



# APPENDIX **A**

## Configuration Checklists and Tips

The following topics are included:

- [Initial Configuration Checklist, page A-1](#)
- [Understanding when You Can Expect to See Results, page A-2](#)
- [Optional Configuration Checklist, page A-2](#)

### Initial Configuration Checklist

[Table A-1](#) lists configuration tasks that you must complete before Service Monitor can start to monitor MOS and send traps.

**Table A-1** *Initial Configuration Task Checklist*

Tasks	Description and Reference
<b>Configuring Service Monitor and Cisco Unified Communications Manager (when Present in your Network)</b>	
	Configure Cisco Unified Communications Manager (Unified Communications Manager) as described in <a href="#">Unified Communications Manager Configuration, page B-1</a> .
	Add credentials for Unified Communications Managers to Service Monitor; see <a href="#">Understanding and Setting Unified Communications Manager Credentials, page 3-2</a> .
<b>Configuring Service Monitor and Sensors (when Present in your Network)</b>	
	Add at least one TFTP server. See <a href="#">Configuring TFTP Servers for Sensor Configuration and Image Files, page 4-3</a> .
	Set up the sensor default configuration file. See <a href="#">Setting Up the Sensor Default Configuration, page 4-4</a> .
	Copy the binary image file to the root location on the TFTP server. See <a href="#">Copying the Binary Image File to the TFTP Server, page 4-4</a> .
<b>Configuring Trap Receivers</b>	
	Service Monitor can send generated SNMP traps to up to four trap receivers. See <a href="#">Configuring Trap Receivers, page 3-1</a> .

### Server and Client Configuration Tasks

On the Service Monitor server, you should exclude the `NMSROOT\databases` directory from virus scanning. Problems can arise if database files are locked because of virus scanning.

**Note**

*NMSROOT* is the directory where Service Monitor is installed on your system. If you selected the default directory during installation, it is C:\Program Files\CSCOPx.

On Service Monitor clients, you must disable any software that you use to prevent popup windows from displaying. Service Monitor must be able to open multiple windows to display information.

## Understanding when You Can Expect to See Results

After you complete the tasks in [Table A-1](#), Service Monitor starts to receive, analyze, and present data as follows:

- Sensors send a record to Service Monitor every 60 seconds, reporting calculated MOS while a call is in progress. Therefore, Service Monitor can start to generate traps while the call ensues. Similarly, sensor data can be displayed in Service Monitor reports while the call is in progress.
- Call data records (CDRs) are only written by Unified Communications Manager after a call has completed. Although Service Monitor might obtain data from Unified Communications Manager every 60 seconds, Service Monitor cannot generate traps until the call is over. Similarly, CVTQ data cannot be displayed in Service Monitor reports until a call has completed.

## Optional Configuration Checklist

These tasks enable you to:

- Update and override the default global thresholds—one per codec—that Service Monitor uses to trigger trap generation.
- Generate most-impacted endpoint reports automatically on a nightly and weekly basis.

**Table A-2**      **Optional Configuration Tasks**

Tasks	Description and Reference
<b>Updating and Overriding Global Thresholds</b>	
	Update global threshold values. See <a href="#">Configuring Global Thresholds, page 5-2</a> .
	Override global threshold values, providing values for selected sensors. See <a href="#">Configuring Sensor Groups, page 5-9</a> .
	Override global threshold values, providing values for selected clusters. See <a href="#">Configuring CVTQ Groups, page 5-3</a> .
<b>Exporting Most-Impacted Endpoint Reports</b>	
	See <a href="#">Configuring Number of Endpoints and Export Settings for Impacted Endpoints Reports, page 3-13</a> .
<b>Updating Report-Related Settings and System Schedules</b>	
	Update the number of minutes that diagnostic reports search for data and the number of records to export to a CSV file. See <a href="#">Configuring Diagnostic Report Search and CSV Export Limit Settings, page 3-17</a> .
	Update system schedules. See <a href="#">Configuring Low-Volume Schedule and Database Purging, page 6-1</a> .