



APPENDIX **A**

User Input for Installation and Reinstallation

This appendix provides information on user input for Operations Manager installation, reinstallation, and silent installation.

This appendix contains:

- [User Input for a Typical Installation, page A-1](#)
- [User Input for a Custom Installation, page A-2](#)
- [User Input for a Silent Installation, page A-5](#)
- [Password Information, page A-6](#)

User Input for a Typical Installation

[Table A-1](#) lists information you need to supply when installing Operations Manager for the first time in Typical mode.

Table A-1 *User Input for New Installation: Typical*

Settings	Value
Applications to install	Select the applications you want to install.
Password for <i>admin</i> 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 Input for New Installation: Typical (continued)

Settings	Value
Password for casuser	If you leave the field blank, the password is generated randomly.
Mail Settings: <ul style="list-style-type: none"> • HTTPS port • Administrator's e-mail address • SMTP server name 	<p>Appears if IIS was detected on your system, and you indicated that you would like to avoid port conflict between IIS and Operations Manager by reconfiguring the default HTTPS port. Otherwise, Mail Settings appears only during a Custom installation.</p> <p>The default values are:</p> <ul style="list-style-type: none"> • Port number 443—Enter a value from the range that is displayed. • admin@domain.com • localhost name <p>If you change the HTTPS port that Operations Manager uses, see Ensuring that Service Statistics Manager Uses the Correct HTTPS Port to Contact Operations Manager, page 2-5.</p>

Table A-2 lists information you need to enter when reinstalling in Typical mode:

Table A-2 User Input for Reinstallation: Typical

Settings	Value
Password for casuser account	If you leave the field blank, the password is generated randomly. (See Fixing Problems That Can Occur When You Change Passwords, page A-6 .)
Applications to install	Select the applications you want to install.

User Input for a Custom Installation

Table A-3 lists the information you must enter when installing for the first time in Custom mode.

Table A-3 User Input for a New Installation: Custom

Settings	Value
Destination folder	<p>The default location is <i>System drive:\Program Files\CSCOPx</i>. If you want to install in a specific location, Select another location.</p> <p>We recommend that you specify a short path for the destination folder.</p>
Applications to install	Select the applications you want to install.
Password for users <i>admin</i> and <i>guest</i> (Mandatory)	No default values. Enter the admin and guest password. For more information on passwords, see Password Information .
Password for System Identity account (Mandatory)	<p>No default values.</p> <p>Enter the system identity account password. For more information on passwords, see Password Information.</p>

Table A-3 *User Input for a New Installation: Custom (continued)*

Settings	Value
Password for user <i>casuser</i>	If you leave the field blank, the password is generated randomly.
Password for the database (Mandatory)	Enter the database password. For more information on passwords, see Password Information .
Mail Settings (Mandatory): <ul style="list-style-type: none"> • HTTPS port • Administrator's e-mail address • SMTP server name 	<p>The default values are:</p> <ul style="list-style-type: none"> • 443—If IIS is installed on your server, enter a port number from the range displayed. • admin@domain.com • localhost name <p>Any time you change the HTTPS port that Operations Manager uses, see Ensuring that Service Statistics Manager Uses the Correct HTTPS Port to Contact Operations Manager, page 2-5.</p>
Data for the Self-signed Certificate (Mandatory): <ul style="list-style-type: none"> • Country Code • State • City • Organization Name • Organization Unit Name • Host name • E-mail Address 	<p>By default, the self-signed certificate is generated using the organization that Windows is registered to, and the hostname.</p> <p>You must enter the hostname. You can leave the other fields blank.</p> <p>Common Services allows you to create security certificates to enable SSL communication between your client browser and management server.</p> <p>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 on which Common Services resides. In Typical mode, this certificate is automatically generated.</p>

If Service Statistics Manager is installed in your network, it will stop collecting data from Operations Manager if you change either of the following:

- The user admin password
- The destination location (the directory in which Operations Manager is installed)

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-4](#) lists the information you must enter while reinstalling in Custom mode.

**Note**

If Service Statistics Manager is installed in your network, it will stop collecting data from Operations Manager if you change either of the following:

- The user admin password
- The destination location (the directory in which Operations Manager is installed)

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-4 User Input for Reinstallation: Custom

Settings	Value
Destination folder	The default location is <i>System drive:\Program Files\CSCOPx</i> . We recommend that you specify a short path for the destination folder.
Password for users <i>admin</i> and <i>guest</i> (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 When You Change Passwords , page A-6.
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 When You Change Passwords , page A-6.
Password for the database (Optional)	Leave the fields blank to retain the existing password.
Mail Settings (Optional): <ul style="list-style-type: none"> • HTTPS port • Administrator's e-mail address • SMTP server name 	You can choose to keep the existing information. If you change the HTTPS port that Operations Manager uses, see Ensuring that Service Statistics Manager Uses the Correct HTTPS Port to Contact Operations Manager , page 2-5.
Data for the Self-signed Certificate (Mandatory): <ul style="list-style-type: none"> • 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 hostname. You must enter the hostname. You can leave the other fields blank. 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.

User Input for a Silent Installation

The answer file is an ASCII file that provides the required inputs for silent or unattended installations. Operations Manager only supports new installations and does not support uninstall/reinstall in silent mode.

Modify the sample text response file with values to suit the desired configuration for your system. The file is located in C:\CSCOpX. The answer file contains the following name=value pairs:

```
# Sample answerfile
#--- begin answerfile
adminPassword=admin
destination=C:\CSCOpX
systemIdentityAccountPassword=admin
casuserPassword=casuser
#--- end of answerfile
```

To improve security, be sure to change the adminPassword from the default value, which is admin.

We recommend that you rename or relocate this file before running the silent-process. Rename the file to something distinguishable, such as *local-om-install*, and relocate it to a temporary folder.



Caution

Ensure you use 8.3 DOS naming conventions for the destination path and that there are no quotes in the destination value. For example, C:\Progra~1\CSCOpX. If you see the following error, you need to remove any quotes in the destination value and retry the installation: Installation cannot create directory "C:\Program Files\CSCOpX". You may not have permissions on the directory or you have specified a read-only device. Please choose another destination folder.



Tip

To find the short path of a directory, type **command** at the command prompt.

Table A-5 lists information you need to supply in the response file in order to install Operations Manager using a silent installation.

Table A-5 User Input for Silent Installation

Settings	Value
adminPassword	No default values. Enter the <i>admin</i> password. It is only used during a fresh installation; reinstallation in quiet mode does not change the password.
systemIdentityAccountPassword	No default values. Enter the System Identity account password.
destination	If no value is specified, the default location will be C:\Program Files\CSCOpX.
casuserPassword	If you leave the field blank, the password is generated randomly.

Password Information

This topic provides information on the usage of passwords during installation.

It contains:

- [Password Rules for a New Installation, page A-6](#)
- [Fixing Problems That Can Occur When You Change Passwords, page A-6](#)
- [Password Rules for a Reinstallation, page A-6](#)
- [Password Descriptions, page A-7](#)
- [Changing Passwords, page A-8](#)

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.

Fixing Problems That Can Occur When You Change Passwords

During reinstallation, you might change the passwords for the admin user and for the casuser account. [Table A-6](#) lists the problems that can occur and provides steps you can take to resolve them.

Table A-6 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 procedures in Release Notes for Cisco Unified Service Statistics Manager 1.3 .
casuser	Operations Manager credentials fail when accessing a Unified Communications Manager version 4.x system for which Windows authentication is configured.	The casuser password on the Operations Manager server must match the casuser password on the Unified Communications server. Log in to the Windows server where Unified Communications Manager is installed and update the casuser password. If you do not know the casuser password on the Operations Manager server, change it. See Changing the casuser Password .

Password Rules for a 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 When You Change Passwords, page A-6](#).
- In Custom mode, you can chose 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 When You Change Passwords, page A-6](#).

Password Descriptions

The types of passwords are as follows:

- [Common Services Admin Password, page A-7](#)
- [System Identity Account Password, page A-7](#)
- [Common Services Guest Password, page A-7](#)
- [Common Services Database Password, page A-7](#)

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 Operations Manager after initial installation. (Be sure to write down the password.)

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

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 installation modes.

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 online help for Common Services.

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 5 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. To re-establish contact, perform the procedures given in [Release Notes for Cisco Unified Service Statistics Manager 1.3](#).

You can change your Common Services Admin password using either of the following methods:

- [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

To change the Admin password using the Password Recovery utility:

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

```
net stop crmdmgt
```

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

```
NMSROOT\bin\resetpasswd username
```

NMSROOT is the directory where you have installed Operations Manager.

A message appears:

```
Enter new password for username:
```

Step 3 Enter the new password for *username*.

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

```
net start crmdmgt
```

Changing the Admin Password from Common Services

To change the admin password from Common Services:

-
- Step 1** Log in to Operations Manager as the admin user.
- Step 2** Select the **Administration > Server Administration (Common Services) > Security > Local User Setup**.
- The Local User Setup page appears.
- Step 3** Click **Modify My Profile**.
- The My Profile popup 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 Operations Manager credential failure when accessing a supported 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. (For supported Unified Communications Managers, see [Supported Devices Table for Cisco Unified Operations Manager](#).)

To change the casuser password:

-
- 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 Operations Manager 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 see online help for Common Services.
-

