CHAPTER A

User Inputs for Installation, Reinstallation, and Upgrade

This appendix provides information on the user inputs during Service Monitor installation, reinstallation, and upgrade.

This appendix contains:

User Inputs for Typical Installation

Table A-1 lists information you need to supply when installing Service Monitor for the first time in Typical mode.

Table A-1 User Inputs for New Installation: Typical

Settings	Value
Applications to install	Select the applications you want to install.
Password for *admin* user	No default values. Enter the admin password. For more information on passwords, see Password Information.
Password for System Identity account	No default values. Enter the System Identity account password. For more information on passwords, see Password Information.

Table A-1 User Inputs for New Installation: Typical (continued)

Settings	Value
Password for casuser	The password is generated randomly if you leave the field blank.
Mail Settings: • HTTPS port • Administrator's e-mail address • SMTP server name	**Note** Appears if IIS was detected on your system, and you indicated that you would like to avoid port conflict between IIS and Service Monitor by reconfiguring the default HTTPS port. Otherwise, Mail Settings appears only during a Custom installation. The default values are: • Port number 443—Enter a value from the range that is displayed. • *admin@domain.com*. • *localhost name*.

Table A-2 lists information you need to enter during an upgrade installation in Typical mode.

Table A-2 User Inputs for Upgrade Installation: Typical

Settings	Value
Password for casuser account	The password is generated randomly if you leave the field blank. (See Fixing Problems That Can Occur After You Change Passwords, page A-7.)
Applications to install	Select the applications you want to install.

Table A-3 lists information you need to enter while reinstalling in Typical mode.

Table A-3 User Inputs for Reinstallation: Typical

Settings	Value
Password for casuser account	The password is generated randomly if you leave the field blank. (See Fixing Problems That Can Occur After You Change Passwords, page A-7.)
Applications to install	Select the applications you want to install.

User Inputs for Custom Installation

Table A-4 lists the information you must enter while installing for the first time in Custom mode.

Table A-4 User Inputs for a New Installation: Custom

Settings	Value
Destination folder	The default location is *System drive:*\Program Files\CSCOpx. Select another location if you want to install in a specific location. We recommend that you specify a short path for the destination folder.
Applications to install	Select the applications you want to install.

Table A-4 User Inputs for a New Installation: Custom (continued)

Settings	Value
Password for users *admin* and *guest* (Mandatory)	No default values. Enter the admin and guest passwords. For more information on passwords, see Password Information.
Password for System Identity account (Mandatory)	No default values. Enter the system identity account password. For more information on passwords, see Password Information.
Password for user *casuser*	The password is generated randomly if you leave the field blank.
Password for the database (Mandatory)	Enter the database password. For more information on passwords, see Password Information.
Mail Settings: (Mandatory) • HTTPS port • Administrator's e-mail address • SMTP server name	The default values are: • *443*—If IIS is installed on your server, enter a port number from the range displayed. • *admin@domain.com*. • *localhost name*.
Data for the Self-signed Certificate: (Mandatory) • Country Code • State • City • Organization Name • Organization Unit Name • Host name • E-mail Address	By default, the self-signed certificate is generated using the organization that Windows is registered to, and the host name. You must enter the host name. You can leave the other fields blank. **Note** Common Services allows you to create security certificates to enable SSL communication between your client browser and management server. Self-signed certificates are valid for five years from the date of creation. When a certificate expires, the browser prompts you to install the certificate again from the server where you have installed Common Services. In Typical mode, this certificate is automatically generated.

Table A-5 lists the information you must enter during an upgrade installation in Custom mode.

Note If Service Statistics Manager is installed in your network and you change either of the following:

- The password for the user admin
- The destination location (the directory in which Service Monitor is installed)

Service Statistics Manager stops collecting data from Service Monitor. You can reenable data collection by performing the procedures that are documented in *Release Notes for Cisco Unified Service Statistics Manager 1.3*.

Table A-5 User Inputs for an Upgrade Installation: Custom

Settings	Value
Applications to install	Select the applications you want to install.
Password for users *admin* and *guest* (Optional)	You can change the passwords for the admin and guest users. To keep the existing passwords, leave the fields blank. (See Fixing Problems That Can Occur After You Change Passwords, page A-7.)
Password for System Identity account (Mandatory)	No default values. Enter the System Identity account password. For more information on passwords, see Password Information.
Password for the user casuser (Optional)	If you do not enter a password, the setup program generates a random password for you. (See Fixing Problems That Can Occur After You Change Passwords, page A-7.)
Password for the database (Optional)	Leave the fields blank to use the existing password.
Mail Settings: (Optional) • HTTPS port • Administrator's e-mail address • SMTP server name	You can choose to keep the existing information.
Data for the Self-signed Certificate: (Mandatory) • Country Code • State • City • Organization • Organization Unit Name • E-mail Address	You can change the Self-signed certificate information. By default, the installation program uses the existing self-signed certificate information. If you want to generate a new certificate, uncheck the Keep Existing Certificate check box, and enter the country code, state, city, company, organization, and host name for HTTPS. You must enter the host name. You can leave the other fields blank. **Note** Common Services allows you to create security certificates to enable SSL communication between your client browser and management server. Self-signed certificates are valid for five years from the date of creation. When the certificate expires, the browser prompts you to install the certificate again from the server where you have installed Common Services. In Typical mode, this certificate is automatically generated.

Table A-6 lists the information you must enter while reinstalling in Custom mode.

Note If you have Service Statistics Manager installed and you change either of the following:

- The password for the user admin
- The destination location (the directory in which Service Monitor is installed)

Service Statistics Manager stops collecting data from Service Monitor. You can reenable data collection by performing the procedures that are documented in *Release Notes for Cisco Unified Service Statistics Manager 1.3*.

Table A-6 User Inputs for Reinstallation: Custom

Settings	Value
Destination folder	The default location is *System drive:*\Program Files\CSCOpx. We recommend that you specify a short path for the destination folder.
Password for users *admin* and *guest* (Optional)	You can change the passwords for the admin and guest users. To keep the existing passwords, leave the fields blank. (If you change the password for the admin user, see Fixing Problems That Can Occur After You Change Passwords, page A-7.)
Password for System Identity account (Mandatory)	You can change the passwords for the System Identity account. To keep the existing passwords, leave the fields blank.
Password for user casuser (Optional)	If you do not enter a password, the setup program generates a random password for you. (See Fixing Problems That Can Occur After You Change Passwords, page A-7.)
Password for the database (Optional)	Leave the fields blank to retain the existing password.

Table A-6 User Inputs for Reinstallation: Custom (continued)

Settings	Value
Mail Settings: (Optional) • HTTPS port • Administrator's e-mail address • SMTP server name	You can choose to keep the existing information.
Data for the Self-signed Certificate: (Mandatory) • Country Code • State • City • Organization Name • Organization Unit Name • Hostname • E-mail Address	By default, the self-signed certificate is generated using the organization that Windows is registered to, and the host name. You must enter the host name. You can leave the other fields blank. **Note** Common Services allows you to create security certificates to enable SSL communication between your client browser and management server. Self-signed certificates are valid for five years from the date of creation. When the certificate expires, the browser prompts you to install the certificate again from the server where you have installed Common Services. In Typical mode, this certificate is automatically generated.

Password Information

This section contains the following topics:

Password Rules for a New Installation

The following rules apply for a new installation:

- In Typical mode, admin, casuser, and System Identity account passwords are mandatory. The installation program generates guest and database passwords randomly.
- In Custom mode, admin, guest, System Identity account, and database passwords are mandatory. You can either enter the casuser password or allow the installation program to randomly generate it.

Note you are allowed to change the built-in administrator password after installation.

Fixing Problems That Can Occur After You Change Passwords

During upgrade and reinstallation, you might change the passwords for the admin user and for the casuser account. Table A-7 lists the problems that can occur and provides steps you can take to resolve them.

Table A-7 Potential Problems

Password Changed	Potential Problem	Workaround
admin	Service Statistics Manager loses contact with Operations Manager and Service Monitor.	If Service Statistics Manager is installed in your network, reestablish contact by performing the procedures in *Release Notes for Cisco Unified Service Statistics Manager.*

Password Rules for an Upgrade Installation

During an upgrade installation, the casuser password is requested; other passwords are retained.

Password Rules for Reinstallation

The following rules apply for reinstallation:

- In Typical mode, the installation program retains passwords for admin, guest, and database.You can either enter the casuser password or allow the installation program to randomly generate it. (See Fixing Problems That Can Occur After You Change Passwords, page A-7.)
- In Custom mode, you can choose to enter new admin, guest, system identity account, and database passwords or retain most existing passwords. You can either enter the casuser password or allow the installation program to randomly generate it. (See Fixing Problems That Can Occur After You Change Passwords, page A-7.)

Password Descriptions

The types of passwords are as follows:

- Common Services admin Password, page A-7
- System Identity Account Password, page A-8
- Common Services Guest Password, page A-8
- Common Services Database Password, page A-8

Common Services admin Password

When entering the password for the admin user, include a minimum of five characters.

The admin user account is the default administrator; you must use the admin username and password to log in to Service Monitor after initial installation. (Be sure to write down the password.)

You are prompted to enter this password in both Typical and Custom modes of installation.

System Identity Account Password

When entering the System Identity account password, use a minimum of five characters.

You are prompted to enter this password in both Typical and Custom modes of installation.

The System Identity account is used in a multiple-server environment. Communication among multiple servers is enabled by a "trust" model addressed by certificates and shared secrets. For more information, see the Common Services online help.

Note You need a System Identity account to configure security with Cisco Secure ACS (which must be installed on a separate server) and to configure the DCR in master and slave mode. (Operations Manager supports the DCR; Service Monitor does not support it.)

Common Services Guest Password

When entering the password for the Common Services guest account, use a minimum of five characters.

Use this password to log into the Common Services server as a guest user. You are prompted to enter this password in Custom installation mode. In Typical mode, this password is randomly generated.

Common Services Database Password

When entering database passwords:

- Use a minimum of five characters and a maximum of 15 characters.
- Do not start the password with a number.
- Do not insert spaces between characters.
- Do not use any special characters.

Changing Passwords

These topics explain how to change the passwords for the admin user and casuser accounts using utilities (or the Common Services user interface, if possible):

- Changing the Common Services Admin Password
- Changing the casuser Password

Changing the Common Services Admin Password

Note If you change the admin password and Service Statistics Manager is in your network, it will lose contact with Operations Manager and Service Monitor. To reestablish contact, perform the procedures in *Release Notes for Cisco Unified Service Statistics Manager*.

You can change your Common Services Admin password either by using the Common Services user password recovery utility or from the user interface.

- Changing the Admin Password Using the Password Recovery Utility
- Changing the Admin Password from Common Services

Changing the Admin Password Using the Password Recovery Utility

Step 1 Stop the daemon manager by entering the following at the shell prompt:

```
net stop crmdmgtd
```

Step 2 Go to *NMSROOT*\bin directory and enter:

NMSROOT/**bin/perl** *NMSROOT*/**bin/ResetPasswd.pl** *userName*

where *NMSROOT* is the directory where you have installed Service Monitor.

Step 3 In the dialog that appears, enter the new password.

Step 4 Start the daemon manager by entering the following at the command prompt:

```
net start crmdmgtd
```

Changing the Admin Password from Common Services

Step 1 Log in with username admin.

Step 2 Select **Administration > Server Administration (Common Services) > Security > Local User Setup**.

The Local User Setup page appears.

Step 3 Click **Modify My Profile**.

The My Profile window appears.

Step 4 Enter the password in the Password field.

Step 5 Re-enter the password in the Verify field.

Step 6 Enter the e-mail ID in the E-mail field.

Step 7 Click **OK**.

Changing the casuser Password

Caution Changing the casuser password might cause Service Monitor credential failure when accessing a Unified Communications Manager version 4.x system for which Windows authentication is configured. Be prepared to log into the Windows server where Unified Communications Manager is installed to update the casuser password to match the new casuser password that you enter.

Step 1 At the command prompt, enter:

*NMSROOT***setup\support\resetCasuser.exe**

Three options are displayed:

1. Randomly generate the password
2. Enter the password
3. Exit.

Step 2 Enter **2**, and press **Enter**.

A message appears, prompting you to enter the password.

Step 3 Confirm the password.

If a local user policy is configured on the Service Monitor server and you enter a password that does not match the password policy, the application exits with an error message. For more information, see Setting up Local User Policy in the Common Services online help.