McAfee GroupShield version 7.0.2 for Microsoft Exchange 2010
User Guide — Addendum

McAfee®

COPYRIGHT

Copyright © 2009 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

AVERT, EPO, EPOLICY ORCHESTRATOR, FOUNDSTONE, GROUPSHIELD, INTRUSHIELD, LINUXSHIELD, MAX (MCAFEE SECURITYALLIANCE EXCHANGE), MCAFEE, NETSHIELD, PORTALSHIELD, PREVENTSYS, SECURITYALLIANCE, SITEADVISOR, TOTAL PROTECTION, VIRUSSCAN, WEBSHIELD are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

License Attributions

Refer to the product Release Notes.

Contents

About GroupShield version 7.0.2 for Microsoft Exchange 2010 . . . . . **4**

System Requirements 5

Status Report **6**

Scheduling a new status report 6

Configuration Report **8**

Scheduling a new configuration report 8

Cluster Replication Setup utility **10**

About GroupShield version 7.0.2 for Microsoft Exchange 2010

McAfee GroupShield version 7.0.2 for Microsoft Exchange software protects Microsoft ® Exchange Server 2010 from virus, phish, spam, unwanted content, potentially unwanted programs, and banned file types/messages. It also supports content filtering within the email messages.

This guide provides information on the changes/additions documented for GroupShield version 7.0.2 for Microsoft Exchange. Changes in this document supersede the information present in the existing *McAfee GroupShield version 7.0 for Exchange — User Guide*.

NOTE: This document should be used in conjunction with other GroupShield version 7.0 for Exchange documentation. Information in this document takes precedence over information in other GroupShield 7.0 for Microsoft Exchange documentation, and all references to Exchange Server 2003 and Exchange Server 2007 should be read as Exchange Server 2010.

Changes include:

- Exchange server support
- Scheduling status reports
- Scheduling configuration reports
- Cluster Replication Setup utility
- User Junk Folder Routing
- On-Demand Scans

What's new

- **Support for Microsoft Exchange Server 2010** — This version of GroupShield supports only Microsoft Exchange Server 2010. To know the supported Exchange server roles, refer to the *System Requirements* section.
- **Data Availability Group (DAG)** — GroupShield 7.0.2 supports Exchange Server 2010 high availability solution.
- **Cluster Replication Setup** — This utility replicates the quarantine database, policy configurations and product updates, depending upon the replication settings across Data Availability Group (DAG) aware GroupShield for Exchange installation.
- **Internet Protocol version 6 (IPv6)** — You can now specify the McAfee Quarantine Manager server address in IPv6 format. For example: 2001:0DB8:2F3B:02AA:00FF:FE28:9C5A:57AB is a valid IPv6 address.
- **Configuration Reports** — You can specify a time when your server should send the configuration reports to the administrator or the recipient email. The configuration report will have a summary of product configurations such as: server information, version information, license status and type, product information, debug logging information, on-access settings, on-access policies, and gateway policies.

- **User Junk Folder Routing** — In the earlier versions of GroupShield, the email routing to user's **Junk E-mail** folder was happening at the Mailbox server level. In GroupShield 7.0.2 for Exchange, email routing to junk folder happens at the Hub server. Due to this, the **Enable routing to the user junk folders on this server** option which was available in earlier versions of GroupShield user interface is now removed.
- **On-Demand Scans** — GroupShield 7.0.2 for Exchange creates an on-demand user **GSOD_<ComputerName>** on all the Mailbox servers, to connect to the Client Access Server (CAS) role.

NOTE: For more information on how to install and configure the software, refer to the *McAfee GroupShield version 7.0.2 for Microsoft Exchange 2010 — Release Notes*.

System Requirements

Before you install GroupShield version 7.0.2 for Exchange, ensure that your server meets these requirements:

Component	Requirement
Supported Operating System	• Microsoft Windows 2008 Standard/Enterprise Server SP2 (64-bit) • Microsoft Windows 2008 Standard/Enterprise Server R2 (64-bit)
Supported Exchange Server	• Microsoft Exchange Server 2010
Supported Exchange Server Role	• Edge Transport Server • Hub Transport Server • Mailbox Server • Mailbox Server + Hub Transport Server NOTE: It also supports Exchange Server 2010 high availability solution, Database Availability Group (DAG).
Supported Browser	• Microsoft Internet Explorer 6.0 or later • Mozilla Firefox 2.0
Processor	• Intel x64 architecture-based processor that supports Intel Extended Memory 64 Technology (Intel EM64T) • AMD x64 architecture-based processor with AMD 64-bit technology
Memory	Minimum: 2 GB RAM (Recommended: 4 GB RAM)
Disk space	Minimum: 740 MB
Network	10/100/1000Mbps Ethernet card
Display	1024 x 768
Supported McAfee Management software (if using any)	• McAfee ePolicy Orchestrator version 4.0 • McAfee ePolicy Orchestrator version 4.5

Status Report

A status report is a scheduled report sent to an administrator at a specific time. The report contains detection statistics within that specified time frame. You can choose a time, recipient email address/distribution list to send the report to, and a subject for the email. Reports are sent in HTML or CSV format.

Scheduling a new status report

1. Click **Dashboard** | **Status Report**. The **Status Reports** page appears.
2. Click **New Report**. The **Report** page appears.
3. In **When to report** page, choose any of these options:
   - **Not scheduled** — Select the checkbox to set up a reporting task that you can activate later. If you are modifying a report schedule, this option allows you to stop an existing report task.
   - **Once** — From the respective drop-down lists, choose a date, month, year and the time when a report task has to start. You can select the checkbox and specify the number of hours and minutes after which the report task has to stop.
   - **Hours** — Specify how frequently, the report task should take place (in hours), and at how many minutes past the hour. You can select the checkbox and specify the number of hours and minutes after which the report task has to stop.
   - **Days** — Specify the time how frequently, in days, the report task should take place and at what time of the day. You can select the checkbox and specify the number of hours and minutes after which the report task has to stop.
   - **Weeks** — Specify how frequently, in weeks, the report task should take place. You can also specify on which days and at what time of day the task should take place. You can select the checkbox and specify the number of hours and minutes after which the report task has to stop.
   - **Months** — On either the first, second, third, fourth or a last day, select a checkbox by clicking on a desired month(s) and specify a time at which a report task has to start. You can select the checkbox and specify the number of hours and minutes after which the report task has to stop.
   - **Stop task after it has run for** — Specify the maximum number of hours and minutes a task can run before it is stopped. Limiting the amount of time a report can run helps preserve system resources. By default there is no limit on report task time.
4. Click **Next**. The **Report Settings** page appears.
5. In **Recipient Email**, specify the recipient's email address to whom the report is to be sent.
6. In **Subject line for report**, specify the subject line in the report that is sent to the recipient.
7. In **Number of Rows**, specify the number of rows (n) to be included in the recipient's status report. Each row in the status report displays the total number of detections for a

particular day. The report contains the detection count for the last (n) days, excluding the day when the status report is triggered. For example: If you specify two, the status report will contain two rows displaying detections for the last two days, excluding today.

8 In **Type of Report**, specify the format of the status report, which is sent to the recipient. The available options are **CSV** or **HTML**.

9 Click **Next**. The **Please enter a task name** page appears.

10 Type a meaningful name for the task.

11 Click **Finish**.

12 Click **Apply** to save the changes.

Configuration Report

A configuration report is a scheduled report sent to an administrator at a specific time. The configuration report will have a summary of product configurations such as: server information, version information, license status and type, product information, debug logging information, on-access settings, on-access policies, and gateway policies.

Scheduling a new configuration report

1. Click **Dashboard** | **Configuration Report**. The **Configuration Report** page appears.
2. Click **New Report**. The **Report** page appears.
3. In the **When to report** page, choose any of these options:
   - **Not scheduled** — Select the checkbox to set up a reporting task that you can activate later. If you are modifying a report schedule, this option allows you to stop an existing report task.
   - **Once** — From the respective drop-down lists, choose a date, month, year and the time when a report task has to start. You can select the checkbox and specify the number of hours and minutes after which the report task has to stop.
   - **Hours** — Specify how frequently, the report task should take place (in hours), and at how many minutes past the hour. You can select the checkbox and specify the number of hours and minutes after which the report task has to stop.
   - **Days** — Specify the time how frequently, in days, the report task should take place and at what time of the day. You can select the checkbox and specify the number of hours and minutes after which the report task has to stop.
   - **Weeks** — Specify how frequently, in weeks, the report task should take place. You can also specify on which days and at what time of day the task should take place. You can select the checkbox and specify the number of hours and minutes after which the report task has to stop.
   - **Months** — On either the first, second, third, fourth or a last day, select a checkbox by clicking on a desired month(s) and specify a time at which a report task has to start. You can select the checkbox and specify the number of hours and minutes after which the report task has to stop.
   - **Stop task after it has run for** — Specify the maximum number of hours and minutes a task can run before it is stopped. Limiting the amount of time a report can run helps preserve system resources. By default there is no limit on report task time.
4. Click **Next**. The **Who to report to** page appears.
5. In **Recipient Email**, specify the recipient's email address to whom the report is to be sent.
6. In **Subject line for report**, specify the subject line in the report that is sent to the recipient.
7. Click **Next**. The **Please enter a task name** page appears.

8 Type a meaningful name for the task.

9 Click **Finish**.

10 Click **Apply** to save the changes.

Cluster Replication Setup utility

Cluster Replication Setup utility replicates the quarantine database, policy configurations and product updates, depending upon the replication settings across Data Availability Group (DAG) aware GroupShield for Exchange installation.

This utility will make quarantined items highly available, by replicating the quarantined items from one server to another server depending up on the configuration. This utility is required only in a DAG aware GroupShield for Exchange installation.

To configure cluster replication for GroupShield's quarantine database

1. From the **Start** menu, click **All Programs** | **McAfee** | **GroupShield for Exchange** | **Cluster Replication Setup**.
2. Select the GroupShield for Exchange Server name from **Server name** drop down, to retrieve the available servers for replication.
3. Select the server from **Available server(s)** list and click **>>** to add it to the **Replication server(s)** list.
4. Click **Apply** to save the changes.

To manage cluster replication in GroupShield for Exchange

1. Select **Start Replication service for:** to enable the available option for replication.
2. Select the following option(s) you want to configure:
   - **Policy Configuration**
   - **Engine/DATs**
   - **Quarantine Database**
3. Click **Apply** to save the changes.
4. A message **Please wait until the replication service is started** appears.

NOTE: You must restart the GroupShield for Exchange service, for the Quarantine Database replication to work. After selecting this option from the cluster replication setup utility, a message will prompt you to restart the GroupShield for Exchange service.