McAfee GroupShield Exchange On-Demand Console

Important information

The GroupShield Exchange On-Demand Console has been supplied by McAfee to provide detection and cleaning for all known viruses and worms, including the new VBS/LOVELETTER worm. Please ensure that you follow the information provided in this guide to ensure that you use the Console properly to scan and detect these viruses.

The GroupShield Exchange On-Demand Console contains a subset of the functionality available in McAfee's GroupShield Exchange software. **This guide provides information taken directly from the GroupShield Exchange software's documentation and, in order to supply you with this information as quickly as possible, this text still refers to the GroupShield Exchange software. Simply apply the actions to the On-Demand Console, in place of the GroupShield Exchange software.**

To ensure that your organization maintains its defense against future virus attacks, McAfee recommends that you upgrade to the GroupShield Exchange software and ensure that it uses the latest anti-virus definition (.DAT) files at all times.

Copyright

Network Associates Trademark Attributions

Introduction

An on-demand scan operation checks for viruses on request or at preset intervals. If a virus is detected, you can have the GroupShield Exchange software attempt to clean the virus or move the infected file or files to a quarantine location.

Depending on how susceptible your e-mail system is to virus infection, you might want to perform an on-demand scan operation as often as once a day. Choose a time when the e-mail throughput is low, to have minimum impact on your mail server. To make sure that your anti-virus software is as up to date as possible, you must regularly update the McAfee virus definition (.DAT) files.

This chapter contains the following sections:

Installing and using the GroupShield Exchange On-Demand Console

To install the GroupShield Exchange On-Demand Console software onto you mail server, your server must:

- Be running either:
  - Microsoft Windows NT v4.0, Service Pack 4.0 (or later), or
  - Microsoft Windows 2000 Server, Build no. 2195 (or later).
- Have Microsoft Exchange Server v5.5 (or later) installed.

To install the GroupShield Exchange On-Demand Console, follow these steps:

1. Log on to the mail server using an administrative account.
2. Copy the SETUP.EXE file for the GroupShield Exchange On-Demand Console software onto a directory on the mail server.
3. Run the SETUP.EXE file.

   The Setup wizard installs the Microsoft Installer program if it does not exist on your server. Reboot the server, if required.
4. Proceed through the installation panels by clicking **Next>**.

   The Setup wizard installs the GroupShield Exchange On-Demand Console onto the server.
5. Click **Finish**, and reboot the server if required.

To open the GroupShield Exchange On-Demand Console, follow these steps:

1. From the Windows **Start** menu, select **Programs**.
2. Click **GroupShield Exchange On-Demand Console**.

   To start using the Console, providing detection and cleaning for the VBS/LOVELETTER worm, select the server (in the Console) and click the  start button.

   The remainder of this guide describes the Console's features in more detail.

Scanning options

Note that an on-demand scan operation can look for viruses written in VBScript and embedded within the body of e-mail messages. A recently discovered "proof-of-concept" virus called VBS/BUBBLEBOY can conceal VBScript code within the body of an e-mail message formatted with HTML tags. Certain Windows and Internet Explorer configurations allow the embedded script to run as soon as it appears in a Microsoft Outlook Express preview pane, or as soon as a message recipient opens an e-mail message in Microsoft Outlook.

To specify certain file extensions that you want to scan, follow these substeps:

1. Open the GroupShield Exchange On-Demand Console. For information on doing this, see "Installing and using the GroupShield Exchange On-Demand Console" on page 3.

2. In the Scanning options box, choose a combination of the following scanning options to tell the GroupShield Exchange software what virus detection methods you want it to use when it performs the on-demand scan operation:

- **Enable program file heuristics** scans program files and identifies potential new file viruses
- **Enable macro heuristics** scans for macros in the attachments (such as those used by Microsoft Word, Microsoft Excel, and Microsoft Office) and identifies potential new macro viruses
- **Expand archive files** scans inside file archives (such as .ZIP or .LZH files). If you are scanning selected file extensions only, include the needed archive file extensions in the list of file extensions that you want the software to scan.
- **Scan all files** scans all attachments
- **Scan files with Extensions** scans all files by default. To tell the GroupShield Exchange software which extension types you want to include in an on-demand scan operation, follow these substeps:

    a. If not already selected, select **Scan files with**, then click **Extensions**. to see the Program File Extensions dialog box (Figure 1-1).

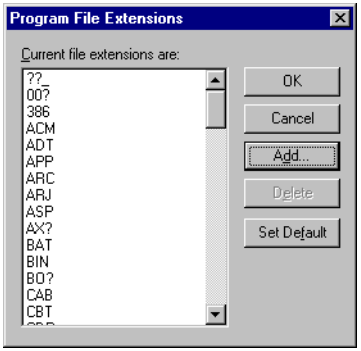

Figure 1-1. On-Demand property page - Program File Extensions dialog box

The Program File Extensions dialog box shows all the file extensions that the GroupShield Exchange software scans. The following options are available:

– To have the GroupShield Exchange software include a new file extension in the on-demand scan operation, click **Add** to see the Scan Types box (Figure 1-2 on page 5).

  Enter the new extension name and click **OK** to return to the Program File Extensions dialog box and register it in the list.

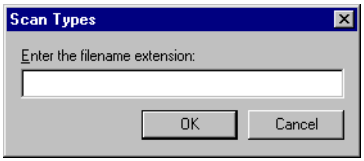

Figure 1-2. Program File Extensions dialog box - Scan Types text box

– To tell the GroupShield Exchange software not to scan a specific file extension during an on-demand scan operation, select it and click **Delete**.

– To return to the original list of file extensions that the GroupShield Exchange software scans in the on-demand scan operation, click **Set Default**.

b. Click **OK** to return to the On-Demand property page.

> **NOTE:** If the scan operation detects an HTML or VBScript virus in an e-mail message, it quarantines the entire message and any attachments it includes even when the Quarantine Attachment option is selected in the On-Demand property page. The Console moves infected messages in to the quarantine database or directory that you designate.

- **Find all macros** scans specifically for attachments that contain macros and treats them as uncleanable viruses. The attachment is quarantined and the Administrator notified of the action.
- **Delete all macros** can only be used with the Find all macros option and identifies any macros and deletes them regardless of whether or not they are infected.
- **Expand compressed program files** scans inside compressed files (such as those compressed with PKLITE). If you are scanning selected file extension only, include the needed compressed file extensions in the list of file extensions to be scanned.

GroupShield Exchange actions on virus detection

To tell the GroupShield Exchange software which actions to perform when it detects an infected e-mail message or attachment, follow these steps:

1. Open the GroupShield Exchange On-Demand Console. For information on doing this, see "Installing and using the GroupShield Exchange On-Demand Console" on page 3.
2. In the Action to Perform upon virus detection box, choose one of the following options to tell the GroupShield Exchange software how it should treat infected attachments during a scan operation:

- **Log infection and continue without attempting to disinfect** records that the GroupShield Exchange software discovered a virus in the McAfee Log Manager and notifies the administrator.

> **NOTE:** McAfee recommends you do **NOT** choose the Log infection and continue without attempting to disinfect option.

- **Quarantine attachment without attempting to disinfect** sends all infected attachments to the quarantine location.
- **Quarantine message without attempting to disinfect** sends all infected messages and their attachments to the quarantine location.

- **Quarantine attachment on failure to disinfect** attempts to clean the attachment. If successful, the message and its attachment are forwarded to the intended recipient. If unsuccessful, the attachment is quarantined. If successful, the intended recipient is not notified that the attachment contained a virus.
- **Quarantine message on failure to disinfect** attempts to clean the attachment. If successful, the message and attachment are forwarded to the intended recipient. If unsuccessful, the attachment AND the message are quarantined.
- **Delete attachment on failure to disinfect** attempts to clean the attachment. If successful, the message and attachment are forwarded to the intended recipient. If unsuccessful, the attachment is deleted and the action logged in the McAfee Log Manager.
- **Delete message on failure to disinfect** attempts to clean the attachment. If successful, the message and attachment are forwarded to the intended recipient. If unsuccessful, the whole message is deleted and the action logged in the McAfee Log Manager.
- **Delete attachment without attempting to disinfect** does not attempt to clean or quarantine an infected attachment. The attachment is deleted and the action logged in the McAfee Log Manager.
- **Delete message without attempting to disinfect** does not attempt to clean or quarantine an infected attachment. The entire message is deleted and the action logged in the McAfee Log Manager.

NOTE: When the GroupShield Exchange software deletes an attachment, the attachment is replaced with the ALERT.TXT message.

The On-Demand report

The GroupShield Exchange software optionally sends a report to the administrators listed on the Administration property page detailing the results of an on-demand scan operation. Use the On-Demand report to analyze the GroupShield Exchange virus scanning statistics or archive it for historical purposes.

The report informs the Administrator(s) of:

- Which Microsoft Exchange server was scanned
- How many messages and attachments were scanned
- When the scan operation was performed
- What time the scan operation started and ended
- How many messages were infected
- How many messages were quarantined
- How many messages were cleaned

Introducing the On-Demand Console

The main features of the Console are that it:

- Can be configured to scan the local computer or a remote one.
- Allows you to start a scan operation, close the console, reopen it and connect to the existing scan operation.
- Can perform an on-demand scan operation at the same time as a scheduled scan operation.

The console reports how many viruses were found, quarantined, cleaned and deleted in each information store on the Microsoft Exchange server and gives a grand total at the top of the panel. The Console can be run from the GroupShield Properties server administration console and also as an independent utility on a server that does not have the GroupShield Properties server administration console installed.

NOTE: The settings button is not available if the On-Demand Console is launched from the GroupShield Properties server administration console and is not run as an independent process.

From the Console, you can start, stop, and pause a scan operation. You can also perform a new on-demand scan operation on another Microsoft Exchange server. When launched from the GroupShield Properties server administration console, the scan operation is configured using the On-Demand property page and the  button on the Console's interface is not available.

The On-Demand Console interface

The On-Demand Console is divided in to four main areas:

- The Menu bar allows you to select the GroupShield Exchange server you want to scan, specify which of the On-Demand Console tool bars you want to see, start, stop and pause a scan operation and get Help. See "The menu bar" on page 9 for a full description of the options available from the Console's menus.
- The Tool bar gives the same options as the menu bar. See "The tool bar" on page 10 for a full description of the options available.
- The Information panel gives a summary report of how many viruses were found, quarantined, cleaned and deleted on the Microsoft Exchange server. It also indicates when the scan operation was started and when it completed, and how many mailboxes and public folders it scanned in total.
- The Results panel. See "The results panel" on page 11 for a full description of the data recorded on the Results panel.

The menu bar

See the following items for an overview of the different menu options available from the menu bar:

- The File menu on page 10
- The View menu on page 10
- The Scan menu on page 10
- The Help menu on page 10

The File menu

- **Settings** opens the Settings panel if the Console is opened through the GroupShield Exchange program directory or on a remote server.

  This option is unavailable when the Console is launched from the On-Demand property page in GroupShield Properties.

- **Change Server** to choose another Microsoft Exchange server to scan.

  See "Changing the target server" on page 14 to learn how to select a different Microsoft Exchange server to scan.

- **Exit** closes the On-Demand Console.

The View menu

- **Toolbar** turns the tool bar on and off.
- **Status Bar** turns the status bar at the bottom of the panel on and off.

The Scan menu

- **Start** starts the scan operation
- **Pause/Continue** pauses the scan operation. Choose the same option to restart the scan operation
- **Stop** terminates the scan operation before it is completed.

The Help menu

- **Help Topics** launches the McAfee On-Demand Console help file
- **About OD Console** shows copyright and version information about the On-Demand Console.

The tool bar

- Use the Server combo box to choose the Microsoft Exchange server you want to scan.
-  opens the Settings panel if the Console is opened through the GroupShield Exchange program directory or on a remote server.

  This button is unavailable when the Console is launched from the GroupShield Properties server administration console.

-  starts the scan operation.

- stops the scan operation before it completes.
- pauses the scan operation.

NOTE: To restart a paused scan operation, click again.

- launches the About GroupShield Exchange On-Demand Console panel.

  Get On-Demand Console copyright details, system information about the current server and connect to Network Associates technical support web site.

  From the About Quarantine Manager panel, click **OK** to go back to the Quarantine Manager.

The results panel

The Results panel gives an individual report of the number of viruses found, quarantined, cleaned and deleted in each public folder and mailbox on the Microsoft Exchange server.

The Results panel is divided in to two clear sections. The top of the panel provides you with a summary report of the scan operation's findings while the bottom panel gives a detailed account shows results for each individual public folder on the server at the top of the Results column and then each individual mailbox. The total number viruses in each mailbox, that is, the in folder, out folder, sent folder and deleted folder is also recorded.

A breakdown of the number of viruses found, quarantined, cleaned or deleted in each target public folder or mailbox are recorded in columns on the right of the panel.

The Mailbox / Folder column records when the scan operation was started and when it completed. Additionally, it can show a time that the scan operation was terminated before it completed, and if it was paused and then restarted.

Using the On-Demand Console from the installation directory

When launched from the installation directory, the scan operation is configured on the Settings panel.

Using this method, you can scan a Microsoft Exchange server that does not have the GroupShield Exchange software installed.

Use the Settings panel to configure a scan operation on a server that does not have the GroupShield Exchange software installed. The Settings button only becomes available on the On-Demand Console when the Console has been launched from GroupShield Exchange i386 program directory on a server with the GroupShield Exchange software installed.

NOTE: McAfee recommends you use the On-Demand Console as an independent process ONLY when the target server does not have the GroupShield Exchange software installed.

For information on opening the GroupShield Exchange On-Demand Console, see "Installing and using the GroupShield Exchange On-Demand Console" on page 3.

To learn how to configure a scan operation using the Settings panel, follow these steps:

1. Open the On-Demand Console.
2. Click  to launch the Settings panel.

   The Settings panel has the following options:

- The Scanning options box tells the GroupShield Exchange software what virus detection methods you want it to use during an on-demand scan operation.

  See "Scanning options" on page 4 to learn how to set the scanning options.

- The Action to Perform upon virus detection combo box tells the GroupShield Exchange software what action you want it to take when it detects a virus during an on-demand scan operation.

  See "GroupShield Exchange actions on virus detection" on page 6 to learn more about the actions the GroupShield Exchange software can take when it performs an on-demand scan operation.

NOTE: McAfee recommends you do NOT choose the **Log infection and continue without attempting to disinfect** option.

- The What to scan combo box tells the GroupShield Exchange software which mailboxes and public folders it should scan on the target server.
- The Notification box displays the name of an administrator that should be notified of a virus infection.

  If the box is empty and you want to select an administrator to notify, click **Notify**.
- Select the **Send On-Demand report when finished** checkbox to have the GroupShield Exchange software send a report detailing the scan operation's results to the administrator you chose in the Notification box.

3. Click **OK** to register the settings and return to the On-Demand Console.

Getting version information

To get version and system information about the GroupShield Exchange On-Demand Console utility, follow these steps:

1. Open the On-Demand Console and choose one of the following options:

- Click  on the tool bar
- Choose the **About OD Console** option from the **Help** menu.

2. From the About GroupShield Exchange On-Demand Console panel, you have three options:

- Click **System Info** to open the Microsoft System Information panel to get information about the current computer, for example, the available physical memory
- Click **Tech Support** to connect to the Network Associates web site and get technical advice about the On-Demand Console
- View the version information and click **OK** to return to the On-Demand Console.

Changing the target server

To change the Microsoft Exchange server that you want to scan, follow these steps:

1. From the **File** menu, select the **Change Server** option.
2. On the Select Computer dialog box browse to the computer you want to scan and select it.

   Browse to the computer using the same method as you would to navigate through the Network Neighborhood structure in Microsoft Windows NT.
3. Click **OK** to register the server and choose one of the following options:

- Click  to open the Settings panel and configure the scan operation
- Click  to start the scan operation with either the default or previous scan operation settings.

Performing an on-demand scan operation from the command line

The GroupShield Exchange v4.5 software lets you specify an on-demand scan operation using the Command Line. Using this method of scanning, you can schedule scan operations and have the software perform a scan operation immediately when an administrator logs on to the server.

NOTE: The account that the scheduler uses to log on must be a user account and not a system account.

To see the list of options from the command prompt, follow these steps:

1. Open the Windows NT program menu and choose the **Command Prompt** and change to the directory into which you installed the GroupShield Exchange On-Demand Console software. The default directory is:

   C:\Program Files\Network Associates\GSEODConsole

NOTE: The location listed is the GroupShield Exchange default installation location. If you chose to install the software in to a location other than the one shown, go to that directory in the Command Prompt window.

2. From there, type the following command to see the first list of switch options:

   ```
   odcmd /?
   ```

3. To see more command line options type the following command

   ```
   odcmd /? | more
   ```

The following table describes the on-demand scanning options available to you from the command line. The options describe how and where the scan operation looks for infected files. Use a combination of the options to shape the scan operation to suit your needs. If the **Default** column entry is “on”, the option automatically runs without your needing to add it to the command line. You may override some of these default options with other options.

Table 1-1. On-Demand scanning options

Option	Description	Default
/NOGUI	This option does not display the scan operation’s progress in the Command Prompt window	Off
/ADMIN	This option specifies the user that you want to receive virus detection reports and on-demand scan reports, for example, /ADMIN=<mailbox name>. To receive an on-demand scan report, the /AUTOREPORT switch must also be specified	Off
/EVENT	This option sets the name of the event in the list of scheduled scan operations, for example, /EVENT=<event name>.	Off

Table 1-1. On-Demand scanning options

Option	Description	Default
/TYPE	This option specifies the type of on-demand scan operation that you want the GroupShield Exchange software to perform. Choose from the following options: **SCHEDULE** is a scheduled on-demand scan operation **MANUAL** is an immediate on-demand scan operation.	The Manual switch is the default if no type is chosen
/DEFAULT	This option uses default GroupShield Exchange on-demand scan operations. The default option uses maximum security settings which means the scan operation can put a strain on system resources at times of peak message throughput. **This command must not be used if the GroupShield Exchange software is not present.**	Off
/AUTOREPORT	This option sends an on-demand scan report to the user that you specified in the /ADMIN switch	Off

Table 1-1. On-Demand scanning options

Option	Description	Default
/OVF action	This option tells the GroupShield Exchange software what action you want it to take when it detects a virus infection during an on-demand scan operation. Choose from the following options: **QM** quarantines the message. **QA** quarantines the attachment. **CQM** attempts to clean the message. If it fails to disinfect the message, it quarantines the entire message. **CQA** attempts to clean the attachment. If it fails to disinfect the attachment, it sends the attachment to the quarantine location. **DM** deletes the message. **DA** deletes the attachment. **CDM** attempts to clean the message. If it fails, the message is deleted. **CDA** attempts to clean the attachment. If it fails, the attachment is deleted.	The CQA switch is the default if not /OVF action is chosen
/HEUR	This option switches on the program file heuristics option that has the Groupshield Exchange software use heuristic detection methods to identify potential new program file viruses.	On
/MACRO	This option switches on the macro file heuristics option that has the GroupShield Exchange software use heuristic detection methods to identify potential new macro file viruses.	On
/ARC	This option scans inside file archives (such as .ZIP or .LZH files). If you are scanning selected file extensions only, include the needed archive file extensions in the list of file extensions that you want the software to scan.	On

Table 1-1. On-Demand scanning options

Option	Description	Default
/ZIPS	This option scans inside compressed files (such as those compressed with PKLITE). If you are scanning selected file extension only, include the needed compressed file extensions in the list of file extensions to be scanned.	On
/FAM	This option scans specifically for attachments that contain macros and treats them as uncleanable viruses. The attachment is quarantined and the Administrator notified of the action.	Off
/DAM	This option can only be used with the Find all macros option and identifies any macros and deletes them regardless of whether or not they are infected.	Off
/EXTN	This option sets the list of files that you want the GroupShield Exchange software to scan. It scans all files by default. Specify the list using commas to separate the extension types, for example, /EXTN=exe,dll,doc	Off
/LIST	This option sets the list of Microsoft Exchange message stores that you want the GroupShield Exchange software to scan. Specify the list using commas to separate the store names, for example, /LIST="\Public Folder1","Mailbox1" Public folder names must begin with a '\' character and are case sensitive. Names with spaces in them must be quoted.	By default, it scans all files
/PRIORITY	This option sets the priority for the scan operation. Choose from the following priority options: **HIGH** **NORMAL** **LOW**	If no priority is set, the default is Normal

Table 1-1. On-Demand scanning options

Option	Description	Default
/WHAT	This option sets the way that you want the GroupShield Exchange software to interpret the list of items using the /LIST option. Choose from the following options: **SEL** scans only listed items **EXPT** scans all except listed items **ALL** scans all items.	If no item is set, the default is ALL
/@ response file	This option specifies a response file to read commands from.	Off

Command line examples

The following examples list some of the ways in which you can use the options to respond to a virus attack.

To run an on-demand scan operation on a server that does not have the GroupShield Exchange software installed, follow these steps:

1. Log on to the server that you want the GroupShield Exchange software to scan.
2. Then, map a network drive to a GroupShield Exchange server.
3. In the Command Prompt, go to the GroupShield Exchange server's installation directory and type the following command on the command line:

   ```
   odcmd /type=manual
   ```

   NOTE: This command runs an on-demand scan operation using maximum GroupShield Exchange anti-virus settings. McAfee recommends that you run this command when your Microsoft Exchange servers have low message throughput to avoid putting a heavy load on the mail servers.

You can override the maximum security settings on either a server with or without the GroupShield Exchange software installed. In the following example command, the GroupShield Exchange software is scanning a Microsoft Exchange server that does not have the GroupShield Exchange software installed. The scan operation is limited to scanning .ZIP files and using heuristics technology to identify virus infection in program files.

To do so, follow these steps:

1. Follow Step 1 and Step 2 in the previous example.
2. At the command prompt on the target server, type the following on the command line:

   ```
   odcmd /type=manual /heur /zips
   ```