CHAPTER 1

Prerequisites

Product Overview

Cisco Prime Unified Service Monitor (Prime USM), a product from the Cisco Unified Communications Management Suite, receives and analyzes data from these sources when they are installed in your voice network and configured properly:

- Cisco Unified Communications Manager (Unified Communications Manager) clusters—Retain Call Detail Records (CDRs) and Call Management Records (CMRs). CDRs include Mean Opinion Score (MOS) values that were calculated on IP phones and voice gateways using the Cisco Voice Transmission Quality (CVTQ) algorithm.

  For Unified Communications Manager versions that Service Monitor supports, see *Cisco Prime Unified Service Monitor 9.0 Compatibility Matrix*. For information about configuring Unified Communications Manager clusters to work with Service Monitor, see *User Guide for Cisco Prime Unified Service Monitor.*

- Sensors—Network Analysis Modules (NAMs) and Cisco 1040 Sensors (Cisco 1040s)—Compute MOS for each RTP stream. Service Monitor obtains data from sensors every 60 seconds.

Prime USM compares MOS against a threshold value—default or user-specified—for the codec in use. When MOS drops below the threshold, Prime USM generates SNMP traps and sends them to up to four recipients. Prime USM stores the data that it obtains in the database, where it is available for display on Service Monitor reports. Service Monitor purges the database daily to maintain a configurable number of days of data. (For more information, see the online help.)

If you configure Cisco Prime Unified Operations Manager (Operations Manager) as a trap receiver for Service Monitor, Operations Manager can further analyze, display, and act on the traps that Prime USM generates. Operations Manager can generate service quality events, display and track these events on a real-time dashboard, and display and store event history. You can configure additional event settings on Operations Manager to alert you if MOS drops below a threshold or if too many (configurable number) service quality events occur during a period of time (configurable number of minutes). In addition, you can configure Operations Manager to send notifications by e-mail, SNMP trap, and syslog message.

Prime USM 9.0 can be installed in two modes—Enterprise Network Deployment mode and Managed Service Provider (MSP) Network Deployment mode. You can specify the mode that you need to use, when you install the product. You need to choose which mode to install based on your requirements. See *User Guide for Cisco Prime Unified Service Monitor* for more details.

Server and Client System Requirements

Server Requirements

Note

- For Service Monitor to coreside on a system with other applications in the Cisco Prime Unified Communications Management Suite, see the coresidence requirements in *Installation Guide for Cisco Prime Unified Operations Manager 9.0.*
- Prime USM supports VMware for virtualization. For more information, see VMware Guidelines, page 1-7.

Table 1-2 lists the server requirements for a standalone installation of Service Monitor.

Table 1-1 Server Requirements for Service Monitor Standalone Installation

Description	Specifications			
System parameters	Up to 1,000 phones	Up to 10,000 phones	Up to 30,000 phones	Up to 60,000 phones (Including 45,000 Phones)
Call rate (CDRs/min)	Up to 50	Up to 150	Up to 500	Up to 800 (for 60,000 Phones) Up to 600 (for 45,000 Phones)
NAM/1040 Sensor RTP Stream rate (Streams/min)	Up to 100	Up to 1000	Up to 5000	Up to 5000
CDR/ RTP Stream rate (together)	Up to 50/100	Up to 150/800	Up to 500/1500	Up to 500/1500
Processor	Two processors or dual core, 2 GHz minimum each	Two processors or dual core, 2 GHz minimum each	Four processors, quad core or two dual core, 2 GHz minimum each	Four processors, quad core or two dual core, 2 GHz minimum each

Table 1-1 Server Requirements for Service Monitor Standalone Installation

Description	Specifications			
Memory (RAM)[1]	4 GB	4 GB	4 GB	8 GB
Page file[2]	8GB	8GB	8GB	12 GB
Disk space[3]	• 84 GB recommended • NTFS file system (required for secure operation). • At least 200 MB in Windows temporary directory (%TEMP%)			
• Software[4] [5] [6] [7]	• Windows Server 2003 Enterprise Edition (32 bit) with Service Pack 1 or 2 • Windows Server 2008 (R1) Standard or Enterprise Edition (32/64 bit) with Service Pack 2 • Windows Server 2008 (R2) Standard or Enterprise Edition (64 bit) with Service Pack 1 • VMware ESXi 4.x or ESXi 5.0. For requirements, see VMware Guidelines. • ODBC Driver Manager[8] 3.5.10 or later. • NTP-Configure the server to use Network Time Protocol (NTP) to synchronize with the timeserver that is used by Unified Communications Managers in your network. See NTP Configuration Notes, page 2-4.			
Hardware	• Color monitor. • CD-ROM drive. • Support for one or two 1-GB NICs (one is required, and the second is for failover support; both NIC cards must have the same IP address)			
CDR processing rate (records per minute)[9]	Up to 50	Up to 200	Up to 800	Up to 800

1. If server RAM size is less than 4 GB, then a warning message appears.
2. While configuring the page file, you should set both the minimum and maximum file size parameters to same size. Page size also needs to be changed from automatic to manual. This ensures that Windows creates a page file of the required size.
3. Disc Space:
   —Do not install Service Monitor on a FAT file system
   —The disc space must be 100GB(exclusive of the HDD space), for profiles with 60,000 phones.
   —The OS space requirement is exclusive of the specified value.
4. You must install Service Monitor on a dedicated system. Do not install Service Monitor on a Primary Domain Controller (PDC) or Backup Domain Controller (BDC). Do not install Service Monitor in an encrypted directory. Service Monitor does not support directory encryption.
5. Immediately following installation, the TCP/IP stack should be hardened to avoid denial of service attacks. Ensure these steps are taken before using the product.
   —Apply Windows security patches. See Microsoft Security Updates for Denial of Service Attacks for details. The system that you use for your Operations Manager server should meet all security guidelines that Microsoft recommends for Windows 2003 or 2008 Server. (CSCsy83124) See the NSA website for security guidance: http://www.nsa.gov.
   —Specifically, the TCP/IP stack should be hardened to avoid denial of service attacks. Refer to the section "Security Consideration for Network Attacks" on page 121 of the The Windows Server 2003 - Security Guide, v2.1 which can be downloaded from the NSA website.
   —On the Windows Server 2003 Enterprise Edition or 2008 Standard or Enterprise Edition server, block remote access to all TCP/UDP ports except for those ports used by Operations Manager required for external access.
6. The default locale for your Windows operating system must be set to US-English.

7. Windows Terminal Services is supported in Remote Administration mode only. Use of Windows Terminal Services or Remote Desktop and Virtual Network Computing (VNC) to remotely control the server is not recommended for performing day-to-day operations (for example, running reports, keeping dashboards open, and so on).
8. To verify the version of ODBC Driver Manager, from the Windows desktop, choose Start > Settings > Control Panel > Administrative Tools > Data Sources (ODBC). Select the About tab. If necessary, install Microsoft Data Access Component (MDAC) 2.5 or later.
9. For 60,000 phones, busy call rate is 1500 CDRs per minute for 2 hours per day.

Table 1-2 lists the server requirements for a coexistent installation of Service Monitor.

Table 1-2 Server Requirements for Service Monitor in Coexistent Installation

Description	Specifications			
System parameters	Up to 1,000 phones	Up to 10,000 phones	Up to 30,000 phones	Up to 60,000 phones (Including 45,000 Phones)
Call rate (CDRs/min)	Up to 50	Up to 150	Up to 500	Up to 800 (normal rate); 1500 peak rate for 2 hours/day for 60,000 phones. Up to 600 (normal rate); 1500 peak rate for 2 hours/day for 45,000 phones.
NAM/1040 Sensor RTP Stream rate (Streams/min)	Up to 100	Up to 1000	Up to 5000	Up to 5000
CDR/ RTP Stream rate (together)	Up to 50/100	Up to 150/800	Up to 500/1500	Up to 500/1500
Processor	Two processors or dual core, 2 GHz minimum each	Two processors or dual core, 2 GHz minimum each	Four processors, quad core or two dual core, 2 GHz minimum each	Four processors, quad core or two dual core, 2 GHz minimum each
Memory (RAM)[1]	4 GB	4 GB	4 GB	8 GB
Page file[2]	8GB	8GB	8GB	12 GB
Disk space[3]	• 84 GB recommended • NTFS file system (required for secure operation). • At least 200 MB in Windows temporary directory (%TEMP%)			

Table 1-2 Server Requirements for Service Monitor in Coexistent Installation

Description	Specifications			
• Software[4 5 6 7]	• Windows Server 2003 Enterprise Edition (32 bit) with Service Pack 1 or 2 • Windows Server 2008 (R1) Standard or Enterprise Edition (32/64 bit) with Service Pack 2 • Windows Server 2008 (R2) Standard or Enterprise Edition (64 bit) with Service Pack 1 • VMware ESXi 4.x or ESXi 5.0. For requirements, see VMware Guidelines. • ODBC Driver Manager[8] 3.5.10 or later. • NTP-Configure the server to use Network Time Protocol (NTP) to synchronize with the timeserver that is used by Unified Communications Managers in your network. See NTP Configuration Notes, page 2-4.			
Hardware	• Color monitor. • CD-ROM drive. • Support for one or two 1-GB NICs (one is required, and the second is for failover support; both NIC cards must have the same IP address)			
CDR processing rate (records per minute)[9]	Up to 50	Up to 200	Up to 800	Up to 800

1. If server RAM size is less than 4 GB, then a warning message appears.
2. While configuring the page file, you should set both the minimum and maximum file size parameters to same size. Page size also needs to be changed from automatic to manual. This ensures that Windows creates a page file of the required size.
3. Disc Space:
   —Do not install Service Monitor on a FAT file system
   —The disc space must be 100GB(exclusive of the HDD space), for profiles with 60,000 phones.
   —The OS space requirement is exclusive of the specified value.
4. You must install Service Monitor on a dedicated system. Do not install Service Monitor on a Primary Domain Controller (PDC) or Backup Domain Controller (BDC). Do not install Service Monitor in an encrypted directory. Service Monitor does not support directory encryption.
5. Immediately following installation, the TCP/IP stack should be hardened to avoid denial of service attacks. Ensure these steps are taken before using the product.
   —Apply Windows security patches. See Microsoft Security Updates for Denial of Service Attacks for details. The system that you use for your Operations Manager server should meet all security guidelines that Microsoft recommends for Windows 2003 or 2008 Server. (CSCsy83124) See the NSA website for security guidance: http://www.nsa.gov.
   —Specifically, the TCP/IP stack should be hardened to avoid denial of service attacks. Refer to the section "Security Consideration for Network Attacks" on page 121 of the The Windows Server 2003 - Security Guide, v2.1 which can be downloaded from the NSA website.
   —On the Windows Server 2003 Enterprise Edition or 2008 Standard or Enterprise Edition server, block remote access to all TCP/UDP ports except for those ports used by Operations Manager required for external access.
6. The default locale for your Windows operating system must be set to US-English.
7. Windows Terminal Services is supported in Remote Administration mode only. Use of Windows Terminal Services or Remote Desktop and Virtual Network Computing (VNC) to remotely control the server is not recommended for performing day-to-day operations (for example, running reports, keeping dashboards open, and so on).
8. To verify the version of ODBC Driver Manager, from the Windows desktop, choose Start > Settings > Control Panel > Administrative Tools > Data Sources (ODBC). Select the About tab. If necessary, install Microsoft Data Access Component (MDAC) 2.5 or later.
9. For 60,000 phones, busy call rate is 1500 CDRs per minute for 2 hours per day.

Note

- If your browser is configured to use a proxy server for your LAN, Service Monitor cannot open some report windows. Disable proxy server settings in Internet Options. (From the Connections tab, click **LAN Settings**.)

- When using Service Monitor, disable any software on your desktop that you use to prevent popup windows from displaying. Service Monitor must be able to open multiple windows to display information.

Client Requirements

Table 1-3 lists the client hardware and software requirements.

Table 1-3 Minimum Client Hardware and Software Requirements

Component	Minimum Requirement
Hardware/software	• Color monitor with video card set to 256 colors (For optimum viewing on the Service Monitor display, We recommend that you use the highest native resolution supported by the client PC and monitor. A large, high-resolution display will also allow for less scrolling through information presented and increase operator efficiency. The minimum resolution recommended is 1440 x 900.) • Any PC or server platform with a Pentium IV processor, 1.0 GHz or greater, running one of the following: – Windows XP Professional Service Pack 2 – Windows 2003 Server (Standard and Enterprise Editions) without Windows Terminal Services – Windows Server 2008 Enterprise Edition Service Pack 2 – Windows Server 2008 Standard Edition Service Pack 2 – Windows Server 2008 R2 (64 bit)
Processor	Dual Core, 2 GHz minimum (Windows PC or Apple Mac)
Memory	2 GB RAM minimum
Browser	• Microsoft Internet Explorer 8.x or 9.x • Firefox 10.0.5 ESR and13.0 **Note** Service Monitor uses popup dialog boxes at many places. If you have a popup-blocker enabled in your browser, none of these popups will appear. Therefore, you should disable the popup-blocker if you have installed it. **Note** We strongly recommend that you use a browser from a client system to perform day-to-day operations (for example, running reports). Use of Windows Terminal Services, Remote Desktop, or VNC to perform day-to-day operations is not recommended. Adobe Flash Player 11.x. Downloading Flash from the Adobe website requires that you install ActiveX cookies on the system.
Concurrent client (browser) logins	5 clients for enterprise deployment. 7 clients for multi-customer deployment

VMware Guidelines

Prime USM supports VMware ESX 3.5, ESXi 4.x, and ESXi 5.0. Prime USM must have the same system resources available to it, inside the virtualization environment that it has for a standard (nonvirtual) installation.

While determining the performance of Prime USM in your virtual setup, you must take into account that the VMware instance will use some system resources that would normally be available to Prime USM in a standard installation. Additional requirements for running Prime USM in a virtualization environment might vary with your environment and system load.

The following configurations are supported for Prime USM in a virtual environment:

- An instance of Prime USM, supporting up to 60,000 phones
- Each of these products installed on a separate virtual machine:
  - Operations Manager
  - Service Monitor
  - Service Statistics Manager
  - Provisioning Manager
- Each product installed on one virtual machine, supporting up to 10,000 phones and 1,000 IP devices.

Service Monitor can be installed on a virtual machine with dynamic MAC address for evaluation. However, you must configure the virtual machine with a static MAC address to purchase the permanent license for Service Monitor.

The static MAC address is required because licensing uses node-locking technology. The license file can only be used with the static MAC address that you supply.

Note The static MAC address must be within the following range: 00:50:56:00:00:00 to 00:50:56:3F:FF:FF.

To set up a static MAC address:

Step 1 Power down the virtual machine.

Step 2 In the Inventory panel, select the virtual machine.

Step 3 Click the Summary tab and then click **Edit Settings**.

Step 4 In the Hardware list, select **Network Adapter**.

Step 5 For MAC address, select **Manual**.

Step 6 Change the current MAC address of the virtual machine to a static MAC address in the following range: 00:50:56:00:00:00 to 00:50:56:3F:FF:FF.

Step 7 Click **OK**.

For more information, see *Best Practices for Cisco Unified Communications Management Suite on Virtualization* at this URL:

http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6491/ps6705/ps6535/white_paper_c11-651585.html

Terminal Server Support for Windows 2003 and Windows 2008

You can install Prime USM on a system with Terminal Services enabled in Remote Administration mode. However, you cannot install Prime USM on a system with Terminal Services enabled in Application mode.

If you have enabled Terminal Services in Application mode, you should disable the Terminal Server, reboot the system, and start the installation again.

Table 1-4 summarizes the Terminal Services features in Windows 2003 and Windows 2008 Server.

Table 1-4 Terminal Services on Windows 2003 and Windows 2008 Server

Windows 2003 /Windows 2008 Server	Features
Terminal Server	Remote access and virtual system. Each client has its own virtual OS environment.
Remote Desktop Administration	Remote access only. All clients use the same (and the only) operating system. **Note** Do not use terminal services to perform day-to-day tasks in Cisco Prime Unified Communications Management Suite applications, such as viewing the Service Level View in Operations Manager or viewing reports in Service Monitor.

Enabling and Disabling Terminal Services on a Windows Server

To enable or disable Terminal Server, go to **Manage Your Server > Add or Remove a Role > Terminal Server**.

To enable or disable Remote Desktop Administration, go to **Control Panel > System > Remote**.

Enabling and Disabling FIPS on a Windows Server

Sometimes, Federal Information Processing Standard (FIPS) compliant encryption algorithms are enabled for Group security policy on Windows server.

When FIPS compliance is activated, the SSL authentication may fail on the Service Monitor server. To allow Service Monitor to work properly, disable FIPS compliance.

To enable or disable FIPS on Windows 2003 server:

Step 1 Go to **Start > Settings > Control Panel > Administrative tools > Local Security Policy**.

The Local Security Policy window appears.

Step 2 Click **Local Polices > Security Options.**

Step 3 Select **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**.

Step 4 Right-click the selected policy and click **Properties**.

Step 5 Select **Enabled or Disabled** to enable or disable FIPS compliant algorithms.

Step 6 Click **Apply**.

You must reboot the server for the changes to take effect.

Port Usage

Before you install Service Monitor, ensure that the ports listed in Table 1-5 and Table 1-6 are free.

Note The ports in Table 1-5 and Table 1-6 should not be scanned.

Table 1-5 lists the ports that Service Monitor uses. Common Services is installed with Service Monitor. Table 1-6 lists the ports that Common Services uses.

Table 1-5 Service Monitor Port Usage

Protocol	Port Number	Service Name
TCP	22	SFTP—Service Monitor uses SFTP to obtain data from Unified Communications Manager versions 5.x and later.
UDP	53	DNS.
UDP	67 and 68	DHCP.
TCP	2000	SCCP—Service Monitor uses SCCP to communicate with Cisco 1040s.
TCP	43459	Database.
UDP	5666	Syslog—Service Monitor receives syslog messages from Cisco 1040s.
TCP	5665–5680	Interprocess communication between the user interface and back-end processes. These ports must be free.

Note Service Monitor uses TFTP to find the configuration file for a given Cisco 1040. Service Monitor by default uses port 69 on the TFTP servers.

Common Services is also installed on the Service Monitor system. Table 1-6 lists the ports used by Common Services.

Table 1-6 Common Services Port Usage

Protocol	Port Number	Service Name
TCP	23	Telnet.
TCP	25	Simple Mail Transfer Protocol (SMTP).
TCP	49	TACACS+ and ACS.
UDP	69	Trivial File Transfer Protocol (TFTP).
UDP	161	Simple Network Management Protocol (SNMP).

Table 1-6 Common Services Port Usage (continued)

Protocol	Port Number	Service Name
TCP	443	Common Services HTTP server in SSL mode. If IIS is on your system, even when IIS is disabled, you will be asked if you want to select an HTTPS port other than 443 during installation or upgrade. To avoid port conflict, select another port.
TCP	514	Remote Copy Protocol.
UDP	514	Syslog.
UDP	1431	Trap Listener to MAC Notification Traps.
TCP	1741	Common Services HTTP Protocol.
—	2002	Communicate with Cisco Secure ACS server when AAA mode is ACS.
TCP	8898	Log Server.
TCP	9007	Tomcat shutdown.
TCP	9009	Ajp13 connector used by Tomcat.
TCP	15000	Log server.
UDP	16236	UT Host acquisition.
TCP	40050-40070	CSTM ports used by Common Services applications, such as Device and Credential Repository (DCR).
TCP	40401	LicenseServer.
TCP	42340	Daemon Manager - Tool for Server Processes.
UDP	42342	OSAGENT.
TCP	42344	ANI HTTP Server.
UDP	42350	Event Services Software (ESS) (alternate port is 44350/udp.)
TCP	42351	Event Services Software (ESS) Listening (alternate port is 44351/tcp.)
TCP	42352	ESS HTTP (alternate port is 44352/tcp.)
TCP	42353	ESS Routing (alternate port is 44352/tcp.)
TCP	43441	CMF Database.
TCP	50001	SOAPMonitor.