



# APPENDIX **B**

## Unified Communications Manager Configuration

---



**Note**

For the Unified Communications Manager versions that Service Monitor supports, see *Release Notes for Cisco Unified Service Monitor 2.1*.

---

Service Monitor can collect and analyze data from Unified Communications Managers only if you first configure Unified Communications Manager systems as described in these topics:

- [Configuration Tasks for Supported Unified Communications Manager Versions, page B-1](#)
- [Configuring Unified Communications Managers, page B-2](#)
- [Configuring Database Authentication on Unified Communications Manager 4.x and 3.3.x Systems, page B-6](#)
- [Configuring Voice Gateways When VAD is Enabled, page B-12](#)

## Configuration Tasks for Supported Unified Communications Manager Versions

For Service Monitor to obtain CVTQ data from a Unified Communications Manager, you first need to perform configuration tasks while logged in to:

- Unified Communications Manager—To access Unified Communications Manager Administration and Unified Communications Manager Serviceability.
- The server where Unified Communications Manager is installed (if using Unified Communications Manager 3.3.x or 4.x)—To access Microsoft SQLServer.

You might also need to perform some additional configuration on H.323 and SIPs gateways if voice activity detection (VAD) is enabled on them so that MOS is calculated properly and, therefore, reported correctly in CDRs.

Depending on the Unified Communications Manager version that you use, you need to perform some subset of the tasks listed in this section. Where tasks themselves differ slightly from one Unified Communications Manager version to another, version-specific steps are noted in the procedures.

[Table B-1](#) lists the configuration tasks you must complete for each version of Unified Communications Manager that you want Service Monitor to obtain CVTQ data from.

**Table B-1** Unified Communications Manager and Microsoft SQL Server Tasks

Configuration Task	Perform Task for These Unified Communications Manager Versions:		
	7.x, 6.x, 5.x	4.x	3.3.x
<a href="#">Setting Unified Communications Manager Service Parameters, page B-2</a>	X	X	X
<a href="#">Setting Unified Communications Manager Enterprise Parameters, page B-3</a>	X	X	X
<a href="#">Adding Service Monitor to Unified Communications Manager 5.x (or 6.x or 7.x) as a Billing Server, page B-4</a>	X	—	—
<a href="#">Activating the AXL Web Service on Unified Communications Manager 5.x, 6.x and 7.x, page B-5</a>	X	—	—
<a href="#">Configuring Database Authentication on Unified Communications Manager 4.x and 3.3.x Systems, page B-6</a>	—	X	X
<a href="#">Configuring Voice Gateways When VAD is Enabled, page B-12</a>	X	X	—

**Caution**

Failure to configure database authentication as documented can prevent Unified Communications Manager 4.x and 3.3.x systems from writing CDRs.

## Configuring Unified Communications Managers

This section contains the following topics:



- [Setting Unified Communications Manager Service Parameters, page B-2](#)
- [Setting Unified Communications Manager Enterprise Parameters, page B-3](#)
- [Adding Service Monitor to Unified Communications Manager 5.x \(or 6.x or 7.x\) as a Billing Server, page B-4](#)
- [Activating the AXL Web Service on Unified Communications Manager 5.x, 6.x and 7.x, page B-5](#)
- [Changing the Password for smuser in Unified Communications Manager 5.x, 6.x, and 7.x, page B-5](#)

For Unified Communications Manager 3.3.x and 4.x, be sure to also complete the tasks in [Configuring Database Authentication on Unified Communications Manager 4.x and 3.3.x Systems, page B-6](#).

## Setting Unified Communications Manager Service Parameters

**Note**

Set these parameters on each Unified Communications Manager in a cluster.

- 
- Step 1** Log in to Unified Communications Manager Administration.
- Step 2** Go to the Service Parameters Configuration page as follows:
- For Unified Communications Manager 3.3 and 4.x, select **Service > Service Parameters**.
  - For Unified Communications Manager 5.x, 6.x, and 7.x, select **System > Service Parameters**.
- The Service Parameters Configuration page appears.
- Step 3** Select the server and the service:
- a. Select the name of the Unified Communications Manager server. This is a Unified Communications Manager from which Service Monitor will gather data.
  - b. Select the Unified Communications Manager service.
- Step 4** Set these parameters:
- For Unified Communications Manager versions 3.3.x and 4.x:
    - CDR Enabled Flag—Scroll down to System. Set to **True**.
    - Call Diagnostics Enabled—Scroll down to Clusterwide Parameters (Device - General). Set to **True**.
-  **Note** It is recommended that you ensure that Call Diagnostics Enabled is set to true on the publisher and on each of the subscribers.
- 
- For Unified Communications Manager 5.x, 6.x, and 7.x:
    - CDR Enabled Flag—Scroll down to System. Set to **True**.
    - Call Diagnostics Enabled—Scroll down to Clusterwide Parameters (Device - General). Set to **Enable Only When CDR Enabled Flag is True**.
-  **Note** It is recommended that you ensure that Call Diagnostics Enabled is set to Enable Only When CDR Enable Flag is True on the publisher and on each of the subscribers.
- 
- Step 5** Click **Update**.
- 

## Setting Unified Communications Manager Enterprise Parameters

Perform this procedure for Unified Communications Manager versions 3.3.x, 4.x, 5.x, 6.x, and 7.x.

- 
- Step 1** Log in to Unified Communications Manager Administration.
- Step 2** Select **System > Enterprise Parameters**. The Enterprise Parameters Configuration page appears.
- Step 3** Scroll down to CDR Parameters and set these parameters:
- For Unified Communications Manager 3.3 and 4.x:
    - CDR File Time Interval (min)—Set to **1**.
    - CDR Format—Select **CDRs will be inserted into database**.
  - For Unified Communications Manager 5.x, 6.x, and 7.x, set CDR File Time Interval (min) to **1**.

- Step 4** Scroll to the Cluster ID. If the cluster ID is already present Service Monitor—see [Understanding and Setting Unified Communications Manager Credentials, page 3-2](#)—change it.



**Note** Each cluster that you add to Service Monitor must have a unique cluster ID.

- Step 5** Click **Update**.

## Adding Service Monitor to Unified Communications Manager 5.x (or 6.x or 7.x) as a Billing Server



- Note**
- Perform this task on Unified Communications Manager version 5.x, 6.x, and 7.x only.
  - Perform this task only while Service Monitor is up and running.

- Step 1** Launch Unified Communications Manager Serviceability.

- Step 2** Select **Tools > CDR Management**.

- Step 3** Scroll down to Billing Applications Server Parameters and click **Add New**.

- Step 4** Enter the following:

- Host Name / IP Address—Enter the IP address of the system where Cisco Unified Service Monitor is installed.
- User Name—Enter smuser.



**Note** Do not enter any username other than smuser.

- Password—Enter a password. The default password is smuser. To change this password:
  - Change it in Service Monitor first. (For more information, see [Configuring and Viewing Other Settings, page 3-15](#).)
  - Enter the same password that you entered for smuser while configuring other settings in Service Monitor.



**Note** If you changed the password in Service Monitor and Unified Communications Manager does not immediately accept the new password, wait one minute and enter the new password again.

- Select SFTP Protocol.
- Directory Path—Enter /home/smuser/.



**Note** Do not enter any directory path other than /home/smuser/.

- Resend on Failure (Displayed in Unified Communications Manager 7.0 and later)—Uncheck this check box.

**Step 5** Click **Add**.



**Note**

In some cases, for CDR/CMR files to be delivered to a newly added billing server, it is necessary to first restart the CDR Repository Management Service.

**Step 1** From Unified Communications Manager Serviceability, select **Tools > Control Center - Network Services**.

**Step 2** From the list of Unified Communications servers, select the publisher.

**Step 3** Scroll down to CDR Services.

**Step 4** Select the **Cisco CDR Repository Manager** radio button.

**Step 5** Click the **Restart** button.

## Activating the AXL Web Service on Unified Communications Manager 5.x, 6.x and 7.x

Perform this procedure for Unified Communications Manager versions 5.x and later.

**Step 1** Launch Unified Communications Manager Serviceability.

**Step 2** Select **Tools > Service Activation**.

**Step 3** Select a server.



**Note** Activate the AXL Web Service on the Publisher node.

**Step 4** Scroll down to Database and Admin Services and select **Cisco AXL Web Service**.

**Step 5** Click **Save**.

## Changing the Password for smuser in Unified Communications Manager 5.x, 6.x, and 7.x



**Note**

Perform this task as needed on Unified Communications Manager versions 5.x, 6.x, and 7.x only.

The SFTP password for smuser in Service Monitor and the password for the Service Monitor Applications Billing Server smuser in Unified Communications Manager 5.x, 6.x, and 7.x must be identical. Any time you change one, you must change the other to match. To change the SFTP password for smuser in Service Monitor, see [Configuring and Viewing Other Settings, page 3-15](#).

Use this procedure to change the password for the Service Monitor Applications Billing Server smuser in Unified Communications Manager 5.x, 6.x, and 7.x.

- 
- Step 1** Launch Unified Communications Manager Serviceability.
- Step 2** Select **Tools > CDR Manageability**.
- Step 3** Scroll down to Billing Applications Server Parameters and double-click the link for the Service Monitor.
- Step 4** Enter a new password.



**Note** If you changed the password in Service Monitor and Unified Communications Manager does not immediately accept the new password, wait one minute and enter the new password again.

Do not change the values in any other fields; Host Name / IP Address, User Name, SFTP Protocol, and Directory Path must remain the same.

- Step 5** Click **Update**.
- 

## Configuring Database Authentication on Unified Communications Manager 4.x and 3.3.x Systems

When you add or edit Unified Communications Manager 3.3.x and 4.x credentials in Service Monitor, you must select the type of database authentication (SQL or Windows authentication) for Service Monitor to use. (For more information, see [Understanding and Setting Unified Communications Manager Credentials, page 3-2](#).) It is recommended that you select the type of database authentication that is already in use on Unified Communications Manager.

Use the procedure [Determining Authentication Mode in Use on a Unified Communications Manager 4.x \(or 3.3.x\) System, page B-6](#) to find out which type of database authentication is in use on Unified Communications Manager. Then, before configuring credentials in Service Monitor, perform the configuration tasks related to the database authentication mode in use:

- SQL Authentication—[Configuring SQL Authentication on a Unified Communications Manager 4.x \(or 3.3.x\) System, page B-7](#)
- Windows Authentication—[Configuring Windows Authentication on a Unified Communications Manager 4.x \(or 3.3.x\) System, page B-10](#)

## Determining Authentication Mode in Use on a Unified Communications Manager 4.x (or 3.3.x) System

- 
- Step 1** Log in to the server where the Unified Communications Manager publisher is installed.
- Step 2** Select **Start > Programs > Microsoft SQL Server Enterprise Manager**.

- Step 3** Select **Console Root > Microsoft SQL Servers > SQL Server Group**.
- Step 4** Right-click (**local**) and select Properties. A dialog box appears.
- Step 5** Select the **Security** tab.
- Step 6** Note which of these is selected:
- SQL Server and Windows
  - Windows only
- Step 7** Click **Cancel**.
- Step 8** For the authentication mode to select in Service Monitor, see [Table B-2](#).

When you add or edit Unified Communications Manager credentials in Service Monitor, you should select the corresponding authentication mode for accessing Unified Communications Manager databases, as shown in [Table B-2](#).

**Table B-2 Database Authentication Selection**

Database Authentication Mode in Use on Unified Communications Manager	Recommended Mode to Select in Unified Communications Manager Credential in Service Monitor
SQL and Windows <b>Note</b> SQL and Windows is also referred to as mixed mode.	At your discretion, select either: <ul style="list-style-type: none"> <li>• Windows Authentication</li> <li>• SQL Authentication</li> </ul>
Windows only	You must select Windows Authentication.

## Configuring SQL Authentication on a Unified Communications Manager 4.x (or 3.3.x) System

Use these procedures after you determine that you should use SQL authentication to access a Unified Communications Manager 3.3.x or 4.x database from Service Monitor. (See [Determining Authentication Mode in Use on a Unified Communications Manager 4.x \(or 3.3.x\) System](#), page B-6 and [Table B-2](#).)

To use SQL authentication:

- The Unified Communications Manager publisher node must be configured to use mixed authentication.
- You must create Microsoft SQL Server user accounts that can access the databases.



**Note** You will need to enter the usernames and passwords for these user accounts when adding Unified Communications Manager 3.3.x and 4.x credentials to Service Monitor.

See [Table B-3](#) to determine the procedures that you should use.

**Table B-3 SQL Authentication Configuration Process**

Unified Communications Manager Version	Default Authentication Mode	To Use SQL Authentication
4.x	Windows	<ol style="list-style-type: none"> <li>1. If Windows only authentication is configured, you must configure mixed authentication. See <a href="#">Configuring Mixed Authentication in Microsoft SQL Server for Unified Communications Manager 4.x</a>, page B-8.</li> <li>2. You must configure user accounts. See <a href="#">Adding Microsoft SQL Server User Accounts for Unified Communications Manager 3.3.x and 4.x</a>, page B-9.</li> </ol>
3.3.x	SQL	

## Configuring Mixed Authentication in Microsoft SQL Server for Unified Communications Manager 4.x

Use this procedure only after you have determined that you should use SQL authentication to access Unified Communications Manager databases from Service Monitor. See [Determining Authentication Mode in Use on a Unified Communications Manager 4.x \(or 3.3.x\) System](#), page B-6 and [Table B-2](#).



### Note

For Unified Communications 3.3.x, mixed authentication should be configured by default. If it is not, you can use this procedure to configure mixed authentication for 3.3.x.



### Caution

Failure to complete this task as documented can prevent Unified Communications Manager from writing CDRs.

Perform this task for Unified Communications Manager 4.x and 3.3.x only.

- Step 1** Log in to the server where Unified Communications Manager is installed.
  - Step 2** Select **Start > Programs > Microsoft SQL Server Enterprise Manager**.
  - Step 3** Select **Console Root > Microsoft SQL Servers > SQL Server Group**.
  - Step 4** Right-click (**local**) and select Properties. A dialog box appears.
  - Step 5** Select the **Security** tab:
    - a. Under Authentication, select **SQL Server and Windows**.
    - b. Click **OK**. A message appears, asking whether to restart the SQL server. Click **No**.
- Note** If Cisco Security Agent runs on the Unified Communications Manager server, it might block the message that asks whether to restart the SQL server, in which case the change is not applied. To work around this problem, open Windows Services user interface and stop Cisco Security Agent. After you complete steps 5b and 6, restart Cisco Security Agent.
- Step 6** Restart the SQL server:
    - a. Select **Start > Settings > Control Panel > Administrative Tools > Services**. The Services window appears.

- b. Right-click MSSQLSERVER and click **Stop**. A list of services that will be stopped in addition to MSSQLSERVER will be displayed. Note them; you will need to start each one in step 6c.
- c. Right-click MSSQLSERVER and click **Start**. For each of the additional services that were stopped during the previous step, right-click the service and click **Start**.

You must also add user accounts as directed in [Adding Microsoft SQLServer User Accounts for Unified Communications Manager 3.3.x and 4.x](#), page B-9.

## Adding Microsoft SQLServer User Accounts for Unified Communications Manager 3.3.x and 4.x

Use this procedure if you have determined that you should use SQL authentication to access Unified Communications Manager databases from Service Monitor. See [Determining Authentication Mode in Use on a Unified Communications Manager 4.x \(or 3.3.x\) System](#), page B-6 and Table B-2.



### Caution

Failure to complete this task as documented can prevent Unified Communications Manager from writing CDRs.

When using SQL authentication, Service Monitor needs at least one Microsoft SQLServer user account to access local databases on the system with Unified Communications Manager 3.3.x and 4.x. Use this procedure to add user accounts on these Unified Communications Manager versions:

- 4.x—Add an account to enable Service Monitor to access the CDR database.
- 3.3.x—Add an account to enable Service Monitor to access the CDR database and the device database, named CCM030*n*; for example, CCM0300. Alternatively, add two accounts: one for the CDR database and another for the CCM030*n* database.

- Step 1** Log in to the server where Unified Communications Manager is installed.
- Step 2** Select **Start > Programs > Microsoft SQL Server Enterprise Manager > Security**.
- Step 3** Right-click **Logins** and select **New Login**. A window appears.



### Note

Be prepared to give the username and password that you enter in [Step 4](#) to the user who enters credentials for Unified Communications Manager in Service Monitor.

- Step 4** On the General tab:
  - a. Enter a username.
  - b. Select **SQL Authentication** and enter a password.



### Note

Make sure that SQL Authentication is selected and *not* Windows Authentication, which is sometimes selected by default.

- Step 5** Select the Server Roles tab and select the System Administrators role.



### Caution

You must complete step 5; otherwise, you might prevent Unified Communications Manager from writing CDRs to the database.

- Step 6** Select the Database Access tab and do the following:
- a. Select databases as follows:
    - For Unified Communications Manager version 4.x, check the Permit column for the CDR database.
    - For Unified Communications Manager version 3.3.x, check the Permit column for the CDR database and for the device database, named CCM030n; for example, CCM0300. Alternatively, select only one database, CDR or the device database, and continue creating the account. After creating one account, repeat the procedure to create another account for the other database.



**Note** Each time you upgrade Unified Communications Manager, the *n* in CCM030n is increased by 1 and a new device database is created. If there are multiple device databases, choose the most recent one (the one with the highest number); for example, CCM0302. If you upgrade Unified Communications Manager 3.3 after you complete this step, you must return to this procedure and repeat this step ([Step 6](#)).

Alternatively, select only one database, CDR or the device database, and continue creating the account. After creating one account, repeat the procedure to create another account for the other database.

At the bottom of the window, database roles for the selected databases are displayed; public is checked by default.

- b. Check the db\_owner role (so that public and db\_owner are checked).



**Caution**

You must complete step [6b](#); otherwise, you can prevent Unified Communications Manager from writing CDRs to the database.

**Step 7** Click **OK**. A confirmation dialog box appears.

**Step 8** Confirm the password (previously entered in step [4b](#)) by entering it again in the dialog box.

## Configuring Windows Authentication on a Unified Communications Manager 4.x (or 3.3.x) System

Use this procedure if you have determined that you should use Windows authentication to access Unified Communications Manager databases from Service Monitor. See [Determining Authentication Mode in Use on a Unified Communications Manager 4.x \(or 3.3.x\) System](#), page B-6 and [Table B-2](#).

A casuser Windows account is created during installation on the Service Monitor system. You must create a casuser Windows account on each Unified Communications Manager 3.3.x and 4.x system that Service Monitor will access using Windows authentication. The password for all casuser accounts must match.

**Step 1** Log into the system where Unified Communications Manager is installed.

**Step 2** Select **Start > Settings > Control panel > Administrative Tools > Computer Management > Users > Local Users and Groups > Users**, right-click and add a new user:

- a. Enter casuser as the username and enter the appropriate full name and description.

- b. Enter a password.



**Note** Be prepared to enter the same password for the casuser account on Service Monitor—as described in [Step 6](#)—and on any other Unified Communications Manager system for which you configure Windows authentication.

- c. Uncheck User must change password at next logon.
- d. Select password never expires.
- e. Click **Create**.

**Step 3** Give the casuser account access to the CDR database:

- a. Select **Start > Programs > Microsoft SQL Server Enterprise Manager > Console Root > Microsoft SQL Servers > SQL Server Group > local > Security > Logins**.
- b. Right-click **Logins** and select **New login**.
- c. On the General tab:
  - For Name, select casuser
  - Select Windows Authentication
  - Under Security access, select Grant access
  - Under Defaults, for Database, select master
- d. On the Database Access tab:
  - Select CDR.
  - Under Database roles for ‘CDR’, select db\_owner and ensure that public is selected (it should be selected by default).



**Note** If you are configuring Windows authentication for Unified Communications Manager 3.3.x, also select the device database, which is named CCM030*n*; for example, CCM0300. Select the db\_owner role and ensure that the public role is selected.

- e. Click **OK**. If you have already determined that Windows only authentication is in use—see [Determining Authentication Mode in Use on a Unified Communications Manager 4.x \(or 3.3.x\) System, page B-6](#)—you can skip Steps 4 and 5; however, be sure to complete [Step 6](#).

**Step 4** Set authentication to Windows only:

- a. Select **Console Root > Microsoft SQL Servers > SQL Server Group**.
- b. Right-click (**local**) and select Properties. A dialog box appears.
- c. Select the **Security** tab.
- d. Under Authentication, select **Windows only**. (If Windows only is already selected, you can click **Cancel** and skip Steps 4e and 5; however, be sure to complete [Step 6](#).)
- e. Click **OK**. A message appears, asking whether to restart the SQL server. Click **No**.



**Note** If Cisco Security Agent runs on the Unified Communications Manager server, it might block the message that asks whether to restart the SQL server, in which case the change is not applied. To work around this problem, open Windows Services user interface and stop Cisco Security Agent. After you complete steps 5b and 6, restart Cisco Security Agent.

- Step 5** Restart the SQL server:
- Select **Start > Settings > Control Panel > Administrative Tools > Services**. The Services window appears.
  - Right-click MSSQLSERVER and click **Stop**. A list of services that will be stopped in addition to MSSQLSERVER will be displayed. Note them; you will need to start each one in step 4c.
  - Right-click MSSQLSERVER and click **Start**. For each of the additional services that were stopped during the previous step, right-click the service and click **Start**.
- Step 6** Reset the password for the casuser account on the Service Monitor system so that it matches the one you entered in [Step 2](#):
- Log into the system where Service Monitor is installed.
  - Go to C:\Program Files\CSCOpX\setup\support\ and double-click the resetCasuser.exe file.
  - Select option 2: Enter causer password.
  - Enter the password and confirm it. An informational window opens.
  - Click **OK**.
  - Stop and start the Daemon Manager by entering these commands:  

```
net stop crmdmgt  
net start crmdmgt
```
- 

## Configuring Voice Gateways When VAD is Enabled

This information applies when using Unified Communications Manager versions 4.x and later. When VAD is enabled on a voice gateway in a cluster, you can see lower MOS values in CVTQ reports for calls between the voice gateway and IP phones. You need to:

- Configure the comfort noise payload type to 13 (from the default of 19) on H.323 and SIP gateways. Doing so enables Cisco IP phones and voice gateways to properly adjust the MOS calculation.



**Note** Performing this configuration does not affect the MOS values that are reported in Cisco 1040 Sensor reports.

---

- Be aware that low MOS will be reported for calls between Cisco IP phones and MGCP gateways on CVTQ reports. (Comfort noise payload type is not configurable on MGCP gateways.)