



APPENDIX C

Helpful Reference Information

This appendix contains the following sections:

- [Understanding User Accounts, page C-1](#)
- [Recommendations for Creating Strong Passwords, page C-2](#)
- [Changing the Default Location for Temporary Files, page C-3](#)
- [Exporting Data from IPS MC 2.2, page C-4](#)
- [Importing IPS MC 2.2 Data, page C-4](#)

Understanding User Accounts

Several security management and application management operations are potentially disruptive to the network or to the applications themselves, and must be protected. To prevent such operations from being used accidentally or maliciously, Common Services and Security Manager use a multilevel security system that allows access to certain features only to users who can authenticate themselves at the appropriate level. For this reason, there are three predefined kinds of login IDs.

See the [Installing and Getting Started With CiscoWorks LAN Management Solution 3.0](#) for detailed information about these user accounts:

- **admin**—The admin login is equivalent to a Windows administrator and provides access to all Common Services and Security Manager tasks. You must enter the password during installation.
- **casuser**—The casuser login is equivalent to a Windows administrator and provides access to all Common Services and Security Manager tasks.
- **<System Identity>**—The System Identity login is equivalent to a Windows administrator and provides access to all Common Services and Security Manager tasks.



Note

- You can choose whether to enter the System Identity username and password after installation. Communication among your servers relies on a trust model that uses certificates and shared secrets. The System Identity login is trustworthy to other servers when you use a multiserver setup and therefore facilitates communication between servers that are part of a domain. There can be *one* System Identity login account on a server.
- If you use Cisco Secure Access Control Server (ACS) for user authentication, you must use it to assign all CiscoWorks privileges to the System Identity user. If you do *not* use ACS for user authentication, the System Identity user must be a local user with system administrator privileges.

An administrator can create additional unique login IDs for users.

Understanding User Account Security Levels

You determine user security levels when you grant login access to Common Services, Security Manager, or other applications that you install. Each login account is associated with one or more roles. For detailed information about user roles and their associated permissions, see the “Default Associations Between Permissions and Roles in Security Manager” topic in the Security Manager online help or read the equivalent section on Cisco.com here:

http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/3.2/user/guide/aduser.html#wp23997.

Understanding User Permissions

The Security Manager server authenticates the username and password of every user who logs in. When you log in to Security Manager, the options displayed in the GUI depend on the roles assigned to your username. A user with system administrator privileges can access all features, while other users see only a subset of features.

Security Manager user authentication and authorization come from Common Services. See the Common Services online help for details.

Recommendations for Creating Strong Passwords

Never write passwords down, on paper or online. Instead, create passwords that you can remember easily but no one can guess easily. One way to do this is create a password that is based on a song title, affirmation, or other phrase. For example, the phrase could be “this may be one way to remember” and the password could be “TmB1w2R!” or “Tmb1W>r~” or some other variation.



Note

Do not use either of those examples as passwords.

Characteristics of a Strong Password

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z).
- Contain numerals and punctuation as well as letters (e.g., 0-9, !@#%&*(~+|= \ { } [] : ; ' < > ? , . /).
- Are at least five alphanumeric characters long.
- Are not a word in any language, and are not slang, dialect, or jargon.
- Are not based on personal information, such as the names of family members.

Characteristics of a Weak Password

A poor, weak password has the following characteristics:

- Contains fewer than eight characters.
- Is a word found in a dictionary (English or foreign).

- Is any other term that is easily guessed or found in common usage, such as:
 - The name of family, pet, friend, coworker, or fantasy character.
 - A computing term or name, such as a command, site, company, model, or application.
 - Is a birthday or another kind of personal information, such as an address or telephone number.
 - Is a predictable letter pattern or number pattern, such as aaabbb, qwerty, zyxwvuts, or 123321.
 - Any of the above, spelled backwards.
 - Any of the above, preceded or followed by a digit, such as secret1 or 1secret.

Password Security Basics

Never reveal a password.

In addition, you must:

- Never talk about a password in front of others.
- Never hint at the format of a password (such as “my family name”).
- Never share a password with family members.
- Never use characters from outside the standard ASCII character set. Some symbols, such the pound sterling symbol (£), are known to cause login problems on some systems.

Changing the Default Location for Temporary Files

The installation utility for Security Manager uses your Windows temporary directory, which Windows associates by default with your C:\ drive. If your target server has more than one local disk drive, and if you have less free space on your C:\ drive than is specified in [Server Requirements, page 2-3](#), you might edit the environment variables for your server so that C:\ is not the default location for temporary files.

To see the environment variables for your sever and edit their values so that you can change the default location for storing temporary files:

Step 1 Right-click **My Computer**, then select **Properties** from the shortcut menu.

Step 2 Click the **Advanced** tab.

Step 3 Click **Environment Variables**.

The Environment Variables window contains one area for variables that are associated with the active username in the current login session, and another area for variables that always apply to your server. Both of these areas can include variables (with names like TEMP, TMP, and TMPDIR) that tell Windows and other software where to store temporary files.

Step 4 Select the name of a variable that you want to change.

Step 5 Click **Edit**, change the value for that variable, then click **OK**.

Exporting Data from IPS MC 2.2

If you migrate data from an installation of IPS MC 2.2, and if the IPS MC server is the *same* server on which you install Security Manager, you must do the following *before* you start installing Security Manager.

**Note**

- We do not support Security Manager coexistence on the same server with VMS 2.3, the suite of applications of which IPS MC is one component. We recommend that you follow all the guidelines in [Chapter 3, “Preparing a Server for Installation.”](#)
- Available space (on the IPS MC server disk partition where you will store your backup) must not be less than the size of the IPS MC database.
- If the IPS MC database that you import contains Security Monitor sensor alarms or syslog events, Security Manager ignores those alarms and events when it imports the database. Security Manager cannot use any records that are associated with Security Monitor.

-
- Step 1** Back up your IPS MC server database files. See http://www.cisco.com/en/US/docs/security/security_management/vms/2.3/install/guide/windows/qsch4.html#wp1038598.
- Step 2** Move the backed-up database from CSCOPx\MDC\backup to a secure volume.
-

Importing IPS MC 2.2 Data

Before You Begin

If you migrate data from IPS MC 2.2 to Security Manager 3.2, you can complete the following procedure successfully only *after* you:

1. Complete the procedure described in [Exporting Data from IPS MC 2.2, page C-4](#).
2. Complete the Security Manager installation. See [Installing Server Applications, page 4-1](#).

**Note**

- If the IPS MC database that you import contains Security Monitor sensor alarms or syslog events, Security Manager ignores those alarms and events when it imports the data. Security Manager cannot use any records that are associated with Security Monitor.
- When you import IPS MC data into Security Manager:
 - Do not use spaces anywhere in the path.
 - Do not use a path that is longer than 67 characters, including the drive letter and any backslash characters.
 - We recommend that available space on the server disk partition be at least twice the size of the database file that you import.

To transfer IPS MC 2.2 data to Security Manager 3.2:

-
- Step 1** Move to your Security Manager server a copy of the IPS MC backup that you saved on a secure volume.
- Step 2** Note the full pathname of the newly transferred copy of your backup file. Example:
c:\backup_2.2\20070104135727
- Step 3** Execute the perl script supplied with Cisco Security Manager to create a special file called the IpsCredentialFile. The IpsCredentialFile is an XML file with IPS credentials that CiscoWorks 3.1 can import via the Device Credentials Repository. Example: c:\progra~1\cscopx\bin>
c:\progra~1\cscopx\mdc\bin\ExportIpsCredentials.pl c:\backup_2.2\20070104135727
c:\IpsCredentials.xml
- Step 4** Log in to your Security Manager server and open CiscoWorks.
- Step 5** Navigate to **Common Services > Device and Credentials > Device Management**.
- Step 6** Click the **Bulk Import** button. The Import Devices dialog box appears.
- Step 7** In the Import File Name field, enter or browse to the IpsCredentialFile that you created earlier in this procedure.
- Step 8** In the Format Selection field, select **XML**.
- Step 9** Enter Scheduling and Job Info information as desired.
- Step 10** Click the **Import** button. The data that you exported from IPS MC 2.2 are imported into the CiscoWorks Device Credential Repository.
- Step 11** Export your IPS devices from the Device Credential Repository (DCR). For detailed instructions on how to export devices from DCR, see the *User Guide for CiscoWorks Common Services 3.1* at the following URL:
http://www.cisco.com/en/US/docs/net_mgmt/ciscoverks_common_services_software/3.1/user/guide/dcr.html#wp1378454.
- Step 12** Add your IPS devices to Security Manager 3.2 from the file you exported from DCR by using the “Add Device From File” option in the New Device wizard.
-

The time required to import IPS MC data varies according to the size of the database file and the percentage of its records that must be discarded because they are associated with Security Monitor.

