

## Anti-virus Administration for GroupShield

The prevalence of viruses today – and living with the resulting constant threat – has created the need for new security products and strategies. This course is specifically designed for individuals who implement gateway-scanning solutions, such as GroupShield 6.0 and SpamKiller 2.1 products. Learn how to protect your network from email viruses, potential threats and unwanted Spam. Learn how to use these perimeter-designed products in a live network setting.



### Skill Building

Before taking this class we recommend that participants have a general understanding of LAN technologies and Windows operating systems, Microsoft Exchange 2000 or 2003 and the ability to demonstrate basic networking skills.

### Exercises

All topics are supported by hands-on exercises specifically designed to increase knowledge retention. Classroom exercises provide the basic hands-on experience needed to install, configure, and manage McAfee Security anti-virus products.

### Course Materials

- Student Manual

### Duration

- Two Days

### Students Learn To

- Identify how viruses can affect a network when found at the mail server and gateway
- Describe the importance of multi-layer defense systems
- Install and compare features in GroupShield 6.0 for Microsoft Exchange
- Describe how GroupShield works with Microsoft Exchange 2000 and 2003
- Describe the features of GroupShield 6.0 for Exchange
- Configure GroupShield 6.0 Policies for Anti-Virus Scanning
- Configure GroupShield 6.0 Policies for Content Scanning
- Install and Configure SpamKiller 2.1 for Microsoft Exchange
- Configure ePolicy Orchestrator to manage GroupShield 6.0 and SpamKiller 2.1
- How to troubleshoot GroupShield 6.0
- Identify other scanning products in the McAfee Security product line

### Suggested Next Course

To gain a core set of skills and knowledge on anti-virus management, participants may also choose to attend:

- McAfee Intranet Defense: VirusScan and ePolicy Orchestrator (TRN-AVD-101-TCL)
- Anti-virus Administration for WebShield (TRN-AVD-301-TCL)

### Contact Information

Phone: 866-210-2715

E-mail: [education@mcafee.com](mailto:education@mcafee.com)

Website: [www.mcafee.com](http://www.mcafee.com)

## Daily Outline

### Day 1

#### **GroupShield Exchange**

- Exchange Concepts
- Understanding Anti-Virus Scanning within Microsoft Exchange
- Scanning methods in GroupShield for Exchange
- Common features
- Protect information as a mail resource and information share
- System Requirements for installing GroupShield 6.0 for Microsoft Exchange
- Methods for installing GroupShield for Exchange
- System changes
- GroupShield Services
- Maintenance including upgrade, repair, and removal
- Lab: Create / configure distribution lists for administrators
- GroupShield 6.0 Features
- GroupShield 6.0 Components
- GroupShield 6.0 Add on packages
- GroupShield Interface – Local, Remote, Web
- How to access the different GroupShield interfaces
- Setting GroupShield access rights
- Lab: Installing GroupShield 6.0 for Exchange 2000
- Lab: Configuring and testing GroupShield access
- Lab: Accessing the GroupShield interface remotely
- Lab: Accessing the GroupShield web interface
- Understanding Threats to your organization
- Understanding GroupShield Policies
- Configure Global Policies for Anti-Virus, Content Scanning, File Filtering, Encryption, Scanner Control, & Signed Messages
- How to configure Disclaimer text in a Gateway Policy
- How to configure the Mail size filtering Policy
- Understanding Rule Group and Content Rules
- How to configure a Rule Group
- How to configure a Content Rule
- Assigning Rule Groups to a Policy Group
- Understand and Configure a Policy Group
- How to setup Notifications in GroupShield 6.0
- Labs: Configure Global On-Access Policy for Anti-Virus, Content Scanning, File Filtering, create a Rule Group, create a Content Rule
- Labs: Testing the Global On-Access Policy
- Labs: Creating a Policy Group
- Labs: Creating a Policy for a Policy Group and testing the policy
- Understanding and configuring the On-Access settings for VSAPI or Transport scanning
- VSAPI 2.0 and VSAPI 2.5 differences
- Detected Items Database
- New Updating features in GroupShield 6.0
- Creating an On-Demand scan with GroupShield Policies
- Labs: Setting an DAT update

#### **OutBreak Manager & Alert Manager**

- Concepts
- Rules – Trigger, Threshold, Reaction, and Response
- Viewing Rule status
- Viewing OutBreak activity
- Lab: Configure an Outbreak Manager rule set

- Lab: Configure GroupShield 6.0 Outbreak Policy settings
- Lab: Simulate an Outbreak and test OutBreak rules

### Day 2

#### **SpamKiller**

- SpamKiller Concepts
- Common system requirements
- Product features
- Methods of Detection
- SpamKiller Console and Settings
- SpamKiller Actions and Rules
- Blacklist and Whitelist
- Management Tasks
- The Web interface
- Create custom rules with Perl regular expressions
- Management Tasks
- Lab: Installing SpamKiller
- Lab: Configure SpamKiller
- Lab: Testing the SpamKiller Installation
- Lab: The Global Blacklist tab
- Lab: The Global Whitelist tab
- Lab: Weighted SPAM
- Lab: Global Blacklist to and Global Whitelist to
- Lab: Configuring User's personal Blacklists and Whitelists
- Lab: Add/Create a rule using PERL
- Lab: Remove SpamKiller

#### **GroupShield and ePolicy Orchestrator**

- Installation review
- GroupShield Configuration
- Adding GroupShield to ePO
- Policy Enforcement
- GroupShield and ePO Policies – Similarities
- GroupShield and ePO Policies – Differences
- Lab: Add the GroupShield NAP files into ePO
- Lab: Deploy the ePO Agent to the GroupShield Server
- Lab: Installing GroupShield 6.0 and SpamKiller from ePO
- Lab: Use ePO to set and enforce a GroupShield policy
- Lab: Use ePO to set and enforce a SpamKiller policy
- Lab: Generate and View Alerts within ePO
- Lab: Confirm ePO GroupShield reports

#### **Monitoring and Troubleshooting GroupShield for Exchange**

- Log Viewer
- Quarantine Viewer
- Performance Monitor
- Troubleshooting Tools
- Minimum Escalation Requirements