CA Unified Communications Monitor

Installation Guide

Version 3.6

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

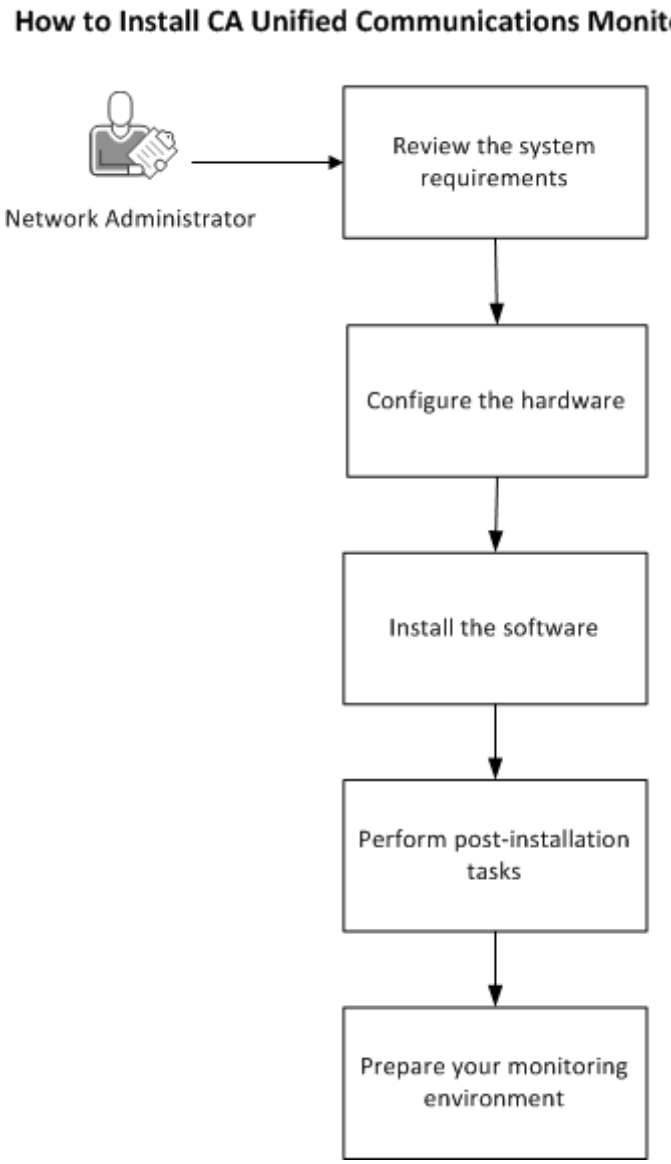
If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Introduction

The following diagram illustrates the process of installing and configuring the hardware and software for CA Unified Communications Monitor (UC Monitor):



More information:

System Requirements (see page 9)
Configuring the Hardware (see page 15)
Post-Installation Tasks (see page 23)
Installing the Software (see page 19)
Preparing Your Monitoring Environment (see page 27)

Chapter 2: System Requirements

This section contains the following topics:

Supported Operating System

All servers that host UC Monitor components have the following operating system requirements.

Management console in a distributed system, or the server in a standalone system.

Microsoft Windows Server 2008 R2, Standard or Enterprise Edition, with the following items installed and enabled:

- The Application Server role with the following role services:
  - Web Server (IIS) Support, with IIS 6 Management Compatibility
  - COM+ Network Access
- .NET Framework 3.5.1 Features. The UC Monitor installation process searches for .NET Framework 3.5.1 features and installs them when they are not present.
- SNMP
- The most recent service pack and important updates

Standard collector or small-site collector in a distributed system.

Microsoft Windows Server 2008 R2, Standard or Enterprise Edition, with the following items installed and enabled:

- .NET Framework 3.5.1 Features. The UC Monitor installation process searches for .NET Framework 3.5.1 features and installs them when they are not present.
- SNMP
- The most recent service pack and important updates

Supported Web Browsers

Access to the management console is supported for the following browsers:

- Microsoft Internet Explorer versions 9 and 10
- Mozilla Firefox (current version)
- Google Chrome (current version)

Other browsers or versions may work but have not been tested with UC Monitor.

Hardware Requirements for a Distributed System

In a *distributed* system, the collectors and the management console are installed on separate servers.

Management Console

The management console server contains the MySQL database and supports approximately ten standard collectors or 30 small-site collectors. CA has tested UC Monitor on servers with the following specifications. CA supports the management console on servers from any vendor, when the servers conform to these specifications, at minimum:

- Two Intel E5520 Xeon quad-core 2.66 GHz, 1333 MHz FSB processors
- 24 GB of RAM
- Six 146-GB SAS hard drives in RAID 5 configuration
- 300 GB of space on the installation drive (to accommodate database growth)
- Intel Copper GB or Intel Fiber GB network interface card
- PCI Express x16 slot expansion card
- Two 10/100/1000 Mbps Ethernet RJ-45 ports
- Intel 82576 Gigabit Ethernet Controller

Standard Collector

CA has tested UC Monitor on servers with the following specifications. CA supports the collector on servers from any vendor, when the servers conform to these specifications, at minimum:

- Intel E5520 Xeon quad-core 2.66 GHz, 1333 MHz FSB processor
- 3 GB of RAM
- Three 146-GB SAS hard drives in RAID 5 configuration
- 300 GB of space on the installation drive (to accommodate database growth)

- Intel Copper GB or Intel Fiber GB network interface card
- PCI Express x16 slot expansion card
- Two 10/100/1000 Mbps Ethernet RJ-45 ports
- Intel 82576 Gigabit Ethernet Controller

Small-site Collector

A distributed *small-site* system is available for deployments with multiple sites of 1,000 phones or fewer. CA supports the small-site collector on servers from any vendor, when the servers conform to the following specifications, at minimum:

- Intel Celeron E1500 2.2 GHz, 800 MHz FSB processor
- 2 GB of RAM
- SATA II 3.5-inch hard drive
- Intel Copper GB or Intel Fiber GB network interface card
- 10/100/1000 Mbps Ethernet RJ-45 port
- Two Intel single-port 82576 PCI-E Gigabit Ethernet Controllers

Hardware Requirements for a Standalone System

A *standalone* system consists of one server on which the management console and collector are installed. CA supports UC Monitor components on servers from any vendor, when the servers conform to the following specifications, at minimum:

- Two Intel E5520 Xeon quad-core 2.66 GHz, 1333 MHz FSB processors
- 24 GB of RAM
- Six 146-GB SAS hard drives in RAID 5 configuration
- 300 GB of space on the installation drive (to accommodate database growth)
- Intel Copper GB or Intel Fiber GB network interface card
- PCI Express x16 slot expansion card
- Two 10/100/1000 Mbps Ethernet RJ-45 ports
- Intel 82576 Gigabit Ethernet Controller

Virtual Machine Requirements

UC Monitor is supported in virtual environments.

- You can install UC Monitor components on virtual machines that meet or exceed the hardware requirements.
- To achieve equal performance in an environment that stresses a physical server, more memory is required on a virtual machine than on a physical server. Physical servers outperform virtual machines in the area of disk I/O. UC Monitor tasks the disk I/O heavily. You can expect less-than-equal performance on a virtual machine.
- In a Cisco environment, send SPAN traffic to the monitor NIC. For more information, see the following topics:
  - Configure Network Interface Cards (see page 17)
  - Preparing a Cisco Environment (see page 28)
- To install the UC Monitor software on a virtual machine, follow the instructions in Installing the Software (see page 19).

More information:

Hardware Requirements for a Standalone System (see page 11)
Hardware Requirements for a Distributed System (see page 10)

Port and Protocol Requirements

UC Monitor uses several ports and protocols to enable communications among the management console, collectors, and monitored systems. Use the following information to ensure that communications can pass active firewalls in your network.

TCP port 21

Open this port to allow the CA UCM Data Transformer service to receive data via FTP for transformation into a format that UC Monitor can process.

Note: UC Monitor configures port 21 by default for FTP functions. If you use a different port, ensure that your firewall is configured accordingly.

TCP port 1000

Open this port for communication from the management console to the collectors. The management console sends instructions, data-collection parameters, and configuration information to the collectors. The CA UCM Collector Communication service uses this port.

TCP port 1001

Open this port for communication from the collectors to the management console. The CA UCM Console Communicator service uses this port.

TCP port 9000

Open this port to receive CDR data from Avaya Communication Manager.

UDP port 161

Open this port to enable queries to Avaya Communication Manager and Cisco gateways.

UDP port 162

Open this port to let the management console send SNMP traps to a trap receiver.

UDP port 5005

Open this port to receive RTCP data from Avaya endpoints.

~~UDP~~ port 8381

Open this port to support Single Sign-on, enabling direct login to UC Monitor and drill-down from CA Performance Center to UC Monitor.

~~UCP~~ port 8681

Open this port to let CA Performance Center access UC Monitor data for CA Performance Center report views. The CA UCM Web Container service uses this port.

UDP port 9995

Open this port to let medianet-enabled devices send data from Cisco IOS Flexible NetFlow to the collector.

Internet Control Message Protocol

Enable ICMP to let the collector send traceroutes to an endpoint.

The default port settings are stored in the UC Monitor database, in configuration files, and in the Windows Registry. You can change the settings when necessary. For assistance, contact CA Technical Support.

Chapter 3: Configuring the Hardware

When configuring the hardware, you need the following types of cables.

Power cable

Connects the UC Monitor server to a power supply, preferably a UPS.

Management NIC cable

One of the following types:

- Copper NIC cable
- Gb fiber NIC cable

When plugged into a switch, the management NIC provides network access to the UC Monitor server and it enables remote viewing of the management console.

Monitor NIC cable

Collects network traffic from a SPAN port on the switch.

This section contains the following topics:

Configure the Server for the Management Console

The management console and the collectors are installed on separate servers in a distributed system. The following procedure describes how to configure the server for the management console.

Follow these steps:

1. Connect one end of the power cable to the power outlet on the server.
2. Connect the other end of the power cable to a power supply.
3. Connect one end of the management cable to a NIC on the server.
4. Connect the other end of the management cable to an appropriate switch.
5. Turn on the server.
6. Configure the management NIC. For more information, see Configure Network Interface Cards (see page 17).
7. Configure the server for the collector. For more information, see Configure the Server for the Collector (see page 16).

Configure the Server for the Collector

The management console and the collectors are installed on separate servers in a distributed system. You can have a maximum of ten standard collectors per management console, or 30 small-site collectors per management console. The following procedure describes how to configure the server for the collector.

Note: In a Cisco Unified Communications Manager environment, place the UC Monitor collector server as physically close to the Cisco call server as possible.

Follow these steps:

1. Connect one end of the power cable to the power outlet on the server.
2. Connect one end of the monitor and management cables to NICs on the server.
3. Connect the monitor cable to the SPAN port.
4. Connect the management cable to the management console server.
5. Turn on the server.
6. Configure the monitor and management NICs. For more information, see Configure Network Interface Cards (see page 17).

Configure the Server for a Standalone System

In a standalone system, the management console and the collector are installed on the same server.

Follow these steps:

1. Connect one end of the power cable to the power outlet on the server.
2. Connect the other end of the power cable to a power supply.
3. Connect one end of the monitor and management cables to NICs on the server.
4. Connect the other end of the monitor cable to the switch where call servers are connected.
5. Connect the other end of the management cable to another switch, to enable network access to the management console.
6. Configure the monitor and management NICs. For more information, see Configure Network Interface Cards (see page 17).

Configure Network Interface Cards

After you connect the hardware, configure the network interface cards (NICs) on the collector and management console servers. In a standalone system, all configuration takes place on one server.

- On each collector server, set up network connections for the management and monitor NICs.
- On the management console server, set the priority of the management NIC.
- Assign a static IP address, subnet mask, and default gateway to the management NIC.

Note: The other NICs on the collector, including the monitor NIC, do not transmit data to the network. Their IP addresses do not need to be valid for the network to which they are connected, nor do they require a default gateway assignment.

When you purchase hardware from CA Technologies, components are delivered with the NIC settings already configured. Use the following procedure to verify the settings or update them as necessary.

When you purchase hardware from a different vendor, perform the following procedure.

Follow these steps:

1. Navigate to the Network Connections window from the Control Panel on the collector and management console computers.
2. Review the names of the LAN or High-Speed Internet Connections. If necessary, change the default names to correspond to the interfaces, as shown in the following table:

   Copper Ethernet adapter

   Default name: Local Area Connection 2

   New name: Management

   Copper Ethernet adapter

   Default name: Local Area Connection 3

   New name: Monitor

   Gigabit fiber port

   Default name: Local Area Connection

   New name: Fiber Monitor

   Tip: To identify devices, disconnect the cable from the back of the device and note which interface status changes to "disconnected" in the Network Connections dialog.

3. Disable unused monitor NICs:
   a. Right-click the NIC.
   b. Select Disable.
4. Click Advanced, Advanced Settings.
5. Click the up arrow to move the management NIC to the first position in the Connections pane. This action sets the priority and enables UC Monitor to operate correctly.
6. Clear the following “Internet Protocol (TCP/IP)” check boxes for the monitor NIC:
   - File and Printer Sharing for Microsoft Networks
   - Client for Microsoft Networks
7. Click OK.
8. Navigate to the Control Panel and select Network Connections, Local Area Connection.
9. Click Properties on the General tab.
10. Select Internet Protocol (TCP/IP) and click Properties.
11. Select “Use the following IP address” and enter an IP address, subnet mask, and default gateway.
12. Select “Use the following DNS Server addresses” and supply the IP address for the DNS server.

    Note: Do not use a DHCP address.
13. Repeat steps 11 and 12 for the monitor NICs, using the following suggested values:

    Monitor NIC

    IP address: 1.1.0.0

    Subnet mask: 255.0.0.0

    Fiber Monitor NIC

    IP address: 1.1.0.1

    Subnet mask: 255.0.0.0

Chapter 4: Installing the Software

When you purchase hardware from CA Technologies, all components are delivered with the UC Monitor software installed. Do not install the software.

When you purchase hardware from a different vendor, install the UC Monitor software on the management console server and all collector servers.

Important: Do not install UC Monitor on a computer on which CA NetQoS Performance Center is installed.

This section contains the following topics:

Installation Prerequisites

Before you install the UC Monitor software, perform the following tasks:

- Install CA Performance Center in your environment. UC Monitor is a data source for CA Performance Center. CA NetQoS Performance Center 6.1 (and its service packs) is also supported.
- Disable the following types of third-party software on all servers that host UC Monitor components:
  - Anti-virus
  - Anti-spyware
  - Server monitoring and maintenance tools such as SMS, SUS, or MoM
- Restart all servers to ensure that available operating system patches are applied.
- Obtain the UC Monitor setup file, UCMSetup3.6.xxx.exe, from CA Technical Support.
- Extract or copy the UCMSetup3.6.xxx.exe file to the servers on which you want to install the software.

Install the Management Console

Distributed systems have separate servers for the UC Monitor management console and the collectors. Use this procedure to install the management console for a distributed system.

Follow these steps:

1. Double-click the setup program.

   The CA Unified Communications Monitor Installer window opens.

2. Click Next.

   The License Agreement appears in the window.

3. Read and accept the license agreement, and then click Next.

   The installation options appear in the window.

4. Select 'Unified Communications Monitor Management Console,' and then click Next.

   The installation folder options appear in the window.

5. (*Optional*) Click Choose to select a different installation location. The default is C:\CA.

6. Click Next.

   An installation summary appears in the window.

7. Click Install.

   The installation process begins. Messages indicate the progress of the installation. When the installation is complete, a "successful installation" message appears in the window.

8. Select 'Yes, restart my system,' and then click Done.

9. Run the setup program on the collector servers (see page 21).

   You can now perform post-installation tasks (see page 23) and prepare your monitoring environment (see page 27).

Install the Collector

Distributed systems have separate servers for the UC Monitor console and the collectors. Use this procedure to install the collectors in a Cisco or Avaya environment.

Note: In a Microsoft Lync environment, you configure a Microsoft server as a Lync collector. For more information, see the UC Monitor online help. Or review the use case titled *Managing Collectors in Microsoft Lync Environments* from the CA Unified Communications Monitor bookshelf.

Follow these steps:

1. Double-click the setup program.

   The CA Unified Communications Monitor Installer window opens.

2. Click Next.

   The License Agreement appears in the window.

3. Read and accept the license agreement, and then click Next.

   The installation options appear in the window.

4. Select 'Unified Communications Monitor Collector,' and then click Next.

   The installation folder options appear in the window.

5. (*Optional*) Click Choose to select a different installation location. The default is C:\CA.

6. Click Next.

   An installation summary appears in the window.

7. Click Install.

   The installation process begins. Messages indicate the progress of the installation. When the installation is complete, a "successful installation" message appears in the window.

8. Select 'Yes, restart my system,' and then click Done.

   You can now perform post-installation tasks (see page 23) and prepare your monitoring environment (see page 27).

Install All Components on One Server

A *standalone* system is one server that hosts the UC Monitor management console and the collector. Use this procedure to install the management console and the collector on one server.

Follow these steps:

1. Double-click the setup program.

   The CA Unified Communications Monitor Installer window opens.

2. Click Next.

   The License Agreement appears in the window.

3. Read and accept the license agreement, and then click Next.

   The installation options appear in the window.

4. Select 'Unified Communications Monitor Standalone,' and then click Next.

   The installation folder options appear in the window.

5. (*Optional*) Click Choose to select a different installation location. The default is C:\CA.

6. Click Next.

   An installation summary appears in the window.

7. Click Install.

   The installation process begins. Messages indicate the progress of the installation. When the installation is complete, a "successful installation" message appears in the window.

8. Select 'Yes, restart my system,' and then click Done.

   You can now perform post-installation tasks (see page 23) and prepare your monitoring environment (see page 27).

Chapter 5: Post-Installation Tasks

This section contains the following topics:

Install Updates

Install all important updates that are available for the Microsoft Windows operating system, including the most recent service pack.

Install any UC Monitor updates available from the CA Support Online website.

Change the Host Name

For the collectors in a distributed system, change the host name to help you identify the collector servers in UC Monitor reports. Use a naming convention similar to the following example:

```
<CollectorName>-<ManagementConsoleName>-<Location>
```

For example:

```
ComMgr1-MainOffice-NYC
```

Update the List of Trusted Internet Sites

Add the console server to the list of trusted Internet sites. The process varies by browser. The following instructions are for Microsoft Internet Explorer.

Follow these steps:

1. Launch Internet Explorer on the console server.
2. Click Tools, Options.
3. Click the Trusted Sites icon on the Security tab.

4. Click Sites.
5. Enter **http://localhost** in the 'Add this Web site to the zone' field.
6. Click Add.

Synchronize the System Time

Synchronize the system time among all servers where you installed UC Monitor components. Perform the following steps on each server.

Follow these steps:

1. Log in as a user who is a member of the Administrators group.
2. Right-click the date or time on the right edge of the taskbar and select 'Adjust date/time.'

   The Date and Time dialog opens.
3. Click the Internet Time tab.
4. Click 'Change settings.'

   The Internet Time Settings dialog opens.
5. Select the 'Synchronize with an Internet time server' check box.
6. Select the server with which you want to synchronize. The default selection is time.windows.com.
7. Click 'Update Now.'

   The system time is synchronized with the selected server.
8. Click OK in the Internet Time Settings dialog.
9. Click OK in the Date and Time dialog.

Note: If you have collectors in different time zones, set each device to its local time zone. Times are converted to Greenwich Mean Time (GMT).

Perform Configuration Tasks from the Management Console

Perform the following configuration tasks from the UC Monitor management console:

- Organize phones, endpoints, gateways, and other network components into Locations.
- Add collection devices.
- Customize collector thresholds.
- Customize performance thresholds.

- Enable incidents to trigger response notifications.
- Register UC Monitor as a data source for CA Performance Center.
- Configure SNMP profiles for Cisco voice gateways and Avaya Communication Manager servers.
- Configure users and their roles.

Note: For instructions, see the UC Monitor online help. Related documentation, including use cases, is also available from the CA Unified Communications Monitor bookshelf.

Chapter 6: Preparing Your Monitoring Environment

This section contains the following topics:

Preparing an Avaya Communication Manager Environment

UC Monitor supports unified communications deployments that use Avaya Communication Manager for call processing. The collector monitors voice calls made with the following Avaya components:

- Desk phones and softphones
- Communication Manager, including Aura Communication Manager
- Avaya voice gateways

Avaya endpoints, including voice gateways, send frequent call-quality reports directly to the collector while calls are in progress. The quality data is sent as RTCP packets. Using SNMP, the collector periodically polls the Communication Manager for device information. The Communication Manager can be configured to send CDR data to the collector after each call is completed.

Many Avaya gateways have an AVAYA_RTP_MIB that can be polled with SNMP. However, RTCP is supported for *all* Avaya gateways. Therefore, UC Monitor relies primarily on RTCP for collecting metrics in an Avaya environment. No switch port or SPAN is required.

An Avaya network administrator performs several tasks to prepare an Avaya environment for monitoring with UC Monitor:

- Enabling access to SNMP agents.
- Enabling Avaya endpoints to send RTCP data to the UC Monitor collector, which takes the role of the RTCP Monitor in an Avaya system.

- Configuring the UC Monitor collector as a CDR recipient.
- Using the Trunk Group Measurement Selection page (in the Communication Manager web interface) to identify the trunk groups that you want to monitor.

Note: Detailed instructions for these tasks are provided in the use case titled *Preparing an Avaya Communication Manager Environment*.

More information:

Port and Protocol Requirements (see page 12)

Preparing a Cisco Unified Communications Manager Environment

UC Monitor supports unified communications deployments that use Cisco Unified Communications Manager for call processing. Cisco endpoints report quality data to their call server at the completion of every call. The UC Monitor collector inspects these flows for performance metrics. The collector transmits to the management console only the data necessary to calculate and report call setup and call quality.

A Cisco network administrator performs several tasks to prepare a Cisco environment for monitoring with UC Monitor:

- Enabling the Call Stats setting in a voice-quality-enabled SIP profile.
- Enabling the collection of voice quality metrics.
- Enabling web access and RTCP on IP phones.
- Configuring SPAN ports to mirror voice traffic to the collector.
- Configuring medianet-enabled devices, including IPv4 routing, the collection interval, a custom Flow Monitor record, and Flow Exporter.

Detailed instructions for these tasks are provided in the following documents on the CA Unified Communications Monitor bookshelf:

- *Preparing a Cisco Unified Communications Manager Environment*
- *Best Practices for Data Acquisition*

Note: UC Monitor automatically reports on call quality metrics from authenticated SIP traffic by parsing packets that contain Transport Layer Security (TLS) authenticated messages.

Cisco Unified Communications Manager uses port 5061 for authenticated SIP traffic.

Preparing a Microsoft Lync Environment

UC Monitor supports unified communications deployments that use Microsoft Lync for call processing. The flexible product architecture lets you monitor Cisco and Avaya call servers *and* the Lync system, or a pure Lync system.

- No dedicated telephony hardware is required in a Lync environment, although the system does support optional integration with a PBX. Instead, the standard system can process VoIP and video calls. Calls are integrated with other Microsoft Office applications, such as Outlook, and with user contact information, such as IP address, SIP URI, and presence status.
- UC Monitor supports hardware-based IP phones, such as Polycom, in a Lync system. Users can make calls from supported phones, or from the lightweight Office Communicator application.

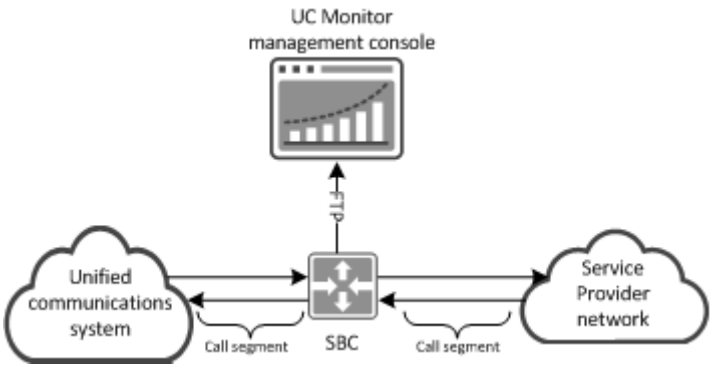
A Lync network administrator can configure HTTPS or use authentication certificates to enable secure communication between Lync servers and UC Monitor. UC Monitor does not require HTTPS or authentication certificates, but your environment may require them.

Note: See the Microsoft website for information about managing certification authority on Microsoft Windows Server 2008 R2: http://technet.microsoft.com/en-us/library/cc772011.aspx.

Preparing Acme Packet Session Border Controllers

UC Monitor supports receiving call detail records (CDRs) from Acme Packet Session Border Controllers (SBCs). The SBCs use FTP to push formatted CDRs to the management console, where they are parsed for data from ingress and egress call segments. The data appears in UC Monitor reports.

The following diagram illustrates how an Acme Packet SBC communicates with UC Monitor:



Notes:

- UC Monitor automatically discovers properly configured Acme Packet SBCs when they push CDRs to the management console. For information about configuring the SBCs, see the use case titled *Preparing to Monitor Acme Packet Session Border Controllers*.
- The UC Monitor installation process creates an FTP site on the management console that allows anonymous users to log in. For secure FTP, you can configure any server as the secure FTP recipient. That server must push the CDRs to the following location on the management console: <*install directory*>\VoipMonitor\FTPSite\ACME.
- UC Monitor support for Acme Packet requires the CA UCM FTP site to be enabled. The installation creates the \VoipMonitor\FTPSite\ACME folder regardless of the enabled or disabled status of FTP, and does not overwrite the existing FTP configuration. If you disabled the CA UCM FTP site for a previous release of UC Monitor, you must re-enable the site to facilitate UC Monitor support for Acme Packet. Similarly, re-enable the site if you disabled the FTP site because you did not need Acme Packet support, but you do want FTP to support another vendor.
- The MOS value for an SBC reflects the MOS *at* the SBC, and not the MOS for the devices on either side of the SBC.

More information:

Port and Protocol Requirements (see page 12)

Preparing Cisco Unified Border Elements

UC Monitor supports Cisco Unified Border Elements (CUBEs), the Cisco session border controller for enterprise IP networks. UC Monitor automatically discovers the devices on which CUBE is enabled and uses SNMP to poll them for the call metrics that appear in UC Monitor reports.

The CUBE device is discovered as a session border controller and appears in the management console on the Other Devices page.

A Cisco network administrator performs the following tasks to prepare a CUBE device for monitoring with UC Monitor:

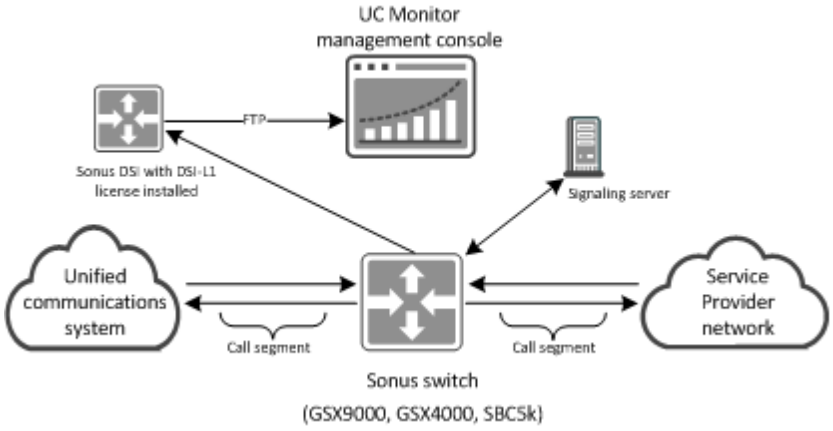
- Enable SNMP on the device.
- Enable end-of-call statistics in SIP BYE messages on the device.
- Create an SNMP profile for the device in the UC Monitor management console.

Important: UC Monitor automatically polls a discovered CUBE device. If you do not enable SNMP and end-of-call statistics, the metrics that UC Monitor collects from the device may not be correct.

Preparing Sonus DataStream Integrators

UC Monitor supports receiving call detail records (CDRs) from a properly configured Sonus DataStream Integrator (DSI). The Transporter service for a DSI uses FTP to push CDRs to the UC Monitor management console. The management console parses the CDRs for the call data from ingress and egress call segments. The data appears in UC Monitor reports.

The following diagram illustrates how a Sonus DSI communicates with UC Monitor:



A Sonus network administrator performs the following tasks to prepare a Sonus DSI for monitoring with UC Monitor:

- Install the Sonus DSI-L1 license, which provides the required Transporter service and FileServices component. You can order the license (part number DSISW-L1) from your Sonus representative.
- Enable RTCP on the DSI, to allow calculations of latency metrics.
- Configure the FileServices filters to process the CDRs that you want to publish to the UC Monitor management console.

  Note: Do not use the compress filter. UC Monitor does not decompress CDRs.
- Configure the Transporter service for publishing CDRs to the FTP site on the management console:

  `ftp://`*`UC Monitor console`*`/sonus`

  UC Monitor console

  Provide the IP address or host name of the UC Monitor management console.

  Note: For information about configuring the FileServices component and the Transporter service, see the *Administration and Maintenance Guide* for your version of the Sonus DSI.

Notes:

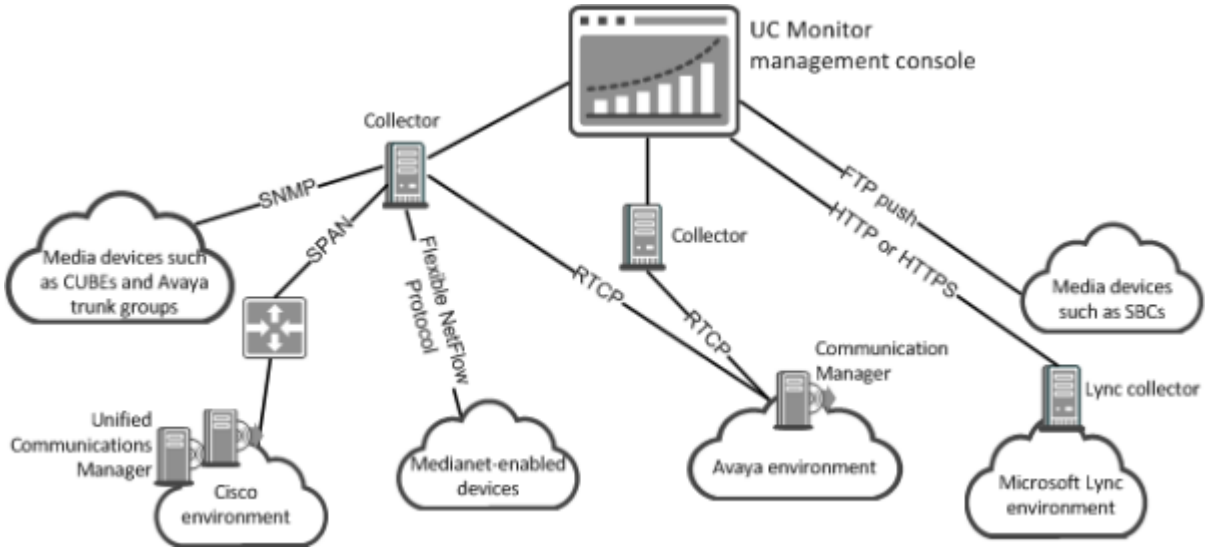
- UC Monitor automatically discovers properly configured Sonus DSIs when they push data to the management console. DSIs appear as session border controllers on the Other Devices page of the management console.
- UC Monitor installation creates an FTP site on the management console that supports logging in by an anonymous user. For sFTP environments, you can configure any server as the sFTP recipient. That server must then push data to the following location on the management console:

  `install directory``\VoipMonitor\FTPSite\Sonus`
- UC Monitor support for Sonus requires the CA UCM FTP site to be enabled. The installation creates the \VoipMonitor\FTPSite\Sonus folder regardless of the enabled or disabled status of FTP, and does not overwrite the existing FTP configuration. If you disabled the CA UCM FTP site for a previous release of UC Monitor, you must re-enable the site to facilitate UC Monitor support for Sonus. Similarly, re-enable the site if you disabled it because you did not need Sonus support, but you do want FTP to support another vendor.

Example of UC Monitor in a Multi-Vendor Environment

You can use a standalone system or a distributed system to monitor an environment that includes a combination of Cisco, Avaya, and Microsoft components. Collectors can collect data from multiple sources, and all data is correlated at the management console.

The following diagram illustrates a multi-vendor environment that includes medianet:



Index