

McAfee System Protection Solutions

McAfee PortalShield

For Microsoft SharePoint Server

A portal provides a way for organizations to connect and share data with employees, customers, and partners. It is vital to ensure that the portal's content is secure, while maintaining uninterrupted access to information. Unfortunately, as users share documents via portals, they also gain the capacity to share harmful viruses, worms, malicious code, and inappropriate content, wreaking havoc on company servers and compromising corporate systems and networks. Weak business justification and organizational confusion (ill-defined roles, ownership, and sponsorship) also add to the problems in securing a portal. As businesses increase productivity and activity over portals, so increases the potential threats associated with securing and maintaining them.

Part of the McAfee® Secure Content Management Family, McAfee PortalShield™ for Microsoft® SharePoint Server is content security for all documents, files, Web content, and document stores. McAfee PortalShield provides:

- Comprehensive protection from viruses
- Enterprise policy management and graphical reporting
- Secure content management
- Lower total cost of ownership

With PortalShield, users of Microsoft SharePoint are able to securely access, find, and share the information they need to be productive in business, regardless of the physical location of information on the portal. PortalShield's capabilities go beyond traditional anti-virus and content security solutions to protect Microsoft SharePoint servers by detecting, cleaning, and removing viruses, as well as searching for banned content within the documents that are stored in SharePoint workspaces, a capability not available with traditional anti-virus or content security solutions.

With a single software package that provides comprehensive anti-virus scanning for all documents, files, Web content, and document stores on servers running SharePoint Portal Server, PortalShield addresses the need for enterprise organizations and small- to medium-sized businesses to deploy comprehensive anti-virus technologies that are flexible and manageable, helping companies reduce their vulnerability to malicious attacks targeted at content and confidential data.

Integrated with McAfee ePolicy Orchestrator® (ePO™), and the first solution to protect Microsoft SharePoint 2003, PortalShield offers comprehensive policy management and enforcement,

enterprise-wide visibility, rapid software deployment, and distribution of the latest virus definition updates to protect the collaborative computing environments.

Proactive Protection from Viruses

McAfee delivers comprehensive *find-and-fix* solutions for today's threats and makes use of advanced heuristic and generic techniques to protect—in advance—against new threats. Using the award-winning virus scanning and cleaning engine, PortalShield protects Microsoft SharePoint's document libraries and Web parts from infection by viruses, worms, Trojans, and other malicious threats.

Graphical Reporting and Centralized Policy Management

PortalShield integrates with ePolicy Orchestrator, enabling organizations to maximize their security management investment. ePO provides a centralized authority to enforce protection as well as comprehensive and graphical reports, detailing critical protection coverage information that answer such questions as *Are all my PortalShield servers protected with the latest engine and DATs?* In addition, ePolicy Orchestrator provides remote deployment, enabling large enterprise deployments to be easily managed from a central location.

Advanced Content Management

The world of e-business presents new threats that render many organizations susceptible to poor image and legal liability from unauthorized information leakage or employee misconduct, which also results in lost productivity. Lexical scanning and content management capabilities enable PortalShield to apply rules to over 280 document types including Adobe Acrobat and Microsoft Office. Using PortalShield content management rules, Microsoft SharePoint 2003 can prevent document download and upload action, in addition to sending alerts to the administrator if the documents contain sensitive or offensive information. Administrators can even avoid bandwidth degradation by not allowing non-business-related files (e.g., MP3 or AVI files) to be uploaded to the SharePoint Server.

Preset Content Rules

The difficulty with preventing inappropriate content such as profanity or racism is knowing what rules you need in order to be effective and lacking time to establish rule sets. PortalShield's preset rules ensure successful content management and provide

ease of use. In addition, administrators can fine-tune rules using advanced custom rule sets.

Web Administration

PortalShield offers administrators a secure and easy-to-use Web-based administration console that provides local and remote management and configuration of PortalShield.

Web-Parts Scanning

PortalShield has the capability to scan Web parts, as well as the document libraries of a server running SharePoint products and technologies. This enables PortalShield to protect, not only document stores, but also the portal's digital dashboard.

Microsoft VSAPI

PortalShield offers tight integration with the Microsoft VSAPI, to provide on-access scanning, on-demand scanning, and background scanning of the document libraries. PortalShield uses Microsoft VSAPI 2.0 for SharePoint Portal Server 2001. When used with SharePoint Server 2003, PortalShield will utilize Microsoft WSS VSAPI 1.0.

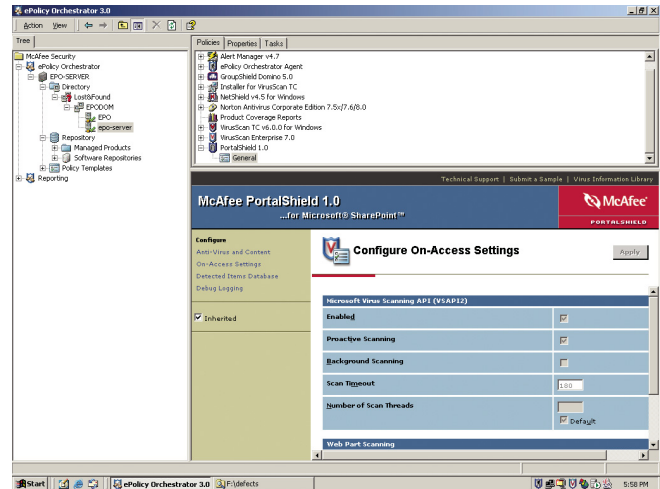
Enterprise Rollout

Using ePolicy Orchestrator, PortalShield can be remotely installed, allowing administrators to easily and rapidly install to multiple locations. ePolicy Orchestrator also enables centralized reporting of PortalShield activity. The ability to centrally manage an organization-wide implementation of the PortalShield software reduces the time required to administer and update systems.

Automatic Updating

Like all McAfee solutions, PortalShield can automatically update virus definitions and engines to ensure that Microsoft SharePoint is protected with the latest protection.

The PortalShield software integrates with Microsoft SharePoint to scan documents and Web parts for viruses and banned content. Each time a document is written or read, or a Web part is written to or from the Web store, PortalShield scans the content and compares it with a list of known viruses and suspected virus-like behavior. PortalShield also scans for content within the document or Web part, using rules and policies defined within PortalShield's content management engine.



PortalShield fits seamlessly into ePolicy Orchestrator and integrates with the enterprise security policy management and reporting strategy.

PortalShield uses the virus-scanning interface provided within SharePoint to gain full access to all documents and discussions that are being read from or written to the Web store by SharePoint. This provides a method where all files are presented to PortalShield for scanning by the virus-scanning and content management engines before being written to the file system or read by users of SharePoint. Once presented to PortalShield, the virus-scanning engine compares the document with all the known virus signatures stored within the current and installed virus definition (DAT) file, as well as checks the document utilizing selected heuristic detection methods. The content management engine searches the document for banned content (as specified in the content management policies) in real time or when an on-demand scan is initiated. If these checks do not find any virus or banned content within the document, PortalShield then passes the information back to virus-scanning API for completion of the original document request within SharePoint.

If a virus is detected within the document or the content management engine detects that a content rule has been violated, PortalShield takes the appropriate actions that have been defined within its configuration settings. These actions are usually set to clean and remove viruses from the document or to block the document if banned content is detected.

System Requirements

Note: The following are general system requirements and may vary depending on the nature of your environment.

Microsoft SharePoint Portal Server 2001

- Windows® Server 2000/2003 and Microsoft Internet Information Services (IIS) 5.0 or later
- Internet Explorer v5.5 or later installed

Microsoft SharePoint Portal Server 2003

- Windows Server 2003 and Microsoft Internet Information Services (IIS) 6.0 or later
- Internet Explorer v6.0 or later installed

Microsoft Windows SharePoint Services

- Windows Server 2003 and Microsoft Internet Information Services (IIS) 6.0 or later
- Internet Explorer v6.0 or later installed

McAfee PrimeSupport

McAfee has pursued a strategy of providing best-of-breed technology for each type of security and performance management application—but the Protection-in-Depth™ Strategy is more than just deploying and implementing best-of-breed solutions today. Prevention is certainly our first priority, but inevitably, you will have to react to a problem.

The McAfee PrimeSupport® program is essential for making the most of your investment in McAfee System and Network Protection Solutions. McAfee's PrimeSupport team has all the right resources and is ready to deliver your needed service solution. PrimeSupport resources include: delivering authorization to access all available maintenance releases and product upgrades, access to a comprehensive suite of additional online self-support capabilities, live telephone support accessible 24/7/365, available assigned support account managers, and a range of software and hardware support solutions that can be tailored to meet your needs.

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com

McAfee® products denote years of experience and commitment to customer satisfaction. The McAfee PrimeSupport® team of responsive, highly skilled support technicians provides tailored solutions, delivering detailed technical assistance in managing the success of mission-critical projects—all with service levels to meet the needs of every customer organization. McAfee Research, a world leader in information systems and security research, continues to spearhead innovation in the development and refinement of all our technologies.

McAfee, PortalShield, ePolicy Orchestrator, ePO, Protection-in-Depth, and PrimeSupport are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. The color 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.
© 2004 Networks Associates Technology, Inc. All Rights Reserved. 1-sps-psh-002-1004