

# Microsoft® Antigen Enterprise Manager

## Centralized Control of E-mail Security

Microsoft® Antigen Enterprise Manager helps businesses centrally control their Antigen protection for Exchange and SMTP Gateway servers.

### Centralized Security Control

As threats to e-mail communication continue to grow and evolve, businesses are adding layers of security to protect this critical entry point and propagation vector against malicious code. As more layers of security are added, however, new challenges arise in the ability to manage and control these defenses.

Providing integrated control over e-mail security allows IT administrators to lower the overall cost of protecting critical communications that help fuel organizational efficiency and innovation, as well as reduce the risk of vulnerabilities with automated updates and central configuration.

### Antigen Enterprise Manager

Antigen Enterprise Manager from Microsoft® helps businesses centrally manage the security of their e-mail servers.

The easy-to-use central console simplifies the management of Antigen antivirus, anti-spam and content filtering technologies, enabling these layered defenses with centralized deployment, configuration and update distribution for maximum protection against the latest security threats.

Antigen Enterprise Manager also ensures performance of Antigen servers with

monitoring and notification features, as well as extensive reporting tools that allow administrators to easily summarize detected threat activity across the organization.

Antigen Enterprise Manager supports Antigen for Exchange, Antigen for SMTP Gateways, and Antigen Spam Manager.

### How Antigen Enterprise Manager Works

Antigen Enterprise Manager is a browser-based management console for all Antigen products, providing remote deployment, distributed quarantine management, centralized updating, comprehensive reporting, and SMTP/SNMP alerting. It can be deployed with Windows® 2000 Server or Windows Server™ 2003 and acts as a central distribution point for antivirus and anti-spam signature updates within an organization. Antigen Enterprise Manager communicates with all Antigen products throughout an enterprise via agents deployed on remote Antigen servers.

### Central Deployment and Configuration

Through a hub and spoke architecture, Antigen Enterprise Manager communicates with agents deployed on Antigen e-mail server security products. With this centralized control, IT administrators can remotely install products, retrieve log files, and apply upgrades, hot fixes, patches, configuration templates and signature files.

Antigen Enterprise Manager maintains constant contact with agents on enterprise servers protected by Antigen, allowing IT administrators to apply configuration changes quickly to individual servers or groups of servers, and centrally configure on-demand and scheduled manual scans of Antigen-protected Exchange Information Store.

### Centralized Updates

Antigen Enterprise Manager automates antivirus and anti-spam engine updates across remote servers with a unique push-pull architecture.

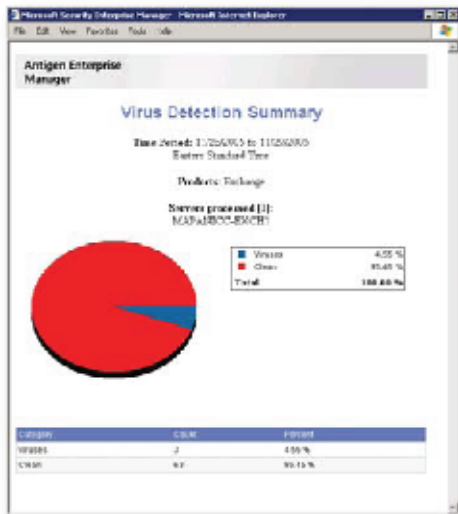
To ensure that engines have the latest signature files, Microsoft's signature update process automatically downloads updates from scan engine partners as soon as they are available and tests them against an internal virus database. Within minutes, these engines and signatures are tested, confirmed, posted, and made available for all Antigen servers.

Antigen Enterprise Manager's integrated scheduler polls the Microsoft web site for updates and downloads every 15 minutes, or an administrator-defined interval. When new signatures are available, Antigen Enterprise Manager downloads the new engines and signature files and then sends an alert to all Antigen servers. Each Antigen server then automatically pulls the update from Antigen Enterprise Manager.

This automation reduces the window of exposure that exists when deploying updated engines and virus signatures, ensuring that businesses are protected against the latest threats. It also provides organizations with more efficient Internet bandwidth usage.

### Distributed Quarantine Management

Antigen Enterprise Manager centrally manages quarantines across multiple Antigen servers, allowing an administrator to easily locate a specific email, no matter which server it resides on. The quarantine can be searched based on sender, recipient, date, or subject line.



### Comprehensive Reports

Antigen Enterprise Manager collects information and generates graphical reports highlighting actions taken, message traffic, unusual detection activity, and current engine versions from all Antigen protected servers.

### Action Reports

Reports that track actions taken by Antigen servers upon detection of a virus, spam or content violation. These reports can be detailed by messages skipped, purged, filtered or deleted.

### Message Traffic Reports

More than a dozen built-in configurable reports are available for administrators to collect and graph SMTP, virus and spam traffic, including bytes processed per Antigen server or group of servers for specified periods of time.

### Detection Reports

Reports that summarize and graph data on detected viruses, spam and filter matches are readily available for administrator-selected servers or groups of Antigen servers.

### Current Engine Reports

Reports allow administrators to easily track and confirm that all antivirus and anti-spam engines have been updated. Each report provides engine version and update status on all Antigen servers in an organization.

### Report Distribution

Through the Antigen Enterprise Manager console, administrators can automatically pre-configure HTML reports and have them regularly e-mailed to selected recipients. These reports can be viewed through Microsoft Outlook®, Internet Explorer or Microsoft Word.

### Outbreak and Engine Alerts

Antigen Enterprise Manager is designed to proactively alert administrators when there is a virus or spam outbreak, or when thresholds are exceeded for file and content filters. Administrators can define and configure specific thresholds (overall count or a percentage), which if exceeded, sends an SMTP or SNMP alert. Antigen Enterprise Manager also provides SMTP and SNMP alerts that inform IT administrators of the success or failure of antivirus or anti-spam scan engine updates. This ensures that all Antigen-protected servers are running with the most current scan engines and signature files available.

This information can also be provided to network management solutions like Microsoft Operations Manager (MOM).

## Antigen Enterprise Manager System Requirements

Features and functionality described require Microsoft® Windows Server™ 2003 or Windows® 2000; 128MB of available RAM; 65 MB of available server disk space; and 183MB available disk space for the following prerequisites: IIS v5.0 or higher, .Net Runtime v1.1, ASP.net v1.1, Microsoft Message Queue and SMMQ Triggers, and MSDE or SQL Server™ 2000.

For more information about Antigen Enterprise Manager, visit: <http://www.microsoft.com/antigen>