Problem Call Min Holds**—Call is classified as a problem if agent has put caller on hold more than specified number. (Registry key: ProblemCallMinHolds)
- **Max Stale Call Duration**—Maximum seconds state of a call can remain unchanged (i.e., does not trigger a CTI event) before deemed stale and removed. (Registry key: MaxStaleCallDuration)
- **CTI OS Trace Mask**—Determines verbosity level for CTI OS CIL messages logged to disk, for all CTI OS connections (i.e., both agent mode and monitor mode). Logging is written to the C:\CiscoRSM\vlengine\ctiosLogs directory. Agent mode CTI OS connections are created on demand for back-end authorization when a login to RSM is requested. Monitor mode connections are created upon startup, and remain active for the life of the application. Used to retrieve information about events in call center environment. (Registry keys: CTIOS\_TraceMask)
- **VLEngine - Log Level**—String which dictates verbosity level of output to the VLEngine log file. INFO and DEBUG are the most commonly used settings. Note that changing this setting requires that you restart the VLEngine. (Registry key: VLEngine\_LogLevel)

- **VLEngine - HTTP Listen Port**—Port number VLEngine listens to for incoming HTTP requests. Default is 8080. (Registry key: VLEngine\_HTTPListenPort)
- **PhoneSim - Audio Buffer Len To VRU**—Bytes of data PhoneSim will buffer before transmission to VRU Voice browser. Used when VRU voice browser receives agent audio data from PhoneSim. Set to 160 for an IP IVR environment, and 480 for a CVP environment. If both IP IVR and CVP are used with the RSM server, set to 480. (Registry key: PhoneSim\_AudioBufferLenToVRU)
- **PhoneSim - Log Level**—String which dictates verbosity level of output to the PhoneSim log file. INFO, DEBUG, and TRACE are the most commonly used settings. Note that changing this setting requires that you restart the PhoneSim. (Registry key: PhoneSim\_LogLevel)
- **PhoneSim - Audio Encoding**—Data encoding method PhoneSim uses for requested audio data. Must be set to **wav-ulaw**. (Registry key: PhoneSim\_LogLevel)
- **PhoneSim - Do HTTP Chunked Transfers**—Enables PhoneSim to transmit HTTP chunking of audio data, from VRU node request. Must be set to **no**. (Registry key: PhoneSim\_DoHTTPChunkedTransfers)
- **PhoneSim - Host Data IP**—Set to the IP address of the RSM server. This is the IP address the PhoneSim server uses to contact other computers in network. Useful when there are multiple NIC machines in network. If blank, IP address of primary network interface is used. This is also the IP address the VLEngine server uses to contact other computers in the network. Useful for multi-NIC machines. If blank, IP address of primary network interface is used. This parameter is important in a large deployment, where VLEngine and PhoneSim are on different servers, and is the address that PhoneSim uses to communicate with VLEngine. (Registry keys: PhoneSim\_HostDataIP and VLEngine\_HostDataIP)

## Define Cluster Configuration Settings

These settings are used to configure each UCM cluster with the agents to be monitored by RSM.

- **ClusterN\_Name**—Alphanumeric name for the cluster, for descriptive purposes. (Registry key: ClusterN\_Name)

- **# Login Pool Simphones**—Number of simphones in the login pool. Set to 5. Refer to the “Login Pool Simphone Setup” topic in Chapter 3, Pre-Installation Tasks, for more information. (Registry key: ClusterN\_NumSimPhonesUsedForCTIOSAgentLogins)
- **# Monitor Pool Simphones**—Maximum simultaneous, real-time monitor requests the platform can handle for the cluster. This should equal the number of simphones in the cluster that are not used in the login pool. For example, if you want to have 40 concurrent monitoring sessions, you must assign 45 simphones in the cluster, with 40 used for monitoring and 5 reserved for login. (Registry key: ClusterN\_MaxNumRequests)
- **Peripheral ID**—Peripheral instrument ID used to denote the cluster in Unified ICME e.g., the ICME peripheral ID of the PIM for the UCM cluster. (Registry key: ClusterN\_PeripheralID)
- **JTAPI Username**—JTAPI application user username used by RSM to connect to the specified UCM servers in the cluster. Refer to the “RSM Application User Creation” topic in Chapter 3, Pre-Installation Tasks, for more information. (Registry key: ClusterN\_JTAPI\_UserName)
- **JTAPI Password**—JTAPI application user password used by RSM to connect to the specified UCM servers in the cluster. Refer to the “RSM Application User Creation” topic in Chapter 3, Pre-Installation Tasks, for more information. (Registry key: ClusterN\_JTAPI\_Password)
- **Start MAC Range**—First MAC address to use for auto-generation of MAC range for simphone device names. For example, if 000000100010 is specified, the range would proceed with SIP000000100010, SIP000000100011, SIP000000100012, and so forth. MAC ranges must not overlap between clusters. Note that the 0000:5Exx range is normally reserved for public use, as per IANA standards. Refer to the “Simulated Phones Configuration” topic in Chapter 3, Pre-Installation Tasks, for more information. (Registry key: ClusterN\_PhoneSim\_StartMACRange)
- **Start Line Num Range**—First extension number to use for auto-generation of line extension range for simphone DNs. Line extension ranges must not overlap between clusters. Correlates to ClusterN\_PhoneSim\_StartMACRange value. If 1000 is specified, and 000000100010 is ClusterN\_PhoneSim\_StartMACRange, then the first simphone device name generated will be SIP000000100010 and will have line extension 1000; SIP000000100011 will have line extension 1001; SIP000000100012 will have line extension 1002, and so forth. Refer to the

“Simulated Phones Configuration” topic in Chapter 3, Pre-Installation Tasks, for more information. (Registry key: ClusterN\_PhoneSim\_StartLineNumRange)

- **SIP Transport**—Tells PhoneSim how to conduct the SIP transmission with Contact Manager for the cluster, via TCP or UDP. Must be set to **tcp**. (Registry key: ClusterN\_PhoneSim\_SIPTransport)

## Call Manager Configuration Settings

- Enter information for the Call Manager UCM server in the cluster (as well as any backup servers) that RSM communicates with. (Registry keys: ClusterN\_VLEngine\_CM1\_Hostname et al, ClusterN\_PhoneSim\_CM2\_CM2\_Port et al, etc.).

# VLEngine and PhoneSim Services

The installer automatically enables the VLEngine and PhoneSim services to run at startup, after you restart your machine. If desired, you can select to run the services after installation.

Refer to Chapter 6, RSM Services, for information on how to start and stop the RSM services.

# Directory Structure

RSM creates the following directories with the following files upon installation:

*Table 4-1 RSM Directory Structure*

Directory	Files
C:\WINDOWS\java\lib	JTAPI client library files
C:\Program Files\JTAPITools	Cisco JTAPI client library sample applications and documentation
C:\CiscoRSM\phonesim\logs	PhoneSim log files
C:\CiscoRSM\docs	RSM documentation
C:\CiscoRSM\vlengine\bin	Runtime RSM dependencies: ICE_JNIRegistry.DLL
C:\CiscoRSM\vlengine\logs	VLEngine log files
C:\CiscoRSM\vlengine\lib	RSM dependency JARs: JavaCIL-7.2.jar - CTI OS jtds-1.2.jar - JTDS (MS SQL connectivity) registry.jar - ICE Registry (Windows regedit)
C:\CiscoRSM\vlengine\tomcat	Apache Tomcat installation directories: conf\wrapper.conf -- launch configuration

# Port Numbers Used

RSM uses the following TCP and UDP ports for the following connections:

*Table 4-2 Port Numbers Used*

Port	Protocol	Description
8080	TCP in	HTTP connections to VLEngine from VRU
8443	TCP in	HTTPS connections to VLEngine from VRU
29001	TCP in	HTPP connections to PhoneSim from VRU
5060	TCP/UDP out	PhoneSim SIP communication with Unified CM
16384-32767	UDP in/out	PhoneSim RTP communication with agent phone endpoints
42028	TCP out	VLEngine communication to CTI OS servers
2789	TCP out	VLEngine communication to Unified CM (JTAPI)

## Environment Variables

After installation, verify the following environment variable settings:

- 
- Step 1** Navigate to **Start > Settings > Control Panel > System > Advanced > Environment Variables**.
- Step 2** Verify the following values for these system variables:
- RSM\_HOME = C:\CiscoRSM\
  - CATALINA\_HOME = C:\ CiscoRSM \tomcat

# Security Settings

This section describes host and network level security considerations for the integration of RSM into a Cisco environment, after RSM is installed.

## Host Level Security

Host level RSM security can be hardened and configured using Windows Server Windows 2003 or 2008 Firewall and Cisco Security Agent (CSA), as described below.

### Windows Security Hardening

It is highly recommended that the ICM recommended Windows Security Hardening policies be applied to the RSM server.

To do this, copy the ICM security hardening script (located in the C:\CiscoUtils\SecurityTemplates directory of any PG in the environment) to the same directory on the RSM server, creating the directory if necessary. The script can then be invoked from the RSM server.

For more information, refer to the “Manually Installing Cisco ICM Security Settings” topic in Chapter 5 of the *Security Best Practices Guide for ICM and IPCC Enterprise & Hosted Editions* document, located at

[http://www.cisco.com/en/US/products/sw/custcosw/ps1844/prod\\_technical\\_reference\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1844/prod_technical_reference_list.html)

### Windows 2003 or 2008 Firewall

Windows Firewall may be manually enabled and used on the RSM server, if desired. Exceptions must be created for ports 8080, 29001, and 5060. (Refer to Table 4-2, Port Numbers Used, for RSM port and protocol usage when creating exceptions.)

If your VLEngine and PhoneSim configuration uses ports other than those listed, be sure to create firewall exceptions for those ports.

**Note**

---

Currently, the Cisco Unified Contact Center Security Wizard's Windows Firewall tool is not programmed to automatically create exceptions for RSM. RSM will not work properly if this tool is used to enable Windows Firewall on the RSM server.

---

## Cisco Security Agent (CSA)

RSM fully supports Cisco Security Agent (CSA) for ICM. It is highly recommended that CSA for ICM be installed on the RSM server. Refer to the “Base System Provisioning” topic in Chapter 3, Pre-Installation Tasks.

## Network Level Security

Currently, network level IP security (IPsec) encryption is the only supported method for securing high-level protocols between RSM and other Unified CCE components.

**Note**

---

For recommended and supported IP sec tunnel configurations, refer to the “Support for IPsec (IP Security) in Transport Mode” topic in Chapter 2 of the *Security Best Practices Guide for ICM and IPCC Enterprise & Hosted Editions* document (cf. “Windows Security Hardening” topic, above).

---

ICM allows IPsec policies to be set up manually (e.g., via the Microsoft 2003 or 2008 Server security tools), or via the Cisco Network Isolation Utility. Note that RSM supports only manually configured peer-to-peer IPsec tunnels and does not support the Cisco Network Isolation Utility.

IPsec for secure CTI OS and JTAPI communication is described below.

## Secure CTI OS Communication Encryption with IPsec

To encrypt CTI OS communications between the RSM server and a PG CTI OS server, an IPsec tunnel may be configured. If the environment has multiple PGs that the RSM server is configured to use, this approach may be used with each PG or only certain ones (e.g., only PGs over a certain insecure network connection).

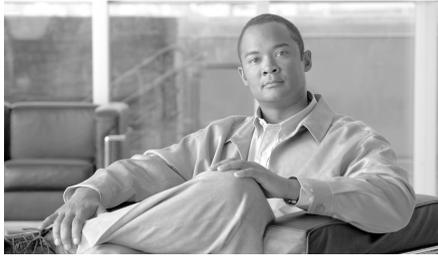
## Secure JTAPI Communication Encryption with IPsec

As CTI OS communications can be encrypted, so can JTAPI communications between RSM and the UCM servers. RSM and UCE both support secure IPsec tunnels for securing JTAPI traffic.

The UCE IPsec configuration must be configured from the UCE OS Administration Web interface. Refer to Chapter 6 of the *Cisco Unified Communications Operating Systems Administration Guide* for your Unified CM release, located at

[http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod\\_maintenance\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html)





## CHAPTER 5

# VRU Configuration

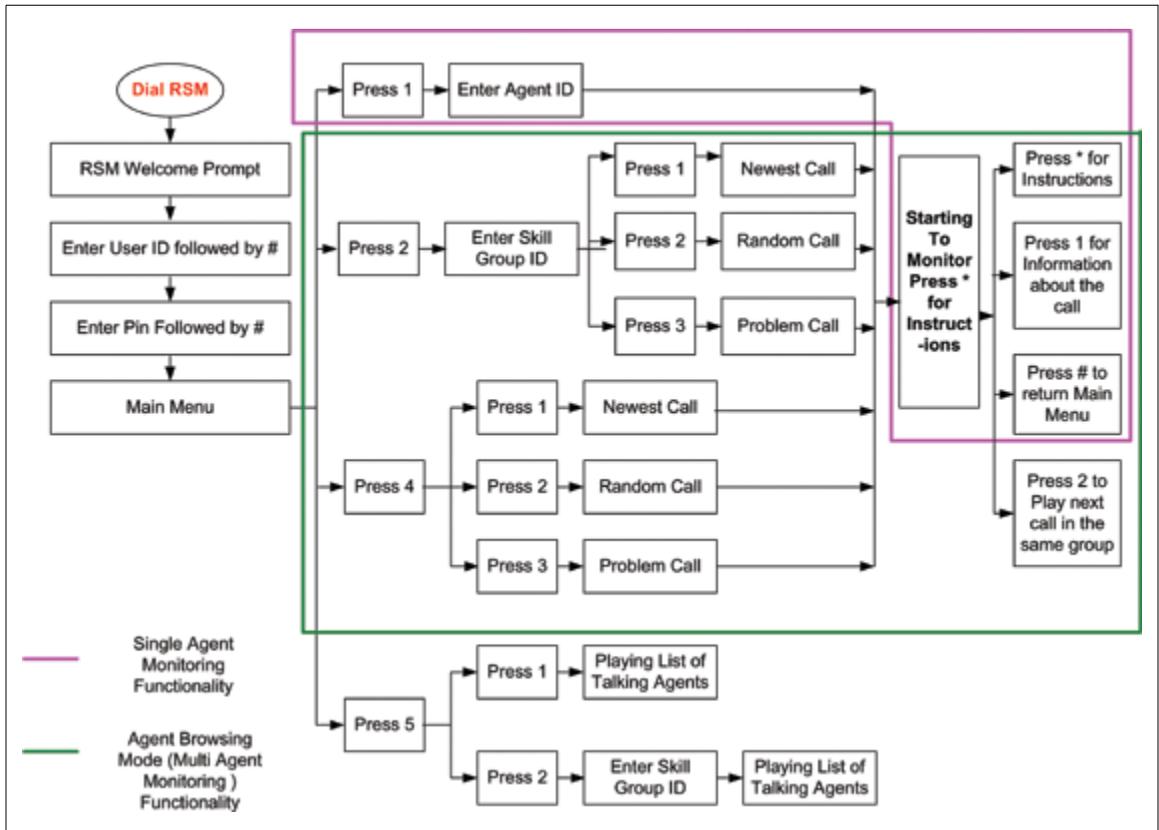
---

This chapter describes the integration of the RSM prompts and call flow script with the Voice Response Unit (VRU). The VRU determines how RSM responds to caller-entered data (press one to continue, press # to cancel, etc.).

IP IVR 5.0(2), 7.0(x), 8.0(x), 8.5(x) or 9.0(x), or CVP 4.0(x), 4.1(x), 7.0(x), 8.0(x), 8.5(x), or 9.0(x) may be used as the VRU, as per your environment.

Figure 5-1 illustrates the default call flow script.

Figure 5-1 Default Call Flow Script



## IP IVR Integration

RSM installs a basic IP IVR call flow script, which is designed to meet the majority of VRU needs without modification. Cisco Unified CM or Unified ICME must be configured to route calls to the RSM call flow on the IP IVR Server.

Refer to the following documents for more information:

*Installation Guide Cisco ICM/IPCC Enterprise & Hosted Editions* for your Unified CCE release, located at

[http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_installation_guides_list.html)

*Cisco Unified Contact Center Enterprise Solution Reference Network Design (SRND)*, located at

[http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products\\_implementation\\_design\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_implementation_design_guides_list.html)

**Note**

Currently, only IP IVR systems with the G.711 codec are enabled. G.729 is not supported.

## Upload RSM Prompts

RSM prompts are the decision tree selections that a caller hears and responds to when they dial into the system. They must be uploaded into the system for IP IVR, as described below.

### To upload RSM prompts:

- Step 1** Navigate to **Applications > Prompt Management**.
- Step 2** Select the **en\_US** directory.
- Step 3** Click the **Create New Folder** link. A new window appears.
- Step 4** Enter **VL** for the Folder Name.
- Step 5** Click **Create**. The Prompt Management page refreshes, and includes the newly created VL directory.
- Step 6** Click the VL directory.
- Step 7** Click the **Upload New Prompts** link. A new window appears.
- Step 8** Click **Browse** and navigate to **C:\CiscoRSM\vlengine\callflows**.
- Step 9** Select the **prompts.zip** file then click **Upload**.
- Step 10** The file is uploaded to the server, populating the directory with the RSM system prompt files.

## IP IVR Integration (non-Unified ICME)

To handle calls transferred directly from Unified CM into RSM, you must install the call flow script and add RSM as a new application on IP IVR.

### To install the call flow script:

- 
- Step 1** Log into IP IVR from the RSM server.
  - Step 2** Navigate to **Applications > Script Management**.
  - Step 3** Click the **Upload New Scripts** link. A new window appears.
  - Step 4** Click **Browse** and navigate to **C:\CiscoRSM\vlengine\callflows\ipivr**.
  - Step 5** Select the **RSM.aef** script then click **Upload**.
  - Step 6** The script now appears in the Script Repository.

### To add RSM as a new application:

- 
- Step 1** Navigate to **Applications > Application Management**.
  - Step 2** Click the **Add a New Application** link.
  - Step 3** Select **Cisco Script Application** for the application type, then click **Next**.
  - Step 4** Enter **RSM** for the script name. (Default values can be used for Description, ID, and Enabled fields.)
  - Step 5** Enter a numeric value in the **Maximum Number of Sessions** field, as per your environment. The exact value is contingent upon factors such as hardware used, IP IVR server capability, Cisco platform, etc. Set this value to the maximum number of users that are expected to dial into the environment, and ensure this figure does not exceed the value of Max Num Requests configuration value. (refer to “Configuration Manager” topic in Chapter 4, Installation).
  - Step 6** Select **RSM.aef** from the **Script** pull-down menu. The page refreshes, allowing you to enter custom values for the script parameters as follows:
    - **VRU\_VL1\_VLEngine\_IP**—IP address of the RSM server where VLEngine is configured.

- **VRU\_VL1\_VLEngine\_Port**—Default, unless the value of the `VLEngine_HTTPListenPort` setting has been changed in the Windows Registry Editor (see Appendix B, Registry Keys).
- **VRU\_VL1\_PhoneSim\_Port**—Default, unless the value of the `PhoneSim_HTTPListenPort` setting has been changed in the Windows Registry Editor (see Appendix B, Registry Keys).
- **MAX\_NUM\_LOGIN\_ATTEMPTS**—Number of invalid login attempts allowed before the system rejects the call. Default value is three (3).
- **TTS\_ENABLED**—Set to true to enable text-to-speech (TTS) functionality. TTS functionality is then allowed for certain portions of the call flow (e.g., agent listing, information about conversations currently being monitored) in lieu of the default pre-recorded prompts.
- **VRU\_VL1\_PhoneSim\_IP**—IP Address of RSM server where PhoneSim service configured

**Step 7** Press **Add**. The application is created.

## IP IVR Integration (Unified ICME)

To handle calls transferred directly from Unified ICME into RSM, you must install the call flow script on IP IVR.

### To install the call flow script:

- 
- Step 1** From the IP IVR web interface, click the **Subsystems > ICM** link.
  - Step 2** Click the **ICM VRU Scripts** link.
  - Step 3** Click the **Add a new VRU Script** link.
  - Step 4** Select **RSM.aef** for the VRU Script Name.
  - Step 5** Select **RSM.aef** for the script.
  - Step 6** Click **Add**. The script is added to Unified ICME environment.
  - Step 7** Navigate to the **Unified ICME Routing.icms** script.
  - Step 8** Open and modify the script to suit your environment, as required (e.g., you may need to associate the script to the appropriate call types in the CallType Manager).

# CVP Integration

The procedure provided for RSM integration with CVP is designed for a basic CVP configuration. Before integrating RSM with CVP:

- Ensure that your CVP VXML Server software is installed and running at C:\Cisco\CVP\VXMLServer;
- Ensure that CVP Unified Call Studio is installed on the user's desktop;
- Ensure that you have the appropriate level of administrator's access to the CVP VXML Server, VXML gateway, and media server components.

## Upload RSM Prompts

RSM prompts are the decision tree selections that a caller hears and responds to when they dial into the system. They must be uploaded into the system for CVP, as described below.

### To upload RSM prompts:

- 
- Step 1** Navigate to your media server directory, at C:\Cisco\CVP\MediaFiles\en-us, and create a new directory labeled **VL**.
  - Step 2** Navigate to C:\CiscoRSM\callflows and unzip the contents of the **prompts.zip** file into the VL directory.
  - Step 3** Right-click the **VL** directory, then click **Properties**.
  - Step 4** Click the **Security** tab, then click **Advanced**.
  - Step 5** Select **Allow inheritable permissions from the parent to propagate to this object and all child objects**.
  - Step 6** Click **OK**.
  - Step 7** Open your web browser and navigate to the VL directory of your media server, i.e., **http://<SERVER IP>/MediaFiles/en-us/VL**. Ensure that the prompt files are listed and accessible.

## CVP Call Flow Integration

To handle calls transferred directly from CVP into RSM, you must install the call flow script on CVP.

### To install the call flow script:

- Step 1** Navigate to the `C:\CiscoRSM\callflows\vxml-cvp` folder on the RSM server.
- Step 2** Copy all the contents from the folder to a directory that can be accessed by the desktop machine hosting CVP Unified Call Studio software (e.g., `C:\RSM-Callflow`).
- Step 3** Open CVP Unified Call Studio and import the RSM Project into your workspace.
- Step 4** Right-click **RSM Project** in the Navigator pane then click **Properties**.
- Step 5** Click **Cisco Unified CVP | Audio Settings**.
- Step 6** Navigate to the **Default Audio Path URI** text field and enter the VL directory on your media server, e.g., `http://10.1.110.110/MediaFiles/en-us/VL`.
- Step 7** Click **OK**.
- Step 8** Navigate to the **DoLogin** page in the Callflow Editor pane for RSM Project.
- Step 9** Select the **SetBaseSessionVars** element then click the element's **Data** tab.
- Step 10** Modify the **VoiceXML Variable settings** for RSM Project as follows:
  - **VL\_VLENGINE\_HOSTNAME**—Hostname or IP address of server running VLEngine service.
  - **VL\_VLENGINE\_PORT**—Port number used by VLEngine service. Usually port 8080.
  - **VL\_PHONESIM\_HOSTNAME**—Hostname or IP address of server running PhoneSim service. Usually same as `VL_VLENGINE_HOSTNAME`.
  - **VL\_PHONESIM\_PORT**—Port number used by PhoneSim service. Usually port 29001.
  - **CVP\_MEDIASVR\_HOSTNAME**—Hostname or IP address of CVP media server with RSM prompts, as found in the `/MediaFiles/en-us/VL` directory.
  - **CVP\_MEDIASVR\_PORT**—Port number of media server daemon. Usually port 80.

- **CVP\_MEDIASVR\_PATH**—Points to the URL path where RSM prompts are uploaded (e.g. /MediaFiles/en-us/VL). NOTE: This path, and the Path component specified in the RSM CVP project's Audio Settings - Default Audio Path URL text field, must be identical.
- **CVP\_VXMLSVR\_HOSTNAME**—Hostname or IP address of server running VXML server.
- **CVP\_VXMLSVR\_PORT**—Port number used by VXML server.
- **MAX\_NUM\_LOGIN\_ATTEMPTS**—Maximum number of failed login attempts allowed before RSM disconnects user.
- **MONITOR\_NEWEST\_REPOLL\_PERIOD**—Time, in seconds, before monitoring for new agent conversations. Normally set to 4 seconds.
- **MONITOR\_NEWEST\_PROMPT\_TO\_END EVERYN**—Number of pollings before progress prompt is stated to caller (i.e., “System is still busy. Press any key to return to main menu or continue to hold.”) Normally set to 3.

**Step 11** Click **Save** to save the RSM Project.

**Step 12** Run a basic test call flow to ensure the system is functioning properly. Customize the call flow script, if desired.

## Call Flow Deployment

Once the call flow script is installed on CVP, it must be deployed for use by CVP VXML Server.

### To deploy the call flow script:

- 
- Step 1** Open CVP Unified Call Studio.
  - Step 2** Right-click **RSM Project** in the Navigator pane, then click **Deploy**.
  - Step 3** Select **Cisco Unified CVP Home** for **Deploy Destination**.
  - Step 4** Enter your VXMLServer home directory in the text box, i.e., **C:\Cisco\CVP\VXMLServer**.
  - Step 5** Click **Finish**. The call flow script is deployed to the CVP server.
  - Step 6** Close CVP Unified Call Studio.

- Step 7** Navigate to the `C:\Cisco\CVP\VXMLServer\applications\RSM\admin` directory, then double-click the `deployApp.bat` file. The batch file is executed in a separate DOS window.
- Step 8** Enter **Y** for yes when prompted to deploy the application. The call flow script is now accessible from the CVP VXML Server.
- Step 9** Configure the appropriate micro-applications on your VXML gateway (VG dial peers, UCM route patterns, etc.) so they can access the script. Refer to the CVP configuration documentation for more information, located at [http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products_installation_and_configuration_guides_list.html)

## Call Flow Troubleshooting

For log file information for any CVP call flow application, refer to the *VoiceXML Server User Guide for Cisco Unified Customer Voice Portal* document, located at [http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products_user_guide_list.html)

## CVP Unified Call Studio Logging

CVP Unified Call Studio contains the VXML output that the VXML Server produces. You can enable additional logging and debugging of RSM in CVP Unified Call Studio, if desired.

### To enable CVP Unified Call Studio logging:

- 
- Step 1** Open **RSM Project** in CVP Unified Call Studio, then navigate to **General Settings**.
- Step 2** Select **Loggers**. A new window appears.
- Step 3** Add the `com.audium.logger.application.debug.ApplicationDebugLogger` to the project.
- Step 4** Click **OK**.

For more information, refer to the *Enable VoiceXML Debug Mode on Cisco Unified Call Services, Universal Edition* document, located at

[http://www.cisco.com/en/US/products/ps7234/products\\_tech\\_note09186a0080874c88.shtml](http://www.cisco.com/en/US/products/ps7234/products_tech_note09186a0080874c88.shtml)

## VXML Gateway Setup Notes

RSM requires a dedicated gateway. RSM is supported on any VXML gateway model and version of Cisco Internetwork Operating System (IOS) that CVP 4.0(2), CVP 4.1(1), CVP 7.0(2), CVP 8.0(1), CVP 8.5(1), or CVP 9.0(1) supports.

### To set up the VXML gateway for use with RSM:

- 
- Step 1** Ensure that IVR prompt streaming is enabled for HTTP by issuing the **ivr prompt streamed http** command;
  - Step 2** Ensure that IVR prompt memory is at least 8M, by issuing the **ivr prompt memory 8000** command.

## Example Configuration

The VXML gateway configuration will vary from system to system. A basic example configuration using a H.323 dial peer is shown below.

```

http client cache memory pool 15000
http client cache memory file 500
http client cache refresh 864000
no http client connection persistent
http client connection timeout 60
http client response timeout 30
ivr prompt memory 8000
ivr prompt streamed http

service RSM flash:CVPSelfService.tcl
paramspace english language en
paramspace english index 0
paramspace english location flash
paramspace english prefix en
param CVPPrimaryVXMLServer 10.1.110.110
param CVPBackupVXMLServer 10.1.110.110
param CVPSelfService-app RSM
param CVPSelfService-port 7000

```

```
dial-peer voice 12345 voip
description ICM VRU label
translation-profile incoming block
service rsm
voice-class codec 1
incoming called-number 12345
dtmf-relay rtp-nte h245-signal h245-alphanumeric
no vad
```

**Note**

---

Refer to the CVP Installation Guide and the CVP SRND for more information about these parameters and VCP configurations, located at [http://www.cisco.com/en/US/products/sw/custcosw/ps1006/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1006/prod_installation_guides_list.html)

[http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products\\_implementation\\_design\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products_implementation_design_guides_list.html)

---

## Disabling Supervisor Team Structure or User Authentication

RSM has built-in user authentication mechanisms that integrate with the agent and supervisor hierarchal team structure of Unified CCE.

It may be desired to edit the call flow script and disable these mechanisms, to allow any supervisor to access any agent, all agent access for anyone who dials into the system, third-party authentication, etc.

### To disable RSM's Supervisor Team Structure Membership (optional):

---

- Step 1** Open the call flow script using the CRS Editor.
- Step 2** Change the **SupervisorID** parameter to zero (0) for all instances of the **canMonitorAgentID**, **getCallToMonitor**, and **getAgentList** API calls.
- Step 3** Edit the **Create URL Document** parameters, as appropriate.
- Step 4** Modify the **supervisorID** entry in the Parameters table to zero (0).

**To disable RSM's user authentication (optional):**

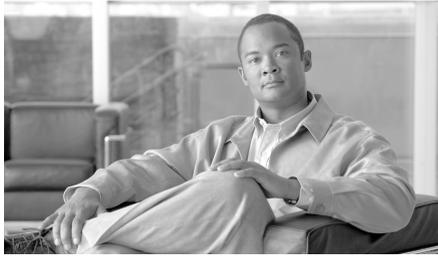
- 
- Step 1** Open the call flow script using the CRS Editor.
- Step 2** Remove the **DoLogin** section in the script, up to (but not including) the **MainMenu** section.
- Step 3** If you are using a third-party authentication tool, modify the **MainMenu** section of the script as per the tool's requirements. In most cases, the **UserID** and **PIN** information will remain the same, but the **Create URL Document** and **Voice Browser** parameters will need to be deleted.
- Step 4** Remove all instances of the **canMonitorAgentID** API call, including the **Create URL Document**, **Voice Browser**, and **Switch** parameters. If you are using a third-party authentication tool, enter the proper parameters to ensure the caller can monitor the agent ID, as entered.
- Step 5** Change the **SupervisorID** parameter for any instances of the **getCallToMonitor** and **getAgentList** API calls to zero (0), editing **Create URL Document** parameters as appropriate and modifying the **supervisorID** entry in the Parameters table to zero (0).
- Step 6** If you are using a third-party authentication tool, you may need to run the returned text through filtering and checks, as required by the tool.



---

**Note** Refer to Appendix A, API Extensions, for detailed information on the API calls described above.

---



# CHAPTER 6

## RSM Services

---

This chapter describes how to enable the two RSM services, Cisco RSM (Tomcat-VLEngine) and Cisco RSM (PhoneSim), so that they run upon startup. (The installer automatically enables the VLEngine and PhoneSim services to run at startup.)

Information on how to remove RSM from your Cisco environment, as well as all of its settings and components, is also provided.

## RSM Enable, Check, Restart

The following procedures describe how to enable VLEngine and PhoneSim, ensure that RSM is properly installed and running, and restart the RSM services, if necessary.

### To enable the VLEngine and PhoneSim services:

- 
- Step 1** Navigate to **Start > Settings > Control Panel**.
  - Step 2** Click **Administrative Tools**, then click **Services**.
  - Step 3** Right-click the **Cisco-RSM-VLEngine** service, then select **Properties**.
  - Step 4** Select **Automatic** from the Startup type pull-down menu.
  - Step 5** Click **Start** for Service status.
  - Step 6** Click **OK** to save your settings. The service will now start upon server startup.

- Step 7** Repeat steps 3 through 6 for the **Cisco-RSM-PhoneSim** service, to start the PhoneSim service upon server startup.

### To ensure RSM is installed and running properly:

- 
- Step 1** Navigate to **Start > Programs > Administrative Tools > Services**.
- Step 2** Verify that the service **Cisco-RSM-VLEngine** is running.
- Step 3** Verify that the service **Cisco-RSM-PhoneSim** is running.
- Step 4** Right-click **Start** then select **Task Manager**.
- Step 5** Select the **Processes** tab. Verify that the **java.exe** and **phonesim.exe** processes for the VLEngine are running.

### To restart the RSM services:

- 
- Step 1** Navigate to **Start > Settings > Control Panel**.
- Step 2** Click **Administrative Tools**, then click **Services**.
- Step 3** Right-click the **Cisco-RSM-VLEngine** service, then click **Restart**.
- Step 4** Right-click the **Cisco RSM - PhoneSim** service, then click **Restart**.

## Removing RSM

The procedures in this section describe how to remove RSM and its components from your IP IVR or CVP environment, if necessary.

### IP IVR Removal

For each IP IVR VRU with RSM integration, you will need to remove the call flow script and the RSM prompts.

### To remove RSM and the call flow script in a non-Unified ICME environment:

- 
- Step 1** Log into the IP IVR web interface.

- Step 2** Navigate to **Applications > Application Management**.
- Step 3** Click the trash can icon for the RSM application, then click **Yes** when prompted to delete the associated trigger.
- Step 4** Navigate to **Applications > Script Management**.
- Step 5** Click the trash can icon for the **RSM.aef** script, then click **OK**.

#### To remove the RSM call flow script in a Unified ICME environment:

---

- Step 1** Log into the IP IVR web interface.
- Step 2** Click the **Subsystems > ICM** link.
- Step 3** Click the **ICM VRU Scripts** link.
- Step 4** Remove the **RSM VRU** script.

#### To remove RSM prompts:

---

- Step 1** Log into the IP IVR web interface.
- Step 2** Navigate to **Applications > Prompt Management**.
- Step 3** Select the **en\_US** directory.
- Step 4** Select the **Delete Folder** link.
- Step 5** Select **VL** from the drop-down list, then click **Delete**.

## CVP Removal

For each CVP VRU with RSM integration, you will need to remove the call flow script, the call flow project files, and the RSM prompts.

#### To remove the RSM call flow script

---

- Step 1** Run the **updateApp.bat** script, located in the **C:\Cisco\CVP\VXMLServer\applications\RSM\admin** directory.
- Step 2** Delete the **C:\Cisco\CVP\VXMLServer\applications\RSM** directory when prompted.

### To delete the RSM call flow project files:

- 
- Step 1 Open the RSM project in VoiceXML Studio,
  - Step 2 Right-click on the project's root icon in the Navigator pane, then select **Delete**.
  - Step 3 Delete both the project and the project files.

### To remove RSM prompts:

- 
- Step 1 Navigate to **C:\Cisco\CVP\MediaFiles\en-us\VL**.
  - Step 2 Delete the directory and all of its contents.

## RSM Application Removal

### To remove the RSM application from your Cisco environment:

- 
- Step 1 Click **Start > Control Panel > Add or Remove Programs**.
  - Step 2 Follow the prompts to remove Cisco Remote Silent Monitoring. All RSM-related service entries will also be deleted.

## Unified ICME Removal

In a Unified ICME environment, you will need to remove all RSM-specific supervisor login accounts.

### To remove the supervisor login accounts:

- 
- Step 1 From the Admin Workstation (AW), click **Start > All Programs > ICM Admin Workstation > Configuration Manager**.
  - Step 2 Expand **Tools > Explorer Tools**.
  - Step 3 Double-click **Agent Explorer**.
  - Step 4 Click **Retrieve** to return a list of all existing agents in the environment.
  - Step 5 Click any account in the list.

- Step 6** Click **Multiple** below the account listing. The Delete Multiple window appears.
- Step 7** Select the RSM-specific agents previously created, then click **Delete**.
- Step 8** Click **OK** to return to the Agent Explorer, then click **Save**.

## Unified CM Removal

To remove RSM from your Unified CM environment, you must perform all of the following tasks for each Unified CM cluster that RSM is installed on.

### To disassociate all simphone devices from pguser:

- 
- Step 1** Log into the Unified CM web interface.
  - Step 2** Navigate to **User Management > Application User**.
  - Step 3** Click **Find** to display all application users. Locate then click the pguser account for your cluster.
  - Step 4** Select the simphone devices in the **Device Information > Controlled Devices** listbox.
  - Step 5** Click the up arrow to move the devices to the Available Devices listbox.
  - Step 6** Click **Save**. Repeat steps 1 through 5 for each cluster.

### To remove the RSM application user account:

- 
- Step 1** Navigate to **User Management > Application User**.
  - Step 2** Click **Find**. A list of application users is displayed.
  - Step 3** Select the **rsmuser** account.
  - Step 4** Click **Delete Selected**. The account is deleted.

### To remove all simphone devices:

- 
- Step 1** Navigate to **Device > Phone**.
  - Step 2** Select **Device Name** and **begins with** search criteria, then enter **00005E** in the **Find** textbox.

- Step 3 Click **Find**. A list of RSM simphones appears.
- Step 4 Click **Select All**, then click **Delete Selected**. The simphone devices are deleted.

#### To remove the RSM SimPhone calling search space:

- 
- Step 1 Navigate to **Call Routing > Class of Control > Calling Search Space**.
  - Step 2 Enter the name of the RSM calling search space previously created (e.g., **RSMSimPhone**) then click **Find**. (If you do not remember the name of the calling search space, click **Find** and search for the entry from the unfiltered results.)
  - Step 3 Select the name then click **Delete Selected**. The calling search space is deleted.

#### To remove the RSM SimPhone partition:

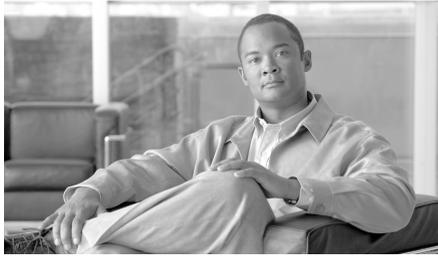
- 
- Step 1 Navigate to **Call Routing > Class of Control > Partition**.
  - Step 2 Enter the name of the RSM partition previously created (e.g., **RSMSimPhone**) then click **Find**. (If you do not remember the name of the partition, click **Find** and search for the entry from the unfiltered results.)
  - Step 3 Select the name then click **Delete Selected**. The partition is deleted.

#### To remove the RSM SimPhone device pool:

- 
- Step 1 Navigate to **System > Device Pool**.
  - Step 2 Enter the name of the RSM device pool previously created (e.g., **RSMSimPhone**) then click **Find**. (If you do not remember the name of the device pool, click **Find** and search for the entry from the unfiltered results.)
  - Step 3 Select the name then click **Delete Selected**. The device pool is deleted.

#### To remove the RSM SimPhone region:

- 
- Step 1 Navigate to **System > Region**.
  - Step 2 Enter the name of the RSM region previously created (e.g., **RSMSimPhone**) then click **Find**. (If you do not remember the name of the region, click **Find** and search for the entry from the unfiltered results.)
  - Step 3 Select the name then click **Delete Selected**. The region is deleted.



# CHAPTER 7

## Troubleshooting

---

This chapter provides information on the RSM log files, and provides case scenarios and troubleshooting guidance for system errors and other issues. Most troubleshooting issues will be related to JTAPI or CTI OS, and can be easily fixed by an experienced Cisco Enterprise Call Center Administrator.

### Log Files

RSM maintains several troubleshooting logs for the VLEngine and PhoneSim services. Note that if you change the VLEngine or Phone Sim Log Level parameters, you must restart the VLEngine or PhoneSim, respectively. :

*Table 7-1 Log Files*

<b>Log File</b>	<b>Directory</b>
VLEngine Logs	vlengine\logs
PhoneSim Logs	phonesim\logs
VLEngine - CTI OS Trace Logs	vlengine\logs\ctiosLogs
VLEngine - JTAPI Trace Logs	As per jtapiprefs setting



**Note**

To verify that RSM can see Agents, Skills, Skill Groups, Supervisor Login, and Active Agent Cells, enter the following URL in your web browser:

[http://<RSM\\_Server\\_IP\\_Address>:8080/vlengine/testEngineServlet.jsp](http://<RSM_Server_IP_Address>:8080/vlengine/testEngineServlet.jsp)

---

# General Call Flow Issues

## Agent Monitoring Request Fails

**Symptom** A supervisor tries to monitor an agent but the monitoring request fails, with no helpful or pertinent feedback from the IVR interface. For example, the supervisor hears, “Starting to monitor” and then, “Conversation has ended, you will now be returned to the main menu.”

**Possible Cause** A JTAPI-related error returns a GENERAL\_ERROR result from the VLEngine or PhoneSim back to the VRU. The VRU tries to play this text data as if it were audio data, and a “cannot recognize the file format” message is returned in the IOS CVP VRU error log files. (IP IVR error log files will show a similar message if the SS\_PROMPT subsystem debugging is turned on.)

### Error Message

```
Mar 29 00:28:17.277: %IVR_MSB-3-NOPROMPT: Could not create IVR prompt
http://10.1.110.110:29001/monitorAgent?agentID=42441&vrimeType=cvp
errno=0=Can not recognize the file format
```

**Recommended Action** Refer to the following topics in this section:

- [JTAPI Timeout on Monitoring Attempt](#)
- [Terminal Not In Domain Log File Message](#)
- [AddressOutOfService Exception](#)
- [CCNException with Error Code -1932787536](#)

## JTAPI Timeout on Monitoring Attempt

**Symptom** JTAPI latency may cause a timeout on the monitoring attempt in certain system environments. Thus, the VLEngine cannot locate an active conversation for the agent who is known to be on a call. This is a rare event, occurring less than 1% of the time for all monitoring attempts.

**Possible Cause** Review the VLEngine logs (located in the C:\CiscoRSM\vlengine\logs directory) and search for the following message:

### Error Message

```
INFO | jvm 1 | 2008/04/03 04:35:28 | - CanMonitorAgentID:
MONITOR ATTEMPT BEGIN
INFO | jvm 1 | 2008/04/03 04:35:28 | - CanMonitorAgentID:
Result: "MAY_MONITOR"
INFO | jvm 1 | 2008/04/03 04:35:34 | - DetermineAgentCluster:
AgentID: 42441; Result: "RSM_Cluster1"
INFO | jvm 1 | 2008/04/03 04:35:34 | - InitiateMonitorAgent
invoked for AgentID: 42441; PhoneID: SEP00005E000050; LineID: 42080
INFO | jvm 1 | 2008/04/03 04:35:34 | - Waiting for call TALKING
event on call observer for initiator terminal "SEP00005E000050",
line ID "42080"; target terminal of "SEP00005E000429", target line
ID "42441" (i.e. Can't find an active call on any line for the
targeted agent's phone yet.)
INFO | jvm 1 | 2008/04/03 04:35:35 | - JTAPI-CLI-1/0:
startMonitoring(): No active target terminal connections (none
present) for address "42441" on terminal "SEP00005E000429" (i.e.
Couldn't find an active call on any line for the targeted agent's
phone in the time allowed, so we gave up.)
INFO | jvm 1 | 2008/04/03 04:35:35 | - InitiateMonitorAgent:
MONITOR ATTEMPT END -- Result: "GENERAL_ERROR; AgentID: 42441;
PhoneID: SEP00005E000050; LineID: 42080; RESCLUSTERID: 0;
TARGETCALLID: 17406159; targetPhoneDeviceID: SEP00005E000429;
targetDN: 42441
```

**Recommended Action** Retry the monitoring request.

## Caller Asked To Hangup After Entering PIN

**Symptom** A caller dials into RSM, hears the normal user ID and PIN prompts. After submitting their PIN, a ring and then an error message is heard, stating, “I’m sorry, we are currently experiencing system problems. Please hang up and try your call again.”

**Possible Cause** VLEngine service is not running properly, or a valid connection to port 8080/TCP cannot be made to the RSM server.

**Recommended Action** Restart the VLEngine service. If Windows firewall is used, ensure that the port used by the VRU to communicate with VLEngine (8080/TCP) is unblocked. (Refer to Chapter 3, RSM Services.)

## Caller Suddenly Asked To Hangup

**Symptom** A caller has been performing normal call flow operations, but suddenly a ring and then an error message is heard, stating, “I’m sorry, we are currently experiencing system problems. Please hang up and try your call again.”

**Possible Cause** The VLEngine or PhoneSim services have stopped running on the RSM server, or were otherwise unable to process the caller’s request. The services may have stopped during a network outage when the VRU was unable to make contact with the RSM servers.

**Recommended Action** Check the status of the VLEngine and PhoneSim services and the RSM servers, and restart them if they are stopped. (Refer to Chapter 3, RSM Services.)

## Invalid Login Message

**Symptom** A valid supervisor account (e.g., DN 42071) is rejected during login and an error message is heard, stating, “Your login was invalid.”

**Possible Cause** CTI OS login, required to validate the caller's credentials as entered, is not working properly. Review the VLEngine logs (located in the C:\CiscoRSM\vlengine\logs directory) for the login request, and search for one of the following messages:

### Error Message

```
17-08-07 11:46:16:871 EDT - {INFO} voicelink.vlengine Thread
[http-8080-Processor25]; Using Instrument "42071" to log in.
```

```
17-08-07 11:46:17:121 EDT - {FATAL} voicelink.vlengine Thread
[JCIL_Sess(7959524)_EvtThd(22293724)]; CTIOS Failure: IPCC
Error [12005]Login could not be performed - Possible causes
are Invalid Instrument; Media Termination Problem or other CM
issue
```

```
17-08-07 11:46:17:418 EDT - {INFO} voicelink.vlengine Thread
[http-8080-Processor25]; LOGIN ATTEMPT -- SupervisorID:
41001; Result: "INVALID_SUPERVISOR_ID"
```

### Recommended Action

- Verify that the PhoneSim service is running, and is properly logged into the device used for the CTI OS login attempt. (Refer to Chapter 3, RSM Services.)
- Verify that the device is registered to the RSM server IP that is running the PhoneSim service, in the Unified CM Administration interface.
- Verify that the device used for the login attempt is a member of the VLEngine login pool. Only DNs in the login pool will be used as the CTI OS login instrument for caller login attempts. If the DN is not a member of the login pool, you may need to adjust the following registry keys for the cluster configuration (refer to Appendix B, Registry Keys):

```
ClusterN_NumSimPhonesUsedForCTIOSAgentLogins
ClusterN_PhoneSim_StartMACRange
ClusterN_PhoneSim_StartLineNumRange
```

- Verify that the DN is listed as a valid device target in Unified ICME. Device target entries must exist in Unified ICME for all device DNs in the VLEngine login pool.
- Verify that the DN is associated with the appropriate pguser account.
- Try logging in with the same agent via the CTI OS desktop, with the same instrument (e.g., 42071). If the login does not work, the problem may be a general CTI OS login issue.
- Try restarting the RSM sever by restarting the VLEngine and PhoneSim services. (Refer to Chapter 3, RSM Services.)

## Invalid Login Error Output

**Symptom** Whenever a supervisor attempts to log into the system using IDs that are known to be valid, an error output is displayed.

**Possible Cause** The Login WaitOnMultipleEvents() timeout is paired with the INVALID\_SUPERVISOR\_ID resultant code. VLEngine is probably not able to use the simulated instrument to log in (e.g., 42002, as per the sample error messages, below, located in the C:\CiscoRSM\vlengine\logs directory).

### Error Message

```
jvm 1 | - CTI-AM-1: Connecting to CTIOS Server
rwcsvr021:42028 (backup is rwcsvr022:43028)

jvm 1 | - CTI-AM-1: Reserved phone ID 42002 with end reserve
time of 1194981846953

jvm 1 | - CTI-AM-1: Login: Instrument "42002". AgentID:
41001; PeripheralID:5000

jvm 1 | - CTI-AM-1(41001): Login WaitOnMultipleEvents()
timeout

jvm 1 | - CTI-AM-1: Disconnecting from CTIOS Servers
rwcsvr021:42028, rwcsvr022:43028

jvm 1 | - CheckUserCredentials: LOGIN ATTEMPT --
SupervisorID: 41001; Result: "INVALID_SUPERVISOR_ID"
```

**Recommended Action**

- Verify that the PhoneSim service is running, and is properly logged into the device used for the CTI OS login attempt (e.g., 42002). (Refer to Chapter 3, RSM Services.)
- Verify that the device being used to make the login attempts (e.g., 42002) is registered to the RSM server IP that is running the PhoneSim service, as configured via the Unified CM Administration interface.
- Verify that the DN is listed as a valid device target in Unified ICME. Device target entries must exist in Unified ICME for all device DNs in the VLEngine login pool.
- Verify that the DN is associated with the appropriate pguser account.
- Try logging in with the same agent via the CTI OS desktop, with the same instrument (e.g., 42071). If the login does not work, the problem may be a general CTI OS login issue.
- Try restarting the RSM sever by restarting the VLEngine and PhoneSim services. (Refer to Chapter 3, RSM Services.)
- Verify that the pguser account is configured as an application user in the Unified CM Administration interface, not an end user. (This may be the case if the CM configuration is the result of a version 4.x upgrade.)

## Silent Monitoring Stops After Ten Minutes (CVP)

**Symptom** After ten minutes of silent monitoring using CVP, the caller is dropped out of the monitoring session, but is not disconnected.

**Possible Cause** The relationship between RSM and the IOS prompt streaming sub-system cannot maintain calls beyond ten minutes.

**Recommended Action** Re-enter the monitoring session or initiate a new session when prompted.

## Agent Is Not A Supervisor Error

**Symptom** An agent tries to log into the system and an error output is displayed.

**Possible Cause** The supervisor account which attempted the login is not flagged as a supervisor login or is not assigned as a supervisor of a team. Review the VLEngine logs (located in the C:\CiscoRSM\vlengine\logs directory) for the login request, and search for one of the following messages:

### Error Message

```
jvm 1 | - CTI-AM-1: Connecting to CTIOS Server
rwcsvr021:42028 (backup is rwcsvr022:43028)

jvm 1 | - CTI-AM-1: Reserved phone ID 42002 with end reserve
time of 1194981846953

jvm 1 | - CTI-AM-1: Login: Instrument "42002". AgentID:
41001; PeripheralID:5000

jvm 1 | - CTI-AM-1(41001): Login failed: Agent is not a
supervisor

jvm 1 | - CTI-AM-1: Disconnecting from CTIOS Servers
rwcsvr021:42028, rwcsvr022:43028

jvm 1 | - CheckUserCredentials: LOGIN ATTEMPT --
SupervisorID: 41001; Result: "NOT_A_SUPERVISOR"
```

**Recommended Action** Ensure that the Supervisor Login Account Creation procedure has been properly followed for the creation of this account. (Refer to Chapter 3, RSM Services.)

# VLEngine Runtime Issues

The following line may appear in your VLEngine log files and may be safely ignored:

```
CTIOS Failure: Agent state has been set to Not Ready
because calls routed to you were not received. Please ask
your Administrator for help.
```

## Terminal Not In Domain Log File Message

**Symptom** The following message or similar is found in the VLEngine log file (located in the C:\CiscoRSM\vlengine\logs directory):

```
com.cisco.jtapi.InvalidArgumentExceptionImpl:
Terminal SEP001BD51242CE is not in provider's domain.
```

**Possible Cause** The specified terminal is probably improperly associated to the RSM application user account that VLEngine is configured to use.

**Recommended Action** Use the Unified CM administration interface to view the application user device associations, and ensure that all RSM simphone devices, as well as all agent phones, have been added to the controlled list.

## Connection to CTI OS Server Denied

**Symptom** Monitor Mode connection to CTI OS is denied.

**Possible Cause** Another application may be accessing the CTI OS server with a monitor mode connection. RSM may also fail to connect if the CTI OS server has security enabled. Check the VLEngine log files, located in the C:\CiscoRSM\vlengine\logs directory.

### Error Message

```
INFO | jvm 1 | 2007/11/06 10:33:31 | - CTIOS: Connecting to
CTIOS Server 10.1.110.18:42028 (backup is 10.1.110.19:43028)
```

```
INFO | jvm 1 | 2007/11/06 10:33:31 | - CTIOS Failure:
WARNING!!! Monitor Mode Connection Is Denied. Number of
supported monitor mode connections [2] by one CTI OS Server
pair has been reached.
```

**Recommended Action** Ensure that no other applications accessing the CTI OS server (e.g., 10.1.110.18 as per sample, above) have monitor mode connections to the CTI OS server.

**Recommended Action** Modify the MaxMonitorModeConnections registry key for the CTI OS server to allow for additional connections. Refer to the *CTI OS System Manager's Guide* document, located at

[http://www.cisco.com/en/US/products/sw/custcosw/ps14/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/custcosw/ps14/prod_installation_guides_list.html)

## Supervisor With Valid ID and PIN Cannot Log In

**Symptom** A supervisor cannot log into RSM, with valid ID and PIN.

**Possible Cause 1.** The supervisor is logged into the CTI OS agent desktop using the same credentials. Check the VLEngine log file (located in the C:\CiscoRSM\vlengine\logs directory) for the following:

```
17-08-07 17:50:18:715 EDT - {DEBUG} voicelink.vlengine Thread
[http-8080-Processor22]; CTIOS-AM: Login: Instrument
"42071". AgentID: 41001; PeripheralID: 5000

17-08-07 17:50:19:215 EDT - {WARN} voicelink.vlengine Thread
[JCIL_Sess(5076865)_EvtThd(6385630)]; CTIOS Failure: IPCC
Error [10102]The agent is already LOGGED ON

17-08-07 17:50:19:762 EDT - {DEBUG} voicelink.vlengine Thread
[http-8080-Processor22]; CTIOS-LOGIN(41001): Logout
unsuccessful: Logout() failure

17-08-07 17:50:19:762 EDT - {DEBUG} voicelink.vlengine Thread
[http-8080-Processor22]; CheckUserCredentials: LOGIN ATTEMPT
-- SupervisorID: 41001; Result: "INVALID_SUPERVISOR_ID"
```

**Recommended Action** Log the supervisor out of the desktop before logging into RSM. Ensure that you have created separate and exclusive supervisor accounts for RSM use, and are not being used for CTI OS agent desktop

logins. Also, ensure that each supervisor login is being used only by one supervisor; multiple simultaneous logins are not supported. (Refer to the “Supervisor Login Account Creation” topic in Chapter 3, Pre-Installation Tasks.)

**Possible Cause 2.** The device the supervisor is using is in an invalid state (e.g., is toggling between reserved and ready) and its status cannot be retrieved during CTI OS login.

**Recommended Action** Restart the PhoneSim service. (Refer to Chapter 3, RSM Services.)

**Possible Cause 3.** The supervisor's login is hung (i.e., stuck). This occurs if the supervisor is not logged into the CTI OS agent desktop, PhoneSim has been restarted, and the error is still being generated.

**Recommended Action** Run the CTI OS SDK AllAgents.exe to log the supervisor out of the system, or restart the VLEngine service. (Refer to Chapter 3, RSM Services.)

## VLEngine Will Not Start

**Symptom** VLEngine will not start.

**Possible Cause** Insufficient memory, as per system requirements. Check the VLEngine log file, located in the C:\CiscoRSM\vlengine\logs directory.

### Error Message

```
ERROR | wrapper | 2007/12/20 08:22:19 | JVM exited while  
loading the application.
```

```
STATUS | wrapper | 2007/12/20 08:22:23 | Launching a JVM...
```

```
INFO | jvm 5 | 2007/12/20 08:22:24 | Error occurred during  
initialization of VM
```

```
INFO | jvm 5 | 2007/12/20 08:22:24 | Could not reserve enough  
space for object heap
```

```
INFO | jvm 5 | 2007/12/20 08:22:24 | Could not create the Java  
virtual machine.
```

```
ERROR | wrapper | 2007/12/20 08:22:24 | JVM exited while  
loading the application.
```

**Recommended Action** If there is enough memory in the system and the error still occurs, you can manually force the VLEngine to run by modifying the **wrapper.java.maxmemory** parameter in the **wrapper.conf** file (located in the C:\CiscoRSM\vlengine directory) to a lower value (e.g., 1000)

**Caution**

Modifying the wrapper.conf file is not supported by Cisco, as it may lead to unreliable system behavior.

## AddressOutOfService Exception

**Symptom** The following error message or similar is found in the VLEngine log file (located in the C:\CiscoRSM\vlengine\logs directory):

**Error Message**

```
com.cisco.jtapi.AddressOutOfService
```

**Possible Cause 1** The simphone device associated with this message may have the wrong device pool setting.

**Recommended Action** Launch the Unified CM administration interface and ensure that the simphone device settings are correct.

**Possible Cause 2** The RSM simphone device pool configuration may be incorrect.

**Recommended Action** Ensure that the RSM simphone device pool settings are configured as described in the “Simphone Device Dependencies” topic in Chapter 3, Pre-Installation Tasks.

## CCNException with Error Code -1932787536

**Symptom** The following message or similar is found in the VLEngine log file (located in the C:\CiscoRSM\vlengine\logs directory):

### Error Message

```
JTAPI-CLI-1/2: Got Exception for call with initiator terminal
"SEP00005E00054f", line ID "42579"; target terminal of
"SEP00005E000423", target line ID
"42435":com.cisco.jtapi.PlatformExceptionImpl: Monitor request
failed:com.cisco.cti.client.CCNException
com.cisco.jtapi.PlatformExceptionImpl: Monitor request
failed:com.cisco.cti.client.CCNException
    at com.cisco.jtapi.CallImpl.startMonitor(CTQF)
    at com.cisco.jtapi.CallImpl.startMonitor(CTQF)
    at com.knoahsoft.voicelink.vlengine.JTAPIClient.
    startMonitoring(JTAPIClient.java:352)
    at com.knoahsoft.voicelink.vlengine.servlet.
    InitiateMonitorAgent.doGet(InitiateMonitorAgent.java:181)
[...]
    at org.apache.tomcat.util.net.LeaderFollowerWorkerThread.
    runIt(LeaderFollowerWorkerThread.java:81)
    at org.apache.tomcat.util.threads.ThreadPool$
    ControlRunnable.run(ThreadPool.java:685)
    at java.lang.Thread.run(Thread.java:619)
JTAPI-CLI-1/2: EXCEPTION Errorcode is: -1932787536
```

**Possible Cause** The built-in-bridge resource is probably not enabled on the agent phone to be monitored (SEP00005E000423 in the above example).

**Recommended Action** Launch the Unified CM administration interface and navigate to the device settings for the agent phone. Ensure that the built-in bridge setting is enabled.

# PhoneSim Runtime Issues

## Simphone Registrations Are Rejected

**Symptom** When starting the PhoneSim service, the Simphone registrations are rejected.

**Possible Cause** Start range of the ClusterN\_PhoneSim\_StartMACRange parameter, as previously configured, does not correspond to start range of ClusterN\_PhoneSim\_StartLineNumRange parameter for cluster N.

For example, if Cluster1\_PhoneSim\_StartMACRange is set to 00005E000047 and Cluster1\_PhoneSim\_StartLineNumRange is set to 42001, then line DN 42001 is probably not assigned to phone device ID 00005E000047.

Check the log files (located in the C:\CiscoRSM\phonesim\logs directory) for the following:

```
08/17/07 11:25:41 (Eastern Daylight Time), [4024]
CHTTPServer.cpp      :236 INFO - Received HTTP request from
machine with ip address 10.1.14.76 on port 1244 with request
uri "/sendRegisterMessage?PhoneSimExt=42001"
```

```
08/17/07 11:25:41 (Eastern Daylight Time), [4024]
VoipCommon.cpp      :986 ERROR - Client Socket : Send
Failed :WSAENOTSOCK
```

```
08/17/07 11:25:41 (Eastern Daylight Time), [4024]
VoipCommon.cpp      :986 ERROR - Client Socket : Unable to
send dataUnknown Error
```

**Recommended Action** Refer to the “Cluster Configuration Registry Keys” topic in Appendix B, Registry Keys, for information on how to modify the start MAC range of the ClusterN\_PhoneSim\_StartMACRange parameter.

## PhoneSim Log File Error Messages

The following table lists all the PhoneSim error messages that may appear in the log files, and their probable causes.

**Table 7-2** *PhoneSim Log File Error Messages*

Error Message	Description	Resolution
Called with unknown alert type <i>&lt;alert type&gt;</i> while sending email alert	An unknown email alert type was received—i.e., it is not on list of five predefined types:  APPLICATION_DOWN PROCESS_CREATION_FAILURE PHONESIM_STARTED VLENGINE_NOT_RUNNING VLENGINE_CONNECTION_CLOSED	This is a benign message. Contact Cisco support if this occurs on a regular basis so the message can be relayed to the RSM development team for review.
Unable to connect to mail server at <i>&lt;mail server exchange IP&gt;</i> on <i>&lt;port number&gt;</i>	PhoneSim is unable to connect to the mail server at IP address on displayed port number	This is a rare, transient phenomenon. Verify that firewall, IP address, and port are working properly (e.g., ping).
Unable to receive data from mail server at <i>&lt;configured mail server exchange IP&gt;</i> on <i>&lt;configured port number&gt;</i>	The socket connected to the mail exchange server is unable to receive data from the server	This is a rare, transient incident. Verify that the firewall, IP address, and port are working properly (e.g., ping).
Failed to connect to <i>&lt;IP address&gt;</i> on <i>&lt;port number&gt;</i> for <i>&lt;socket client name&gt;</i>	Socket failed to connect to displayed client name	This is a rare, transient phenomenon. Verify that firewall, IP address, and port are working properly (e.g., ping). If this error appears on a regular basis, restart the PhoneSim service (note that doing so will cancel all sessions currently being monitored).
Number of call managers exceeds limit	Number of configured Call Managers is greater than number allowed by RSM, which is three (3).	An improper change was probably made to a cluster registry key. Refer to the “Cluster Configuration Keys” topic in Appendix B, Registry Keys.

Table 7-2 PhoneSim Log File Error Messages

Socket connection closed abruptly from machine with <IP address>, <port number of machine>	HTTP/Timer for the IP address socket connection returned an invalid value for received data on the socket	This is a rare, transient phenomenon. Verify that firewall, IP address, and port are working properly (e.g., ping). If this error appears on a regular basis, contact Cisco support so the message can be relayed to the RSM development team for review.
Socket accept failed for HTTP server thread last error = <previous error code>	Failed to accept HTTP server socket connection request	This is a rare, transient phenomenon that may occur when the PhoneSim service is terminating. If this error appears on a regular basis, or at any other time other than when the service is shutting down, contact Cisco support so the message can be relayed to the RSM development team for review.
Buffer exceeded: available buffer size = <available size value>, needed = <needed size value> for SIP/Timer socket buffer	Buffer exceeded limit when parsing SIP/Timer socket message data	This is a rare, transient phenomenon. Save the SIP/ HTTP packet capture dump from the RSM server (using packet sniffing software such as Wireshark), then send this information to Cisco support so the message can be relayed to the RSM development team for review.
Buffer exceeded: available buffer size = <available value>, needed = <needed value> for timer socket buffer	Buffer exceeded limit when parsing HTTP Timer socket message data	This is a rare, transient phenomenon. Save the SIP/ HTTP packet capture dump on the RSM server (using packet sniffing software such as Wireshark), then send this information to Cisco support so the message can be relayed to the RSM development team for review.
Socket connection closed abruptly for VLEngine from machine with <IP address of VLEngine>, <port number>	This occurs if the VLEngine takes too long to respond to PhoneSim requests	The VLEngine service is probably at its maximum load capacity. Disconnect, then try another monitoring session.
Failed to locate the socket table index for HTTP response message	Reading and processing of HTTP/VLEngine messages via connected socket failed	This is a benign message. Contact Cisco support so the message can be relayed to the RSM development team for review.

Table 7-2 PhoneSim Log File Error Messages

Received <i>&lt;error return code&gt;</i> for <i>&lt;action URL&gt;</i> and <i>&lt;agent ID trying to monitor&gt;</i> from <i>&lt;client socket IP address&gt;</i> and <i>&lt;port number&gt;</i>	This error code is displayed when PhoneSim is exchanging messages with VLEngine	Review the returned values of the message—URL, agent ID, client IP address, and port number—, and troubleshoot accordingly (e.g., ensure agent ID is in the system, that the port is working, etc.).
Unable to get cluster index for <i>&lt;cluster_name&gt;</i>	PhoneSim service is unable to return cluster information from the VLEngine service for the agent the system is attempting to monitor	There is probably an inconsistency between the PhoneSim and VLEngine cluster configurations. This may occur in a multiple server scenario, where the PhoneSim and VLEngine services are installed on separate machines. The services were either improperly configured during installation, or an improper change was made to a registry key. Refer to the “Cluster Configuration Keys” topic in Appendix B, Registry Keys.
Could not open connection with VLEngine at machine with <i>&lt;machine IP address&gt;</i> , <i>&lt;port number&gt;</i>	Failed to open a socket connection with VLEngine for specified IP address and port number	This is a rare, transient phenomenon. Confirm that the IP address and port numbers for the VLEngine service are properly configured. Ensure that the port is enabled by the firewall. (This may also occur if there are too many pending requests to the VLEngine and PhoneSim is unable to allocate a new socket for connecting to VLEngine.)
Failed to open <i>&lt;PhoneSimStats.txt&gt;</i> statistics file	Failed to open text file to write configured simulated phones statistics, as per command from PhoneSimDynConfig	The RSM installation drive (e.g., C:\) is probably full and cannot create the file. Create space on the drive, then ensure the file is created.

Table 7-2 PhoneSim Log File Error Messages

Failed to write Phonesim statistics to <i>&lt;PhoneSimStats.txt&gt;</i> file	Unable to write to PhoneSimStats.txt file, after command was issued and file was opened	The permissions for the file were probably improperly modified. Check the file to ensure it is configured for write permission.  The RSM installation drive may also be full and cannot create the file. Create space on the drive, then ensure the file is created.
The connection to SIP proxy server at <i>&lt;CallManager IP&gt;</i> and <i>&lt;SIP standard Port number&gt;</i> for phone with <i>&lt;simulated phone extension number&gt;</i> closed	Simulated phone failed to keep its registered binding open with SIP Proxy in the Call Manager	Check basic network connectivity. Verify that Call Manager is running and not blocked by the firewall.  Verify that no secondary or other RSM servers are configured for the same simphone extensions.  (NOTE: It is recommended that the Call Manager and Peripheral Gateway machines be located in the same geographical vicinity and within the same network as the RSM server to better isolate the problem.)
Socket read failed for agent with <i>&lt;simulated phone extension number&gt;</i>	Simulated phone SIP socket failed to read data received from remote machine (i.e., Call Manager)	Check data in the PhoneSimStats file (from the PhoneSimDynConfig application) to determine if this is a recurring socket failure. If so, check basic network connectivity and firewall settings to verify that Call Manager is running and not being blocked by the firewall.  If this error appears on a regular basis, the Call Manager may be too busy (i.e., overloaded) or may be trying to disconnect the simphone due to improper or duplicate registration of the simphone.
<i>&lt;SIP warning message&gt;</i> received for phone with <i>&lt;simulated phone extension number&gt;</i>	SIP warning response message for SIP request, when warning message is received	Forward the reason code and cause number in the SIP warning header to Cisco support. This information will be used to discern why Call Manager rejected the simphone request.

Table 7-2 PhoneSim Log File Error Messages

Failed to open <PhoneSim configuration file>	Failed to open PhoneSim configuration file when initiating the PhoneSim service, in order to read configured keyword names and respective values	<p>Check the file to ensure it is configured for read permission.</p> <p>Ensure that PhoneSim.ini file exists in the C:\CiscoRSM\PhoneSim directory. Create a blank file if it does not exist.</p> <p>It is also possible that the file is corrupt, in which case you can delete the file and create a new blank one.</p>
Failed to load <PhoneSim configuration file>	Failed to load the PhoneSim configuration file when initiating the PhoneSim service, in order to read configured keyword names and respective values	<p>Check the file to ensure it is configured for read permission.</p> <p>Ensure that PhoneSim.ini file exists in the C:\CiscoRSM\PhoneSim directory. Create a blank file if it does not exist.</p> <p>It is also possible that the file is corrupt, in which case you can delete the file and create a new blank one.</p>
OpenSCManager failed, error code = <error code>	<p>MFC service manager failed to initiate the PhoneSim service while trying to open it.</p> <p>Refer to Microsoft documentation for standard list of MFC error codes.</p>	RSM was probably installed while logged in on the machine as a user other than the administrator. If this is the case, you must reinstall RSM.
OpenService failed, error code = <error code>	<p>MFC service manager failed to initiate the PhoneSim service while trying to open it.</p> <p>Refer to Microsoft documentation for standard list of MFC error codes.</p>	<p>RSM was probably installed while logged in on the machine as a user other than the administrator. If this is the case, you must reinstall RSM.</p> <p>It is also possible that the PhoneSim service was never properly installed during the RSM installation process.</p>

Table 7-2 PhoneSim Log File Error Messages

StartService failed, error code = <i>&lt;error code&gt;</i>	MFC service manager failed to initiate the PhoneSim service while trying to start it.  Refer to Microsoft documentation for standard list of MFC error codes.	RSM was probably installed while logged in on the machine as a user other than the administrator. If this is the case, you must reinstall RSM.  It is also possible that the PhoneSim service was never properly installed during the RSM installation process.  It is also possible that the log on password for the service was changed and so the account needs to be reconfigured for the service.
Mac Address is not configured correctly: length should be 12 character only	Cisco IP phones MAC addresses are twelve (12) characters by default	An improper change was probably made to a MAC-related registry key. Refer to Appendix B, Registry Keys, and ensure all MAC address configurations are compliant.
Mac Address is not configured correctly: Invalid character <i>&lt;character in MAC address&gt;</i> in Mac Address <i>&lt;MAC Address&gt;</i>	Characters in MAC address not: 0 through 9; a through f; or A through F.	An improper change was probably made to a MAC-related registry key. Refer to Appendix B, Registry Keys, and ensure characters in all MAC address configurations are compliant.
<i>&lt;Cluster name&gt;</i> : No of phones for CTIOS login <i>&lt;number of login pool phones&gt;</i> exceeds or equals max number of phones in the cluster	Number of login pool phones is equal or greater to maximum number of phones allowed in cluster	An improper change was probably made to a login or cluster registry key. Refer to Appendix B, Registry Keys.
<i>&lt;Cluster name&gt;</i> : Invalid call manager index <i>&lt;call manager index in cluster&gt;</i>	This message appears if RSM has been configured for more than three (3) Call Managers	An improper change was probably made to a cluster registry key. Refer to the “Cluster Configuration Keys” topic in Appendix B, Registry Keys.
Illegal value for registry keyword <i>&lt;registry name&gt;</i>	Registry value is either unacceptable or was improperly entered	An improper change was probably made to a registry key. Refer to Appendix B, Registry Keys, and check configuration values for Call Manager port numbers, CTIOS servers, PhoneSim, and VLEngine.

Table 7-2 PhoneSim Log File Error Messages

Failed to stop the <thread name> thread	Thread tried to stop, or is already stopped, when stopping the PhoneSim service	This is a rare, benign message that occurs during PhoneSim service shutdown.
Sum total of simulated phones in all clusters <sum value> exceeds MaxNumRequests <configured value>	Configured value for simphones and cluster do not match	An improper change was probably made to a registry key. Refer to Appendix B, Registry Keys, and check configuration values for clusters and MaxNumRequests key.
Illegal value for MaxNumRequests	Number of monitoring phones configured is greater than configured value of maximum number of phones allowed	An improper change was probably made to a registry key. Refer to Appendix B, Registry Keys, and check configuration values for clusters and MaxNumRequests key.
No of simulated phones must be specified	Number of simulated phones is configured for none (zero)	An improper change was probably made to a simphone registry key. Refer to Appendix B, Registry Keys.
Failed to sender e-mail address	Sender email address is not configured and is empty	An improper change was probably made to an email registry key. Refer to Appendix B, Registry Keys.
Failed to load an email address for alert notification	Sender email address is not configured and is empty	An improper change was probably made to an email registry key. Refer to Appendix B, Registry Keys.
Failed to retrieve domain name from sender's email address	Sender email address is configured so that the address does not specify a domain or IP address after the @ symbol	An improper change was probably made to an email registry key. Refer to Appendix B, Registry Keys.
Illegal keyword <keyword specified in PhoneSim configuration file> in configuration file	Keyword configured in PhoneSim configuration file does not exist	The PhoneSim.ini file was probably improperly modified, or there is a misspelling.
Illegal value <keyword value> for <keyword name>	Keyword has incorrect value	The PhoneSim.ini file was probably improperly modified, or there is a misspelling.

## Fatal Error Messages

The following table lists rare, fatal PhoneSim error messages that may appear in the log files, and their probable causes. Generally speaking, these errors occur if you are using a server that does not meet the minimum system requirements, as detailed in Chapter 2 (e.g., insufficient memory installed.) Restarting the service should resolve the issue.

**Table 7-3** PhoneSim Log File Fatal Error Messages

<b>Error Message</b>	<b>Description</b>
Unable to allocate memory of amount xx <numeric value> bytes for xx <object number> <application objects	Insufficient memory allocated for cluster, Call Manager, SupervisorPhones objects
Failed to allocate memory of XX <numeric value> bytes for send data buffer for supervisor phone with extension XX	Buffer size used to send voice data using this listener object failed to create the buffer size listed, before the simulated phones listener object was created
Failed to allocate memory of xx <numeric value> bytes for x listener objects for supervisor phone with extension xx	Simulated phone listener object creation failed when starting the service
Unable to allocate memory for CKeepAlive	Insufficient memory allocated for sending and receiving simulated SIP phones CKeepalive messages from Call Manager
Failed to allocate memory of size xx <numeric value> for receive audio buffer for phone with extension xx	Receiving audio buffer length is not configured or is empty
Failed to read the values from registry	Unable to read registry field values or registry does not exist (e.g., was mistakenly deleted), when starting service
Illegal value for NoOfClusters	Number of configured clusters has exceeded limit
MAC Address wrapped at max limit of xx	Maximum limit of MAC addresses for this value has been reached and new values cannot be generated by RSM for simphones
CKeepAlive Thread Creation failed	Initialization or creation of CKeepAlive thread failed

Table 7-3 PhoneSim Log File Fatal Error Messages

Failed to open timer socket connection	Timer socket connection failed when service started
RTPReceiver thread creation failed	Initialization or creation of RTPReceiver thread failed
Unable to allocate memory for XMLMessagesStack	Initialization or creation of XMLMessagesStack class object failed when starting service
CVoipLoggerThread thread creation failed	While initializing or creation of the CVoipLoggerThread thread object fails then this error could occur.
CAlertMessg thread creation failed	While initializing or creation of the CAlertMessg thread object fails then this error could occur.
CPhoneSimDynConfig thread creation failed	While initializing or creation of the CPhoneSimDynConfig thread object fails then this error could occur.
CPhoneSimServer thread not created. Last error = xx	While initializing or creation of the CPhoneSimServer thread object fails then this error could occur.
CHealthMonitor Thread Creation failed	While initializing or creation of the CHealthMonitor thread object fails then this error could occur.
<Thread name> thread creation failed	Initialization or creation of thread object failed





## APPENDIX **A**

# API Extensions

---

Cisco's Remote Silent Monitoring includes a simple HTTP-driven API for making service requests into the system, as well as IP IVR and CVP call flow scripts which demonstrate the use of this API. The specific APIs are for RSM's two services, VLEngine and PhoneSim.

CVP Unified Call Studio can make calls to most of these APIs by using the Subdialog element, and the response is dynamic VXML (with optional formatting).

IP IVR's CRS Editor prohibits direct invocation of the call flow scripts and parsing of return data. To handle these interactions, the VoiceBrowser step makes requests to an API URL, and a result code is returned, encoded as a variable in a VXML document (appropriately) named result.

## JSP Suffix

All documented HTTP API calls that can be called by a VRU call flow script also have a jsp suffix (with the exception of the determineAgentCluster and initiateMonitorAgent calls).

This allows the calls to be used in environments (e.g., IP IVR 5.0.2) that make assumptions, based on the URL filename extension, as to whether or not a URL is for dynamic data.

For example, the getAgentList call is available as both getAgentList and getAgentList.jsp. Both versions function identically. It is recommended that the jsp suffix always be used.

# VLEngine HTTP API

## checkUserCredentials.jsp

Checks validity of user ID (i.e., the Cisco agent ID) and PIN. Called by VRU call flow script (VXML, IP IVR, CVP).

### Parameters

**userID:** ID of user logging in.

**pin:** Password of user logging in.

**outputFormat:** Specifies format of returned data:

**plain:** Returned data contains no formatting. CREDENTIALS\_VALID result will be returned as simple text (i.e., CREDENTIALS\_VALID), for example. Appropriate for hand-written VXML scripts or anything that can perform a HTML request and process the result directly.

**vxml:** Data formatted in result variable of returned VXML document. Returned page has an <exit> statement that specifies a result variable in its namelist parameter, and which contains the return code for the operation. Appropriate for IP IVR's VoiceBrowser step.

**vxml-cvp:** VXML output. Includes extra data usable by a CVP Unified Call Studio call flow (specifies output as VXML sub-dialog, contains Audium tags, etc.).

### Returns

Parameter	Type
CREDENTIALS_VALID	Information supplied is valid
INVALID_USER_ID	Caller's user ID is invalid
INVALID_USER_PIN	PIN is not valid for the user
NOT_A_SUPERVISOR	Agent userID is not a supervisor in CTI OS

Parameter	Type
INVALID_PARAMETERS	One or more required parameters not specified
GENERAL_ERROR	See " <a href="#">Agent Monitoring Request Fails</a> " topic in Chapter 7, Troubleshooting

## canMonitorAgentID.jsp

Checks validity of agent ID, if the agent is logged in, and if the supervisor has the necessary permissions to monitor the agent. Called by the VXML script before calling monitorAgent on the PhoneSim service. Called by the VRU call flow script (VXML, IP IVR, CVP).

### Parameters

**agentID:** ID of agent to be checked.

**supervisorID:** ID of supervisor (i.e., caller) to be checked. Set to 0 to not perform supervisor permission-type checks (e.g., only agent availability checks will happen, where the system checks that the agent is logged in and talking).

**outputFormat:** Specifies format of returned data:

**plain:** Returned data contains no formatting. For example, a CREDENTIALS\_VALID result will be returned as simple text (i.e., CREDENTIALS\_VALID). This output method is appropriate for hand-written VXML scripts or anything that can perform a HTML request and process the result directly.

**vxml:** Returned data is formatted in result variable of returned VXML document. Returned page has an <exit> statement that specifies a result variable in its namelist parameter, which contains the return code for the operation. This output format is appropriate for IP IVR's VoiceBrowser step.

**vxml-cvp:** VXML output, which includes extra data that makes it usable by a CVP Unified Call Studio call flow (e.g., specifying the output as a VXML sub-dialog, contains Audium tags, etc.).

## Returns

Parameter	Type
MAY_MONITOR	All checks passed, supervisor can monitor agent
INVALID_AGENT_ID	Agent ID is invalid
INVALID_USER_ID	Caller's user ID is invalid
INVALID_PARAMETERS	One or more required parameters not specified
AGENT_CANT_MONITOR	Agent ID is valid but the agent is currently not known by the system to be logged in and active. The agent ID specified is valid, but either: the agent is not active (i.e., currently logged in and talking) and therefore has no active call ID; or the agent cannot otherwise be monitored (e.g., too many monitoring sessions already on their phone).
NO_PERMISSIONS	Specified supervisor does not have the proper permissions to monitor the specified agent
GENERAL_ERROR	See " <a href="#">Agent Monitoring Request Fails</a> " topic in Chapter 7, Troubleshooting

## getCallToMonitor.jsp

Returns ID of agent handling the most recent call for the specified skillgroup ID, which the specified supervisor may monitor. Called by VRU call flow script (VXML, IP IVR, or CVP).



### Note

Call type monitoring is currently not implemented, as the functionality to track calls by type is not yet available with CTI.

## Parameters

**selectionType:** Either skillgroup (if ID is a skillgroup ID) or calltype (if ID is a call type ID). If selectionID is set to 0, this parameter will be left blank and ignored.

**selectionID:** ID of the skillgroup or call type to monitor. Can be set to 0 to not limit by a particular skillgroup or call type.

**supervisorID:** ID of the supervisor (i.e., caller) requesting to monitor the skillgroup. Selected call will be restricted to calls for agents on the supervisor's team. If set to zero, any call in the system may be selected, effectively disabling the built-in permissions check of this API call.

**selectionMode:** Newest, random, or problem:

**newest:** The newest call in the group.

**random:** A random call in the group.

**problem:** Problem calls in the group. Problem calls are defined by the registry configuration values of the ProblemCallMinHolds and ProblemCallMinHolds parameters. (See Appendix B, Registry Keys.)

**outputFormat:** Specifies format of returned data:

**plain:** Returned data contains no formatting. For example, a CREDENTIALS\_VALID result will be returned as simple text (i.e., CREDENTIALS\_VALID). This output method is appropriate for hand-written VXML scripts or anything that can perform a HTML request and process the result directly.

**vxml:** Returned data is formatted in result variable of returned VXML document. Returned page has an <exit> statement that specifies a result variable in its namelist parameter, which contains the return code for the operation. This output format is appropriate for IP IVR's VoiceBrowser step.

**vxml-cvp:** VXML output, which includes extra data that makes it usable by a CVP Unified Call Studio call flow (e.g., specifying the output as a VXML sub-dialog, contains Audium tags, etc.).

## Returns

Return	Description
<NUMERIC AGENT ID>	ID of agent handling selected call and skillgroup
INVALID_SELECTION_ID	Skillgroup or call type ID is invalid or not recognized
INVALID_USER_ID	Caller's user ID is invalid

INVALID_PARAMETERS	One or more required parameters not specified
NO_TALKING_AGENTS	Currently no active agents for specified skillgroup
NO_PERMISSIONS	Specified supervisor does not have the proper permissions to monitor the specified skillgroup
GENERAL_ERROR	See " <a href="#">Agent Monitoring Request Fails</a> " topic in Chapter 7, Troubleshooting

## getConvoInfo.jsp

**Description:** Returns either text data that can be read via TTS, or a VXML sub-dialog that allows call flow script to play information about a conversation. Called by VRU call flow script (VXML, IP IVR, or CVP).

### Parameters

**agentID:** ID of agent to get current conversation information.

**supervisorID:** ID of supervisor (i.e., caller) requesting agent's conversation information.

**outputFormat:** Specifies format of returned data:

**plain:** Equivalent to vxml (below).

**vxml:** Returned data is formatted in result variable of returned VXML document. Returned page has an <exit> statement that specifies a result variable in its namelist parameter, which contains the return code for the operation. This output format is appropriate for IP IVR's VoiceBrowser step.

**vxml-cvp:** VXML output, which includes extra data that makes it usable by a CVP Unified Call Studio call flow (e.g., specifying the output as a VXML sub-dialog, contains Audium tags, etc.).

**hasTTS:** True or false. If true, text data that can be read by TTS via <prompt> statement is returned. If false, data returned plays information about the conversation via pre-recorded audio prompts, using <audio> statement upon success.

**activeVLHostName:** Value of activeVLHostName parameter in VXML script.

**activeVLEnginePort:** Value of activeVLEnginePort parameter in VXML script.

## Returns

Parameter	Type
<TEXTUAL DATA>	The conversation sub-dialog VXML page, as per outputFormat parameter. The returned VXML document or sub-dialog will also exit or return one of the parameters listed below (INVALID_USER_ID, SUCCESS, etc.).
INVALID_AGENT_ID	Agent ID is invalid
INVALID_USER_ID	Caller's user ID is invalid
INVALID_PARAMETERS	One or more required parameters not specified
AGENT_NOT_TALKING	Agent ID is valid, but agent is not currently active (i.e., logged in and talking) and therefore has no active call ID
GENERAL_ERROR	See " <a href="#">Agent Monitoring Request Fails</a> " topic in Chapter 7, Troubleshooting
SUCCESS	Operation was successful

## getAgentList.jsp

Returns a sub-dialog with list of currently talking agents, as called by VRU. Format of returned data, and how it is used, is specified by hasTTS parameter. Called by VRU call flow script (VXML, IP IVR, or CVP).

## Parameters

**supervisorID:** ID of supervisor (i.e., caller) requesting list of agents, filtered to supervisor's team members. If set to zero, team filtering is not performed.

**outputFormat:** Specifies format of returned data:

**plain:** Equivalent to vxml (below).

**vxml:** Returned data is formatted in result variable of returned VXML document. Returned page has <exit> statement that specifies result variable in its namelist parameter, which contains return code for operation. This output format is appropriate for IP IVR's VoiceBrowser step.

**vxml-cvp:** VXML output, which includes extra data that makes it usable by a CVP Unified Call Studio call flow (e.g., specifying the output as a VXML sub-dialog, contains Audium tags, etc.).

**hasTTS:** True or false. If true, returned sub-dialog reads data out via TTS. If false, returned sub-dialog plays pre-recorded prompts to list each agent.

**filterBy:** Set to skillgroup to filter list by skillgroup ID, as specified by filterID parameter. Set to blank for no filtering.

**filterID:** Skillgroup or calltype ID, as used by filterBy parameter. Set to blank if filterBy is set to blank, for no filtering.

**activeCVPMediaSvrHostName:** (*CVP only*) Hostname or IP address of CVP media server with RSM prompts installed, in the MediaFiles/en-us/VL/ directory. Must be specified if using vxml-cvp outputFormat parameter. Not required if outputFormat parameter is vxml or plain.

**activeCVPMediaSvrPort:** (*CVP only*) Port number of CVP media server web server process. Must be specified if using vxml-cvp outputFormat parameter. Not required if outputFormat parameter is vxml or plain.

## Returns

Parameter	Type
<TEXTUAL DATA>	Conversation sub-dialog VXML page, as per outputFormat and hasTTS parameter. Also, returned VXML document or sub-dialog will also exit or return one of parameters listed below (INVALID_USER_ID, SUCCESS, etc.).
INVALID_USER_ID	Caller's user ID is invalid
INVALID_FILTER_ID	Skillgroup or call type ID is invalid or cannot be recognized
INVALID_PARAMETERS	One or more required parameters not specified
NO_TALKING_AGENTS	No agents are currently talking in the system
GENERAL_ERROR	See " <a href="#">Agent Monitoring Request Fails</a> " topic in Chapter 7, Troubleshooting
SUCCESS	Operation was successful

## proxyMonitorAgentForVRU.jsp

Allows monitoring of calls on IP IVR or CVP VRU. Handles requests for streaming audio data, which the IP IVR CRS Editor's Prompt step does not provide. Called by call flow script (IP IVR, or CVP).

## Parameters

**agentID:** ID of agent to monitor.

**escapeOnDTMF2:** True or false. Set to true to escape monitoring when DTMF 2 is pressed (i.e., the number 2) or when a browsing mode is enabled (i.e., press the 2 key to advance to next agent). Set to false when a single agent is being monitored (i.e., the 2 key has no meaning).

**outputFormat:** Specifies format of returned data:

**plain:** Equivalent to vxml (below).

**vxml:** Returned data is formatted in result variable of returned VXML document. Returned page has <exit> statement that specifies result variable in its namelist parameter, which contains return code for operation. This output format is appropriate for IP IVR's VoiceBrowser step.

**vxml-cvp:** VXML output, which includes extra data that makes it usable by a CVP Unified Call Studio call flow (e.g., specifying the output as a VXML sub-dialog, contains Audium tags, etc.).

## Returns

Returns VXML code, which, when executed, sends request to PhoneSim monitorAgent API call to stream in voice data. Data is returned as VXML page with <audio> statement that makes a request for voice data from the PhoneSim monitorAgent API.

The page is run by a VoiceXML browser, and the following code is returned:

Parameter	Type
GENERAL_ERROR	See " <a href="#">Agent Monitoring Request Fails</a> " topic in Chapter 7, Troubleshooting
INVALID_PARAMETERS	One or more required parameters not specified
NOTHING_PRESSED	Monitoring was successful, call ended naturally. User did not press anything on the keypad.
ONE_PRESSED	Monitoring was successful. User terminated call prematurely by pressing DTMF [1].
TWO_PRESSED	Monitoring was successful. User terminated call prematurely by pressing DTMF [2].
STAR_PRESSED	Monitoring was successful. User terminated call prematurely by pressing DTMF [*].
POUND_PRESSED	Monitoring was successful. User terminated call prematurely by pressing DTMF [#].

## determineAgentCluster

Allows VLEngine to know which Unified CM cluster is managing agent whose ID is

specified. Allows VLEngine to choose an idle simulated phone registered to that cluster. Called by VLEngine when it receives a monitorAgent request.

## Parameters

**correlationID:** Unique ID for request, as generated by VLEngine. ID is specified so PhoneSim can correlate VLEngine response with its initial request, which allows it to run all HTTP request traffic over single persistent socket. The correlationID must be alphanumeric, and is passed back in response message.

**agentID:** ID of agent.

## Returns



Note

Each return is prefaced by the string **correlationID =<correlationID>&result=**

Parameter	Type
<CLUSTER_NAME>	Routing client name of cluster handling agent (e.g., CM1_PIM)
INVALID_AGENT_ID	Specified agent ID is invalid
GENERAL_ERROR	See " <a href="#">Agent Monitoring Request Fails</a> " topic in Chapter 7, Troubleshooting
INVALID_PARAMETERS	One or more required parameters not specified

## initiateMonitorAgent

Tells VLEngine (which manages JTAPI connections) to tell appropriate Unified CM cluster (via JTAPI) to initiate a monitoring session for specified simulated supervisor phone. Parameters passed are for a phone registered to the same cluster and returned by determineAgentCluster request. Called by VLEngine upon receipt of successful return code from determineAgentCluster request.

### Parameters

**correlationID:** Unique ID for request, as generated by VLEngine. ID is specified so VLEngine can correlate response with its initial request, which allows it to run all HTTP request traffic over a single persistent socket. The correlationID must be alphanumeric, and is passed back in response message.

**agentID:** Agent ID to initiate monitoring.

**phoneID:** Device ID of simphone to initiate monitoring (e.g., SEP00005E000001).

**lineID:** Line DN on passed simphoneID to take call.

### Returns



Note

Each return is prefaced by string **correlationID** =<correlationID>&result=

Parameter	Type
INVALID_PARAMETERS	One or more required parameters not specified
AGENT_NOT_TALKING	ID specified is valid, but agent is currently not active (i.e., logged in and talking) and therefore has no active call ID.
NO_PERMISSIONS	Specified caller does not have permissions required to monitor specified agent.
GENERAL_ERROR	See " <a href="#">Agent Monitoring Request Fails</a> " topic in Chapter 7, Troubleshooting

## testEngineServlet.jsp

Called manually, for debugging purposes.

### Parameters

None.

### Returns

Provides information about current active agents and calls in system.

## PhoneSim HTTP API

### monitorAgent.jsp

Checks if agent ID is valid and agent is currently talking, by proxying an error return code, from subsequent call to initiateMonitorAgent, to the VLEngine. Called by VXML script to allow it to monitor specified agent. Called by VRU call flow script (VXML, IP IVR, or CVP) or VLEngine. Call is made after VXML script calls canMonitorAgentID. Does not perform permissions check.

### Parameters

**agentID:** ID of agent to monitor.

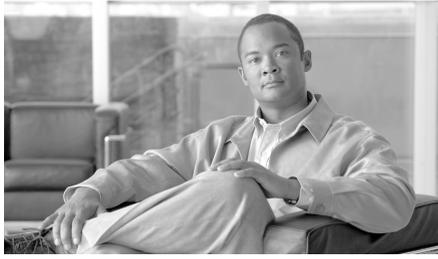
**vruParam:** Specifies VRU type making the call. Impacts VRU-specific details of returned data (e.g., data length stated in the audio header file, etc).

**Values:** ipivr and cvp. If not specified, ipivr is default.

**chunkedTransferMode:** (*optional*) TRUE or FALSE. Allows call flow script to turn on (TRUE) or off (FALSE) chunked transfer mode for returned audio stream. If not specified, the value in the PhoneSim\_DoHTTPChunkedTransfers registry key used.

## Returns

**GENERAL\_ERROR:** See "[Agent Monitoring Request Fails](#)" topic in Chapter 7, Troubleshooting



## APPENDIX **B**

# Registry Keys

---

The configuration parameters for RSM, as entered during the installation process, are stored in the Windows registry.

If you need to modify these settings (e.g., a port number or error message email address has changed), you can do so in one of two ways:

- Re-run the installer, via the Windows Add or Remove Programs control panel, and run the Configuration Manager
- Manually edit the registry keys with Windows Registry Editor

The registry keys are divided into two sections: general settings, and those related to cluster configuration.

# Changing RSM Registry Keys

## To change configuration parameters via the installer:

1. Navigate to **Start > Control Panel > Add or Remove Programs**.
2. Select **Cisco Remote Silent Monitoring** from the currently installed programs list.
3. Click **Change**. The RSM installer appears.
4. Navigate through the installer to the Configuration Manager, and modify the settings you wish to change.
5. Navigate to the last screen of the installer and click **Finish** to save your changes.
6. Restart the VLEngine and PhoneSim services (refer to the “Restart RSM Services” topic in Chapter 6, RSM Services).

## To change configuration parameters with Windows Register Editor:

1. Navigate to **Start > Run**.
2. Enter **regedit.exe** then click **OK**. The Windows Registry Editor window appears.
3. Navigate to **HKEY\_LOCAL\_MACHINE\SOFTWARE\Cisco Systems, Inc.\Remote Silent Monitoring**.
4. Modify the registry values as required (refer to the “General Registry Keys” topic, below).
5. When finished, restart the VLEngine and PhoneSim services (refer to the “Restart RSM Services” topic in Chapter 6, RSM Services).

# General Registry Keys

## Version

Product version number. Set during product installation. Value cannot be altered.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** Any numeric value, in X.Y.Z format

**Default Value:** 1.0.0

## NumClusterConfigs

Number of valid cluster configurations in registry. Numbers must be contiguous, fully entered, and valid for first through last cluster (Cluster1 through ClusterN). Minimum one valid configuration required.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** Any numeric value less than 100

**Default Value:** 1

## MaxNumRequests

Maximum number of simultaneous real-time monitor requests that platform and RSM can handle (i.e., the maximum number of supervisors that can be logged in and using RSM at the same time). Must equal number of simphones created across all clusters, minus the number of simphones in the login pool (normally 5 per cluster). For example, if the environment has 2 clusters, each with 40 simphone devices, and the login pool size for each cluster is 5, then this will be  $(40 - 5) + (40 - 5) = 70$ .

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** Integer greater than 0, and less than or equal to 500

**Default Value:** 80

## ProblemCallMinHolds

Call is classified as a problem if agent has put caller on hold more than specified number.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** Integer greater than 0, and less than or equal to 500

**Default Value:** 4

## ProblemCallMinDuration

Call is classified as a problem if it exceeds specified minimum seconds.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** Integer greater than 0, and less than or equal to 120000

**Default Value:** 1800

## MaxStaleCallDuration

Maximum seconds state of a call can remain unchanged (i.e., does not trigger a CTI event) before deemed stale and removed.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** Integer greater than 60 seconds, and less than or equal to 172800 seconds (2 days)

**Default Value:** 3600 seconds (1 hour)

## SMTP\_HostName

Hostname or IP address of SMTP server that VLEngine and PhoneSim use to email program errors or exceptions. Blank entry disables feature.

**Type:** REG\_SZ

**Value Required:** No

**Valid Values:** Valid IP address, in dotted decimal notation, or hostname

**Default Value:** None

## SMTP\_Port

Port number used to connect to SMTP server, as specified by SMTP\_Hostname parameter.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** Integer greater than 0, and less than or equal to 65534

**Default Value:** 25

## SMTP\_SenderEmailAddress

Sender email address for error message emails. Value must be entered, even if SMTP\_Hostname parameter is blank.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** Valid email address

**Default Value:** voicelink@knoahsoft.com

## SMTP\_ReceiverEmailAddress1

Recipient email address for error message emails. Value must be entered, even if SMTP\_Hostname parameter is blank.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** Valid email address

**Default Value:** None

## SMTP\_ReceiverEmailAddress2

Recipient email address for error message emails. Not used if SMTP\_Hostname parameter is blank.

**Type:** REG\_SZ

**Value Required:** No

**Valid Values:** Valid email address

**Default Value:** None

## SMTP\_ReceiverEmailAddress3

Recipient email address for error message emails. Not used if SMTP\_Hostname parameter is blank.

**Type:** REG\_SZ

**Value Required:** No

**Valid Values:** Valid email address

**Default Value:** None

## SMTP\_ReceiverEmailAddress4

Recipient email address for error message emails. Not used if SMTP\_Hostname parameter is blank.

**Type:** REG\_SZ

**Value Required:** No

**Valid Values:** Valid email address

**Default Value:** None

## VLEngine\_LogLevel

String which dictates verbosity level of output to the VLEngine log file.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values (lowest to highest verbosity):** FATAL, WARN, INFO, DEBUG, TRACE, ALL

**Default Value:** INFO

## PhoneSim\_LogLevel

String which dictates verbosity level of output to the PhoneSim log file.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values (lowest to highest verbosity):** FATAL, WARN, INFO, DEBUG, TRACE, ALL

**Default Value:** INFO

## VLEngine\_HostDataIP

IP address of VLEngine server used to contact other computers in the network. Useful for multi-NIC machines. If blank, IP address of primary network interface is used.

This parameter is important in a large deployment, where VLEngine and PhoneSim are on different servers, and is the address that PhoneSim uses to communicate with VLEngine.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** IP address, in dotted decimal notation

**Default Value:** None

## VLEngine\_HTTPListenPort

Port number VLEngine listens to for incoming HTTP requests.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** Integer greater than 0, and less than or equal to 65534

**Default Value:** 8080

## PhoneSim\_HTTPListenPort

Port number PhoneSim listens to for incoming HTTP requests.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** Integer greater than 0, less than or equal to 65534

**Default Value:** 29001

## PhoneSim\_AudioEncoding

Data encoding method PhoneSim uses for requested audio data.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** wav-pcm, au-ulaw, wav-ulaw, or au-pcm

**Default Value:** au-ulaw

## PhoneSim\_DoHTTPChunkedTransfers

Enables PhoneSim to transmit HTTP chunking of audio data, from VRU request.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** yes or no

**Default Value:** yes

## PhoneSim\_AudioBufferLenToVRU

Bytes of data PhoneSim will buffer before transmission to VRU Voice browser. Used when VRU voice browser receives agent audio data from PhoneSim.

Set to 160 for an IP IVR environment, and 480 for a CVP environment. If both IP IVR and CVP are used with the RSM server, set to 480.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** Integer greater than 20, and less than or equal to 1000000

**Default Value:** 160

## PhoneSim\_HostDataIP

IP address PhoneSim server uses to contact other computers in network. Useful when there are multiple NIC machines in network. If blank, IP address of primary network interface is used.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** IP address, in dotted decimal notation

**Default Value:** None

## CTIOS\_TraceMask

Trace mask used to log CTI OS CIL messages to disk for CTI OS mode connections. CTI OS connections are created upon startup, and remain active for life of application. Used to retrieve information about events in call center environment.

Setting determines how much CIL output data is logged in C:\CiscoRSM\vlengine\ctiosLogs directory files for these connections.

**Type:** REG\_SZ

**Value Required:** No

**Valid Values:** Eight-digit numerical hexadecimal, as the CTI OS trace mask to use, or blank. If blank, tracing to file is disabled. Refer to the *CTI OS Developer Guide* for more information.

**Default Value:** None

## CTIOS\_AgentModeTraceMask

Trace mask used to log CTI OS CIL messages to disk for the CTI OS agent mode connections. Connections are created on demand for back-end authorization when login to RSM is requested.

Setting determines how much CIL output data is logged to ctiosAMLogs directory for these connections.

**Type:** REG\_SZ

**Value Required:** No

**Valid Values:** Eight-digit numerical hexadecimal of CTI OS trace mask, or blank. If blank, tracing to file will be disabled.

**Default Value:** None

## VLEngine\_PassPrefix

Prefix for supervisor password used when creating accounts. Refer to “Supervisor Login Account Creation” topic in Chapter 3, Pre-Installation Tasks.

For example, if set to RSM1RSM, and you want a supervisor to log in with PIN 1234, then set supervisor's password to RSM1RSM1234. VLEngine prepends the RSM1RSM string before it submits the password to CTI OS for validation.

**Type:** REG\_SZ

**Value Required:** No

**Valid Values:** Any string of letters, numbers, and valid password symbols (e.g., no whitespace and control characters).

**Default Value:** Blank string

# Cluster Configuration Registry Keys

These configuration parameters are duplicated for each supported cluster, where N goes from 1 to the setting of the NumClusterConfigs value.

When configuring multiple CTI OS servers, pair the hostname and port keys (i.e., ClusterN\_VLEngine\_CTIOS1\_HostName, ClusterN\_VLEngine\_CTIOS1\_Port) in A/B fashion as follows:

Registry Key	CTI OS Server
ClusterN_VLEngine_CTIOS1	CTIOS1A
ClusterN_VLEngine_CTIOS2	CTIOS1B
ClusterN_VLEngine_CTIOS21	CTIOS2A
ClusterN_VLEngine_CTIOS22	CTIOS2B
ClusterN_VLEngine_CTIOS31	CTIOS3A
ClusterN_VLEngine_CTIOS32	CTIOS3B
ClusterN_VLEngine_CTIOS41	CTIOS4A
ClusterN_VLEngine_CTIOS42	CTIOS4B

## ClusterN\_Name

Client name in IPPC, for cluster's routing.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** Alphanumeric string (underscore and emdash allowed)

**Default Value:** None

## ClusterN\_MaxNumRequests

Maximum simultaneous, real-time monitor requests the platform can handle for the cluster. Equal to number of simphones in cluster not used in the login pool. For example, if the cluster has 50 devices and 5 in the login pool, then value is 45.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** Numerical value less than or equal to MaxNumRequests

**Default Value:** None

## ClusterN\_PeripheralID

Peripheral instrument ID used to denote the cluster in Unified ICME (e.g., the ICM peripheral ID of the PIM for the UCM cluster).

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** Numeric string

**Default Value:** None

## ClusterN\_JTAPI\_UserName

JTAPI application user username used by RSM to connect to the specified UCM servers in the cluster.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** Alphanumeric string

**Default Value:** None

## ClusterN\_JTAPI\_Password

JTAPI user password, as per ClusterN\_JTAPI\_User parameter

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** String (alphanumeric special non-whitespace characters allowed)

**Default Value:** None

## ClusterN\_NumSimPhonesUsedForCTIOSAgentLogins

Number of simphones in the login pool for the given cluster configuration. Normally this value is set to 5 and should not be changed. For more information, refer to the “Login Pool Simphone Setup” topic in Chapter 3, Pre-Installation Tasks.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** Any numeric string between 1 and 10

**Default Value:** 5

## ClusterN\_PhoneSim\_StartMACRange

First MAC address to use for auto-generation of MAC range for simphone device names. For example, if 000000100010 is specified, the range would proceed with SIP000000100010, SIP000000100011, SIP000000100012, and so forth.

MAC ranges must not overlap between clusters. Note that the 0000:5Exx range is normally reserved for public use, as per IANA standards.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** Twelve-digit, numerical hexadecimal

**Default Value:** 00005E000001

## ClusterN\_PhoneSim\_StartLineNumRange

First extension number to use for auto-generation of line extension range for simphone DNs. Correlates to ClusterN\_PhoneSim\_StartMACRange value.

If 1000 is specified, and 000000100010 is ClusterN\_PhoneSim\_StartMACRange, then the first simphone device name generated will be SIP000000100010 and will have line extension 1000; SIP000000100011 will have line extension 1001; SIP000000100012 will have line extension 1002, and so forth.

Line extension ranges must not overlap between clusters.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** Four to six digit number

**Default Value:** 1000

## ClusterN\_PhoneSim\_SIPTransport

Tells PhoneSim how to conduct the SIP transmission with Contact Manager for the cluster, via TCP or UDP.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** tcp or udp

**Default Value:** tcp

## ClusterN\_PhoneSim\_CM1\_HostName

IP address or hostname of the primary Contact Manager that PhoneSim will hone its simphones to for the cluster.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** Valid IP address, in dotted decimal notation; or hostname

**Default Value:** None

## ClusterN\_PhoneSim\_CM1\_Port

Port PhoneSim uses to send its SIP messages to Contact Manager 1. If TCP is used, connections will be made to this port. If UDP is use, datagrams will be sent to this port.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** Integer greater than 0 and less than or equal to 65534

**Default Value:** 5060

## ClusterN\_PhoneSim\_CM2\_HostName

*(optional)* IP address or hostname of the Contact Manager 2 that PhoneSim hones its simphones to as a secondary (i.e., failover) Contact Manager for the cluster.

**Type:** REG\_SZ

**Value Required:** No

**Valid Values:** Valid IP address, in dotted decimal notation; or hostname

**Default Value:** None

## ClusterN\_PhoneSim\_CM2\_Port

Port PhoneSim uses to send its SIP messages to Contact Manager 2. If TCP is used, connections will be made to this port. If UDP is use, datagrams will be sent to this port.

**Type:** REG\_SZ

**Value Required:** If ClusterN\_PhoneSim\_CM2\_Port is specified

**Valid Values:** Integer greater than 0, and less than or equal to 65534

**Default Value:** 5060

## ClusterN\_VLEngine\_CM1\_HostName

IP address or hostname of Contact Manager 1 for the cluster that VLEngine connects to via JTAPI, to make its JTAPI requests.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** Valid IP address, in dotted decimal notation; or hostname

**Default Value:** None

## ClusterN\_VLEngine\_CM2\_HostName

*(optional)* IP address or hostname of Contact Manager 2 for the cluster that VLEngine connects to via JTAPI, to make its JTAPI requests. Contact Manager 2 is used in conjunction with Contact Manager 1, in round-robin fashion, for JTAPI requests.

**Type:** REG\_SZ

**Value Required:** No

**Valid Values:** Valid IP address, in dotted decimal notation; or hostname

**Default Value:** None (blank)

## ClusterN\_VLEngine\_CTIOS1\_HostName

IP address or hostname of primary CTI OS server for the cluster; or, if the cluster has multiple CTI OS pairs, this is the primary server of the first pair. If another cluster is using the same set of CTI OS servers, enter only these servers in the configuration for one of the clusters, and leave the other clusters CTI OS server configuration blank.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** Valid IP address, in dotted decimal notation; or hostname

**Default Value:** None

## ClusterN\_VLEngine\_CTIOS1\_Port

Connection port for the cluster's primary CTI OS server.

**Type:** REG\_SZ

**Value Required:** Yes

**Valid Values:** Integer greater than 0, and less than or equal to 65534

**Default Value:** 42028

## ClusterN\_VLEngine\_CTIOS2\_HostName

IP address or hostname of secondary (i.e., backup) CTI OS server for cluster; or, if the cluster has multiple CTI OS pairs, this is the secondary server of the first pair.

**Type:** REG\_SZ

**Value Required:** No

**Valid Values:** Valid IP address, in dotted decimal notation; or hostname

**Default Value:** None (blank)

## ClusterN\_VLEngine\_CTIOS2\_Port

Used when RSM must connect to more than one CTI OS server pair per cluster. This is the connection port of the primary CTI OS server for the second pair.

**Type:** REG\_SZ

**Value Required:** If ClusterN\_VLEngine\_CTIOS2\_HostName is specified

**Valid Values:** Integer greater than 0, and less than or equal to 65534

**Default Value:** 4202

## ClusterN\_VLEngine\_CTIOS21\_HostName

Used when RSM must connect to more than one CTI OS server pair per cluster. This is the IP address or hostname of the primary CTI OS server for the second pair.

**Type:** REG\_SZ

**Value Required:** No

**Valid Values:** Valid IP address, in dotted decimal notation; or hostname

**Default Value:** None

## ClusterN\_VLEngine\_CTIOS21\_Port

Used when RSM must connect to more than one CTI OS server pair per cluster. This is the connection port of the primary CTI OS server for the second pair.

**Type:** REG\_SZ

**Value Required:** If ClusterN\_VLEngine\_CTIOS21\_HostName is specified

**Valid Values:** Integer greater than 0, and less than or equal to 65534

**Default Value:** 42028

## ClusterN\_VLEngine\_CTIOS22\_HostName

Used when RSM must connect to more than one CTI OS server pair per cluster. This is the IP address or hostname of the secondary CTI OS server for the second pair.

**Type:** REG\_SZ

**Value Required:** No

**Valid Values:** Valid IP address, in dotted decimal notation; or hostname

**Default Value:** None (blank)

## ClusterN\_VLEngine\_CTIOS22\_Port

Used in cases where RSM must connect to more than one CTI OS server pair per cluster. This is the connection port of the secondary CTI OS server for the second pair.

**Type:** REG\_SZ

**Value Required:** If ClusterN\_VLEngine\_CTIOS22\_HostName is specified

**Valid Values:** Integer greater than 0, and less than or equal to 65534

**Default Value:** 42028

## ClusterN\_VLEngine\_CTIOS31\_HostName

Used in cases where RSM must connect to more than one CTI OS server pair per cluster. This is the IP address or hostname of the primary CTI OS server for the 3rd pair.

**Type:** REG\_SZ

**Value Required:** No

**Valid Values:** Valid IP address, in dotted decimal notation; or hostname

**Default Value:** None

## ClusterN\_VLEngine\_CTIOS31\_Port

Used in cases where RSM must connect to more than one CTI OS server pair per cluster. This is the connection port of the primary CTI OS server for the third pair.

**Type:** REG\_SZ

**Value Required:** If ClusterN\_VLEngine\_CTIOS31\_HostName is specified

**Valid Values:** Integer greater than 0, and less than or equal to 65534

**Default Value:** 42028

## ClusterN\_VLEngine\_CTIOS32\_HostName

Used in cases where RSM must connect to more than one CTI OS server pair per cluster. This is the IP address or hostname of the secondary CTI OS server for the third pair.

**Type:** REG\_SZ

**Value Required:** No

**Valid Values:** Valid IP address, in dotted decimal notation; or hostname

**Default Value:** None (blank)

## ClusterN\_VLEngine\_CTIOS32\_Port

Used in cases where RSM must connect to more than one CTI OS server pair per cluster. This is the connection port of the secondary CTI OS server for the third pair.

**Type:** REG\_SZ

**Value Required:** If ClusterN\_VLEngine\_CTIOS32\_HostName is specified

**Valid Values:** Integer greater than 0, and less than or equal to 65534

**Default Value:** 42028

## ClusterN\_VLEngine\_CTIOS41\_HostName

Used in cases where RSM must connect to more than one CTI OS server pair per cluster. This is the IP address or hostname of the primary CTI OS server for the fourth pair.

**Type:** REG\_SZ

**Value Required:** No

**Valid Values:** Valid IP address, in dotted decimal notation; or hostname

**Default Value:** None

## ClusterN\_VLEngine\_CTIOS41\_Port

Used in cases where RSM must connect to more than one CTI OS server pair per cluster. This is the connection port of the primary CTI OS server for the fourth pair.

**Type:** REG\_SZ

**Value Required:** If ClusterN\_VLEngine\_CTIOS41\_HostName is specified

**Valid Values:** Integer greater than 0, and less than or equal to 65534

**Default Value:** 42028

## ClusterN\_VLEngine\_CTIOS42\_HostName

Used in cases where RSM must connect to more than one CTI OS server pair per cluster. This is the IP address or hostname of the secondary CTI OS server for the fourth pair.

**Type:** REG\_SZ

**Value Required:** No

**Valid Values:** Valid IP address, in dotted decimal notation; or hostname

**Default Value:** None (blank)

## ClusterN\_VLEngine\_CTIOS42\_Port

Used in cases where RSM must connect to more than one CTI OS server pair per cluster. This is the connection port of the secondary CTI OS server for the fourth pair.

**Type:** REG\_SZ

**Value Required:** If ClusterN\_VLEngine\_CTIOS42\_HostName is specified

**Valid Values:** Integer greater than 0, and less than or equal to 65534

**Default Value:** 42028



## INDEX

- 
- ### A
- agent device setup [3-13](#)
  - agent phone device setup [3-13](#)
  - anti-virus software [3-2](#)
  - Apache Tomcat server
    - configuration [1-3](#)
    - installation [4-2](#)
  - API extensions [A-1](#)
    - JSP suffix [A-1](#)
    - PhoneSim [A-13](#)
    - VLEngine [A-2](#)
  - application connectivity [1-4](#)
  - application user
    - JTAPI user [1-6](#)
    - JTAPI username [4-5, B-13](#)
    - login pool [3-10](#)
    - RSM creation [3-12](#)
    - RSM removal [6-5](#)
    - terminal domain error [7-9](#)
    - Unified CM removal [6-5](#)
  - associate a pguser [3-10](#)
- 
- ### B
- base system provisioning [3-2](#)
  - BAT tool, simphones [3-8](#)
- 
- ### C
- call flow [1-2](#)
    - text-to-speech (TTS) [5-5](#)
    - troubleshooting [7-2](#)
    - troubleshooting, CVP [5-9](#)
    - VXML deployment [5-8](#)
  - call flow script
    - CVP integration [5-7](#)
    - disable built-in user authentication [5-11](#)
    - editing tools [1-2](#)
    - IP IVR integration (non-Unified ICME) [5-4](#)
    - IP IVR integration (Unified ICME) [5-5](#)
    - VRU integration [5-2](#)
  - check RSM services [6-2](#)
  - Cisco hardware and software requirements [2-1](#)
  - Cisco Internetwork Operating System (IOS) [5-10](#)
  - Cisco Security Agent (CSA) [4-10](#)
    - disable [4-2](#)

Configuration Manager

- Call Manager settings [4-6](#)
- define cluster settings [4-4](#)
- installation [4-2](#)
- miscellaneous settings [4-3](#)

CVP

- audio buffer [4-4](#)
- call flow deployment [5-8](#)
- call flow integration [5-7](#)
- call flow troubleshooting [5-9](#)
- Cisco documentation [5-9](#)
- media server [5-7](#)
- media server port number [A-8](#)
- RSM integration [5-6](#)
- RSM removal [6-3](#)
- upload RSM prompts [5-6](#)

CVP Unified Call Studio [5-6](#)

- API extensions [A-1](#)
- logging [5-9](#)

CVP VXML Server

- installation location [5-6](#)

---

**D**

directory structure [4-7](#)

disable

- Cisco Security Agent (CSA) [4-2](#)
- supervisor team structure [5-11](#)
- user authentication [5-11](#)

disassociate simphone devices, pguser [6-5](#)

---

**E**

- enable RSM services [6-1](#)
- environment variables [4-8](#)
- error messages
  - PhoneSim log file [7-15](#)

---

**F**

firewall, Windows 2003 [4-9](#)

---

**G**

- G.711 codec [5-3](#)
- G.729 codec [5-3](#)
- general call flow troubleshooting [7-2](#)

---

**H**

- hardware and software requirements, Cisco [2-1](#)
- host level security [4-9](#)

---

**I**

installation [4-1](#)

Internetwork Operating System (IOS) [5-10](#)

IP IVR

- CRS Editor and APIs [A-1](#)
- integration (non-Unified ICME) [5-4](#)

integration (Unified ICME) [5-5](#)  
 integration overview [5-2](#)  
 removal [6-2](#)

IP security (IPsec) [4-10](#)

---

## J

Java Service Wrapper [4-2](#)

JTAPI [1-1](#)

- application username [B-13](#)
- client libraries installation [3-3](#)
- client library directory [4-7](#)
- encryption [4-11](#)
- IPsec CTI OS communication [4-10](#)
- trace logs [7-1](#)
- troubleshooting [7-1](#)
- username [4-5](#)
- user password [B-14](#)
- VLEngine connections [A-12](#)

---

## L

line DN

- add to simphone device [3-8](#)
- parameters [3-8](#)
- simphone device association [3-7](#)

log files [7-1](#)

- PhoneSim error messages [7-15](#)

login pool

- Configuration Manager [4-5](#)
- invalid login [7-5](#)

- login error [7-7](#)
- rsmuser association [3-12](#)
- simphone setup [3-10](#)

---

## M

Microsoft's Baseline Security Analyzer (MBSA) [3-2](#)

multi-site deployment [1-6](#)

---

## P

pguser

- association [3-10](#)
- disassociate simphone devices [6-5](#)

PhoneSim [1-3](#)

- HTTP API [A-13](#)
- log file error messages [7-15](#)
- runtime troubleshooting [7-14](#)

port numbers [4-8](#)

pre-installation tasks [3-1](#)

prompts

- CVP upload [5-6](#)
- IP IVR upload [5-3](#)

---

## R

registry keys [B-1](#)

- cluster configuration [B-12](#)
- general [B-3](#)

- modifying [B-2](#)
- Remote Silent Monitoring (see RSM) [1-1](#)
- remove
  - application user [6-5](#)
  - CVP [6-3](#)
  - IP IVR [6-2](#)
  - RSM [6-2](#)
  - supervisor login account [6-4](#)
  - Unified CM [6-5](#)
  - Unified ICME [6-4](#)
- restart RSM services [6-2](#)
- RSM [1-1](#)
  - application user creation [3-12](#)
  - directory structure [4-7](#)
  - removal [6-2](#)
  - services enablement [6-1](#)
  - services overview [1-3](#)
  - user group, create [3-11](#)
  - VLAN configuration [1-4](#)
- RSM.aef [5-4](#)
- RSM prompts
  - upload for CVP [5-6](#)
  - upload for IP IVR [5-3](#)
- rsmuser
  - application user [3-12](#)

---

## S

- security [4-9](#)
  - CTI OS encryption [4-10](#)
  - hardening [4-9](#)

- host level [4-9](#)
- JTAPI encryption [4-11](#)
- simphone
  - BAT tool [3-8](#)
  - calling search space, create [3-5](#)
  - configuration [3-3](#)
  - login pool setup [3-10](#)
  - region, create [3-4](#)
  - route partition, create [3-5](#)
- simphone device
  - add line DN [3-8](#)
  - create [3-6](#)
  - dependencies [3-4](#)
  - line DN association [3-7](#)
- simphone device pool
  - create [3-5](#)
- supervisor login account
  - create [3-13](#)
  - remove [6-4](#)
- supervisor team structure, disabling [5-11](#)
- system overview [1-1](#)
- system requirements [2-1](#)

---

## T

- troubleshooting
  - general call flow [7-2](#)
  - JTAPI, CTI OS [7-1](#)
  - PhoneSim runtime issues [7-14](#)
  - VLEngine runtime issues [7-9](#)

---

**U**

## Unified CM

- group create [3-4](#)
- removal [6-5](#)
- services enablement [3-3](#)

## Unified ICME

- device target, create [3-11](#)
- removal [6-4](#)

## upload RSM prompts

- CVP [5-6](#)
- IP IVR [5-3](#)

user authentication, disabling [5-11](#)user group, RSM [3-11](#)

---

**W**Windows 2003 Firewall [4-9](#)Windows automatic updates [3-2](#)Windows Security hardening [4-9](#)

---

**V**VLAN configuration [1-4](#)VLEngine [A-2](#)

- HTTP API [A-2](#)
- overview [1-3](#)

## VLEngine runtime troubleshooting

[7-9](#)VRU configuration [5-1](#)vxml-cvp [A-2](#)VXML gateway [5-10](#)

- sample code [5-10](#)

