



## CHAPTER 7

# Using Administration

---

Service Statistics Manager offers a series of configurable options for setting user preferences under the Administration tab. The Administration tab has various options that work interactively to manage and customize your Service Statistics Manager work environment. The following topics are included in this section:

- [Changing Your Password, page 7-1](#)
- [Selecting Your Dashboard View, page 7-1](#)
- [Selecting Your Home View, page 7-2](#)
- [Performing Advanced Administration Tasks, page 7-2](#)
- [Working with Downloads, page 7-15](#)

## Changing Your Password

Change the password for the admin user using this procedure.

- 
- Step 1** Select the **Administration** tab; then, in the User ID and Password pane, click the **Edit** link. The Change Password window appears.
- Step 2** Enter appropriate passwords in each of these fields:
- Enter Old Password
  - Enter New Password
  - Confirm New Password
- Step 3** Click **Apply**.
- 

## Selecting Your Dashboard View

Views provide rapid access to information in an easy-to-interpret and concise manner. From a view, you can drill down into the data to gain insight into specific areas. If you select a dashboard view, it is displayed at the top of the Reports tab. Each user can select a different view for use as a dashboard view.

- 
- Step 1** Select the **Administration** tab and scroll to Dashboard View.

**Step 2** Select a view from **Show Dashboard View**.



**Note** Only views that you have access to appear in the list. Contact a user in the Administration role to request access to additional views.

**Step 3** Click **Apply**.

---

## Selecting Your Home View

Your home view is displayed on the Views tab at login and each time you select the Views tab. If you do not select a home view, the default home view for your role is displayed; for more information, see [Table 2-1](#).

**Step 1** Select the **Administration** tab and scroll to Home View.

**Step 2** Select a view from **Show Home View**.



**Note** Only views to which you have access appear in the list. Contact a user in the Administration role to request access to additional views.

**Step 3** Click **Apply**.

---

## Performing Advanced Administration Tasks

From the Advanced pane on the Administration tab, you can add, edit, or delete attribute sets, schedules, phone-based groups, call quality ranges, and Operations Manager and Service Monitor details. In addition, for Service Statistics Manager to classify calls correctly, you should configure dial plans (and call classification), gateway codes, toll-free numbers, and service numbers in Service Monitor. For more information, see *User Guide for Cisco Unified Service Monitor 9.0*.

If a lock icon appears next to a task name in the Advanced pane, you do not have the necessary privileges to perform the task. For more information, see [Managing User Roles and Privileges, page 6-8](#).

- [Configuring Attribute Sets, page 7-3](#)
- [Configuring Schedules, page 7-5](#)
- [Configuring Phone-Based Groups, page 7-7](#)
- [Integrating with Operations Manager and Service Monitor, page 7-8](#)

## Configuring Attribute Sets



Note

To configure attribute sets, you must have the privilege to do so; for more information, see [Managing User Roles and Privileges, page 6-8](#).

An attribute set includes attributes—types of data, such as database availability, number of good calls, or trunk utilization—that Service Statistics Manager can collect for monitor types, such as call quality by cluster monitors, call volume by clusters monitors, and trunk utilization monitors. For monitor types and the attributes of each, see the following:

- [Service Monitor Database Monitor Types, page A-2](#)
- [Operations Manager File-Based Monitor Types, page A-18](#)

To configure an attribute set, see the following:

- [Adding an Attribute Set, page 7-3](#)
- [Editing an Attribute Set, page 7-4](#)
- [Deleting an Attribute Set, page 7-5](#)

### Adding an Attribute Set

- 
- Step 1** Select the **Administration** tab and scroll to Advanced.
- Step 2** In the Attribute Sets row, click the **Edit** link. (If there is no Edit link, you do not have the necessary privileges. For more information, see [Managing User Roles and Privileges, page 6-8](#).)
- The Attribute Set Administration window appears, displaying any existing attribute set by name and type.
- Step 3** Click **Add**. The Add Attribute Set page appears.
- Step 4** Select one of these attribute set types:
- Global—Configure reports and SLAs.
  - Reports—Configure reports only.
  - SLA Type—Configure SLAs only.



Note

After you add the attribute set, you cannot update its attribute set type.


- Step 5** Select one or more monitor types from the Monitor Type list; use the Ctrl and Shift keys to make multiple selections. Optionally, enter a monitor type in the Search field to find a specific type.
- Step 6** Click **Next**. Service Statistics Manager displays one list of attributes for each monitor type that you selected.
- Step 7** Select attributes from each list:
- a. (Optional) Enter an attribute name or part of an attribute name in the Search field to filter the attributes.
  - b. Use the Ctrl and Shift keys to make multiple selections.
- Step 8** Click **Next**. The Add Attribute Set window appears.
- Step 9** Enter a name in the Attribute Set Name field.

- Step 10** Click **Finish**. The window closes and the newly added attribute set is listed in the Attribute Set Administration window.
- 

## Editing an Attribute Set

You can edit any attribute sets that you have added as well as the default attribute sets that Service Statistics Manager provides. Default attribute sets include:

- Route Group Utilization
  - System Utilization
  - Trunk Utilization
  - Unified CM Performance
- 

- Step 1** To open the Edit Attribute Set window, do the following:
- a. Select the **Administration** tab and scroll to Advanced.
  - b. In the Attribute Sets row, click the **Edit** link. (If there is no Edit link, you do not have the necessary privileges. For more information, see [Managing User Roles and Privileges, page 6-8.](#))  
The Attribute Set Administration window appears.
  - c. Locate the attribute set that interests you and click the **Edit** link. The Edit Attribute Set window appears, displaying the monitor type and the selected attributes in a table.
- Step 2** To add attributes, click **Add Attributes**. The Edit Attribute Set window remains open, displaying a Monitor Types list:
- a. Select one or more monitor types from the list—Use the Ctrl and Shift keys to make multiple selections. Optionally, enter a monitor type in the Search field to find a specific type.  
(For a list monitor types and the attributes that are available for them, see [Service Monitor Database Monitor Types, page A-2](#) and [Operations Manager File-Based Monitor Types, page A-18.](#))
  - b. Click **Next**. Service Statistics Manager displays one list of attributes for each monitor type that you selected.
  - c. Select attributes:
    - (Optional) Enter an attribute name or part of an attribute name to filter the attribute list.
    - Use the Ctrl and Shift keys to make multiple selections.
  - d. Click **Next**. The Edit Attribute Set window displays a table with the monitor types and attributes that are included in the set.
- Step 3** To delete monitor types and attributes from the set, select them and click **Delete**.
-  **Note** At least one monitor type and attribute must remain in the set. To completely delete an attribute set, see [Deleting an Attribute Set, page 7-5.](#)
- 
- Step 4** Repeat steps 2 and 3 to add or delete additional attributes.
- Step 5** Click **Finish** to save the changes to the attribute set.
-

## Deleting an Attribute Set

You cannot delete the default attribute sets that Service Statistics Manager provides:

- Route Group Utilization
- Trunk Utilization
- System Utilization (for Unity)
- Unified CM Performance

You can delete any user-created attribute set.

- 
- Step 1** Select the **Administration** tab and scroll to Advanced.
- Step 2** In the Attribute Sets row, click the **Edit** link. (If there is no Edit link, you do not have the necessary privileges. For more information, see [Managing User Roles and Privileges, page 6-8](#).)
- The Attribute Set Administration window appears, displaying a list of attribute sets.
- Step 3** Select desired check boxes.
- Step 4** Click **Delete**. Service Statistics Manager displays a confirmation message.
- Step 5** Click **OK**.
- 

## Configuring Schedules



### Note

To configure schedules, you must have the privilege to do so. If you have the privilege to manage reports or SLAs, then you also have the privilege to configure schedules. For more information, see [Managing User Roles and Privileges, page 6-8](#).

Schedules are used to limit the data that is included in a report, a graph, or SLA computations to only the data that was collected during the time specified in the schedule. You select a schedule for a report or an SLA when you configure the report or SLA. Service Statistics Manager provides two default schedules: 24x7 and Business Hours (8:00 a.m. to 5:00 p.m., Monday through Friday). Changes that you make to a schedule affect each report, custom graph (in a graph-based view), or SLA that uses the schedule.

If you are permitted to configure schedules, you can do so:

- When you configure reports or SLAs—You can add or update schedules from the page where you are required to select a schedule. For related procedures, see [Defining Schedules, page 5-16](#).
- From the Administration tab—See the following procedures:
  - [Adding a Schedule, page 7-5](#)
  - [Editing a Schedule, page 7-6](#)
  - [Deleting a Schedule, page 7-7](#)

## Adding a Schedule

- 
- Step 1** Select the **Administration** tab and scroll to Advanced.

**Step 2** In the Schedules row, click the **Edit** link. (If there is no Edit link, you do not have the necessary privileges. For more information, see [Managing User Roles and Privileges, page 6-8.](#))

The Schedule Administration window appears.

**Step 3** Click **Add**. The Create New Schedules window appears.

**Step 4** Enter a name for the schedule.

**Step 5** Define schedule criteria:

- You must define at least one inclusion period; see [Step 6](#).
- You can define one or more exclusion periods; see [Step 7](#).




---

**Note** If you define an exclusion period, it takes precedence over inclusion periods.

---

**Step 6** Define times to include in the schedule by selecting the **Inclusion** radio button and selecting the **Select All Days** check box or to define a time range for a single day:

- a. Select the check box for one of the days (listed beside **Days**).
- b. Select the Start Time and End Time from the list.
- c. Click **Add**. Service Statistics Manager adds the new time range to the table in the lower portion of the window.

**Step 7** To define an exclusion period:

- a. Select the **Exclusion** radio buttons
- b. Select one of these and define criteria for it:
  - One Time Setting—Select the From and To time and date period to exclude.
  - Monthly—Select the day of the month (1, 2...31) or the week of the month (First, Second...), and the hours to exclude.
- c. Click **Add**. Service Statistics Manager adds the schedule criteria to the table in the lower portion of the window.

**Step 8** Repeat [Step 6](#) and [Step 7](#) until schedules for all days are correct.

**Step 9** Click **Done**. Service Statistics Manager displays a confirmation message and displays the Schedule Administration window.

---

## Editing a Schedule




---


**Note** Any changes you make to a schedule affect all reports and SLAs that are associated with the schedule. Unless you are sure that the change is appropriate for all, consider creating a new schedule or using a different schedule for your purpose.

---

**Step 1** Select the **Administration** tab and scroll to Advanced.

**Step 2** In the Schedules row, click the **Edit** link. (If there is no Edit link, you do not have the necessary privileges. For more information, see [Managing User Roles and Privileges, page 6-8.](#))

The Schedule Administration window appears.

- Step 3** Click the **Edit** link for a schedule. If the schedule is in use—associated with a report or an SLA—a confirmation window lists the associated items and asks whether you want to continue.
- If appropriate, click **OK**. Service Statistics Manager displays the Edit Schedule window. Existing schedule criteria are displayed in the table in the lower portion of the window.
- Step 4** To change the schedule name, enter a new name.
- If the schedule is used elsewhere—associated with another SLA or a report for example—a confirmation window lists them and asks whether you want to continue. If appropriate, click **OK**.
- Service Statistics Manager displays the Edit Schedule window. Existing schedule criteria are displayed in the table in the lower portion of the window.
- Step 5** Update the schedule as needed:
- To delete criteria from the schedule, select them from the table and click the **Delete** button above and to the right of the table.
-  **Caution** Be sure to click the Delete button above and to the right of the table. The Delete Schedule button below the table deletes the entire schedule.
- To add criteria to the schedule, select the Inclusion or Exclusion radio button, select the appropriate time period to include or exclude, and click **Add**.
- Step 6** When you have finished updating the schedule, click **Done**. Service Statistics Manager stores the changes and displays the Schedule Administration window.

## Deleting a Schedule

- Step 1** Select the **Administration** tab and scroll to Advanced.
- Step 2** In the Schedules row, click the **Edit** link. (If there is no Edit link, you do not have the necessary privileges. For more information, see [Managing User Roles and Privileges, page 6-8.](#))
- The Schedule Administration window appears.
- Step 3** Select desired check boxes.
- Step 4** Click **Delete**. Service Statistics Manager displays a confirmation message:
- If the schedule is still associated with SLAs or reports, they are listed. You cannot complete this procedure. You must either delete these SLAs or reports, or reconfigure them to use a different schedule before you try to delete the schedule again.
  - If the schedule is not associated with SLAs or reports, click **OK**. Service Statistics Manager deletes the schedule and displays the Schedule Administration window.

## Configuring Phone-Based Groups

You can use phone-based groups to include only certain phones in the following reports:

- Cause Code Analysis
- Call Quality Summary

- Top N Dialed Numbers
- Top N Calls
- Top N Users
- Traffic Summary

---

**Step 1** Select the **Administration** tab and scroll to Advanced.

**Step 2** In the Phone-Based Groups row, click the **Edit** link. (If there is no Edit link, you do not have the necessary privileges. For more information, see [Managing User Roles and Privileges, page 6-8](#).)

The Phone-Based Groups window appears, displaying a text box in which you can add, edit, and delete phone-based groups.

**Step 3** To add or edit a phone-based group, define it following this template:

*GroupName = Phone numbers belonging to PhoneGroup*

- **GroupName**—Do not include any special characters (a white space is considered a special character).
- **Phone numbers belonging to PhoneGroup**—Enter any combination of the following, separated by commas:
  - **Range of phone numbers**—Specify a range using a hyphen (-) between two numbers expressed numerically. For example, (56005200-56005230) means all phone numbers from 56005200 to 56005230.
  - **Phone numbers specified using an exclamation mark (!) as a regular expression**—The exclamation mark represents any alphanumeric character, and can appear any number of times. For example:
    - 5610!—Matches phone number 5610 or any phone number that starts with 5610.
    - !60!52!—Matches phone number 6052 or any phone number that includes both 60 and 52 in it.
  - **Individual phone numbers** can also be specified; for example, 56005210.




---

**Note** Phone-based groups support phone numbers with up to 18 digits.

---

**Step 4** To delete a phone group, select the entire definition for the group (*GroupName = Phone numbers belonging to PhoneGroup*) and delete it.

**Step 5** Click **Apply**.

---

## Integrating with Operations Manager and Service Monitor

Ensure that the SSM Agent software is installed on any remote Operations Manager or Service Monitor system from which you expect to collect data; see [Installing SSM Agent on Another System, page 7-16](#). After the SSM Agent software is installed, run discovery to connect the SSM Agents to Service Statistics Manager.

You must have privileges to perform the tasks described in these topics:

- [Triggering Discovery, page 7-9](#)
- [Retriggering Discovery, page 7-11](#)



- [Editing Operations Manager and Service Monitor IP Addresses, page 7-13](#)
- [Deleting a Service Monitor from Service Statistics Manager, page 7-14](#)

## Triggering Discovery

Before running discovery for the first time, ensure that:

- SSM Agent software is installed on each of the following:
  - The Operations Manager system from which you will obtain data.
  - Any Service Monitor system that has been added to the Operations Manager.

For more information, see [Installing SSM Agent on Another System, page 7-16](#).

- You have run the command described in [Configuring Service Statistics Manager to Connect with Operations Manager, page 7-10](#).

Discovery connects the SSM Agents that are installed on the Operations Manager and Service Monitor systems to the Service Statistics Manager server and creates the appropriate monitors on the agents.



**Note**

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

After you run discovery for the first time, to run it again, see [Retriggering Discovery, page 7-11](#).

- 
- Step 1** Disable Cisco Security Agent:
- 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 other systems, disable Cisco Security Agent on those systems too.
- Step 2** Select the **Administration** tab and scroll to Advanced.
- Step 3** In the Operations Manager/Service Monitor Details row, click the **Show** link. The Operations Manager/Service Monitor Details window appears.
- Step 4** Click the **Discover** button. The Discovery window appears.



**Note**

The Discover button is displayed only if you have the correct privilege. For more information, see [Managing User Roles and Privileges, page 6-8](#).

- Step 5** In the Operations Manager IP Address/Hostname field, enter the IP address or the hostname of the server where Operations Manager resides.
- Step 6** Enter the username for an Operations Manager user who has both of these privileges:
- Network Administrator
  - System Administrator



**Note**

Ensure that you enter a valid username and password for Operations Manager. Discovery fails if the information that you enter is not correct or if the user does not have the correct privileges. Service Statistics Manager does not verify this information when you enter it. For more information, see [Download Operations Manager Certificate in SSM Server, page 7-10](#).

- Step 7** Enter the password for the user.
- Step 8** Click **Discover** to trigger discovery. Service Statistics Manager displays a confirmation message.
- Step 9** Click **Close**.
- Discovery takes some time to complete. During this period, all the buttons on this screen are disabled. After discovery completes, the buttons are enabled.
- When discovery is complete, the required SSM Agents are connected to the Service Statistics Manager server and monitors are created. SSM Agent status is displayed as follows:
- Green—Agent is added and connected to the Service Statistics Manager server.
  - Red—Agent is either disconnected or not added to the Service Statistics Manager server.
- Step 10** 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.
- 

### Configuring Service Statistics Manager to Connect with Operations Manager

You must perform this procedure before you run discovery for the first time so that Service Statistics Manager obtains the necessary security certificate from Operations Manager. If you reinstall Operations Manager, you must also perform this procedure afterward to ensure that Service Statistics Manager obtains an updated security certificate. If Service Statistics Manager does not have an up-to-date security certificate, discovery will not complete; in this case, errors indicate license invalidity.



#### Note

The procedure below is also included in *Quick Start Guide for Cisco Unified Service Statistics Manager* (post-installation configuration steps). If you are not sure whether the command has been run, you can run it.

---

- Step 1** Determine whether Operations Manager uses an SSL port other than 443 (the default SSL port).
- Step 2** 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
- Step 3** Restart the Service Statistics Manager server. From the command prompt, type:  
**pw sys start**
- Step 4** Close any existing browser sessions.
- Step 5** Start your browser again and log in to Service Statistics Manager.
- 

### Download Operations Manager Certificate in SSM Server

Perform the steps given below to download Operations Manager (OM) Certificate in SSM server.

---

- Step 1** Open the OM login page through browser in the SSM server. Click **Certificate Error** and then **View Certificates**.
- Step 2** Go to **Details** tab and click **Copy to File**.

- Step 3** The Certificate Export Wizard opens. On “Welcome to the Certificate Export Wizard” page, click **Next**.
- Step 4** Click **Next** on “Export File Format” page.
- Step 5** **File to Export** page opens. Browse your file and click **Next**.
- Step 6** Click **Finish** and you will get a message “The Export was successful”.
- Step 7** Run the following command to import the downloaded certificates to keystore in SSM host.
- ```
keytool -import -alias OMCertificate -file <file> -keystore
%java_home%\lib\security\jssecacerts -storepass changeit
```
- Step 8** Re-start SSM server.

## Selecting an Operations Manager Username and Maintaining an Up-to-Date Password in Service Statistics Manager

The Operations Manager username and password that you must enter for Service Statistics Manager to perform discovery are defined in Common Services on the Operations Manager server:

- Username—Must have Network Administrator and System Administrator privileges.
- Password—Must not contain any of these characters: tilde (~), percent sign (%), ampersand (&), underscore (\_), plus sign (+), apostrophe (’), or comma (,).



**Note** If the password contains any of the characters listed above, discovery will fail.

The default Operations Manager administrative user, admin, has the necessary privileges. Although you can enter admin as the username in Service Statistics Manager, be aware that, during upgrade and reinstallation, Operations Manager users might be prompted to change the password for the admin user.

If the password changes for the Operations Manager user that you entered, Service Statistics Manager can no longer access Operations Manager. Although privileged Operations Manager users can add, update, and delete usernames and passwords at any time, in practice, it might not occur frequently. The password for the admin user can be changed during any reinstallation or upgrade to Operations Manager which, likewise, might not occur frequently.

For more information, including how to reset the password for the Operations Manager user in Service Statistics Manager, see *Release Notes for Cisco Unified Service Statistics Manager 1.2*.

## What to Do if SSM Agent Status Is Red

If SSM Agent status is red, do the following:

1. Verify that you have a valid username and password for Operations Manager. If you receive a new username and password, enter them when retriggering discovery. See [Retriggering Discovery, page 7-11](#).
2. Contact a user with Windows system administrator privilege who can perform the tasks listed in [SSM Agent Troubleshooting Tips, page 6-14](#).
3. Contact a Service Statistics Manager user in the Administration role; such a user can log into the SSM Administration Console and perform tasks listed in [Managing Remote Agents, page 6-12](#).

## Retriggering Discovery

You can retrigger discovery any time to add new agents or create new monitors.




---

**Note** If you reinstalled Operations Manager, you must perform the procedure documented in [Configuring Service Statistics Manager to Connect with Operations Manager, page 7-10](#) before you retrigger discovery.

---

- Step 1** Disable Cisco Security Agent:
- a. If Cisco Security Agent is running on your system, disable it.
  - b. If the Operations Manager or the Service Monitors that are being discovered are on other systems, disable Cisco Security Agent on those systems too.
- Step 2** Select the **Administration** tab and scroll to Advanced.
- Step 3** Click the Operations Manager/Service Monitor Details **Show** link. The Operations Manager/Service Monitor Details window appears.
- Step 4** Click **Discover**. The Discovery window appears.




---

**Note** The Discover button is displayed only if you have the correct privilege. For more information, see [Managing User Roles and Privileges, page 6-8](#).

---

- Step 5** In the Operations Manager IP Address/Hostname field, the IP address or the hostname for Operations Manager is displayed.




---

**Note** If the IP address has changed, see [Editing Operations Manager and Service Monitor IP Addresses, page 7-13](#).

---

- Step 6** Enter the username for an Operations Manager user.




---

**Note** Ensure that you enter a valid username and password for Operations Manager. Discovery fails if the information that you enter is not correct or if the user does not have the correct privileges. Service Statistics Manager does not verify this information when you enter it. For more information, see [Download Operations Manager Certificate in SSM Server, page 7-10](#).

---

- Step 7** Enter the password for the user.
- Step 8** Click **Discover**. Service Statistics Manager displays a confirmation message. Discovery takes some time to complete. During this period, a progress bar is displayed and the buttons on this screen are disabled. After discovery completes, the buttons are enabled.
- When discovery is complete, the required SSM Agents are connected to the Service Statistics Manager server and monitors are created. SSM Agent status is displayed as follows:
- Green—Agent is added and connected to the Service Statistics Manager server.
  - Red—Agent is either disconnected or not added to the Service Statistics Manager server. See [What to Do if SSM Agent Status Is Red, page 7-11](#).
- Step 9** 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.
-

## Editing Operations Manager and Service Monitor IP Addresses

Editing the IP addresses for Operations Manager and Service Monitor enables you to preserve existing data and continue reporting from a new IP address after any of the following occurs:

- You change the IP address of the server where Operations Manager or Service Monitor is installed.
- You move Operations Manager and/or Service Monitor to a different server and, consequently, to a different IP address.



### Note

How to maintain Operations Manager and Service Monitor while changing the IP address on the server or moving the product to a different server is outside of the scope of this document.

To change the IP address for Operations Manager only or Service Monitor only, use the appropriate procedure:

- [Editing the IP Address for the SSM Agent on the Operations Manager Server, page 7-13](#)
- [Editing the IP Address for an SSM Agent on a Server Where Service Monitor Is Installed, page 7-14](#)

To change the IP address when Operations Manager and Service Monitor are running on the same server, perform both of these procedures:

- [Editing the IP Address for the SSM Agent on the Operations Manager Server, page 7-13](#)
- [Editing the IP Address for an SSM Agent on a Server Where Service Monitor Is Installed, page 7-14](#)

### Editing the IP Address for the SSM Agent on the Operations Manager Server

After the IP address for the Operations Manager server has changed, update the IP address for Operations Manager in Service Statistics Manager. (To also update Service Monitor, if present, see [Editing the IP Address for an SSM Agent on a Server Where Service Monitor Is Installed, page 7-14.](#))

- Step 1** Select the **Administration** tab and scroll to Advanced.
- Step 2** Click the Operations Manager/Service Monitor Details **Show** link. The Operations Manager/Service Monitor Details window appears.
- Step 3** Select the check box for Operations Manager.
- Step 4** Click **Edit**. The Edit Operations Manager IP Address/Hostname window appears.



### Note

The Edit button is displayed only if you have the correct privilege. For more information, see [Managing User Roles and Privileges, page 6-8.](#)

- Step 5** Update the address or hostname in the Operations Manager IP Address/Hostname field.
- Step 6** Enter the username for an Operations Manager user.



### Note

Ensure that you enter a valid username and password for Operations Manager. Discovery fails if the information that you enter is not correct or if the user does not have the correct privileges. Service Statistics Manager does not verify this information when you enter it. For more information, see [Download Operations Manager Certificate in SSM Server, page 7-10.](#)

- Step 7** Enter the password for the user.

- Step 8** Click **Apply**. A confirmation window is displayed.
- Step 9** Click **OK**. A progress message is displayed. Service Statistics Manager takes some time to update and move Operations Manager monitors to the new IP address.



**Note** To move Service Monitor monitors also, see [Editing the IP Address for an SSM Agent on a Server Where Service Monitor Is Installed, page 7-14](#)

### Editing the IP Address for an SSM Agent on a Server Where Service Monitor Is Installed

After the IP address changes for the server where Service Monitor is installed, update the IP address for Service Monitor in Service Statistics Manager. You can use this procedure to update and move Service Monitor monitors from a server where Service Monitor only is installed or where Service Monitor and Operations Manager are installed. (To move Operations Manager monitors, see [Editing the IP Address for the SSM Agent on the Operations Manager Server, page 7-13.](#))

- Step 1** Select the **Administration** tab and scroll to Advanced.
- Step 2** Click the Operations Manager/Service Monitor Details **Show** link. The Operations Manager/Service Monitor Details window appears.
- Step 3** Select the check box for the Service Monitor.
- Step 4** Click **Edit**. The Edit Service Monitor IP window appears.



**Note** The Edit button is displayed only if you have the correct privilege. For more information, see [Managing User Roles and Privileges, page 6-8.](#)

- Step 5** Update the address in the Service Monitor IP field.
- Step 6** Click **Apply**. Service Statistics Manager displays a confirmation window.
- Step 7** Click **OK**. A progress message is displayed while Service Statistics Manager updates the monitors and moves them to the new IP address. This will take some time.

### Deleting a Service Monitor from Service Statistics Manager

- Step 1** Select the **Administration** tab and scroll to Advanced.
- Step 2** Click the Operations Manager/Service Monitor Details **Show** link. The Operations Manager/Service Monitor Details window appears.
- Step 3** Select the check box for the Service Monitor.
- Step 4** Click **Delete**. Service Statistics Manager displays a confirmation message and deletes the Service Monitor.

**Note**

The Delete button is displayed only if you have the correct privilege. For more information, see [Managing User Roles and Privileges, page 6-8](#).

## Working with Downloads

You can install the following downloads from the Administration tab:

- SSM Administration Console—Enables a user in the Administrator role to maintain users, groups, and access controls and to reset SSM Agents on remote systems.
- SSM Agent—Periodically polls for data on Operations Manager and Service Monitor systems and sends data to Service Statistics Manager.

## Installing the SSM Administration Console on Another System

The SSM Administration Console is automatically installed on the system with Service Statistics Manager. However, you can install it on another system.

**Step 1** Log in to the system where you want to install the SSM Administration Console.

**Step 2** Download the image and start the installation:

- a. Log in to Service Statistics Manager and select the **Administration** tab.
- b. Under Downloads, click **Admin.exe**. A File Download window appears.
- c. Click **Save** and save Admin.exe to the desktop.



**Note** Alternatively, click **Open** and go to [Step 3](#).

- d. Double-click **Admin.exe** to start the installation. An InstallShield window appears with a Welcome message.

**Step 3** Click **Next**. A License Agreement window appears.

**Step 4** Click **Accept**. An Information window appears.

**Step 5** Click **Next**. A Choose Destination Location window appears, displaying the default destination directory.

**Step 6** (Optional) To install the SSM Administration Console in a different directory, enter the full path to the directory or click **Browse** to select it.

Click **Next**. The Start Copying Files window displays information about current settings.

**Step 7** Click **Next**. The Setup Status window displays information during the installation; the Setup complete window appears with the Launch SSM Administration Console check box selected.

**Step 8** (Optional) Deselect the Launch SSM Administration Console check box. Click **Finish**. (For more information, see [Launching the SSM Administration Console, page 6-2](#).)

## Installing SSM Agent on Another System

SSM Agent is already automatically installed on the system with Service Statistics Manager. You must install SSM Agent on any other system where it is required but not yet installed. SSM Agent must be installed on:

- The single Operations Manager 9.0 system that Service Statistics Manager supports. If Operations Manager is installed on a system that is remote from Service Statistics Manager, you must install SSM Agent on the remote system.



---

**Note** After you install SSM Agent on the Operations Manager system, you must add Operations Manager to Service Statistics Manager. See [Triggering Discovery, page 7-9](#).

---

- Each Service Monitor 9.0 system that has been added to the Operations Manager system. If Service Monitor is installed on a system that is remote from Service Statistics Manager, you must install SSM Agent on the remote system.

---

**Step 1** Log in to the system where you want to install SSM Agent.

**Step 2** Download the image and start the installation:

- a. Log in to Service Statistics Manager and select the **Administration** tab.
- b. Under Downloads, click **Agent.exe**. A File Download window appears.
- c. Click **Save** and save Agent.exe to the desktop.



---

**Note** Alternatively, click **Open** and go to [Step 3](#).

---

- d. Double-click **Agent.exe** to start the installation. An InstallShield window appears with a Welcome message.

**Step 3** Click **Next**. A License Agreement window appears.

**Step 4** Click **Accept**. An Information window appears.

**Step 5** Click **Next**. A Choose Destination Location window appears, displaying the default destination directory.



---

**Note** If you are installing SSM Agent on a system where SSM Administration Console is installed, do not install SSM Agent in the directory with the SSM Administration Console.

---

**Step 6** To change the destination location, enter a new one or click **Browse** to find one.

**Step 7** Click **Next**. A Start Copying Files window appears.

**Step 8** Review settings for the installation; if they are correct, click **Next**. A Setup Status window appears, displaying setup progress. An Edit Data window appears.

**Step 9** Enter an unused port number for the agent and click **Next**. If you assign a port that is already in use, a message is displayed asking you to specify an unused port number. An Edit Data window appears.

**Step 10** Enter a display name for the agent and click **Next**. (The display name will appear on Windows Services and on Add/ Remove Programs displays.) The InstallShield Wizard Complete window appears.



**Step 11** Click **Finish**.

---

## Verifying the SSM Agent and SSM Administration Console Software Version

This procedure is provided for your information. You might not need to execute it.

- 
- Step 1** On the desktop, select **Start > All Programs > Accessories > Notepad**. The system opens an untitled Notepad window.
- Step 2** Select **File > Open** and navigate to the installation directory for SSM Agent or SSM Administration Console. The default paths are, respectively:
- C:\Program Files\Service Statistics Manager Agent\pronto\bin\
  - C:\Program Files\Service Statistics Manager Admin\agent\pronto\bin\version
- The exact path might vary based on the actual installation.
- Step 3** Select **All Files** in the Files of type field.
- Step 4** Open the file for the component to see the software version number:
- SSM Agent—AGENT\_VERSION
  - SSM Administration Console—Version
- 

## Uninstalling a Remote SSM Agent

To uninstall the local SSM Agent, see *Quick Start Guide for Cisco Unified Service Statistics Manager 1.1* and follow the instructions for uninstalling Service Statistics Manager.



### Note

You can uninstall only one instance of SSM Agent at a time.

---

- Step 1** Log in to the system as a Windows system administrator.
- Step 2** Select **Start > Settings > Control Panel**.
- Step 3** Double-click **Add or Remove Programs**.
- Step 4** In the Add or Remove Programs window, scroll to Cisco Unified Service Statistics Manager Agent and click **Change/Remove**. The system displays a confirmation message.
- Step 5** Click **OK**.
- Step 6** Follow the prompts on the Maintenance screen to complete the process.
- Step 7** From your desktop, navigate to the folder where you installed SSM Agent (for example, C:\Program Files\Service Statistics Manager Agent).
- Step 8** Delete the folder. Service Statistics Manager uninstalls all installed features of the agent, and the Maintenance Complete message is displayed.

**Step 9** Click **Finish**.

---

## Uninstalling a Remote SSM Administration Console

To uninstall the local SSM Administration Console, see *Quick Start Guide for Cisco Unified Service Statistics Manager 1.1* and follow the instructions for uninstalling Service Statistics Manager.

---

- Step 1** Log in to the system as a Windows system administrator.
  - Step 2** Select **Start > Settings > Control Panel**.
  - Step 3** Double-click **Add or Remove Programs**.
  - Step 4** In the Add or Remove Programs window, scroll to Cisco Unified Service Statistics Manager Admin and click **Change/Remove**. The system displays a confirmation message.
  - Step 5** Click **OK**.
  - Step 6** Follow the prompts on the Maintenance screen to complete the process.
  - Step 7** Click **Finish**.
-