

Chapter 5 Using the Security Features

Chapter 4 explained how to set up applications for software metering. This chapter explains how to use the security features available with SiteMeter.

Introduction

SiteMeter offers a number of features that secure and protect your network software by preventing viruses and unauthorized access to local drives.

The file integrity scanning feature guards your LAN against potential infection from viruses. A virus is an additional process that attaches itself to or maliciously alters an executable file. A virus can cause many problems on your network, such as:

- ☐ Renaming or destroying data
- ☐ Creating a program that can cause the workstation to hang or possibly crash
- ☐ Causing a program to run in a continuous loop
- ☐ Making a program consume more memory than is necessary

With file integrity scanning you reduce the risk of virus infection.

SiteMeter provides other security features related to local drive use. You can control which users have access to their local drives to prevent unauthorized software and program installation. With SiteMeter, you can define rights to local execution for all users or for specific users.

Access to Security Functions

The security functions are accessed in two ways:

- ☐ by choosing the Security button from the tool bar, or
- ☐ by choosing Security from the Administration menu.

What's in this Chapter

The following chart describes the sections in this chapter:

SECTION	DESCRIPTION
File Integrity Scanning	Describes procedures for defining authorized files on your network.
Running Unauthorized Files	Describes procedures for allowing unauthorized files to run on your network.
Specifying the File Scan Interval.	Describes procedures for instructing SiteMeter how often it should check for unauthorized files on the network.
Specifying the Security Scan Interval	Describes procedures for instructing SiteMeter how often it should check for network users who have not loaded Swatcher.
Disabling Local Drives	Describes procedures for denying users any access to their local drives.
Restricting Local Execution	Describes procedures for disallowing users to execute applications from their local drives.
Specifying Security Exceptions	Describes procedures for determining which users are allowed to use the network without loading Swatcher.

File Integrity Scanning

To prevent virus infection, SiteMeter checks files for changes before allowing them to execute. The first step is registering (or authorizing) your files for scanning. Once you register your software, only files that have a fingerprint matching the fingerprint registered are allowed to run.

Every time the file is run (or at specified intervals), the fingerprint value is recalculated and compared to the value that had been originally registered. If the two do NOT match, the file is not allowed to run.

With this method of file protection it is not necessary to recognize a particular virus strain. Any byte change is detected and treated as a potential virus.

This section describes the two steps to file integrity scanning:

- ☐ Register (or Authorize) the files
- ☐ Set the File Integrity Scan Interval

What Are Authorized Files?

An authorized file is a file that has been registered for file integrity scanning. If a file is not an authorized file and you do NOT allow unauthorized files to be run, it will not be allowed to execute.

Metering records the characteristics of each authorized file and stores this value in the NetWare bindery.

With the security features included in SiteMeter, you can:

- ☐ **Add** - new files to the list of authorized files.
- ☐ **Reprotect** - files that have been changed, as in the case of an upgrade.
- ☐ **Delete** - files from the authorized files list.

Adding Authorized Files

To register a file for virus protection, you need to add it to the list of authorized files.

Use the following procedure to add a file to the authorized files list.

- 1. Choose Security from the Administration menu. From the sub-menu that is displayed, choose the Define Authorized Files command.**

The Define Authorized Files dialog box is displayed, as shown in Figure 5-1.

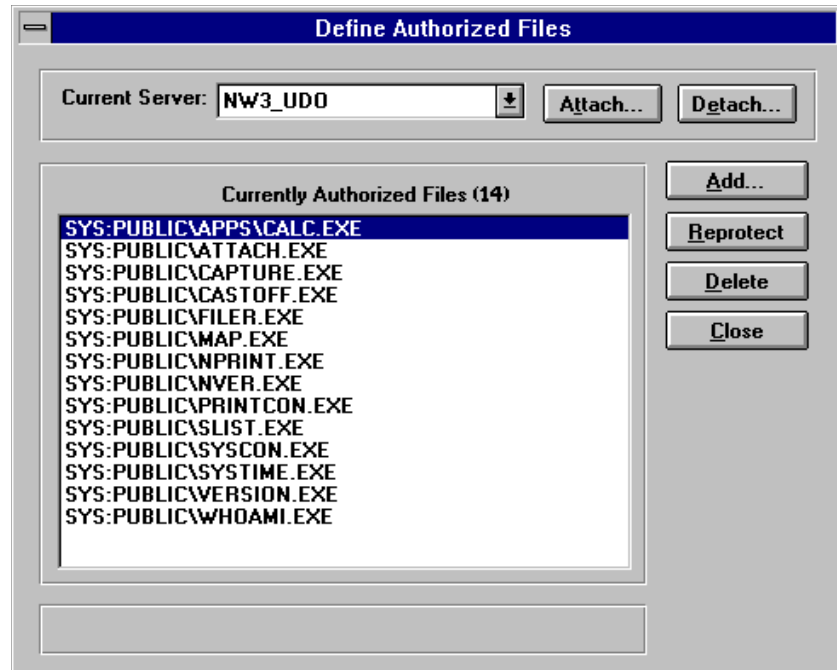


Figure 5-1: Defining Authorized Files

From this dialog box you can:

- ☐ **Add** files to the Currently Authorized Files list.
- ☐ **Reprotect** files that are already authorized.
- ☐ **Delete** files that have been authorized.

2. Choose the Add button.

The Browse for Files to Authorize dialog box is displayed, as in Figure 5-2.

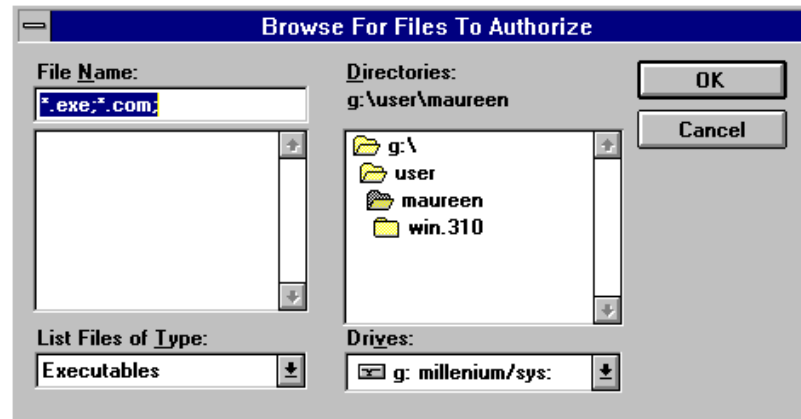


Figure 5-2: Browsing for Files to Authorize

3. **Select the desired drive and directory.**
4. **Select a file from the File Name list.**

You can select all the files in this directory by pointing to the first file in the File Name list, holding down the left mouse button and dragging the cursor down. This highlights all the files that will be authorized.

5. **Choose the OK button.**

Any files you just chose now appear in the Currently Authorized Files list.

Reprotecting Authorized Files

You can reprotect a previously authorized file, which should be done for applications that have been upgraded. Reprotecting a file recalculates the file's checksum value.

NOTE:

If you are using Swatcher to meter and file protect your network, make sure Swatcher is not loaded when reprotecting a file.

Use the following procedure to reprotect a file.

1. **Choose Security from the Administration menu. From the sub-menu that is displayed, choose the Define Authorized Files command.**

The Define Authorized Files dialog box is displayed.

2. **Choose the file you wish to reprotect.**

3. Choose the Reprotect button.

A message is displayed at the bottom of the window indicating that the file is being updated for protection.

NOTE:

You can also reprotect a file by double clicking on the appropriate filename in the Currently Authorized Files list.

Deleting Authorized Files

You can remove authorization from a file. This does not remove the file from the network; it merely removes the SiteMeter security protection features from the file. When you do this, the file will be permitted to execute regardless of any changes made to the file. (It will not, however, be allowed to run at all when unauthorized files cannot be run.)

Use the following procedure to remove an authorized file from registration for file integrity scanning.

1. Choose Security from the Administration menu. From the sub-menu that is displayed, choose the Define Authorized Files command.

The Define Authorized Files dialog box is displayed.

2. Select the file to be deleted.**3. Choose the Delete button.**

A prompt is displayed, as in Figure 5-3, asking you to verify your choice to delete the file protection from this file.



Figure 5-3: Removing File Protection

4. Choose the Yes button if you wish to remove the file protection.

Running Unauthorized Files

What is “Run Unauthorized Files”?

This option instructs SiteMeter whether or not to permit execution of currently unauthorized files on the network. Using this option prevents unauthorized software from being run on the network. When this option is enabled, only the listed application files are allowed to run. The Specify Policy dialog box lets you specify on which file server(s) you wish to allow or disallow unauthorized files to run.

NOTE:

Make sure SITEMETR.EXE is always an authorized file. If SITEMETR.EXE is not an authorized file and you choose to use the unauthorized files option, you will NOT be able to run SiteMeter. Also make sure LOGIN.EXE is always an authorized file. If LOGIN.EXE is not an authorized file and you choose to use the unauthorized files option, users will be unable to log in to the network.

Using Run Unauthorized Files

Use the following procedure to specify whether or not unauthorized files should be run.

1. **Choose Security from the Administration menu. From the sub-menu that is displayed, choose the Specify Policy command.**

The Specify Policy dialog box is displayed, as shown in Figure 5-4.

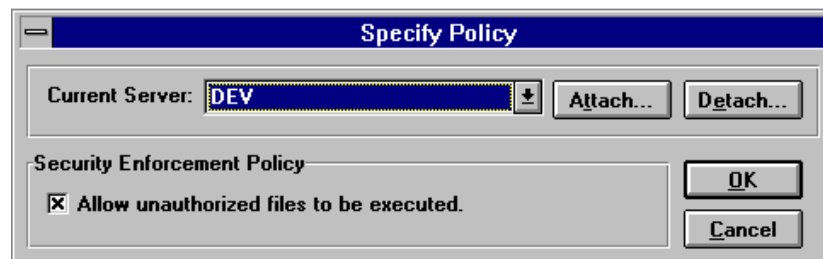


Figure 5-4: Running Unauthorized Files

This dialog box allows you to specify on which file servers you allow unauthorized files to run.

The Current Server list box automatically displays your current server. You can attach to or detach from other file servers using the Attach and Detach buttons. (Refer to “Attaching to and Detaching from File Servers” in Chapter 4.)

NOTE:

The default is to have the option enabled. Step 2 disables this option.

- 2. If you do not wish to allow unauthorized files to be executed, select the “Allow unauthorized files to be executed” option.**

The “x” disappears from the box, indicating that you do not allow files that are not authorized to run on the network.

- 3. Choose the OK button to save your change and exit the dialog box.**

Specifying the File Scan Interval

What is “Specify File Scan Interval”?

File Scan Interval tells SiteMeter how often to check the executable program against the registered copy of that file.

To check a file every time it is requested, set the File Scan Interval to zero (0). If your file server has heavy network traffic, however, you may want to adjust this value to a figure more appropriate for your needs.

The value can range from 0 to 1440 minutes (once every 24 hours). The value you set applies to ALL authorized files.

Regardless of the value, the file is always checked against the registered copy the first time it is requested. If the field is set to 15 minutes, however, no matter how many times the file is executed it will not be checked again for 15 minutes after the first check. The first attempt to run the software after the 15 minute interval will reset the time interval.

For example, you run LOTUS for the first time at 11:00 a.m. at which time SiteMeter checks the file. The next time the file will be checked will be the first time it is requested after 11:15 a.m. (if the File Scan Interval has been set to 15).

Specifying the File Scan Interval

Use the following procedure to specify the file scan interval.

1. **Choose Security from the Administration menu. From the sub-menu that is displayed, choose the Specify File Scan Interval command.**

The Specify File Scan Interval dialog box is displayed, as in Figure 5-5.

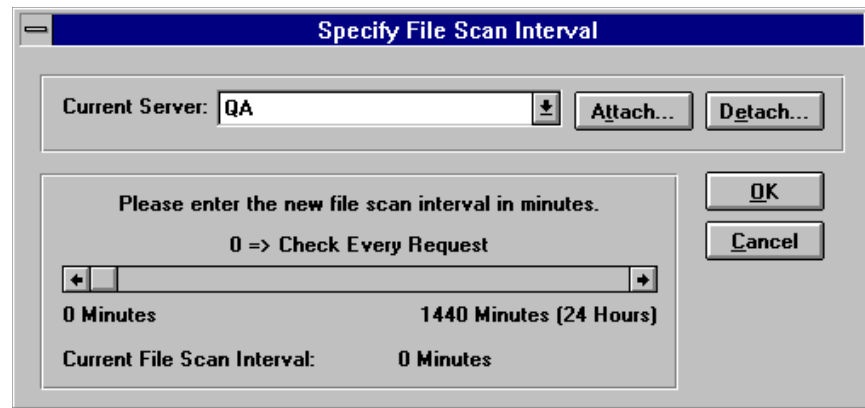


Figure 5-5: Specifying the File Scan Interval

From this dialog box you can:

- ☐ Set the scan interval
 - ☐ Attach to/Detach from a file server (refer to “Attaching to and Detaching from File Servers” in Chapter 4 for more instructions)
2. **Use one of the following methods to set the interval and specify how frequently SiteMeter checks the executable:**
 - ☐ Click on the slide bar arrows to increment/decrement the value in one minute intervals,
 - ☐ Slide the slide bar to the appropriate value, or
 - ☐ Click on either side of the slide bar to increment/decrement the value by 10 minute intervals.
 3. **Once you have selected the appropriate time, choose the OK button.**

Specifying the Security Scan Interval

What is “Specify Security Scan Interval”?

The Security Scan Interval is the length of time between Security Scan checks. This value indicates how frequently SiteMeter scans the network to be sure users on the network either have loaded the Swatcher TSR or are listed as Security Exceptions.

If a user is not a Security Exception and has not loaded Swatcher, SiteMeter sends a NetWare Send message to the user indicating that he or she will be logged off the file server in 30 seconds. This allows the user enough time to save his or her work before being disconnected automatically from the network. The user must load Swatcher before logging in to the network again.

NOTE:

Trying to load Swatcher after receiving the 30 second warning will not prevent the user from being logged out.

*Setting the value to 0 minutes informs metering not to check if Swatcher is loaded. **This is mandatory if you are NOT using the Swatcher TSR as your choice to meter and file protect your network.***

Specifying the Security Scan Interval

Use the following procedure to specify the security scan interval.

1. **Choose Security from the Administration menu. From the sub-menu that is displayed, choose the Specify Security Scan Interval command.**

The Specify Security Scan Interval dialog box is displayed, as in Figure 5-6.

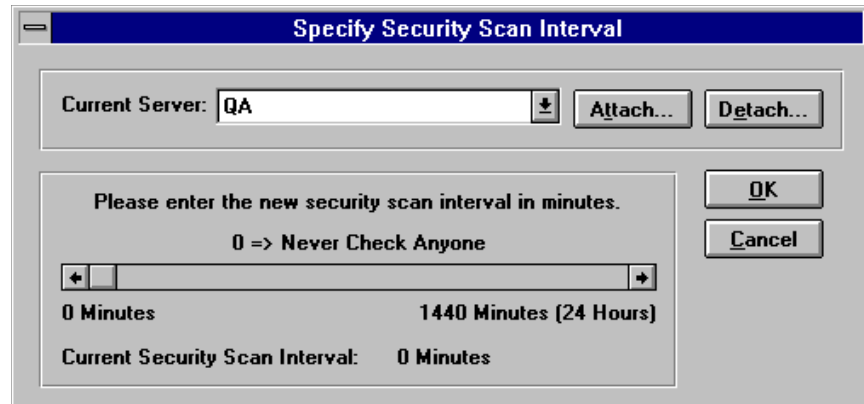


Figure 5-6: Specifying the Security Scan Interval

From this dialog box you can:

- ☐ Set the scan interval
 - ☐ Attach to/Detach from file servers (refer to “Attaching to and Detaching from File Servers” in Chapter 4 for more instructions)
2. **Use one of the following methods to set the interval and specify how often SiteMeter capability checks users for the Swatcher TSR:**
- ☐ Click the slide bar arrows to increment/decrement the value in one minute intervals,
 - ☐ Slide the slide bar to the appropriate value, or
 - ☐ Click on either side of the slide bar to increment/decrement the value in 10 minute intervals.

NOTE:

*Setting the value to 0 minutes informs metering not to check if Swatcher is loaded. **This is mandatory if you are NOT using the Swatcher TSR as your choice to meter and file protect your network.***

3. Once you have selected the appropriate time, choose the OK button.

Disabling Local Drives

What is “Disable Local Drives”?

This option allows you to specify whether or not to disable local drives entirely, essentially rendering the PC diskless. Disable Local Drives is only available if you use Swatcher, the workstation security agent method for metering and file protecting your LAN.

Using Disable Local Drives

To use this option you must specify a Novell Group in which users will not have access to their local disk drives. For example, you may want to create a group named NODRIVE.

This NODRIVE group must be unique; the group you select for Disable Local Drives cannot also be used for Restrict Local Execution.

NOTE:

For information on creating these groups, refer to your Novell User Manuals.

Use the following procedure to disable local drives.

1. **Choose Security from the Administration menu. From the sub-menu that is displayed, choose the Disable Local Drives command.**

The Disable Local Drives dialog box is displayed, as in Figure 5-7.

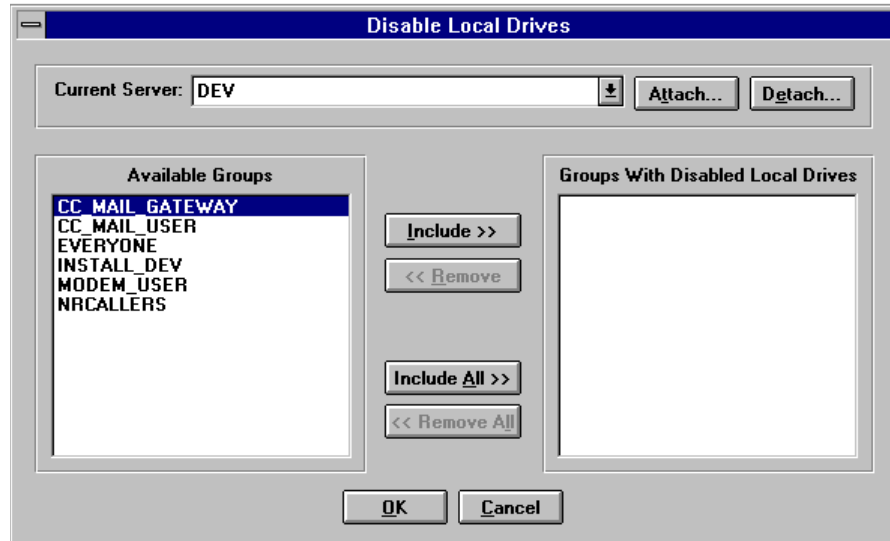


Figure 5-7: Disabling Local Drives

From this dialog box you can:

- ☐ Include groups
- ☐ Remove groups
- ☐ Attach to/Detach from file servers (refer to “Attaching to and Detaching from File Servers” in Chapter 4 for more instructions)

2. If you wish to add a group to the Groups With Disabled Local Drives list, select the desired group from the Available Groups list and choose the Include button.

The group is then moved from the Available Groups list to the Groups With Disabled Local Drives list.

You can include all the available groups by choosing the Include All button.

The groups you included now do not have access to their local drives.

3. If you wish to remove a group from the Groups With Disabled Local Drives list, select the desired group from this list and choose the Remove button.

The group is then moved from the Groups With Disabled Local Drives list to the Available Groups list.

You can remove all groups from the disabled drives list by choosing the Remove All button.

The groups you removed now have access to their local drives.

4. **When you have completed moving groups, choose the OK button to save your changes and exit.**

Restricting Local Execution

What is “Restrict Local Execution”?

SiteMeter provides an option that restricts execution of applications from local drives. By using this option, you can disallow network users from running applications or other programs from the hard drive. Users will still be able to access their local drives, but will not be able to run any applications locally. This feature provides an added layer of control over software usage on your network.

NOTE:

If you decide to use this option please refer to the section entitled DSW in Appendix A.

This option is only available if you are using Swatcher, the workstation security agent method of metering and file protecting your LAN.

Using Restrict Local Execution

To use this option you must specify a Novell Group in which users will not be able to execute files from their local drives. For example, you may want to name this group NOEXEC.

NOTE:

For information on creating these groups, refer to your Novell User Manuals.

Use the following procedure to restrict local execution.

- 1. Choose Security from the Administration menu. From the sub-menu that is displayed, choose the Restrict Local Execution command.**

The Restrict Local Execution dialog box is displayed, as in Figure 5-8.

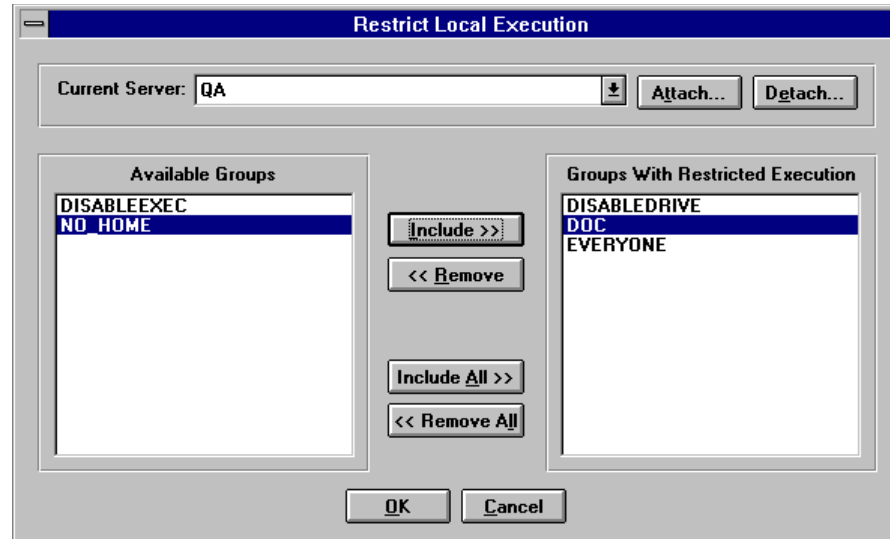


Figure 5-8: Restricting Local Execution

From this dialog box you can:

- ☐ Include groups
 - ☐ Remove groups
 - ☐ Attach to/Detach from file servers (refer to “Attaching to and Detaching from File Servers” in Chapter 4 for more instructions)
2. **To add a group to the Groups With Restricted Execution list, select the desired group from the Available Groups list and choose the Include button.**

The group is then moved from the Available Groups list to the Groups With Restricted Execution list.

You can include all the available groups by choosing the Include All button.

The groups you included now cannot execute applications from their local drives.

3. **To remove a group from the Groups With Restricted Execution list, select the desired group from this list and choose the Remove button.**

The group is then moved from the Groups With Restricted Execution list to the Available Groups list.

You can remove all groups from the restricted list by choosing the Remove All button.

The groups you removed now can execute all applications from their local drives.

- 4. When you have completed moving groups, choose the OK button to save your changes and exit.**

Specifying Security Exceptions

If you are using Swatcher to meter and file protect your LAN, this option allows you to specify those users who are not required to load Swatcher.

NOTE:

If you decide to use this option please refer to the section entitled DSW in Appendix A.

What is Specifying Security Exceptions?

The Security Exceptions is a list of users who are not required to load the Swatcher TSR when logging in to the network.

How Security Exceptions Work

When using the Swatcher TSR method of metering and file protecting, you can set a Security Scan Interval. (Refer to the section Specify Security Scan Interval in this chapter.) This interval instructs SiteMeter how often it should check to verify that all users have loaded the Swatcher TSR, except those specified in the Security Exceptions list.

If a user is a member of this list, he or she will not be disconnected from the network if SiteMeter finds that he or she does not have the Swatcher TSR loaded.

Using Security Exceptions

Use the following procedure to define security exceptions.

1. **Choose Security from the Administration menu. From the sub-menu that is displayed, choose the Specify Security Exceptions command.**

The Specify Security Exceptions dialog box is displayed, as in Figure 5-9.

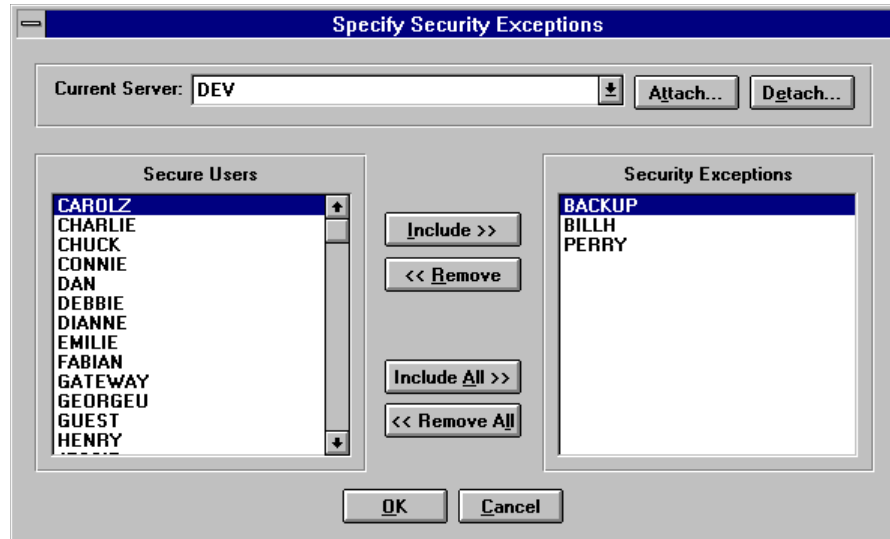


Figure 5-9: Specifying Security Exceptions

From this dialog box you can:

- ☐ Include users
- ☐ Remove users
- ☐ Attach to/Detach from file servers (refer to “Attaching to and Detaching from File Servers” in Chapter 4 for more instructions)

2. To add a user to the Security Exceptions list, select the desired user from the Secure Users list and choose the Include button.

The user is then moved from the Secure Users list to the Security Exceptions list.

You can include all the Secure Users by choosing the Include All button.

The users you included now are not required to load Swatcher when using the network.

3. To remove a user from the Security Exceptions list, select the desired user from this list and choose the Remove button.

The user is then moved from the Security Exceptions list to the Secure Users list.

You can remove all users from the security exceptions list by choosing the Remove All button.

The users you removed now are required to load Swatcher.

4. **When you have completed moving users, choose the OK button to save your changes and exit.**