Release Notes for
Cisco Remote Silent Monitoring Release 9.0(1)

October 15, 2012

Contents

Introduction

This document discusses the features and caveats for Cisco Remote Silent Monitoring (RSM) Release 9.0(1). RSM 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.

Information on which software releases are supported by Remote Silent Monitoring Release 9.0(1) is available in the Cisco Unified Contact Center Enterprise (Unified CCE) Software Compatibility Guide, accessible from

http://www.cisco.com/en/US/docs/voice_ip_comm/cust_contact/contact_center/ipcc_enterprise/compatibility_matrix/ipcccompat.pdf

Remote Silent Monitoring Release 9.0(1) supports Microsoft Windows2003 Server R2 or SP2, or Windows 2008 R2.

About Release 9.0(1)

Cisco Remote Silent Monitoring Release 9.0(1) is a major release, delivered in an installer. The installer supports both a full installation of RSM 9.0(1) as well as support for upgrading all previously released base versions of RSM, as described below. The installer is available from www.cisco.com.

Supported Base Install Versions

This release has been tested to be compatible with the following base releases: Cisco RSM 1.0(1), 1.0(2), 1.0(2) ES1, 1.0(2) ES2, 1.0(2) ES3, 1.0(2) ES4, 1.0(2) ES5, 8.0(1), 8.5(1), and 8.5(2).

⚠️
Caution   If you are updating from a previous version of RSM, the VLEngine and PhoneSim services are stopped during installation and then re-started once installation is complete. Thus, all monitoring sessions in progress will be terminated, and no new sessions can be initiated until installation is complete.

The release can be uninstalled via Control Panel > Add or Remove Programs.

✎
Note   The most up-to-date version of these release notes is available on the Web at
http://www.cisco.com/en/US/products/sw/custcosw/ps1844/prod_release_notes_list.html

⚠️
Caution   This release includes an updated CVP callflow script/application. Unless this updated script is deployed on the VXML server, some of the defects mentioned in this release will not be resolved. Note that any previous RSM CVP callflow script changes will be lost and will have to be added to the new script.

System Requirements

For Unified CM and Unified CCE specifications required for this release, refer to the *Hardware and System Software Specification (Bill of Materials): Cisco ICM/IPCC Enterprise & Hosted Editions*, which is accessible from
http://www.cisco.com/en/US/products/sw/custcosw/ps1844/prod_technical_reference_list.html

See the *Cisco Remote Silent Monitoring Installation and Administration Guide* for detailed information on RSM hardware requirements, which are based on anticipated monitoring sessions and agent usage.

Anti-Virus Software Requirements

RSM requires the use of one of the following Cisco approved anti-virus software:

- Trend Micro ServerProtect 5.7
- McAfee VirusScan Enterprise 8.7i
- Symantec Endpoint Protection 11.0

Refer to Chapter 2, Cisco Hardware and Software Requirements, of the *Cisco Remote Silent Monitoring Installation and Administration Guide* for BOM information.

Related Documentation

Documentation for Cisco Unified Contact Center Enterprise and Hosted Editions, as well as most related documentation, is accessible from
http://www.cisco.com

- Related documentation includes the documentation sets for Cisco CTI Object Server (CTI OS), Cisco Agent Desktop (CAD), Cisco Agent Desktop - Browser Edition (CAD-BE), Cisco Unified Contact Center Management Portal, Cisco E-Mail Manager Option, Cisco Web Collaboration Option (including Cisco Collaboration Server, Cisco Dynamic Content Adapter, Cisco Media Blender), Cisco Unified Customer Voice Portal (CVP), Cisco IP IVR, Cisco Support Tools, and Cisco Unified Communications Manager.
- Technical Support documentation and tools can be accessed from
  http://www.cisco.com/en/US/support/index.html
- The Product Alert tool can be accessed through
  http://www.cisco.com/cgi-bin/Support/FieldNoticeTool/field-notice

New and Changed Information

The following changes have been introduced for Cisco Remote Silent Monitoring Release 9.0(1)

Support for Virtualization

RSM 9.0(1) release now supports virtualization profiles for 80 concurrent monitoring sessions. Here are the supported virtualization specifications:

- VMWare ESXi 4 or above
- 2 virtual CPU cores at minimum 2.13 Ghz each
- 4 GB virtual RAM
- One 50 GB virtual Disk
- One virtual NIC
- Windows 2008 R2

Support for Windows 2008 R2

RSM 9.0(1) release now supports Windows 2008 R2 64-bit or 32-bit in addition to Windows 2003

Java JRE bundled

No longer requires downloading Java JDK. The latest 1.6 JRE for Windows x86 is bundled with the installation.

Limitations and Restrictions

The following notes describe the known limitations of Cisco Remote Silent Monitoring Release 9.0(1) in a Cisco environment, as well as information about other important system integration issues.

Monitoring of Simphones via Supervisor Desktop

Currently, you cannot monitor RSM simulated supervisor phones (i.e, simphones) via Cisco Supervisor Desktop (CSD), as the simphones are purposefully added to the Communications Manager platform with their BiB (built-in-bridge) disabled.

Failover Redundancy and Load Balancing with CVP

Currently, RSM does not support load balancing and clustering if CVP is used as a VRU. (Load balancing support is defined as the association of multiple RSM servers so that the incoming request load is distributed among them. Failover redundancy is defined as the association of RSM servers so that if one fails, the others will act in its place.)

Mobile Agent Support

RSM uses the Unified Communications Manager (Unified CM) monitoring mechanism, which currently does not support Cisco Mobile Agent monitoring. Subsequently, RSM does not support monitoring Mobile Agents.

IP IVR HTTP Security

Currently, IP IVR supports only HTTP communication with the RSM server. TLS HTTPS is not supported.

Multiple Clusters and JTAPI Libraries

If a single RSM server is configured to use Unified CM multiple clusters, each cluster's constituent servers must be running the same build of Unified CM. Attaching to multiple clusters running different versions of Unified CM is not supported, as there may be JTAPI library incompatibilities between versions.

Unified Unified CCE Supported IP Phones

Agents must use a third-generation or later Unified CCE supported IP phone with RSM (note that Personal Communicator is not supported by Unified CCE). Phones supported include:

- 7906G, 7911G, 7921G (Aug 08 upd), 7925G, 7931G, 7941G/GE, 7942G, 7945G, 7961G/GE, 7962G, 7965G, 7970G, 7971G-GE, 7975G, 6900, and IP Communicator 7.0(1) and higher. (Note: See "Support for 6900, 8900, 9900 Phones" topic, below, for 6900 information.)

Phones not supported include:

- 7910, 7912, 7940, 7960

All new phones will be supported. For phone support information, 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

Support for 6900, 8900 and 9900 Phones

6900, 8900 and 9900 phone models have Join, Join Across Lines (JAL), Direct Transfer, and Direct Transfer Across Lines (DTAL) features, which RSM does not support. 6900 phones allow disabling of these features, and so RSM can support monitoring these phones if these features are disabled; but 8900 and 9900 phones do not allow for disabling of these features, and so RSM does not support monitoring of these phones.

Encrypted Call Monitoring

RSM does not allow for the monitoring of encrypted calls.

Transfers and Alternate Call Monitoring

Transfers and alternate calls require manual intervention to continue monitoring. RSM does not do this automatically. So, when an agent starts a consult call, RSM stops monitoring the customer call, which is now on hold, and starts monitoring the consult call, if desired. When the agent transfers the call to another agent, the RSM monitoring session is terminated.

Agent Monitoring on Hold

An agent can be monitored with RSM only when they are talking on a call. They cannot be monitored while on hold or not on a call. Calls on hold before the supervisor initiates a monitoring session will not be picked up for monitoring. The VLEngine will filter these calls from being monitored by any of the IVR options (e.g., agentid, skill group, newest call, random call or list of talking agents).

However, if the agent puts the caller on hold while being monitored by a supervisor, then the monitoring session is kept alive for the duration of the hold period. If the supervisor exits out of the monitoring session by pressing * or 1 for information or instructions, then they will not be able to resume monitoring. This is due to BiB functionality, where a monitoring call can be established only if the agent is in a talking state.

Monitoring Sessions Per Agent

Unified CM provides for one active monitoring session per agent, as the agent's phone can handle only one active monitoring session and one active recording session at any given time. If a third-party recorder is recording the agent's conversations, the agent can still be monitored by a supervisor using the supervisor desktop or RSM; however, if a RSM-based supervisor and a supervisor desktop-based supervisor both try to monitor the agent simultaneously, the request will fail.

RSM will set up only one monitoring session through Unified CM for a single monitored agent, even if two or more RSM users are requesting to monitor the agent's call at the same time. In this case, RSM forks the stream to cover all RSM users, so that more than two RSM-based supervisors can monitor the same agent. However, if there are multiple RSM servers in the environment that monitor the same agent, they each make a separate monitoring call to that agent.

If the monitoring call limit has been reached for a specific agent, and a dialed-in supervisor then attempts to monitor this same agent, the request will be denied via an audio prompt feedback from the system, stating that the agent cannot be monitored.

Bandwidth

There must be sufficient bandwidth available from the agent IP phone to the RSM server to support the monitoring voice stream, in addition to the regular voice streams for the call. This is important for employees who work remotely, at home, and small branches on limited bandwidth. Regular Call Admission Control (CAC) and bandwidth calculations are applicable for monitoring calls.

Since G.711 is the codec supported for monitoring calls between agent IP phone and RSM server (phonesim), use the Cisco TAC Voice Bandwidth Codec Calculator for additional bandwidth capacity planning, at

http://tools.cisco.com/Support/VBC/jsp/Codec_Calc1.jsp

IP Communicator Support With Optimize for Low Bandwidth Option

RSM fails to monitor an agent IPC 7.x phone when the Optimize for Low Bandwidth option is enabled in the phone preferences. When this option is enabled, IPC forces a G.729 or similar low bandwidth codec on all its audio streams, including the BiB monitoring stream. This is irrespective of the UCM region settings of the end points, and this option overrides UCM settings.

Although RSM SimPhones are required to be configured in G.711 only region in UCM, IPC overrides this configuration and sends a G.729 monitoring stream, which RSM fails to monitor. Because RSM does not support G.729 for its SimPhones, IPC 7.x monitoring is not supported when this option is enabled. (Note that it is not enabled in IPC by default.)

VLEngine and Email Alerts

Currently, the VLEngine service does not support the sending of email alerts in error situations.

Gateway Memory

1G of gateway memory is recommended for use with RSM, and the gateway can support 40 users.

RSM Requires a Dedicated VXML Gateway

When RSM is used with CVP, the gateway 'IVR prompt streaming for HTTP' needs to be enabled (see Chapter 5 of the *RSM Installation and Administration Guide*). Note that this setting is not recommended for other CVP applications. Therefore RSM requires a dedicated VXML gateway. This gateway must not be used for other CVP applications.

IP IVR Execution Steps

IP IVR can execute up to 25,000 steps per script session. The Max Number of Executed Steps parameter is used to configure this setting, and has a default setting of 1,000 steps.

RSM can reliably monitor up to 10 agents consecutively before the 1,000 steps limit is reached, at which point a system error message is displayed and IP IVR abruptly closes. To enable the monitoring of multiple agents in one session, modify the Max Number of Executed Steps configuration parameter in IP IVR to its upper limit of 25,000. (This value has been successfully tested to monitor at least 40 agents consecutively, with calls up to 600 seconds in duration, and at least one hold event per call.)

For information on modifying the Max Number of Executed Steps parameter, refer to the *Cisco IP IVR/CRS 5.0/7.0/8.0 Administration Guide*, accessible from http://www.cisco.com/

Support for Calls Established Before VLEngine Services Start

RSM does not support monitoring calls that have been established before the RSM VLEngine service starts. Only calls that start after the VLEngine starts up can be monitored.

Installation Notes

See the *Cisco Remote Silent Monitoring Installation and Administration Guide Release 9.0(1)* for specific instructions on how to plan, deploy, and integrate RSM into your Cisco environment. This guide also provides important pre-installation tasks that must be considered, including:

- Provisioning the base operating system
- Enabling Unified CM services
- Configuring simulated phones
- Associating simphones with the system pguser
- Adding an RSM application user
- Creating a supervisor login account
- Installing the JTAPI client libraries required to run RSM

Note You will need administration access for both Unified CM and Administration and Data Server (ADS) to perform many of the pre-installation and installation tasks described in the RSM documentation.

Caution This release includes an updated CVP callflow script/application. Unless this updated script is deployed on the VXML server, some of the defects mentioned in this release will not be resolved. Note that any previous RSM CVP callflow script changes will be lost and will have to be added to the new script.

Caveats

Using Bug Toolkit

Known problems (bugs) are graded according to severity level. These release notes contain descriptions of the following:

- All severity level 1, 2, and 3 bugs.
- Significant severity level 4 bugs.

You can search for problems by using the Cisco Software Bug Toolkit.

Before You Begin

To access Bug Toolkit, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

Procedure

Step 1 To access the Bug Toolkit, go to
http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs.

Step 2 Log in with your Cisco.com user ID and password.

Step 3 To look for information about a specific problem, enter the bug ID number in the "Search for Bug ID" field, then click **Go**.

For information about how to search for bugs, create saved searches, and create bug groups, click **Help** in the Bug Toolkit page.

Open Caveats

The caveats in Table 1 describe possible unexpected behavior in the latest Cisco Remote Silent Monitoring release. These caveats may also be open in previous releases. Bugs are listed in order of severity and then in alphanumeric order by bug identifier.

⌕
Tip If you have an account with Cisco.com, you can use the Bug Toolkit to find caveats of any severity for any release. Bug Toolkit may also provide a more current listing than is reflected in this document. To access the Bug Toolkit, log onto http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Table 1   Open Caveats for Cisco Remote Silent Monitoring Release 9.0(1)

Identifier	Severity	Component	Headline
CSCtz64640	Moderate	CVP-Call Flow	End of call event in VLEngine RSM takes 15 seconds after the actual end
CSCuc57716	Moderate	cvp-callflow	3 to 4 seconds delay in hearing live audio call

Resolved Caveats

This section lists caveats that are resolved but that may have been open in previous releases.

Bugs are listed in order of severity and then in alphanumeric order by bug identifier. Because defect status continually changes, be aware that this document reflects a snapshot of the defects that were resolved at the time this report was compiled. For an updated view of resolved defects, access the Bug Toolkit (see the "Using Bug Toolkit" section on page 8.)

The following table lists caveats that are resolved in Cisco Remote Silent Monitoring but that may have been open in previous releases:

Release 9.0(1)

Table 2 lists the caveats that were resolved in Release 9.0(1).

Table 2   *Resolved in Release 9.0(1)*

Identifier	Severity	Component	Headline
CSCtx64569	Severe	VLEngine	RSM sometimes drops CVP and IPIVR sessions in option 4 and 5
CSCub00218	Severe	Installer	RSM 8.5(2) installer does not include the CVP Callflow script/appication
CSCsy18327	Minor	Installer	All RSM related files and folders must be closed when applying patches
CSCtb44669	Minor	VLEngine	CVP based setting for prompts path (Default Audio Path URI) is hard coded. This has to be made configurable from RSM side
CSCtx54969	Minor	Documentation	RSM Additional PG Configuration documentation clarification
CSCub06430	Minor	Documentation	RSM 8.5 is full install not service patch

> **Note** This release includes an updated CVP callflow script/application. Unless this updated RSM CVP script is deployed on VXML server, CSCtb44669 and CSCts38489 defects will not be resolved.

> **Note** Resolving defect CSCtb44669 requires configuring a new CVP session variable in the call flow script. This variable, CVP_MEDIASVR_AUDIO_PATH, allows you to specify a different media file path instead of the default path /MediaFiles/en-us/new/VL

Troubleshooting

See the *Cisco Remote Silent Monitoring Installation and Administration Guide 8.5(2)* for detailed information on RSM troubleshooting information, including case scenarios and specific fixes, located at

http://www.cisco.com/en/US/products/sw/custcosw/ps1844/prod_installation_guides_list.html

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; 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

We appreciate your comments.