QUICK START GUIDE

Cisco Unified Service Statistics Manager 1.3

1 SUPPLEMENTAL LICENSE AGREEMENT

SUPPLEMENTAL LICENSE AGREEMENT FOR CISCO SYSTEMS NETWORK MANAGEMENT SOFTWARE: CISCO UNIFIED Service Statistics Manager.

IMPORTANT-READ CAREFULLY: This Supplemental License Agreement ("SLA") contains additional limitations on the license to the Software provided to Customer under the End User License Agreement between Customer and Cisco. Capitalized terms used in this SLA and not otherwise defined herein shall have the meanings assigned to them in the End User License Agreement. To the extent that there is a conflict among any of these terms and conditions applicable to the Software, the terms and conditions in this SLA shall take precedence.

By installing, downloading, accessing or otherwise using the Software, Customer agrees to be bound by the terms of this SLA. If Customer does not agree to the terms of this SLA, Customer may not install, download or otherwise use the Software. When used below, the term "server" refers to central processor unit.

1. ADDITIONAL LICENSE RESTRICTIONS.

- **Installation and Use.** The Software components are provided to Customer solely to install, update, supplement, or replace existing functionality of the applicable Network Management Software product. Customer may install and use the following Software components:
  - Cisco Unified Service Statistics Manager: May be installed on one (1) server in Customer's network management environment.
  - SSM Administration Console: May be installed on four (4) servers in Customer's network management environment.
  - SSM Agent: May be installed on one (1) server with Cisco Unified Operations Manager and on multiple servers with Cisco Unified Service Monitor.
- **Number of IP Phones.** For each Software license granted, Customer may install and run the Software on a single server to manage the number of IP phones specified in the license file provided with the Software, or as specified in the Software License Claim Certificate. Customers whose requirements exceed the IP phone limit must purchase upgrade licenses or additional copies of the Software. The IP phone limit is enforced by license registration.
- **Cisco Unified Service Statistics Manager Standard Edition.** Customer may install and run the Software on a single server. This version of Service Statistics Manager limits the features available to the customer. The following feature is not accessible: Service Level Agreements (SLAs)
- **Cisco Unified Service Statistics Manager Premium Edition.** Customer may install and run the Software on a single server. Customer has access to all features of the Software. Use of this product is enforced by license registration.
- **Reproduction and Distribution.** Customer may not reproduce nor distribute the Software.

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

Please refer to the Cisco Systems, Inc. End User License Agreement.

2 Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)".
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)".

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS"' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

3 Cisco Unified Service Statistics Manager Overview

Cisco Unified Service Statistics Manager (Service Statistics Manager) is a product from the Cisco Unified Communications Management Suite that collects and stores short-term operational data to perform longer-term analysis of IP telephony service quality, service availability, call volume, service trends, and resource utilization. Service Statistics Manager does the following:

- Extracts data collected by Cisco Unified Operations Manager (Operations Manager) and Cisco Unified Service Monitor (Service Monitor) and stores this short-term data in the Service Statistics Manager database. Operations Manager and Service Monitor collect Cisco Unified Communications statistics from various Cisco devices and systems.
- Analyzes the stored data and generates out-of-the box reports designed for users in executive, operations, capacity planning, and network administration roles.

Depending on your license level, Service Statistics Manager can also enable you to define Service Level Agreements (SLAs) as well as measure and verify them based on collected statistics.

Service Statistics Manager Components

When you install Service Statistics Manager, the following components are installed:

- **Service Statistics Manager**—Includes:
  - The application server with the database and the backend processes that analyze data and create the reports.
  - The web server through which you can access the user interface and view reports.
- **SSM Agent**—Obtains data for Service Statistics Manager on the Operations Manager or Service Monitor system where it is installed.
- **SSM Administration Console**—Manage groups, users, and roles. Only a user with admin privilege in Service Statistics Manager can log into this console.

After you install Service Statistics Manager, you can install SSM Agent and SSM Administration Console from the Service Statistics Manager user interface onto additional systems as needed:

- **SSM Agent**—You must have an SSM Agent installed on a single Operations Manager system and on the system for each instance of Service Monitor that has been added to Operations Manager.
- **SSM Administration Console**—A remotely installed SSM Administration Console communicates with the server where Service Statistics Manager is installed and updates the database on the server. SSM Administration Console is not accessible through a browser. You must launch SSM Administration Console while logged into the system—locally or using VNC—where it is installed.

Licensing

Service Statistics Manager features software-based product registration and license key activation technologies.

Note You do not need to perform this procedure if you are installing Service Statistics Manager for evaluation only.

You must perform the procedures in this section when you do any of the following:

- Initially install a purchased version of Service Statistics Manager.
- Upgrade from an earlier version of Service Statistics Manager.
- Upgrade from an Evaluation license to a purchased license for Service Statistics Manager.
- Add support for additional phones with an incremental license for Service Statistics Manager.

To license your product:

1. Obtain a product authorization key (PAK) and a license file before you perform an installation or an upgrade. See Obtaining a PAK, page 6 and Obtaining a License File, page 6.
2. Install the license file or files after you install or upgrade the product. See Installing a License File, page 6

Obtaining a PAK

The PAK is located on the software claim certificate. You can obtain the claim certificate through the eDelivery system; for information on eDelivery, see http://www.cisco.com/web/partners/tools/edelivery.html.

Obtaining a License File

Note

- Licensing uses node-locking technology. The license file can only be used with the MAC address that you supply.
- To obtain a license and to run a licensed copy of Service Statistics Manager on VMware, configure a static MAC address for the virtual machine. (You must supply a static MAC address when you register the product.) For more information, see VMware Guidelines, page 6.

To obtain a license file, you must, register the Service Statistics Manager product with Cisco.com using the PAK and the MAC address of the server on which Service Statistics Manager will reside. Get your license file from:

http://www.cisco.com/go/license

Note You will be asked to log in. You must be a registered user of Cisco.com to log in.

Logging in allows your Cisco user profile information to autopopulate many of the product registration fields. Login is case sensitive.

If you purchased an incremental license to support additional phones, use each PAK that you received to obtain a license file.

Installing a License File

Step 1 Copy all license files—the product license file and incremental license files, if any—to the Service Statistics Manager server into this directory: *Installation Directory*\pw\licenses\cisco\etc\licenses.

Step 2 Restart the server by selecting **Start > Programs > Cisco Unified Service Statistics Manager > Start Server**.

Note You do not need to first select Stop Server because Start Server restarts the server.

VMware Guidelines

Service Statistics Manager supports VMware ESX 3.5 and ESXi 4.x. Service Statistics Manager must have the same system resources available to it inside the virtualization environment that it has for a standard (nonvirtual) installation. When determining the performance of Service Statistics Manager in your virtual setup, you must take into account that the VMware instance will use some system resources that would normally be available to Service Statistics Manager in a standard installation. Additional requirements for running Service Statistics Manager in a virtualization environment might vary with your environment and system load. For more information, see *Best Practices for Cisco Unified Communications Management Suite on Virtualization* under this URL:

http://www.cisco.com/en/US/products/ps6535/prod_white_papers_list.html

The following configurations are supported for Service Statistics Manager in a virtual environment:

- One instance of Service Statistics Manager supporting up to 30,000 phones
- Each of these products installed on a separate virtual machine:
  - Operations Manager
  - Service Monitor

- Service Statistics Manager
- Provisioning Manager

with each supporting up to 10,000 phones and 1,000 IP devices. (Running one instance of an application in one virtual machine is the only supported configuration.)

Note For more information, see *Best Practices for Cisco Unified Communications Management Suite on Virtualization* under this URL: http://www.cisco.com/en/US/products/ps6535/prod_white_papers_list.html.

When setting up Service Statistics Manager in a VMware environment, keep in mind the following guidelines:

- Resources must be reserved at 100% of requirements for the virtual machine.
- To use a licensed Service Statistics Manager in a VMware environment, you must configure your virtual machine with a static MAC address.

Note You can run Service Statistics Manager in Evaluation mode with a dynamic MAC address. However, before you can run a licensed copy of Service Statistics Manager, you must configure a static MAC address.

To set up a static MAC address, do the following:

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.

When assigning a static MAC address, we recommend choosing a complex address. An example of a complex MAC address is 00:50:56:01:3B:9F. A less complex MAC address is 00:50:56:11:11:11, because of the repeating ones (1).

Note Choosing a complex address makes it less likely that you will choose an address being used by another customer. This can prevent accidental licensing overlap between different customers.

Step 7 Click **OK**.

4 Server and Client System Requirements

For Service Statistics Manager requirements, see:

- Table 1—Lists minimum server requirements for installing Service Statistics Manager alone.

Note
- Service Statistics Manager supports VMware for virtualization. For more information, see VMware Guidelines, page 6.
- Hardware requirements for installing Service Statistics Manager on a system with Operations Manager and Service Monitor are provided in the Coresident Guidelines section in *Installation Guide for Cisco Unified Operations Manager 2.3 (Includes Service Monitor)*.

- Table 2—Lists minimum client requirements.
- Table 3—Lists browser requirements.

Server requirements for SSM Administration Console and SSM Agent are included in Table 4 and Table 5, respectively.

Table 1 Minimum Service Statistics Manager Server Requirements

Component	Minimum Requirement
Hardware	• Server platform with one of the following processors: – Single or dual-core Pentium 4 greater than 2.0 GHz—Small deployments (up to 1,000 phones). – Single or dual-core Pentium 4 or Xeon, greater than 3.0 GHz—Medium deployments (up to 10,000 phones). – Dual-core Pentium 4 or Xeon, greater than 3.0 GHz—Large deployments (up to 45,000 phones). • One NIC only. • Color monitor with video card capable of 256 colors or more • CD-ROM drive
Software	One of these: • Windows Server 2003 Service Pack 2, Standard and Enterprise editions (32-bit) • Windows Server 2003 R2 Service Pack 2, Standard or Enterprise editions (32-bit) **Note** • Windows Terminal Services is not supported. • Only US-English is supported for System locale and Regional and Language settings. • Perl installation on this system is not recommended. • Necessary security precautions are listed in Preparing the Server Before You Install or Upgrade, page 10.
Memory (RAM)	• 4 GB
Available virtual memory	• Service Statistics Manager Standard Edition: – 4 GB (up to 1,000 phones) – 8 GB (up to 5,000 phones) • Service Statistics Manager Premium Edition—8 GB (up to 45,000 phones)
Available disk space	60 GB NTFS file system[1]

1. Do not install Service Statistics Manager on a FAT file system. To verify the file system, open My Computer on the Windows desktop, right-click the drive and select **Properties** from the popup menu. The file system field appears in the General tab of the Properties dialog box.

Table 2 Minimum Client Hardware and Software Requirements

Component	Minimum Requirement
Hardware/software	• Any PC or server platform with a Pentium 4 processor, 1 GHz or greater, running one of the following: – Windows 2000 SP3 – Windows XP Professional SP2 – Windows Server 2003, Standard and Enterprise editions – Windows Server 2003 R2, Standard and Enterprise editions without Windows Terminal Services • Color monitor with video card set to 256 colors **Note** If you are using a VGA monitor, be sure to install and use the manufacturer's display adapter driver. SSM Administration Console is not compatible and will not display with the Windows NT/2000 generic driver (named VGA Compatible Display Adapter).
Available virtual memory	2 GB virtual memory
Available memory (RAM)	1 GB minimum We recommend that you set virtual memory to twice the size of RAM.

Table 3 Client Browser Requirements

Browser	Version
Internet Explorer	One of the following: 6.0. 7.0

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

Table 4 lists minimum requirements for installing an additional instance of SSM Administration Console alone on system.

Table 4 Minimum Server Requirements for SSM Administration Console Installed Standalone

Component	Minimum Requirement
Hardware	• Any PC or server platform with a Pentium 4 processor, 1.0 GHz or greater • CD-ROM drive • Color monitor with video card capable of 256 colors or more **Note** If you are using a VGA monitor, be sure to install and use the manufacturer's display adapter driver. SSM Administration Console is not compatible and will not display with the Windows NT/2000 generic driver (named VGA Compatible Display Adapter).
Software for Windows	Windows Server 2003 Service Pack 2, Standard and Enterprise editions without Windows Terminal Services
Available memory (RAM)	256 MB
Available disk space	150 MB

Table 5 lists additional requirements for installing SSM Agent on a system with Operations Manager or Service Monitor.

Table 5 Minimum Server Requirements for SSM Agent

Component	Minimum Requirement
Memory	512MB
Available disk space	300 MB
Swap space	1024 MB
TCP control port	12124

Preparing the Server Before You Install or Upgrade

Before you install or upgrade, ensure that you have performed the following tasks:

- Ensuring the Security of Your Windows 2003 Server, page 10
- Installing Win32 OpenSSL on the Server System, page 10
- Installing Required Windows Service Packs Before You Upgrade, page 11
- If you are installing Service Statistics Manager on a system with Operations Manager or Service Monitor, you should verified that the full 4 GB of RAM is enabled (see Enabling the Full 4 GB of RAM, page 11).

Ensuring the Security of Your Windows 2003 Server

The system that you use for your Service Statistics Manager server should meet all the security guidelines that Microsoft recommends for Windows 2003 Server. See the NSA website for security guidance: (http://www.nsa.gov/ia/guidance/security_configuration_guides/operating_systems.shtml#microsoft).

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 103 of the The Windows Server 2003 - Security Guide, v2.1 which can be downloaded from the NSA website.

Installing Win32 OpenSSL on the Server System

Perform these steps on the system where you will install or upgrade the Service Statistics Manager server.

Step 1 Download and install the Microsoft Visual C++ 2010 Redistributable Package (x86) from this URL:

http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=a7b7a05e-6de6-4d3a-a423-37bf0912db84

Step 2 Download Win32 OpenSSL as follows:

a. Log in to Cisco.com.

b. Go to the Cisco Unified Service Statistics Manager product support page: http://www.cisco.com/en/US/products/ps7285/tsd_products_support_series_home.html

c. Select the **Download Software** link and select **Cisco Unified Service Statistics Manager 1.3**.

d. Download the OpenSSL-0.9.8n-Win32-CSCtd05778.zip file.

Note The download includes only the latest version of Win32 OpenSSL that was tested with Service Statistics Manager 1.3.

Step 3 Extract the the contents of the OpenSSL-0.9.8n-Win32-CSCtd05778.zip file into a directory of your making on the server. If prompted to overwrite existing files, answer Yes. The following files are extracted:

bin/openssl.exe

bin/libeay32.dll

bin/ssleay32.dll

conf/openssl.cnf

Note Additional steps are required to enable SSL on the Service Statistics Manager server. The steps are provided in the installation and upgrade procedures.

Installing Required Windows Service Packs Before You Upgrade

You can perform an upgrade from Service Statistics Manager 1.2 to Service Statistics Manager 1.3 on the server where Service Statistics Manager 1.2 is installed. If the system is not on Windows 2003 SP2, upgrade to Windows 2003 SP2 before you upgrade to Service Statistics Manager 1.3.

Enabling the Full 4 GB of RAM

If you are installing Service Statistics Manager on a system with Operations Manager or Service Monitor, you should make sure that all 4 GB of RAM is enabled. There is a known issue with Windows 2003 when working with certain hardware. Even though 4 GB of memory is installed on the system, Windows 2003 reports that there is less than 4 GB of memory installed. For more details, see http://msdn2.microsoft.com/en-us/library/ms791485.aspx.

To enable all 4 GB of RAM on the system, use the following procedure:

Step 1 On the Service Statistics Manager system, in Windows right-click **My Computer**.

Step 2 Select **Properties**.

Step 3 Select the **Advanced** tab.

Step 4 Under Startup and Recovery, click **Settings**.

Step 5 Click **Edit**. The boot.ini file opens.

Step 6 In the file, add **`"/PAE"`** in line starting with "multi(0)disk(0)rdisk(0)partition(1)\WINDOWS=..."

Step 7 Restart the system.

Cisco Unified Service Statistics Manager Port Usage

Table 6 lists TCP ports that Service Statistics Manager uses; the ports must be free or Service Statistics Manager installation will not proceed. To check whether a port is in use, from a command line enter this command:

`netstat -anb | findstr` ***`portnumber`***

If there is no output from the command, the port is free.

Table 6 Service Statistics Manager Port Usage

Port Number	Service Name
8007	Apache JServ
8008	Tunnel Proxy
8009	Tomcat
8093	JMS Server
9149	JServer Event

Table 6 Service Statistics Manager Port Usage (continued)

Port Number	Service Name
48099	Remote Method Invocation **Note** To configure Service Statistics Manager to use a port other than 48099, see Reconfiguring Selected Ports and Properties for Service Statistics Manager, page 29.
48100	JBOSS **Note** To configure Service Statistics Manager to use a port other than 48100, see Reconfiguring Selected Ports and Properties for Service Statistics Manager, page 29.
48101	HTTP—Web server
48102	Database
12123	Agent Controller Listener
12124	Used by SSM Agent to listen to messages from the SSM server
12125	Database access port that interacts between the agent controller and the database.
12126	Agent controller callback—This port is used by remote SSM agents to send data back to the Service Statistics Manager server.
12130	Checkpoint monitor (for receiving log messages)
12140	CLServer
12141	Log Server
18000	Rate
40402	Licensing
45000	Message server
48443	HTTPS—Secure web server

5 Installation and Upgrade Paths

See the following sections:

- Supported Installation Paths, page 13
- Supported Upgrade Paths, page 13

Supported Installation Paths

Table 7 lists the supported installation paths for Service Statistics Manager.

Table 7 Supported Configurations and Installation Paths

Supported Configuration	Required Order of Installation	Maximum Supported Phones	For Hardware Requirements, see...
Cisco Unified Communications Manager products installed on one dedicated server	**1.** Operations Manager (includes Service Monitor) must be installed before Service Statistics Manager. **2.** Service Statistics Manager. **3.** Provisioning Manager (installed in advance mode to resolve port conflicts with already installed applications). **Note** It is permissible to install Provisioning Manager before either Operations Manager or Service Statistics Manager.	10,000	Coresident Guidelines in *Installation Guide for Cisco Unified Operations Manager 2.3 (Includes Service Monitor)*.
Service Statistics Manager only installed on a dedicated server	**1.** Operations Manager (includes Service Monitor) must be installed elsewhere in your network. **2.** Service Monitor (if installed on a server separate from the one where Operations Manager is installed). **3.** Service Statistics Manager. **4.** SSM Agent—Install on any server where Service Monitor is installed alone and on the server where Operations Manager (includes Service Monitor) is installed.	45,000	Table 1 on page 8

For supported installation in a virtualization environment, see VMware Guidelines, page 6.

Supported Upgrade Paths

Dial plan and call classification configuration is removed from Service Statistics Manager 1.3 and added to Service Monitor 2.3. You cannot automatically migrate dial plan and call classification data from Service Statistics Manager 1.2 to Service Monitor 2.3.

Caution When you upgrade to Service Statistics Manager 1.3, dial plan and call classification data is lost. Before upgrading, see Manually Recording Dial Plan and Call Classification Data from Service Statistics Manager 1.2, page 19.

Note Upgrade from releases prior to Service Statistics Manager 1.2 is not supported.

Table 8 Supported Upgrade Paths

To upgrade to Service Statistics Manager 1.3 on a system where...	You will need to do this
Operations Manager (includes Service Monitor) is installed	1. If Operations Manager has not been upgraded to 2.3 yet, do this: a. Determine whether to perform the task described in Manually Recording Dial Plan and Call Classification Data from Service Statistics Manager 1.2, page 19. b. Stop Service Statistics Manager 1.2. c. Upgrade to Operations Manager 2.3. (For more information, see *Installation Guide for Cisco Unified Operations Manager 2.3 (Includes Service Monitor).)* d. Configure call classification in Service Monitor 2.3. 2. Upgrade to Service Statistics Manager 1.3. See Upgrading to Cisco Unified Service Statistics Manager 1.3, page 18. 3. If SSM Agent is installed on another system, such as one on which Service Monitor is installed, upgrade SSM Agent on that system. (Ensure that Service Monitor has been upgraded to 2.3 before you upgrade the SSM Agent.) See Upgrading the SSM Agent, page 21. 4. Run discovery from Service Statistics Manager; see Running Discovery, page 29. (Operations Manager and Service Monitor must be running for discovery to succeed.) 5. If SSM Administration Console is installed on another system, upgrade SSM Administration Console on that system. See Upgrading the SSM Administration Console, page 21.
Service Statistics Manager 1.2 only is installed	1. Determine whether to perform the task described in Manually Recording Dial Plan and Call Classification Data from Service Statistics Manager 1.2, page 19. 2. If the Operations Manager system in your network has not been upgraded to 2.3 yet, upgrade Operations Manager to 2.3. (For more information, see *Installation Guide for Cisco Unified Operations Manager 2.3 (Includes Service Monitor).)* 3. If Service Monitor is installed alone on a system in your network and Service Monitor has not been upgraded to 2.3 yet, do this: a. On the Service Statistics Manager server, stop Service Statistics Manager 1.2. b. On the server where Service Monitor is installed, perform the upgrade to Service Monitor 2.3. (For more information, see *Installation Guide for Cisco Unified Service Monitor 2.3.)* 4. Configure call classification in Service Monitor 2.3. 5. Upgrade to Service Statistics Manager 1.3. See Upgrading to Cisco Unified Service Statistics Manager 1.3, page 18. 6. Upgrade the SSM Agent on the system where Operations Manager 2.3 is installed and on each system where Service Monitor 2.3 is installed. See Upgrading the SSM Agent, page 21. 7. Run discovery from Service Statistics Manager. (See Running Discovery, page 29.) 8. If SSM Administration Console is installed on another system, upgrade SSM Administration Console on that system. See Upgrading the SSM Administration Console, page 21.

6 Installing Cisco Unified Service Statistics Manager

This section includes the following topics:

Before You Install Service Statistics Manager

Be sure to complete the tasks in Preparing the Server Before You Install or Upgrade, page 10.

Operations Manager 2.3 and Service Monitor 2.3 must be installed on a system in your network before you install Service Statistics Manager 1.3.

Find out which port Operations Manager uses for SSL; if Operations Manager uses a port other than the default (443), you will need to reconfigure Service Statistics Manager before you can log in.

Do not install Service Statistics Manager on a system where the SSM Agent or SSM Administration Console is installed.

Note To uninstall SSM Agent or SSM Administration Console, use Add/Remove Programs from the Windows Control Panel and uninstall Service Statistics Manager Agent or Service Statistics Manager Admin.

Disable the virus scan software on your system. You can restart it after installation is complete.

If Cisco Security Agent runs on your system, disable it before starting the installation and re-enable it after you complete the installation and run discovery to completion.

Make sure your system meets the prerequisites:

- Required (or desired) operating system upgrades have been performed.
- Required Windows service packs are installed.
- Required minimum amount (or more) of RAM is available.
- Ports that Service Statistics Manager uses are free; see Table 6.

During the installation, you will need to supply contact information—name, email address, and SMTP server—for a system administrator to be notified if a problem occurs during the weekly server restart on Sunday or if disk space usage reaches 80% on the system.

You will also need to enter a password for admin, the default user account. The admin user can perform all Service Statistics Manager tasks and all SSM Administration Console tasks. You must log in to the SSM Administration Console as admin to configure additional users.

Note Take note of the password that you enter for admin so that you can log in to Service Statistics Manager after you complete the installation.

Installing Service Statistics Manager

Step 1 As the local administrator, log in to the machine on which you will install the Service Statistics Manager software, and insert the Service Statistics Manager CD-ROM into the CD-ROM drive.

Step 2 Navigate to and click **Setup.exe**. The Cisco Unified Service Statistics Manager 1.3 Setup window opens, displaying a Welcome message

Step 3 Click **Next**. If SSM Agent or SSM Administration Console is installed, an error message is displayed; click **OK**; the installation stops.

Otherwise, the Software License Agreement is displayed.

Step 4 Click **Accept**. The minimum required system configuration is displayed.

Step 5 Click **Next**. A pre-installation check runs to verify that the required configuration is present. When the check completes, the results are displayed.

If mandatory requirements are not met, the installation stops. Read the log file, ProactivePreInstall.log, on the desktop and correct errors before trying to install the Service Statistics Manager server again.

Step 6 Click **Next**. An Admin Information page is displayed.

Step 7 Enter (and confirm) a password for the user *admin*.

Note Take careful note of the password. You must enter it when you log in to Service Statistics Manager.

Step 8 Click **Next**. The Administrator Information page is displayed.

Step 9 Enter contact information for the system administrator who is responsible for this server:

- Administrator E-Mail ID—Enter the complete e-mail address for the system administrator (*username@domain*). If disk space is less than 80% or if a problem occurs with the weekly (Sunday) system restart, Service Statistics Manager sends e-mail to this address.
- From E-Mail ID—Enter the e-mail address from which Service Statistics Manager should send scheduled reports.
- Name or IP Address of SMTP Server—Enter an IP address or DNS name for an SMTP server.

Step 10 Click **Next**. The Choose Destination Location page appears, displaying a default destination location.

Note Do not install Service Statistics Manager on a shared drive. Doing so can create a conflict in registry entries.

If you do not want to use the default destination location, click **Browse** and select another location.

Step 11 Click **Next**. The installation begins; status is displayed during this process. The Installation Completed Successfully page is displayed.

Step 12 Click **Finish**.

Step 13 Complete these tasks:

Note To put the changes made in steps b, c, and d into effect, you must restart the Service Statistics Manager server (as directed in step e).

a. Stop the Service Statistics Manager server. Enter this command:

```
pw sys stop
```

b. Copy the Service Statistics Manager license file to the server into this directory: *Installation Directory*\pw\licenses\cisco\etc\licenses. (If you are evaluating Service Statistics Manager, you can skip this step.)

c. Enable SSL:

- Ensure that you have completed the steps in Installing Win32 OpenSSL on the Server System, page 10.
- Copy the ssleay32.dll, libeay32.dll, and openssl.exe files (located in the *OpenSSL Win32 Installation Directory*\bin folder) to the *Service Statistics Manager Installation Directory*\pw\ApacheGroup\Apache\bin folder.
- Copy the openssl.cnf file (located in the *OpenSSL Win32 Installation Directory*\conf folder) to the *Service Statistics Manager Installation Directory*\pw\ApacheGroup\Apache\conf folder.

d. If Operations Manager uses an SSL port other than 443, perform these steps on the Service Statistics Manager server:

- Navigate to this directory: *Installation Directory*\pw\pronto\conf
- Edit the pronet.conf file and, find this line: pronet.ssm.om.port.https=443
- Replace 443 with the SSL port that Operations Manager uses

e. Restart the Service Statistics Manager server. From the command prompt, type:

```
pw sys start
```

(The command stops the server, if it is running, and starts the server.)

Step 14 Verify that Service Statistics Manager was installed correctly by logging in to Service Statistics Manager. See Logging in to Cisco Unified Service Statistics Manager, page 22.

Step 15 Perform the post-installation steps listed in Post-Installation Configuration Summary, page 30.

Installing SSM Agent

Before you install SSM Agent, ensure that:

- Service Statistics Manager is already installed in your network.
- Operations Manager or Service Monitor is already installed on the system where you will install SSM Agent.
- The system meets the prerequisites in Table 5.

Step 1 From a browser on the Operations Manager or Service Monitor system where you will install SSM Agent, log in to Service Statistics Manager as an admin user. See Logging in to Cisco Unified Service Statistics Manager, page 22.

Step 2 Download the image and start the installation:

a. Select the **Administration** tab.

Note For more detailed installation instructions than those presented in this procedure, click **Help** in the upper-right corner of the Service Statistics Manager window.

b. Under Downloads, click Agent.exe. A File Download window appears.

c. Do one of the following:

- Click **Save** and save Agent.exe to the desktop; then double-click Agent.exe to start the installation.
- Click **Open**. Some time might elapse while Agent.exe downloads.

An InstallShield window appears with a Welcome message.

Step 3 Follow the online prompts to complete the installation. For more information, see online help.

Installing SSM Administration Console

SSM Administration Console is already installed on the system with Service Statistics Manager. Optionally, you can install SSM Administration Console on another system. Before you install SSM Administration Console, ensure that:

- Service Statistics Manager is already installed in your network.
- The system meets the prerequisites in Table 4.

Step 1 From a browser on the Operations Manager or Service Monitor system where you will install SSM Administration Console, log in to Service Statistics Manager as an admin user. See Logging in to Cisco Unified Service Statistics Manager, page 22.

Step 2 Download the image and start the installation:

a. Select the **Administration** tab.

Note For more detailed installation instructions than those presented in this procedure, click the **Help** link in the upper-right corner of the Service Statistics Manager window.

b. Under Downloads, click Admin.exe. A File Download window appears.

c. Do one of the following:
   - Click **Save** and save Admin.exe to the desktop; then double-click Admin.exe to start the installation.
   - Click **Open**. Some time might elapse while Admin.exe downloads.

An InstallShield window appears with a Welcome message.

Step 3 Follow the prompts on the windows to complete the installation. (For more information, see online help.)

7 Upgrading to Cisco Unified Service Statistics Manager 1.3

This section includes the following topics:

Before You Upgrade to Service Statistics Manager 1.3

Before you start your upgrade, ensure that you complete the following:

1. Complete the tasks in Preparing the Server Before You Install or Upgrade, page 10.
2. Record any dial plan data from Service Statistics Manager 1.2 that you want to reconfigure in Service Monitor 2.3; see Manually Recording Dial Plan and Call Classification Data from Service Statistics Manager 1.2, page 19.
3. We strongly recommend that you back up the database before starting the upgrade. See Performing a System Backup, page 19. (The upgrade procedure does not perform a backup.)
4. If the system where the Service Statistics Manager 1.2 server is installed is not on Windows 2003 SP2, upgrade to Windows 2003 SP2 before you upgrade to SSM 1.3.
5. Complete the upgrades to Operations Manager 2.3 and Service Monitor 2.3 on the systems where they are installed. (before you upgrade any system where Service Monitor is running, shut down Service Statistics Manager.) For more information, see *Installation Guide for Cisco Unified Operations Manager 2.3 (Includes Service Monitor)* and, if Service Monitor is installed standalone, see *Installation Guide for Cisco Unified Service Monitor 2.3*.
6. Complete call classification configuration in Service Monitor 2.3.
7. Perform these steps on the Service Statistics Manager server:
   - If Cisco Security Agent runs on your system, you must disable it before starting the upgrade and re-enable it after the upgrade completes and you have run discovery.
   - Disable the virus scan software on your system. You can restart it after upgrade is complete.
   - Make sure your system meets the prerequisites:

     Required Windows service packs are installed; SP2 is required.

     Required minimum amount (or more) of RAM is available.

     Ports that Service Statistics Manager uses are free; see Table 6.

With the previous list of tasks completed, you can start your upgrade. See Upgrading the Server to Service Statistics Manager 1.3, page 19.

Note For information on how the upgrade affects existing reports, see the New Features and Upgrade Notes sections of *Release Notes for Cisco Unified Service Monitor 2.3*.

Manually Recording Dial Plan and Call Classification Data from Service Statistics Manager 1.2

When you upgrade, the ability to configure dial plan and call classification is removed from Service Statistics Manager and dial plan and call classification configuration data is lost. Service Statistics Manager 1.3 relies on the dial plans and call classification that you configure in Service Monitor 2.3; Service Monitor supplies categorized call volume data to Service Statistics Manager 1.3 for reports.

You cannot automatically migrate dial plan and call classification data from Service Statistics Manager 1.2 to Service Monitor 2.3 due to these differences:

- Call category types and names used in Service Monitor are different from those used previously in Service Statistics Manager. For information, see *User Guide for Cisco Unified Service Monitor.*
- Dial plans are assigned on a per cluster basis in Service Monitor.
- Toll-free numbers and service numbers are configured in each dial plan in Service Monitor.

Before you upgrade, consider taking screenshots or otherwise making a record of the following data that is configured on the Administration tab in Service Statistics Manager 1.2:

- Dial plan entries
- Gateway codes
- Toll-free numbers
- Service numbers

Use your notes or screenshots to help you configure appropriate data in Service Monitor 2.3. For more information, see Configuring Service Monitor to Categorize Call Data from Unified Communications Manager, page 27.

Performing a System Backup

Step 1 Select **Start > Programs > Cisco Unified Service Statistics Manager Server > Stop Server.**

Step 2 Copy all files and folders from *Installation Directory*\pw\ to another location.

Upgrading the Server to Service Statistics Manager 1.3

This procedure upgrades the Service Statistics Manager server, the SSM Administration Console, and the SSM Agent on a single server. After you complete this procedure, if SSM Administration Console and SSM Agent are installed on additional servers, you must upgrade them using these procedures: Upgrading the SSM Administration Console, page 21 and Upgrading the SSM Agent, page 21.

Note

- Ensure that you have completed the necessary steps in Before You Upgrade to Service Statistics Manager 1.3, page 18.
- During the upgrade, some messages might be displayed that refer to a reinstallation even though you are actually performing an upgrade.

Step 1 As the local administrator, log in to the machine on which you will upgrade the Service Statistics Manager software, and insert the Service Statistics Manager CD-ROM into the CD-ROM drive.

Step 2 Navigate to and click **Setup.exe**. The Cisco Unified Service Statistics Manager 1.3 Setup window opens, displaying a Welcome message and these radio buttons:

- Reinstall/Upgrade
- Remove

Step 3 Select Reinstall/Upgrade and click **Next**. A message appears, asking whether you are sure that you want to upgrade and letting you know that Service Statistics Manager will shut down during the installation.

Step 4 Click **OK**. The License Agreement page appears.

Step 5 Click **Accept**. An Information window appears, displaying the minimum system requirements.

Step 6 Click **Next**. A pre-installation check runs to verify that the required configuration is present. When the check completes, the results are displayed.

If mandatory requirements are not met, the upgrade stops. Read the log file, ProactivePreInstall.log, on the desktop and correct errors before trying to upgrade the Service Statistics Manager server again.

Step 7 Click **Next**. The following windows appear:

- Setup status.
- A message explaining that the upgrade can take a long time.
- Completion status.

Step 8 Click **Finish**.

Step 9 Complete these tasks:

Note To put the changes made in steps b, c, and d into effect, you must restart the Service Statistics Manager server (as directed in step e).

a. Stop the Service Statistics Manager server. Enter this command:

```
pw sys stop
```

b. Copy the Service Statistics Manager upgrade license file to the server into this directory: *Installation Directory*\pw\licenses\cisco\etc\licenses.

c. Enable SSL:

- Ensure that you have completed the steps in Installing Win32 OpenSSL on the Server System, page 10.
- Copy the ssleay32.dll, libeay32.dll, and openssl.exe files (located in the *OpenSSL Win32 Installation Directory*\bin folder) to the *Service Statistics Manager Installation Directory*\pw\ApacheGroup\Apache\bin folder.
- Copy the openssl.cnf file (located in the *OpenSSL Win32 Installation Directory*\conf folder) to the *Service Statistics Manager Installation Directory*\pw\ApacheGroup\Apache\conf folder.

d. If Operations Manager uses an SSL port other than 443, perform these steps on the Service Statistics Manager server:

- Navigate to this directory: *Installation Directory*\pw\reports\cache.
- Edit the pronet.conf file and, find this line: pronet.ssm.om.port.https=443
- Replace 443 with the SSL port that Operations Manager uses

e. Restart the Service Statistics Manager server. From the command prompt, type:

pw sys start

f. Close any existing browser sessions.

Step 10 Before you continue, wait for 30 minutes when both of the following are true:

- You performed the upgrade on a server where Operations Manager is also installed.
- You restarted the Windows server.

Waiting enables Operations Manager processes to come up fully and ensures a proper response during your initial post-upgrade login to Service Statistics Manager. (If you are unable to log in, restart the Service Statistics Manager server.)

Step 11 Verify that Service Statistics Manager was upgraded correctly by logging in to Service Statistics Manager. See Logging in to Cisco Unified Service Statistics Manager, page 22.

Step 12 Upgrade the SSM Agent on any other systems where it is installed. See Upgrading the SSM Agent, page 21.

Step 13 Run discovery. (See Running Discovery, page 29.)

Upgrading the SSM Agent

The SSM Agent is already upgraded on the system where you upgraded the Service Statistics Manager server. (See Upgrading the Server to Service Statistics Manager 1.3, page 19.) However, you need to upgrade each additional server where the SSM Agent is installed. (The server where Operations Manager runs and each server where Service Monitor runs must have an SSM Agent installed on it.)

Step 1 From a browser on the Operations Manager or Service Monitor system where you will upgrade the SSM Agent, log in to Service Statistics Manager as an admin user. See Logging in to Cisco Unified Service Statistics Manager, page 22.

Step 2 Download the SSM Agent image and start the installation:

a. Select the **Administration** tab.

Note If you want more detailed installation instructions than those presented in this procedure, click **Help** from the Administration tab.

b. Under Downloads, click **Agent.exe**. A File Download window appears.

c. Do one of the following:

- Click **Save** and save Agent.exe to the desktop; then double-click the Agent.exe file to start the installation.
- Click **Open**. Some time might elapse while the Agent.exe file downloads.

An InstallShield window appears with a Welcome message.

Step 3 Follow the online prompts to complete the installation. For more information, see online help.

Upgrading the SSM Administration Console

The SSM Administration Console is already upgraded on the server where you upgraded the Service Statistics Manager server. (See Upgrading the Server to Service Statistics Manager 1.3, page 19.) However, if SSM Administration Console is installed on another server, you must upgrade it.

Step 1 From a browser on the system where you will upgrade SSM Administration Console, log in to Service Statistics Manager as an admin user. See Logging in to Cisco Unified Service Statistics Manager, page 22.

Step 2 Download the SSM Administrator Console image and start the installation:

a. Select the **Administration** tab.

Note If you want more detailed installation instructions than those presented in this procedure, click **Help** from the Administration tab.

b. Under Downloads, click **Admin.exe**. A File Download window appears.

c. Do one of the following:

- Click **Save** and save Admin.exe to the desktop; then double-click Admin.exe to start the installation.
- Click **Open**. Some time might elapse while Admin.exe downloads.

An InstallShield window appears with a Welcome message.

Step 3 Follow the prompts on the windows to complete the installation. (For more information, see online help.)

8 Logging in to Cisco Unified Service Statistics Manager

To ensure that you can log in to Service Statistics Manager 1.3, you must apply a patch to Operations Manager 2.3. For more information, see CSCtf42151 in the Known Problems table in *Release Notes for Cisco Unified Service Statistics Manager 1.3*.

Step 1 In your browser, type one of the following addresses:

http://*servername:*48101

https://*servername:*48443

where

- servername is the IP address or DNS name of the server where Service Statistics Manager resides
- 48101 is the HTTP web server port
- 48443 is the secure HTTP web server port

Note Verify that OpenSSL Win32 is enabled, by logging in using this address: https://https://*servername:*48443.

A login page is displayed.

Step 2 Enter the username and password for the default administrative user:

- User ID: admin
- Password: *as entered during installation*

The Service Statistics Manager home page appears. (If you installed Service Statistics Manager for evaluation, a message window displays number of days left in the evaluation period; click **OK**. For information about your license, click the **About** link at the top of the window.)

Note The default admin user has access to all licensed features of Service Statistics Manager and SSM Administration Console. To change the password for the default admin user, select the **Administration** tab and click the **Edit** link in the User ID and Password pane. (To create additional users, log into SSM Administration Console.)

Starting SSM Administration Console

Step 1 Log into the system where SSM Administration Console is installed.

Step 2 Select whichever of these is available:

- **Start > Programs > Cisco Unified Service Statistics Manager > Cisco Unified Service Statistics Manager Admin.**
- **Start > Programs > Cisco Unified Service Statistics Manager Admin 1.3 > Cisco Unified Service Statistics Manager Admin.**

The SSM Administration Console login page appears.

Note If you installed Service Statistics Manager for evaluation, a message indicating the number of days left in the evaluation period is displayed; click **OK**.

Step 3 Enter the username and password for the default administrative user:

- User ID: admin
- Password: *as entered during installation*

The SSM Administration Console home page appears.

To add a user, right-click the **Users** folder and select **Add**. For more information, click **Help**.

Note If you encounter problems, see Administration Console Troubleshooting Tips, page 23.

Administration Console Troubleshooting Tips

Use information in Table 9 to troubleshoot problems encountered when displaying or using the SSM Administration Console.

Table 9 SSM Administration Console Troubleshooting

Symptom	Cause	Resolution
The message Invalid Login/Password is displayed although a valid login name and password were entered correctly.	Multiple logins to the same account, or other activities at Service Statistics Manager Server	Close Service Statistics Manager server windows and terminals; log out of the account if already logged in elsewhere. If still unsuccessful, verify that Service Statistics Manager servers are running.
Logon screen does not appear.	Service Statistics Manager server processes are not running	Verify that all Service Statistics Manager server processes are running.
	Network connection does not allow access	Check network operation between the Web browser system and the Service Statistics Manager server.
Cannot refresh the SSM Administration Console to show changes (new folders).	Accessing the SSM Administration Console from a remote Windows machine using a remote control application which might not refresh correctly	Minimize the remote control application and then display again. This refreshes the screen.

9 Post-Installation Configuration

Before you configure Service Statistics Manager, configure Operations Manager and Service Monitor to ensure that data is available for Service Statistics Manager reports. If you have already configured Operations Manager and Service Monitor, verify the configuration. Use these procedures:

- Configuring Operations Manager, page 23
- Configuring Service Monitor, page 26

After you verify the Operations Manager and Service Monitor configurations, configure Service Statistics Manager; see Configuring Service Statistics Manager, page 28.

Configuring Operations Manager

To ensure that you can log in to Service Statistics Manager 1.3, you must apply a patch to Operations Manager 2.3. For more information, see CSCtf42151 in the Known Problems table in *Release Notes for Cisco Unified Service Statistics Manager 1.3*.

Note If you have already configured Operations Manager, verify the configuration starting with Step 6 of the following procedure.

For complete instructions, see the online help for Operations Manager.

Step 1 Add these types of devices to Operations Manager and allow inventory collection to complete:

- H323 gateways
- MGCP gateways

- Cisco Unified Communications Manager

Note Include the Unified Communications Managers that will be managed by each Service Monitor.

- Cisco Unified Communications Manager Express
- Cisco Unity
- Cisco Unity Express
- Cisco Unity Connection

Note For devices that Operations Manager supports, see *Supported Devices Table for Cisco Unified Operations Manager* at this URL: http://www.cisco.com/en/US/products/ps6535/products_device_support_tables_list.html.

Step 2 To verify that inventory collection is complete, select **Devices > Device Management**. There should be no devices in the Inventory Collection in Progress state on the Device Management: Summary page.

Step 3 Enable performance polling. Repeat these steps for each type of device that you added:

a. From the Service Level View, select and right-click one of these types of devices:
- Unified Communications Manager
- Unified Communications Manager Express
- H323 gateway
- MGCP gateway
- Cisco Unity
- Cisco Unity Express
- Cisco Unity Connection

b. Select **Polling Parameters**. An Edit Polling Parameters window appears displaying the highest priority device group to which the device belongs.

Note When you edit polling parameters, you edit settings that are associated with a device group, not with an individual device.

c. Select the **Voice Utilization Settings** parameter type and select the **Polling Enabled** check box in the column heading.

d. To save your changes, click **Save**.

e. If you need to enable polling for additional device types, close the Edit Polling Parameters window by clicking **Cancel** and return to the start of Step 3. Otherwise, click **Apply** to apply all saved changes to the system.

Note Applying changes is a CPU-intensive event that might take between one and five minutes to complete.

Operations Manager starts performance polling after the configuration is applied.

Step 4 Configure any node-to-node tests that you would like.

Step 5 Add Service Monitor to Operations Manager.

Note Even when Service Monitor is installed on the same system, you must still add it to Operations Manager.

Step 6 Verify that each Service Monitor that interests you has been added to Operations Manager; to do so, select **UC Management Suite > Service Monitor**.

Step 7 Confirm that performance polling data is available by viewing performance graphs. Repeat these steps for each type of device that you added to Operations Manager:

a. From the Service Level View, select and right-click one of these types of devices:

- Unified Communications Manager
- Unified Communications Manager Express
- H323 gateway
- MGCP gateway
- Cisco Unity
- Cisco Unity Express
- Cisco Unity Connection

Note To find a device in which you are interested, search for the device by name or locate it in the tree view or the map view.

b. Select **Performance**; one of the following occurs:

- A message is displayed stating that performance polling is not enabled for the device. In this case, go to Step 3.
- The Select Metrics dialog box appears; in this case, continue to Step 7c.

c. Select some representative metrics—see table below—and click **View Graph**. The presence of data in the graph confirms that performance polling data is available.

Device Type	Suggested Performance Metrics to Select
Unified Communications Manager	Active Calls (Number) Total CPU Usage (Percentage) T1 CAS Channel Utilization (Percentage)
Unified Communications Manager Express	CPU 1 last 1 minute Usage (Percentage) Processor memory Usage (Percentage) I/O memory Usage (Percentage)
H323 gateways	FXS Port Utilization (Percentage) E1 CAS Channel Utilization (Percentage) Processor memory Usage (Percentage)
MGCP gateways	FXS Port Utilization (Percentage) T1 PRI Channel Utilization (Percentage) E1 PRI Channel Utilization (Percentage)
Cisco Unity	Total CPU Usage (Percentage) Memory Usage (Percentage)
Cisco Unity Express	CPU 1 last 1 minute Usage (Percentage)
Cisco Unity Connection	Total CPU Usage (Percentage) Memory Usage (Percentage)

Step 8 To confirm that node-to-node test data is available, view performance graphs from Operations Manager:

a. Select **Diagnostics > Node-to-Node Tests**.

b. Select a test and click **Trend**. The presence of data in the graph confirms that data is available for the selected node-to-node test.

Configuring Service Monitor

Service Statistics Manager uses the data that Service Monitor collects from Unified Communications Managers and from sensors (1040s and NAMs). See these topics:

- Configuring Service Monitor to Collect Data from Unified Communications Manager, page 26
- Configuring Service Monitor to Categorize Call Data from Unified Communications Manager, page 27
- Configuring Service Monitor to Collect Sensor-Based Data, page 27

Configuring Service Monitor to Collect Data from Unified Communications Manager

For supported versions of Unified Communications Manager and for required Cisco Unified IP phone models—those that support the Cisco Voice Transmission Quality (CVTQ) algorithm—see *Cisco Unified Service Monitor 2.3 Compatibility Matrix* at this URL: http://cisco.com/en/US/docs/net_mgmt/cisco_unified_service_monitor/2.3/sdt/CiscoUnifiedServiceMonitorCompatibilityMatrix23.html.

For complete instructions, see the online help for Service Monitor.

Note If you have already configured Service Monitor to collect data from Unified Communications Manager, verify the configuration starting with Step 5 of the following procedure.

Step 1 Confirm that the Unified Communications Managers exist in Operations Manager device inventory.

Step 2 Ensure that up-to-date patches have been applied to the Unified Communications Managers:

- Check http://www.cisco.com for the most recent patches.
- See *Release Notes for Cisco Unified Service Monitor 2.3* for a list of recommended patches and workarounds for Unified Communications Manager.

Step 3 Configure Unified Communications Managers for use with Service Monitor.

Note Required configuration steps vary depending on the Unified Communications Manager software version. For more information, see Unified Communications Manager Configuration in *User Guide for Cisco Unified Service Monitor* 2.3.

Step 4 Add credentials for each Unified Communications Manager publisher server to Service Monitor.

Step 5 Verify that the configuration is successful in Service Monitor:

a. From the Unified Communications Manager Credentials page, confirm that Status for each Unified Communications Manager is Success. If not, take steps to establish contact, including correcting the credentials and verifying that Unified Communications Manager is correctly configured for use with Service Monitor.

b. Run a CVTQ report, including all Unified Communications Managers in the report filter. If the report contains expected data, the configuration is successful.

Step 6 Configure Service Monitor to categorize calls for the cluster. See Configuring Service Monitor to Categorize Call Data from Unified Communications Manager, page 27.

Note To add NAMs and Cisco 1040s to Service Monitor, see Configuring Service Monitor to Collect Data from NAMs, page 27 and Configuring Service Monitor to Collect Data from Cisco 1040s, page 28.

Configuring Service Monitor to Categorize Call Data from Unified Communications Manager

Service Statistics Manager reports that are based on the Call Volume monitor display calls by category. Service Monitor provides the categorized call data for such reports. By default, Service Monitor categorizes calls into default, system-defined call categories, such as voice gateway or trunk incoming (VG/Trunk-Incoming), intercluster trunk (ICT), Tandem, and so on. To enable Service Monitor to additionally categorize calls in to user-definable call categories—such as Local, Long Distance, International and so on—you must define call classification. Call classification configuration includes the following:

- Gateway codes—Assign area codes to any of the gateways that are known to Service Monitor. When you define dial patterns, you can use gateway codes to differentiate between Local and Long Distance calls for example.
- Dial plans—A dial plan includes a name, any toll free numbers, and dial patterns that you assign to user-definable call categories. At a minimum, configure one dial plan. Alternatively, configure multiple dial plans, designing each for a specific cluster.
- Assignment of dial plans to clusters.

Configure call classification from the Configuration tab in Service Monitor as follows.

Step 1 Configure gateway codes.

Step 2 Configure dial plans. In a dial plan:

- Optionally, configure a list of toll free numbers.
- Configure dial patterns that enable Service Monitor to categorize calls into user-definable call category types:
  - Conference
  - International
  - Emergency
  - Local
  - Long Distance
  - Service
  - Toll Free
  - Voicemail

Step 3 Assign an appropriately configured dial plan to each cluster in Service Monitor.

Step 4 Verify the call classification configuration by running CDR Call Reports from the Reports tab in Service Monitor. CDR Call Reports show calls by category.

Configuring Service Monitor to Collect Sensor-Based Data

Service Monitor can collect analyze data from these sensors: Cisco 1040 Sensors (Cisco 1040s) and from Cisco Network Analysis Modules (NAMs).

Configuring Service Monitor to Collect Data from NAMs

For Service Monitor to collect data from a Cisco Network Analysis Module (NAM), you must:

Step 1 Configure an http or https server on the NAM and enable RTP stream monitoring on it.

Step 2 Add credentials for the NAM to Service Monitor.

For more information, see *User Guide for Cisco Unified Service Monitor 2.3*.

For supported versions of NAM hardware and software, see *Cisco Unified Service Monitor 2.3 Compatibility Matrix*.

Configuring Service Monitor to Collect Data from Cisco 1040s

For Cisco 1040 Sensor installation procedures and regulatory compliance and safety information, see *Quick Start Guide for Cisco 1040 Sensor*. (Be sure to configure DHCP and DNS for Cisco 1040s as directed in the quick start guide.)

To configure Service Monitor to obtain data from Cisco 1040s, you must:

Step 1 Add at least one TFTP server to Service Monitor.

Step 2 Edit the Cisco 1040 sensor default configuration file.

Step 3 Copy the binary image to the root location on the TFTP server.

Step 4 Verify that the configuration is successful in Service Monitor:

a. From the Cisco 1040 Sensor Details page, confirm that the Registered with column for each sensor contains an IP address. If not, take steps to establish contact. (For more information, see online help.)

b. Run a sensor report, including all Cisco 1040s in the report filter. If the report contains expected data, the configuration is successful.

For supported binary images, see *Cisco Unified Service Monitor 2.3 Compatibility Matrix*.

Configuring Service Statistics Manager

Before you configure Service Statistics Manager:

- SSM Agent must be installed on the Operations Manager server and on the Service Monitor servers. (See Installing SSM Agent, page 17.)
- Operations Manager and Service Monitor must be configured as explained in Configuring Operations Manager, page 23 and Configuring Service Monitor, page 26.

For complete instructions, see the online help for Service Statistics Manager.

Step 1 Run discovery from Service Statistics Manager. (See Running Discovery, page 29.)

Step 2 Confirm the status of the SSM Agents that you installed on Operations Manager and each Service Monitor that has been added to Operations Manager:

a. In Service Statistics Manager, select the **Administration** tab and scroll to Advanced.

b. Click the Operations Manager/Service Monitor Details **Show** link. The Operations Manager/Service Monitor Details window appears. The status for each SSM Agent—one for Operations Manager and one for each Service Monitor—should be green. Green indicates that the SSM Agent is connected to and communicating with Service Statistics Manager.

c. If an SSM Agent Status is red, a user with Administrator role should access the SSM Administration Console and perform troubleshooting; see instructions in *User Guide for Cisco Unified Service Statistics Manager 1.3*.

After each SSM Agent status is green, Service Statistics Manager is configured correctly.

Note Service Statistics Manager reports are generated once daily at 4:30 AM and will be available the day after you complete steps 1 and 2. At that time, view daily Service Statistics Manager reports to verify that Operations Manager and Service Monitor are configured correctly to provide information to Service Statistics Manager and perform additional configuration if necessary.

Step 3 The day after you configure Service Statistics Manager, view some daily reports—weekly and monthly reports will not be available yet. View reports with data from:

- Service Monitor:
  - Call Traffic and Duration Across Clusters—Daily.
  - Call Volume Report on H.323 Gateways.

- Operations Manager:
  - Detailed Performance—Daily. This report contains data for these device types: Cisco Unified Communications Manager, Cisco Unified Communications Manager Express, Cisco Unity, Cisco Unity Express, Cisco Unity Connection.
  - Gateway Utilization—Daily. This report contains data for H323 gateways and MGCP gateways.

Running Discovery

Only one NIC is supported on your system. Before you start, ensure that only one NIC is enabled. If more than one NIC card is enabled, discovery can fail.

Step 1 If Cisco Security Agent is running on your system, disable it. If the Operations Manager or the Service Monitors that are being discovered are on another server, disable Cisco Security Agent on those systems too.

Step 2 Start discovery and allow it to complete. This might take some time.

Note If discovery fails and more than one NIC is enabled, disable all but one NIC, go into the SSM Administration Console and delete the SSM Agent for Operations Manager, and start discovery again. (Do not delete SSMServer. It is the local SSM Agent on the Service Statistics Manager server and must always appear in the SSM Agents folder.)

Step 3 If you disabled Cisco Security Agent (in Step 1), re-enable it on the Service Statistics Manager server and any other server on which you disabled it.

Note During initial discovery only, Service Statistics Manager collects ten records for the previous hour from Service Monitor.

Reconfiguring Selected Ports and Properties for Service Statistics Manager

After installation or upgrade, you can optionally reconfigure some ports and properties.

Step 1 Log in to the Service Statistics Manager server as a Windows administrator.

Step 2 Edit the *Installation Directory*\pw\pronto\conf\pronet.conf file and change the value any of the following variables:

- pronet.rmi.port=48099
- pronet.jndi.port=48100
- java.naming.provider.url=jnp://127.0.0.1:48100

Step 3 To change the database port, edit the *Installation Directory*\pw\custom\conf\pronet.conf file and replace 48102 in this line:

pronet.api.database.portnum=48102

Step 4 To change the value of the Http Web Server port (default 48101), edit the *Installation Directory*\pw\ApacheGroup\Apache\conf\httpd.conf file; replace 48101 in these lines:

```
Port 48101
<IfDefine SSL>
Listen 48101
Listen 444
</IfDefine>
```

Step 5 To change the value of the secure Http Web Server port (default 48443), edit the *Installation Directory*\pw\ApacheGroup\Apache\conf\httpd-ssl.conf file; replace all 3 occurrences of 48443.

Step 6 Restart the server by selecting **Start > Programs > Cisco Unified Service Statistics Manager > Start Server**.

Note It's not necessary to first select Stop Server because Start Server restarts the server.

Post-Installation Configuration Summary

Table 10 summarizes how to verify that Operations Manager, Service Monitor, Unified Communications Manager, and Service Statistics Manager are configured properly. To facilitate any corrections, Table 10 provides references back to steps in these sections:

- Configuring Operations Manager, page 23
- Configuring Service Monitor, page 26
- Configuring Service Statistics Manager, page 28

Table 10 Configuration Checklist

Product	Is configured correctly if...	Configuration Procedures
Operations Manager	• Devices are in inventory and inventory collection is complete. • Performance graphs are available for: – H323 and MGCP gateways and supported Unified Communications Applications. – Node-to-node tests. • Service Monitor 2.3 has been added to Operations Manager and you can see data on Service Quality Alert Display.	Configuring Operations Manager, page 23: • Step 1 on page 23 • Step 2 on page 24 • Step 3 on page 24 • Step 4 on page 24 • Step 5 on page 24
Unified Communications Manager	• Latest patches installed. • Applicable version-specific configuration complete as detailed in *User Guide for Cisco Unified Service Monitor 2.3*.	Configuring Service Monitor, page 26: • Step 2 on page 26 • Step 3 on page 26

Table 10 Configuration Checklist (continued)

Product	Is configured correctly if...	Configuration Procedures
Service Monitor	• Credentials status for Unified Communications Manager must be Success. • Data appears in CVTQ reports. • Cisco 1040s are registered with Service Monitor. • Data appears from Cisco 1040s and NAMs in Sensor Reports. • Calls are categorized correctly in CDR Call Reports	• Configuring Service Monitor to Collect Data from Unified Communications Manager, page 26 • Configuring Service Monitor to Categorize Call Data from Unified Communications Manager, page 27 • Configuring Service Monitor to Collect Data from Cisco 1040s, page 28 • Configuring Service Monitor to Collect Data from NAMs, page 27
Service Statistics Manager	• SSL is configured for communicating with Operations Manager. (If Operations Manager uses an SSL port other than 443, follow the instructions for changing the value of pronet.ssm.om.port.https in the pronet.conf file; instructions are provided in the procedures for installing, upgrading, and reinstalling the Service Statistics Manager server.) • Discovery is complete. • SSM Agent status is green for Operations Manager and each Service Monitor. • Daily reports contain data.	Configuring Service Statistics Manager, page 28: • Step 1 on page 28 • Step 2 on page 28 • Step 3 on page 28

10 Uninstalling and Reinstalling Service Statistics Manager

This section contains:

Uninstalling Service Statistics Manager

This procedure removes Service Statistics Manager server, SSM Administration Console, and SSM Agent from the local server.

Caution You must use the recommended uninstallation procedures to remove Service Statistics Manager from your system. If you try to remove the files and programs manually, you can seriously damage your system.

Step 1 As the local administrator, log in to the system on which Service Statistics Manager is installed.

Step 2 To start the uninstallation process, do one of the following:

- Select **Start > Programs > Cisco Unified Service Statistics Manager > Uninstall Cisco Unified Service Statistics Manager.**
- Select **Start > Settings > Control Panel > Add/Remove Programs > Cisco Unified Service Statistics Manager.**

The Cisco Unified Service Statistics Manager 1.3 Setup window appears.

Step 3 Select the **Remove** radio button and click **Next**. The uninstallation begins; the Setup Status page displays the progress. When complete, the InstallShield Wizard Complete page appears.

Step 4 Click **Finish**.

Step 5 Restart your Windows system. Doing so prevents ports from being blocked and ensures that the Windows registry remains clean.

Note To uninstall remote instances of SSM Agent and SSM Administration Console, use Add/Remove Programs from the Windows Control Panel on the remote systems and uninstall Service Statistics Manager Agent or Service Statistics Manager Admin.

Reinstalling Service Statistics Manager

The existing database is preserved when you reinstall Service Statistics Manager. As a precaution, back up the system prior to copying and installing new files on your system. (Recommended procedures for backing up your system are included in online help.)

Use this procedure if you need to install Service Statistics Manager 1.3 on a system where Service Statistics Manager 1.3 is already installed.

Note During the reinstallation, some messages might be displayed that refer to an upgrade even though you are actually installing the same software version.

Step 1 As the local administrator, log in to the system on which Service Statistics Manager is installed.

Step 2 To reinstall on a system where Operations Manager is installed, stop the daemon manager.

Step 3 To start the reinstallation process, do one of the following:

- Select **Start > Programs > Cisco Unified Service Statistics Manager > Uninstall Cisco Unified Service Statistics Manager.**
- Select **Start > Settings > Control Panel > Add/Remove Programs > Cisco Unified Service Statistics Manager.**

The Welcome window appears.

Step 4 Select **Reinstall/Upgrade** and click **Next**.

Step 5 Follow the online prompts until the Setup Complete window appears.

Step 6 If you stopped the daemon manager (see Step 2), start it again. Allow 30 minutes to elapse between the time that you restart the daemon manager and you log in to Service Statistics Manager (as directed in Step 8e).

Step 7 Click **Finish**.

Step 8 Configure Service Statistics Manager to communicate with Operations Manager as follows:

a. Determine whether Operations Manager uses an SSL port other than 443 (the default SSL port).

b. If Operations Manager uses an SSL port other than 443, perform these steps:

- Navigate to this directory: *Installation Directory*\pw\pronto\conf
- Edit the pronet.conf file and, find this line: pronet.ssm.om.port.https=443
- Replace 443 with the SSL port that Operations Manager uses

c. Restart the Service Statistics Manager server. From the command prompt, type:

pw sys start

d. Close any existing browser sessions.

e. Start your browser again and log in to Service Statistics Manager.

Note You must repeat Step 8 any time that you reinstall or upgrade Operations Manager or Service Statistics Manager.

11 Where to Go Next

After you have installed Service Statistics Manager, you are ready to configure it and start reporting on IP telephony service quality, call volume, and resource utilization. For more information, see *User Guide for Cisco Unified Service Statistics Manager 1.3*.

You can access this document:

- In PDF format, in the Documentation directory on the respective product CD-ROM.
- From the online help integrated into the product.

12 Related Documentation

Note The originally published printed and electronic documentation is included with your product. Any changes after original publication are reflected on Cisco.com, where you will find the most up-to-date documentation.

For information about installing, troubleshooting, and using the applications and tools in the Cisco Unified Communications Management Suite, see the sources of information described in Table 11.

Table 11 Related Documentation

To learn more about...	See this document	In the product package?	On the product CD?[1]	On Cisco.com?	In the online help?
The known product bugs (DDTSs)	*Release Notes for Cisco Unified Service Statistics Manager 1.3*	No	Yes	Yes	No
	Release Notes for Cisco Unified Operations Manager 2.3	No	No	Yes	No
	Release Notes for Cisco Unified Service Monitor 2.3	No	No	Yes	No
	Release Notes for Cisco Unified Provisioning Manager 2.1	No	No	Yes	No
Performing a typical installation	*Installation Guide for Cisco Unified Operations Manager (includes Service Monitor) 2.3*	No	No	Yes	No
	Installation Guide for Cisco Unified Service Monitor 2.3	No	No	Yes	No
	Quick Start Guide for Cisco 1040 Sensor	No	No	Yes	No
	Installation Guide for Cisco Unified Provisioning Manager 2.1	No	No	Yes	No
Features, tasks, and troubleshooting	*User Guide for Cisco Unified Service Statistics Manager* 1.3	No	Yes	Yes	Yes
	User Guide for Cisco Unified Service Monitor 2.3	No	No	Yes	No
	User Guide for Cisco Unified Operations Manager 2.3	No	No	Yes	No
	User Guide for Cisco Unified Provisioning Manager	No	No	Yes	No

1. Provided in PDF format, in the Documentation folder on the product CD.

13 Obtaining Documentation and Submitting a Service Request

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

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

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

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

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

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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

OL-20793-01