Adds a notification alert recipient.

Enter the modem's maximum baud rate.

Opens the Browse dialog box where you can select a computer.

Opens the Browse dialog box where you can select a printer to receive notifications.

Enter the amount of time between dialing the phone number and sending the message.

No help topic is associated with this item.

No help topic is associated with this item.

Lists currently configured alert recipients.

Enter any prefix required to get an outside line (eg: 9).

Selects Pulse dialing.

Enter any necessary suffix (eg: password).

Selects Tone dialing.

Enables SNMP. For more information on SNMP, refer to the operating system user's manual.

Enter the name of the email message sender.

Enter the pager ID.

Enter the Login name for the server.

Enter the message to send on detection of a virus.

Opens the Modem Settings dialog box where you can configure the modem.

Enter the modem brand and model. If your modem is not listed, select a generic modem.

Enter the pager password (if applicable).

Enter the COM port where the modem is attached.

Sets the priority level for the selected alert notification. To set the alert for low, medium, and high priority alerts, select Low. To set the alert for medium and high priority alerts, select Medium. To set the alert for high priority alerts only, select High.

Displays the properties for the selected alert notification item.

Select the type of pager to receive notifications (alphanumeric or numeric).

Enter the e-mail address of the message recipient.

Removes the selected alert notification item.

Enter the amount of time between dialing the phone number and sending the message.

Enter the name of the server.

Enter the pager ID.

Enter a custom message.

Opens the SMTP (Simple Mail Transfer Protocol) configuration dialog box.

Configures SNMP. Refer to Windows NT documentation for more information.

Enter the pager password (if applicable).

Turns the modem speaker off.

Enter the amount of time between dialing the phone number and sending the message.

Sets the priority level for the selected alert notification. To set the alert for low, medium, and high priority alerts, select Low. To set the alert for medium and high priority alerts, select Medium. To set the alert for high priority alerts only, select High.

Enter an E-mail Subject line.

Tests the alert notification.

When selected, the pager receives the default alert message.

When selected, the pager receives the custom message shown below.

Enter the maximum number of characters that can be sent to the pager.

Select the modem parity settings.

The Alert Manager supports the sending of alert notifications to pagers. To send alert notifications to pagers, complete the following procedure:

1 Click Add.

2 Select the type of pager:

{button ,JI(`SHIELD.HLP',`Alphanumeric_pager')} Alphanumeric pager

{button ,JI(`SHIELD.HLP',`Numeric_pager')} Numeric pager

- To send pager notifications, a modem must be installed in the NetShield server. If the server does not have a modem, send a Forward to a modem-equipped NetShield server.

To configure an alphanumeric pager:

1. Enter the pager phone number, enter an ID or a PIN number (if applicable), and enter a password (if applicable).
2. To use the standard alert message, click the Use standard alert message option button.
3. To use a custom message, click the Use custom alert message option button and enter a message in the following field.
4. To configure the modem settings, click Modem.
5. To test the pager, click Test.
6. To set the priority level of alert notifications this pager receives, click Priority Level.
7. Click OK.
8. To add another pager to receive notifications, click Add.
9. To configure other notification options, select another property page. To save the changes and exit, click OK. To cancel any changes, click Cancel.

To configure a numeric pager:

1. Enter the pager phone number.
2. Enter a numeric message.
3. Enter the delay time between dialing and sending the alert message.
4. To configure the modem settings, click Modem.
5. To test the pager, click Test.
6. To set the priority level of alert notifications this pager receives, click Priority Level.
7. Click OK.
8. To add another pager to receive notifications, click Add.
9. To configure other notification options, select another property page. To save the changes and exit, click OK. To cancel any changes, click Cancel.

Enter the server name as an Internet Protocol (IP) address, as a name your local domain name server can recognize, or in Universal Naming Convention (UNC) notation. Click OK to save your changes and return to the E-Mail Properties dialog box.

This page lists all alert notification items. To view the properties of an alert notification item, select the item and click Properties. To remove an alert notification item, select the item and click Remove.

To configure priority settings for the selected alert, drag the slider to the right to send the destination computer fewer, but higher priority, messages. Drag the slider to the left to send the destination computer more alert messages, including lower priority messages.

Alert Manager can send the alert messages that NetShield generates to other computers on your network using a standard Windows NT network message. The alert message appears on the destination computer's screen and requires the recipient to acknowledge it.

To send alerts via network messages, your NetShield server must have the Alerter and Messenger Windows NT services running. The destination computers running Windows NT must have the Messenger service running to receive alert messages. Those running Windows 95 or Windows 3.1x must also be running the WinPopup utility to receive network messages. WinPopup comes with some Windows versions. See your Windows documentation for details.

Use the Network Message property page to send alert notifications via network messages and follow these steps:

1. Open the Alert Manager Properties dialog box.
2. Click the Network Message tab.
3. To update this list, you can:
   - Remove a listed computer. Select one of the destination computers listed, then click Remove.
   - Add a computer to the list. Click Add to open the Network Message Properties dialog box (Figure 7-7), then enter the name of the destination computer in the text box provided. You can enter the computer name in Universal Naming Convention (UNC) notation, or you can click Browse to locate the computer on the network. To choose additional options, continue with Step 4.
   - Change configuration options. Select one of the destination computers listed, then click Properties. Alert Manager opens the Network Message Properties dialog box (Figure 7-7). Change any of the information you want to change in the Computer text box, then continue with Step 4 to learn how to choose new or different configuration options.
4. Click Priority Leve to specify which types of alert messages the destination computer will receive.
5. Click OK to save your changes and return to the Network Message Properties dialog box.
6. Click Test to send the destination computer a test message. The message will appear instantly on the destination computer's screen and the recipient will need to click OK to acknowledge it. If your recipient does not receive the message, check the Windows NT Event Viewer for an error message.

Alert Manager and DMI work together to alert the DMI management console instantly of a virus infection. When a virus is detected, DMI immediately generates an alert message for Alert Manager to display on the DMI management console.

Use the DMI property page to generate DMI alert notifications and follow these steps:

Open the Alert Manager Properties dialog box.

1. Click the DMI tab.
2. Click the Enable DMI Usage checkbox. Enable this option on the NetShield servers.
3. Click Priority Level to specify which types of alert messages the destination computer will receive.
4. Click OK to save your changes and return to the DMI dialog box.

DMI (Desktop Management Interface) is an industry interface for keeping track of and monitoring the status of components, including hardware and software, in the computers on your network. For more information about DMI, refer to your Intel documentation or visit the Desktop Management Task Force website at http:\\www.dmtf.org.

Alert Manager can be configured to launch any program or batch file on alert. For example, if your company is using cc:Mail or a special mail package that is not recognized by Network Associates, you could write a batch file to send notifications to your mail package.

Any program launched from Alert Manager runs in the background without a visible user interface.

To configure NetShield to execute a program on alert, follow these steps:

1. Open the Alert Manager Properties dialog box.
2. Click the Execute Program checkbox.
3. Enter the name and path of the program you want NetShield to run upon detecting a virus. You can enter the program name in Universal Naming Convention (UNC) notation, or you can click Browse to locate the program on the network.
4. To execute the program on the first alert event only, click the First Time option button. To execute the program every time an alert event occurs, click the Every Time option button.
5. Click Priority Level to specify which types of alert messages the destination computer will receive.

Alert Manager can log the alert messages that NetShield generates to other computers on your network in a standard Windows NT Event Log. The alert message appears on the destination computer's event log and requires the recipient to acknowledge it.

To configure Alert Manager's Logging options, follow these steps:

1. Open the Alert Manager Properties dialog box.
2. Click the Logging tab. The Recipient list displays a list of all of the computers you have chosen to receive alert logging. If you have not yet chosen any destination computers, this list will be blank.
3. To update this list, you can:
    - Remove a listed computer. Select one of the destination computers listed, then click Remove.
    - Add a computer to the list. Click Add to open the Logging dialog box, then enter the name of the destination computer in the text box provided. You can enter the computer name in Universal Naming Convention (UNC) notation, or you can click Browse to locate the computer on the network.
    - Change configuration options. Select one of the destination computers listed, then click Properties. Alert Manager opens the Logging Properties dialog box. Change any of the information you want to change in the Computer text box. Enter the computer to receive network messages or click Browse to locate the computer.
4. Click Priority Level to specify which types of alert messages the destination computer will receive.

Alert Manager can use .WAV files to sound an audible alert on your system when NetShield detects a virus. To use this option, your system must have a sound card.

To configure Alert Manager's Sound options, follow these steps:

1. Open the Alert Manager Properties dialog box.
2. Click the Sound tab.
3. Click the Enable Audible Alerts checkbox.
4. In the text box provided, enter the name of the sound file you want Alert Manager to run when NetShield detects a virus. The sound file must have a .WAV extension. You can enter the file name in Universal Naming Convention (UNC) notation, or you can click Browse to locate the file on your computer.
5. Leave the text box blank to use the default system sound when NetShield detects a virus.
6. Click Priority Level to specify which types of alert messages the destination computer will receive.

In addition to automatically responding to viruses (cleaning, deleting, moving, etc.), NetShield may be configured to run a program on alert, maintain information in an event log, and alert personnel by:

forwarding alert messages
printing alert messages
e-mailing alert messages
generating DMI alerts
sending alerts messages to a pager
SNMP
broadcasting network messages
audible alerting
Centralized Alerting
logging alert messages

NetShield supports the use of any combination of notification methods and multiples of each.

NetShield uses Network Associates' Alert Manager utility to notify you or others when it detects a virus or malicious code in files on your servers. Alert Manager gives you a wide variety of notification options that you can use individually or in combinations that suit your needs.

If you have Alert Manager installed on other computers on your network, you can also forward alert messages to computers in other domains, which can in turn notify the workstations that they host about infected files on your server.

In large organizations, use Forward to send alerts to centralized notification systems or to MIS departments to keep track of virus statistics and problem areas.

Alert Manager can forward the alert messages that NetShield generates to other computers on your network. If you have installed Alert Manager on each of the destination computers, they can in turn forward alert messages to the recipients listed in their Alert Manager Summary pages. You might use this feature to pass alert messages across network domains or to construct a hierarchical arrangement for passing alert messages.

To configure Alert Manager's Forwarding options, follow these steps:

1. Open the Alert Manager Properties dialog box.
2. Click the Forward tab. The Forward page appears with a list of all of the computers you have chosen to receive forwarded messages. If you have not yet chosen any destination computers, this list will be blank.
3. To update this list, you can:
   - § Remove a listed computer
   - § Add a computer to the list
   - § Change configuration options
4. Click Priority Level to specify which types of alert messages the destination computer will receive.
5. Click Test to send the destination computer a test message. The message will appear instantly on the destination computer's screen and the recipient will need to click OK to acknowledge it. If your recipient does not receive the message, check the Windows NT Event Viewer for an error message.
6. Click OK to return to the Alert Manager dialog box.

Note

- n NetShield must be installed and running on the server receiving forwarded messages.

Select one of the destination computers listed, then click Remove.

Click Add to open the Forward Properties dialog box, then enter the name of the computer that will receive forwarded messages in the text box provided. You can enter the computer name in Universal Naming Convention (UNC) notation, or you can click Browse to locate the computer on the network.

Select one of the destination computers listed, then click Properties. Alert Manager opens the Forward Properties dialog box. Change any of the information you want to change in the Computer text.

The Alert Manager supports the sending of SNMP traps. To enable SNMP, complete the following procedure:

1. Select the Enable SNMP checkbox.
2. To configure SNMP services, click Configure. The Microsoft NT Network Settings property sheet is displayed.
3. To complete configuration of SNMP services, refer to the network operating system documentation.
4. To configure other notification options, select another property page. To save the changes and exit, click OK. To cancel any changes, click Cancel.

The Alert Manager supports the sending of email messages. To send alert notifications via email, complete the following procedure:

1. Click Add.
2. Enter an email address, fill out the Subject line, and fill out the From line.
3. To configure SMTP settings, click Configure SMTP and enter the name of the Server and Login.
4. To test the connection, click Test. The message recipient receives a test message.
5. To set the priority level of the messages this email address receives, click Priority Level.
6. Click OK. To add another recipient to receive alert notifications, repeat steps 1 through 5.

To configure other notification options, select another property page. To save the changes and exit, click OK. To cancel any changes, click Cancel.

To configure modem settings, complete the following procedure.

2 Choose the modem brand and model from the drop down list.

3 Select the COM port.

4 Set the maximum baud rate.

5 Select any prefix required to get an outside line.

6 Select tone or pulse dialing.

7 Click OK.

The Alert Manager supports the sending of alert notifications to printers. To send alert notifications to printers, complete the following procedure:

1. Click Add.
2. Click Browse to locate the printer.
3. To test the connection, click Test. The printer prints a test message.
4. To set the priority level of the messages this printer receives, click Priority Level.
5. Click OK.
6. To add another printer to receive alert notifications, repeat steps 1 through 5.
7. To configure other notification options, select another property page. To save the changes and exit, click OK. To cancel any changes, click Cancel.

Note

- Prior to configuring this notification option, the printer must be configured.

The Alert Manager supports the sending of alert notifications to pagers. To send alert notifications to pagers, complete the following procedure:

1 Click Add.

2 Select the type of pager:

{button ,JI(`SHIELD.HLP',`Alphanumeric_pager')} Alphanumeric pager

{button ,JI(`SHIELD.HLP',`Numeric_pager')} Numeric pager

Note

- To send pager notifications, a modem must be installed in the NetShield server. If the server does not have a modem, send a Forward to a modem-equipped NetShield server.

Enter the server name as an Internet Protocol (IP) address, as a name your local domain name server can recognize, or in Universal Naming Convention (UNC) notation. Click OK to save your changes and return to the E-Mail Properties dialog box.

The Summary page lists all of the alert methods you've told NetShield to use to notify you when it finds a virus or other malicious code on your NetShield server. Click + next to each listed alert method to display the computers, printers, phone numbers, or e-mail addresses that will receive alert messages from NetShield. To remove an alert method, select it, then click Remove. To change the configuration options for a listed method, select it, then click Properties. Alert Manager will open the same property page you used to configure your options for that alert method.

Centralized Alerting is a powerful feature for alerting the appropriate personnel of workstation virus activity. Once Centralized Alerting is enabled and configured, workstations using Network Associates client antivirus software, such as VirusScan, report virus activity to NetShield servers. NetShield then notifies the appropriate personnel (through pagers, printers, e-mail, fax, etc.) listed in the Alert Manager Summary property page.

See also

{button ,JI(`alrtmgr.HLP',`How_Centralized_Alerting_works')} How Centralized Alerting works

{button ,JI(`alrtmgr.HLP',`Configuring_Centralized_Alerting')} Configuring Centralized Alerting

{button ,JI(`alrtmgr.HLP',`Centralized_Alerting_file_format')} Centralized Alerting file format

The NetShield server is configured to monitor an Alert Folder where all users have create, write, and delete rights. When a virus event occurs on a workstation, the workstation sends a Centralized Alerting file to the server's Alert Folder. The server then reads the file and notifies the appropriate personnel specified in Alert Manager.

See also

{button ,JI(`alrtmgr.HLP',`Configuring_Centralized_Alerting')} Configuring Centralized Alerting

{button ,JI(`alrtmgr.HLP',`Centralized_Alerting_file_format')} Centralized Alerting file format

The .ALR file is a text file that contains Centralized Alerting virus event variables. Each variable in the file has a name followed by the equal (=) sign and a value. The following is a line-by-line description of the Centralized Alerting ALR file format:

[CentralAlert]	Centralized Alerting identifier.
uFileVersion	Type: Integer Centralized Alerting version number.
uStatus	Reserved
szVirusName	Type: String The name of the virus.
szItemName	Type: String The infected file name and path.
szUserName	Type: String The user name.
szSoftware	Type: String The name of the Network Associates virus application installed on the reporting machine.
szSoftwareVersion	Type: String The version of the virus application.
szComputerName	Type: String The name of the machine reporting the event.
uYear	Type: Integer (0000-9999) The year of the event.
uMonth	Type: Integer (1-12) The month of the event.
uDay	Type: Integer (1-31) The day of the event.
uHour	Type: Integer (0-23) The hour of the event.
uMinute	Type: Integer (0-59) The minute of the event.

uSecond	Type: Integer (0-59) The second of the event.

1. To configure Centralized Alerting, follow these steps:
2. Select Alerts from the Tools menu.
3. Select Enable Centralized Alerting (in most cases, Centralized Alerting is enabled by default).
4. Enter the location of the Alert Folder in the text box provided. You can click Browse to locate the Alert folder on the network. The default Alert folder is located in C:\Program\Mcafee\NetShield\Alert. All users must have create, write, and delete rights to the Alert Folder.
5. Click OK.
6. Configure the desktop machines which will report virus activity. For more information, refer to the documentation which accompanied VirusScan.

To enable and disable alerts, complete the following procedure.

1. Select Alerts from the Tools menu and click the Messages tab.
2. To enable an alert, select its checkbox.
3. To disable an alert, deselect its checkbox.
4. To save the changes and exit, click OK. To exit without saving changes, click Cancel.

See also

{button ,JI(`alrtmgr.HLP',`Changing_the_priority_of_an_alert')} Changing the priority of an alert

{button ,JI(`alrtmgr.HLP',`Customizing_an_alert_message')} Customizing an alert message

{button ,JI(`alrtmgr.HLP',`Alert_Message_variables')} Alert message variables

To change the priority level of an alert, follow these steps:

1. Select Alerts from the Tools menu and click the Messages tab.
2. Highlight an alert and click Edit.
3. Select a priority level.
4. Click OK.

See also

{button ,JI(`alrtmgr.HLP',`Customizing_an_alert_message')} Customizing an alert message

{button ,JI(`alrtmgr.HLP',`Alert_Message_variables')} Alert message variables

{button ,JI(`alrtmgr.HLP',`Enabling_and_disabling_alerts')} Enabling and disabling alerts

While an alert message can be customized, the reason for the alert does not change (e.g. when a task starts, the ‘task has started’ message is generated). Be careful not to modify the meaning of the alert message. Otherwise, notifications may become confusing or erroneous.

To customize an alert message, follow these steps:

1. Select Alerts from the Tools menu and click the Messages tab.
2. Highlight an alert and click Edit.
3. Enter a custom message in the text field.
4. Click OK.

See also

{button ,JI(`alrtmgr.HLP',`Alert_Message_variables')} Alert message variables

{button ,JI(`alrtmgr.HLP',`Changing_the_priority_of_an_alert')} Changing the priority of an alert

{button ,JI(`alrtmgr.HLP',`Enabling_and_disabling_alerts')} Enabling and disabling alerts

Alert messages generated by NetShield **may** contain following variables:

%FILENAME%	Name of the infected file
%TASKNAME%	Name of the task that detected the virus
%VIRUSNAME%	Name of the virus
%DATE%	Date of the event
%TIME%	Time of the event
%COMPUTERNAME%	Name of the infected computer
%SOTWARENAME%	Name of the software that detected the virus
%USERNAME%	Name of the local user
%SOFTWAREVERSION%	Version number of the software that detected the virus