Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes and the latest version of the Getting Started Guide, which are available from Trend Micro’s Web site at:

www.trendmicro.com/download/

NOTE: A license to the Trend Micro Software usually includes the right to product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase only. Maintenance must be reviewed on an annual basis at Trend Micro’s then-current Maintenance fees.

Trend Micro, the Trend Micro t-ball logo, PortalProtect, IntelliScan, ActiveAction, and MacroTrap are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright© 2002 - 2011 Trend Micro Incorporated. All rights reserved. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted without the express prior written consent of Trend Micro Incorporated.

Document Part No. PPEM24425/100310

Release Date: June, 2011

Protected by U.S. Patent No. 5,951,698

The Administrator’s Guide for Trend Micro PortalProtect is intended to introduce the main features of the software and provides instructions to configure Portal Protect according to your specific needs. You should read this guide completely before installing or using the software.
For technical support, please refer to Contacting Trend Micro in this Administrator’s Guide. Detailed information about how to use specific features within the software is available in the Online Help file and online Solution Bank at Trend Micro’s Web site.

Trend Micro is always seeking to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please contact us at docs@trendmicro.com. Your feedback is always welcome. Please evaluate this documentation on the following site:

www.trendmicro.com/download/documentation/rating.asp
Chapter 1: Welcome to Trend Micro™ PortalProtect™

What’s New in PortalProtect Version 2.0 ................................................. 1-2
  Installation Enhancements ................................................................. 1-3
  Supports both Local and Remote Installation .................................. 1-4
  Installation with Remote SQL ............................................................ 1-4
  Content Filtering Scans .................................................................... 1-4
  Management Enhancements .............................................................. 1-5
    Single Sign On (SSO) ................................................................. 1-5
    Real-time Monitor .................................................................... 1-5
    Server Management ................................................................. 1-5
    Quarantine Management ............................................................ 1-5
What’s New in PortalProtect 2.1 .............................................................. 1-5
  Smart Scan ................................................................................... 1-5
  Supports Trend Micro Control Manager 5.5 SP1 ................................. 1-6
  Web Reputation for Document ......................................................... 1-6
  Data Protection ............................................................................... 1-6
  Event Tracking ............................................................................... 1-6
  Access Control ............................................................................... 1-6
  RBS Support ................................................................................. 1-6
  Configuration for Automatic Replication ......................................... 1-7
Global Approved List ........................................................................ 1-7
Benefits and Capabilities .................................................................. 1-9
How Viruses Infect SharePoint Environments ...................................... 1-10
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>How PortalProtect Protects SharePoint Servers</td>
<td>1-10</td>
</tr>
<tr>
<td>PortalProtect Architecture</td>
<td>1-12</td>
</tr>
<tr>
<td>Controlling Outbreaks</td>
<td>1-13</td>
</tr>
<tr>
<td>PortalProtect Technology</td>
<td>1-14</td>
</tr>
<tr>
<td>About the Trend Micro Scan Engine</td>
<td>1-15</td>
</tr>
<tr>
<td>About Scan Engine Updates</td>
<td>1-16</td>
</tr>
<tr>
<td>About the Virus Pattern File</td>
<td>1-16</td>
</tr>
<tr>
<td>How Scanning Works</td>
<td>1-17</td>
</tr>
<tr>
<td>Pattern File Numbering</td>
<td>1-17</td>
</tr>
<tr>
<td>About ActiveUpdate</td>
<td>1-18</td>
</tr>
<tr>
<td>Incremental Updates of the Virus Pattern File</td>
<td>1-18</td>
</tr>
<tr>
<td>Using ActiveUpdate with PortalProtect</td>
<td>1-18</td>
</tr>
<tr>
<td>About Trend Micro IntelliScan™</td>
<td>1-18</td>
</tr>
<tr>
<td>About Smart Protection Network</td>
<td>1-19</td>
</tr>
<tr>
<td>Smart Protection Services</td>
<td>1-19</td>
</tr>
<tr>
<td>Web Reputation</td>
<td>1-20</td>
</tr>
<tr>
<td>Smart Protection Sources</td>
<td>1-20</td>
</tr>
<tr>
<td>True File Types</td>
<td>1-20</td>
</tr>
<tr>
<td>About IntelliTrap</td>
<td>1-21</td>
</tr>
<tr>
<td>Trend Micro™ ActiveAction™</td>
<td>1-22</td>
</tr>
<tr>
<td>Customized Settings</td>
<td>1-22</td>
</tr>
<tr>
<td>Using Customized Scan Actions</td>
<td>1-22</td>
</tr>
<tr>
<td>Types of Threats</td>
<td>1-23</td>
</tr>
<tr>
<td>Possible Actions</td>
<td>1-23</td>
</tr>
<tr>
<td>About Macro Viruses</td>
<td>1-25</td>
</tr>
<tr>
<td>About Encrypted and Password Protected Files</td>
<td>1-25</td>
</tr>
<tr>
<td>About Unscannable Files</td>
<td>1-26</td>
</tr>
<tr>
<td>Scan Compressed Files</td>
<td>1-26</td>
</tr>
<tr>
<td>Maintenance Agreement</td>
<td>1-27</td>
</tr>
<tr>
<td>Renewing Your Maintenance Agreement</td>
<td>1-28</td>
</tr>
</tbody>
</table>

**Chapter 2: Getting Started with PortalProtect**

- Viewing the PortalProtect Web Management Console                     | 2-2
- Registering PortalProtect                                             | 2-3
- Activating PortalProtect                                               | 2-4
Chapter 3: Configuring Scanning and Blocking

About Scans ..................................................................................................... 3-2
Configuring Scan Options ............................................................................. 3-2
About Scanning .......................................................................................... 3-3
   Enabling and Disabling Real-time Security Risk Scan ....................... 3-4
Smart Protection Source ........................................................................... 3-4
Backup Files Before Taking Action ............................................................ 3-6
   Specify a Backup Folder for Security Risk Scan ............................... 3-7
   Specify a Backup Folder for Manual Scan ........................................ 3-8
   Specify a Backup Folder for Scheduled Scan .................................... 3-11
About Advanced Macro Scan ..................................................................... 3-13

Chapter 4: Security Risk Scans

File Reputation .............................................................................................. 4-1
   Choose a Security Risk Scan Method .................................................. 4-2
   Enable or Disable Real-time Security Risk Scan ................................. 4-3
About Security Risk Scan Target Settings ............................................... 4-3
   Security Risk Scan Target Settings .................................................... 4-3
Configure Macro Scanning Options for Real-time Security Risk Scan
4-5
About Security Risk Scan Action Settings ..............................................4-6
Configuring Security Risk Scan Action Settings ....................................4-6
Scan Compressed Files ..............................................................................4-8

Chapter 5: File Blocking
About File Blocking Action Settings .......................................................5-2
Possible Actions .....................................................................................5-3
Configuring File Blocking for MOSS 2010/WSS 4.0 .............................5-4
Adding a File Blocking Policy (MOSS 2010/WSS 4.0) .........................5-4
Configuring File Blocking for MOSS 2007/WSS 3.0 ...........................5-10
Configuring File Blocking: Target Settings ......................................5-10
Configuring File Blocking: Action Settings ..........................................5-12
About Available File Types .....................................................................5-12
Application and Executables .............................................................5-12
Documents ...........................................................................................5-13
Images ...................................................................................................5-15
Video .....................................................................................................5-15
Audio .....................................................................................................5-16
Compressed Files .................................................................................5-17

Chapter 6: Content Filtering
About Content Filtering Action Settings ...............................................6-2
Content Filtering Policies ..........................................................................6-3
Policy Exceptions ..................................................................................6-3
Global Approved List (Real-time) ......................................................6-4
Configuring Content Filtering ..............................................................6-7
Adding a Content Filtering Policy (MOSS 2010/WSS 4.0) .................6-9
Adding a Content Filtering Policy (MOSS 2007/WSS 3.0) .............6-18
Edit a Content Filtering Policy (MOSS 2010/WSS 4.0) .................6-24
Edit a Content Filtering Policy (MOSS 2007/WSS 3.0) .............6-27

Chapter 7: Data Protection
Configuring Data Protection Policies ......................................................7-1
Adding a Data Protection Policy (MOSS 2010/WSS 4.0) .................7-2
Chapter 8: Web Reputation

Local and Global Smart Protection .......................................................... 8-2
Choose a Web Reputation Source ......................................................... 8-3
Enabling Real-time Web Reputation ...................................................... 8-4
About Web Reputation: Target Settings ................................................ 8-5
Configuring Web Reputation: Target Settings ....................................... 8-6
About Web Reputation: Action Settings ................................................. 8-7
Configuring Web Reputation: Action Settings ....................................... 8-8
Web Reputation: Notifications ............................................................... 8-8
Smart Protection Network ....................................................................... 8-8

Chapter 9: Manual Scan

Configuring a Manual Scan ................................................................. 9-3
Scan Compressed Files for Manual Scan ............................................. 9-4
Configure Macro Scanning Options for Manual Scan ...................... 9-5
Configure Manual Scan: Security Risk Scan .................................... 9-6
Configure Manual Scan: File Blocking .............................................. 9-10
Configure Manual Scan: Content Filtering ...................................... 9-14
Configure Manual Scan: Data Protection ......................................... 9-20
Configure Manual Scan: Web Reputation ........................................ 9-24

Chapter 10: Scheduled Scan

Configuring a Scheduled Scan .......................................................... 10-2
Add or Edit a Scheduled Scan Task ..................................................... 10-2
Configure Macro Scanning Options for Scheduled Scan ............. 10-5
Scan Compressed Files for Scheduled Scan ................................. 10-5
Configure Scheduled Scan: Security Risk Scan ......................... 10-6
Configure Scheduled Scan: File Blocking Scan ........................................... 10-8
Configure Scheduled Scan: Content Filtering ............................................ 10-11
Configure Scheduled Scan: Data Protection .............................................. 10-13
Configure Scheduled Scan: Web Reputation ............................................. 10-15

Chapter 11: Notifications, Alerts, Logs, and Reports

Configuring Notifications ................................................................................. 11-2
Global Notification Settings ........................................................................... 11-2
  Security Risk Scan Notifications ............................................................... 11-3
  File Blocking Notifications ..................................................................... 11-4
  Content Filtering Notifications ............................................................... 11-6
  Data Protection Notifications ................................................................. 11-7
  Web Reputation Notifications .................................................................. 11-8

Manual Scan Notifications ............................................................................ 11-10
  Manual Scan Notifications—Security Risk Scan ...................................... 11-10
  Manual Scan Notifications—File Blocking .............................................. 11-11
  Manual Scan Notifications—Content Filtering ....................................... 11-13
  Manual Scan Notifications—Data Protection .......................................... 11-14
  Manual Scan Notifications—Web Reputation .......................................... 11-16

Scheduled Scan Notifications—Security Risk Scan ...................................... 11-18
Scheduled Scan Notifications—File Blocking .............................................. 11-19
Scheduled Scan Notifications—Content Filtering ....................................... 11-21
Scheduled Scan Notifications—Data Protection .......................................... 11-23
Scheduled Scan Notifications—Web Reputation .......................................... 11-25

Alerts ............................................................................................................. 11-26
  System Events .......................................................................................... 11-26
  Outbreak Alert ......................................................................................... 11-31

About Access Control .................................................................................... 11-32
  Access Control Authentication .................................................................. 11-33
  Access Control Permissions ...................................................................... 11-34

Working with Logs ....................................................................................... 11-34
  Query Logs .............................................................................................. 11-35
  Log Maintenance ..................................................................................... 11-37
    Manually Delete Logs ........................................................................... 11-37
    Automatically Delete Logs .................................................................... 11-38
Central Quarantine Management ............................................................. 11-40
Quarantine Query .................................................................................. 11-40
Delete, Restore, or Download Quarantined Files ............................. 11-44
Quarantine Maintenance ....................................................................... 11-45
Viewing and Generating Reports ............................................................. 11-47

Chapter 12: Getting Support and Contacting Trend Micro

Contacting Trend Micro .............................................................................. 12-2
Before Contacting Technical Support ......................................................... 12-2
Contacting Technical Support ................................................................. 12-3
TrendLabs ................................................................................................. 12-4

Frequently Asked Questions (FAQ) .......................................................... 12-5
    Scanning ............................................................................................... 12-5
    Active Update ...................................................................................... 12-9
    General Issues ................................................................................... 12-10

Appendix A: Using Control Manager with PortalProtect

Introducing Control Manager ................................................................. A-2
    Key Features ........................................................................................ A-2
    Using Control Manager with PortalProtect ........................................ A-3

Introducing the Control Manager Management Communication Protocol A-3

Introducing Outbreak Prevention Services ................................................. A-4

Using Control Manager to Administrate PortalProtect ......................... A-4
    Accessing the Control Manager Management Console .................. A-5
    Managing PortalProtect from the Control Manager Management Console .......................................................... A-5

    Viewing an Active Outbreak Prevention Policy ............................. A-6

Create a Report Template ............................................................................. A-6

Appendix B: About Regular Expressions
Preface

Welcome to the Trend Micro™ PortalProtect™ Administrator’s Guide. This guide contains the information you need to configure PortalProtect to protect your SharePoint servers according to your specific needs.

This preface discusses the following topics:

- **PortalProtect Documentation**
- **Audience**
- **Document Conventions**

**PortalProtect Documentation**

PortalProtect documentation consists of the following:

- **Online Help**—Web-based documentation that is accessible from the product console. The Online Help contains explanations about PortalProtect features.
- **Installation and Deployment Guide (IG)**—PDF documentation that is accessible from the Solutions DVD for PortalProtect. It can also be downloaded from the Trend Micro Web site. This document contains instructions about deploying PortalProtect, a task that includes planning and testing.
- **Administrator’s Guide**—Helps you configure all product settings.
• **Readme File**—Contains late-breaking product information that might not be found in the other documentation. Topics include a description of features, installation tips, known issues, and product release history.

**Tip:** Trend Micro recommends checking the corresponding link from the Update Center (http://www.trendmicro.com/download) for updates to the documentation.

**Audience**

PortalProtect documentation assumes a basic knowledge of security systems and administration of SharePoint services. The Installation and Deployment Guide, Administrator’s Guide, and Online Help are designed for network administrators.

**Document Conventions**

To help you locate and interpret information easily, the PortalProtect documentation uses the following conventions.

<table>
<thead>
<tr>
<th><strong>TABLE I-1. Conventions used in PortalProtect documentation</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CONVENTION</strong></td>
</tr>
<tr>
<td>ALL CAPITALS</td>
</tr>
<tr>
<td><strong>Bold</strong></td>
</tr>
<tr>
<td>Monospace</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td><strong>Tip:</strong></td>
</tr>
</tbody>
</table>
### TABLE I-1. Conventions used in PortalProtect documentation

<table>
<thead>
<tr>
<th>CONVENTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WARNING!</strong></td>
<td>Reminders on actions or configurations that should be avoided</td>
</tr>
</tbody>
</table>
Welcome to Trend Micro™ PortalProtect™

Trend Micro PortalProtect™ is a server-based security solution for Microsoft Windows™ SharePoint™ Services 3/4, including Microsoft Office SharePoint™ Server 2007/2010. Trend Micro designed PortalProtect to provide protection against attacks from viruses and other security threats.

Trend Micro designed PortalProtect to integrate with Microsoft Windows™ SharePoint™ Services and built it on proven enterprise security technology. It provides real-time background scanning of all content whenever it is checked-in, checked-out or published to a SharePoint Server. It also provides manual and scheduled scanning of content stored in the SharePoint Services SQL content store.

PortalProtect offers comprehensive and centralized management and notification features. You can use these features to perform tasks like: sending notifications, generating reports, and making log queries. Automated notification features like Outbreak Alert allow you to detect attacks early and react decisively.

This chapter introduces PortalProtect, including its benefits and capabilities. It discusses the security threats to your SharePoint environments and how PortalProtect protects against these threats.
In this chapter, you will find information about:

- What’s New in PortalProtect Version 2.0 on page 1-2
- What’s New in PortalProtect 2.1 on page 1-5
- Global Approved List on page 1-7
- Benefits and Capabilities on page 1-9
- How Viruses Infect SharePoint Environments on page 1-10
- How PortalProtect Protects SharePoint Servers on page 1-10
- PortalProtect Architecture on page 1-12
- PortalProtect Technology on page 1-14
- Maintenance Agreement on page 1-27

What’s New in PortalProtect Version 2.0

Installation Enhancements (see Installation Enhancements on page 1-3)

- Supports the latest versions of SharePoint
- Supports both local and remote installation
- Supports installation with remote SQL server

Content Filtering (see Content Filtering Scans on page 1-4)

- Provides real-time, manual, and scheduled Content Filtering for both file and Web content

Web Reputation Filtering (see Management Enhancements on page 1-5)

- Web Reputation scans URLs in Web content and applies configurable actions when malicious URLs are detected.
Microsoft Active Directory (AD) Integration
• This enhancement supports File Blocking policies and Content Filtering policies with Active Directory users and groups as an exception list.

SharePoint User(s)/Group(s) Integration
• This enhancement supports File Blocking policies and Content Filtering policies with SharePoint users and groups as an exception list.

Management Enhancements (see Management Enhancements on page 1-5)
• Supports Single Sign-On (SSO)
• Provides a Real-Time Monitor
• Server Management
• Quarantine Management

Installation Enhancements
PortalProtect 2.0 supports the latest versions of Windows and SharePoint, including:

SharePoint Versions
• Windows SharePoint Services (WSS) 3.0 x86/x64
• Window SharePoint Services (WSS) 4.0 x64
• Microsoft Office SharePoint Server (MOSS) 2007 x86/x64
• Microsoft Office SharePoint Server (MOSS) 2010 x64

Windows Versions
• Windows 2003 Series
  Windows Server 2003, Standard Edition x86/x64
  Windows Server 2003, Enterprise Edition x86/x64
  Windows Server 2003 R2, Standard Edition x86/x64
  Windows Server 2003 R2, Enterprise Edition x86/x64
• Windows 2008 series
  Windows Server 2008 Standard Edition x86/x64
  Windows Server 2008 Enterprise Edition x86/x64
  Windows Server 2008 R2 Enterprise Edition x64
Windows Server 2008 R2 Standard Edition x64
Microsoft Windows Server 2008 Datacenter x64
Microsoft Windows Web Server 2008 x64
Microsoft Windows Server 2008 HPC x64

Supports both Local and Remote Installation

The previous version of PortalProtect (1.8) supported only remote installation. PortalProtect 2.0 supports both local and remote installation in the user interface. The local installation option enables you to install to a single machine. Remote installation enables you to install to multiple servers during the installation process.

Installation with Remote SQL

PortalProtect 2.0 supports storing the PortalProtect database on a remote SQL server when performing a fresh installation. The following Windows platforms are supported:

- All Windows platforms are supported in the 2003/2008 series

The following SQL server versions are supported:

- SQL 2005 Express Edition
- SQL 2005 Standard Edition
- SQL 2005 Enterprise Edition
- SQL 2008 Express Edition
- SQL 2008 Standard Edition
- SQL 2008 Enterprise Edition

Content Filtering Scans

Whenever a file or Web content is uploaded or posted to SharePoint sites, Content Filtering evaluates it according to user-defined policies. Each policy contains a list of keywords and phrases. Content filtering compares the file or Web content with the list of these keywords and phrases and takes the pre-selected action against it in real-time.

Additionally, this enhancement enables the user to select both manual and scheduled scans for Content Filtering.
Management Enhancements

PortalProtect provides several management enhancements for this release. This section provides a summary:

Single Sign On (SSO)

This enhancement enables the user to logon using the same credentials as their Windows account. This option is presented from the Web UI during logon.

Real-time Monitor

The Real-time Monitor provides a quick view of the activity and settings for PP 2.0, including the Server Name, Virus Pattern, Scanning Status, Scanned Messages, and so on. You can reset the various counts and clear contents as needed.

Server Management

Server management provides the functionality to query information and do settings replication of all PP servers in a farm. The information includes engine/pattern version, scanning status, scanning result and last replication.

Quarantine Management

Quarantine Management provides the functionality to manage all quarantined files in a farm even though they were quarantined by a different PortalProtect on different server. The PortalProtect administrator can query, delete, restore or download quarantined files.

What’s New in PortalProtect 2.1

Smart Scan

Smart scan moves security capabilities from the server to the cloud. As an integral part of the Trend Micro Smart Protection Network, smart scan provides the following benefits:

- Fast, real-time security status lookup capabilities in the cloud
- Reduces the overall time it takes to deliver protection against emerging threats
• Lowers memory consumption on endpoints

Supports Trend Micro Control Manager 5.5 SP1

This version of PortalProtect supports Trend Micro Control Manager 5.5 SP1.

Web Reputation for Document

Web reputation now scans for URLs contained within documents and then applies configurable actions when malicious URLs are detected. Additionally, this enhancement enables the user to select both manual and scheduled scans for Web Reputation. See About Smart Protection Network on page 1-19 and Web Reputation on page 1-20 and for more information.

Data Protection

This version of PortalProtect includes new functionality for Data Protection. These new functions include: new compliance templates, data prevention for documents and data prevention for Web content. See Data Protection starting on page 7-1.

Event Tracking

An event tracking log will record information about product console operations.

Access Control

The role based administration feature is used to grant and control access to the product console menu and submenu items.

RBS Support

Remote Blob Storage or “RBS” is a set of standardized APIs that enable you to store and retrieve binary large objects (BLOBs) outside your main SQL database. RBS is able to move BLOBs from database servers to commodity storage solutions. Real-time scan, manual scan and scheduled scan are all supported when RBS is installed on SharePoint.
Configuration for Automatic Replication

Configuration changes can be automatically replicated to other servers in one farm. See Understanding the Server Management Console on page 2-14.

Global Approved List

PortalProtect provides an additional feature called the Global Approved List for Data Protection, Content Filtering and File Blocking. This is a white list that enables the administrator to add Active Directory users and groups for which Data Protection, File Blocking and Content Filtering policies will be excluded. Real-time Content Filtering is available for both documents and Web content.

Table 1-1 lists the filters and MOSS platforms for which the Global Approved List is available.

Note: Real-time functionality for the Global Approved list is supported only for the MOSS 2010 and WSS 4 platforms.
<table>
<thead>
<tr>
<th>Filter Type</th>
<th>Supported Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Real-time Content Filtering for Documents</td>
<td>MOSS 2010 and WSS 4</td>
</tr>
<tr>
<td>• Real-time Content Filtering for Web Content</td>
<td></td>
</tr>
<tr>
<td>• Real-time File Blocking</td>
<td></td>
</tr>
<tr>
<td>• Real-time Data Protection for Documents</td>
<td></td>
</tr>
<tr>
<td>• Real-time Data Protection for Web Content</td>
<td></td>
</tr>
<tr>
<td>• Manual Scan Content Filtering</td>
<td></td>
</tr>
<tr>
<td>• Manual Scan File Blocking</td>
<td></td>
</tr>
<tr>
<td>• Manual Scan for Data Protection</td>
<td></td>
</tr>
<tr>
<td>• Scheduled Scan Content Filtering</td>
<td></td>
</tr>
<tr>
<td>• Scheduled Scan File Blocking</td>
<td></td>
</tr>
<tr>
<td>• Scheduled Scan for Data Protection</td>
<td></td>
</tr>
<tr>
<td>MOSS 2007 and WSS 3</td>
<td></td>
</tr>
<tr>
<td>• Manual Scan Content Filtering</td>
<td></td>
</tr>
<tr>
<td>• Manual Scan File Blocking</td>
<td></td>
</tr>
<tr>
<td>• Manual Scan for Data Protection</td>
<td></td>
</tr>
<tr>
<td>• Scheduled Scan Content Filtering</td>
<td></td>
</tr>
<tr>
<td>• Scheduled Scan File Blocking</td>
<td></td>
</tr>
<tr>
<td>• Scheduled Scan for Data Protection</td>
<td></td>
</tr>
</tbody>
</table>
Benefits and Capabilities

Trend Micro PortalProtect provides many benefits and capabilities, including the following:

Fast and Simple Installation
• Install to a single or multiple SharePoint server(s) using a single installation program.

Powerful and Creative Antivirus Features
• Uses proactive multi-threaded scanning to detect and clean viruses in real-time from multiple access points when authors check documents in or out, or when someone opens it for reading.
• Uses Trend Micro IntelliScan™ to detect and scan true file types regardless whether the file extension was changed.
• Detects and removes potentially harmful macros viruses.
• Uses ActiveAction to sort threats into such categories such as viruses, malicious macro codes, and additional threats.

File Blocking
• Uses file blocking during a virus outbreak to temporarily block all files types as designated by the administrator.
• Provides policy based file blocking that is integrated with Microsoft Active Directory users/groups or SharePoint users/groups.

Content Filtering
• Use rule-based filters to screen files and Web content deemed to be offensive or otherwise objectionable.
• Provides policy based content filtering that is integrated with Microsoft Active Directory users/groups or SharePoint users/groups.

Web Reputation
• Uses Web Reputation filters to block Web-based security risks.

Data Protection
• Uses standard or user-customized templates to prevent Personally Identifiable Information (PII) from being posted to or retrieved from a document library, wiki, blog, discussion forum, and so on.
Quarantine
• Provides central quarantine management for quarantined files in one farm.

Manual and Scheduled Scan
• Provides manual and scheduled scans of the SharePoint SQL Server content store for added protection against any malicious code or virus threats in addition to real-time scanning.

Updates
• Provides a way to easily keep protection current with manual and scheduled updates.
• Uses Trend Micro ActiveUpdate to automatically search for and download the latest virus pattern and scan engine updates.

Easy Management
• Includes centralized configuration, reporting, logs, update, and real-time notification of customizable warning messages to administrators, workspace coordinators, and other recipients.
• Integrates with Trend Micro Control Manager.

How Viruses Infect SharePoint Environments
As people within an organization create and collect information, they begin to spend increasing amounts of time searching, organizing, and managing that information. SharePoint Server combines the ability to quickly create corporate Web portals with search functions, document management features, and collaboration options. Although SharePoint Server makes it possible to easily share information among users regardless of their physical location, it also provides an environment where viruses and malicious programs like trojans and worms can thrive and cause damage.

How PortalProtect Protects SharePoint Servers
PortalProtect guards the SharePoint Server and SharePoint Services in a number of ways. Scanning and blocking content is the central function. You can configure PortalProtect to take actions whenever it blocks a file or detects a virus. Furthermore, you can have PortalProtect send notifications of these events to administrators or other recipients.
• PortalProtect can scan files or Web content and determine whether any of that content violates a policy. When a violation is detected, PortalProtect will take an action like: quarantine or delete, as pre-configured by the administrator.

• PortalProtect can scan URL in Web content to detect malicious URL, it takes an action like: block or pass, as pre-configured by the administrator.

• PortalProtect can block files based on the file extension, file name, or true file type. When it detects a file type, it takes an action like: quarantine or delete, as pre-configured by the administrator.

• Scanning employs the latest version of the Trend Micro scan engine to detect viruses and other malicious code. When PortalProtect detects a virus or malicious code, it performs a number of actions like: quarantine or delete, according to how the administrator has it configured. The scan engine can maintain multiple threads, thus processing many requests simultaneously. It can also prioritize requests.

PortalProtect provides constant feedback and reporting to keep you informed about the latest security threats and system status. It logs significant events like: component updates and scan actions. You can query these events to create logs that provide you with current and detailed information. You can also set PortalProtect to generate reports that can be printed or exported for analysis.

The scan engine scans all content according to the following models:

**Real-time Scan**—When you have enabled SharePoint Services antivirus features, PortalProtect performs a scan in real time on the file whenever the file is checked in, checked out, saved or retrieved. It scans all incoming or outgoing files for viruses or other malicious code. The scan engine has the capacity to maintain multiple threads and process many requests simultaneously.

**Manual Scan (Scan Now)**—Manual Scan occurs momentarily after you start it and scans all or some of the files in your Document Library, depending on the configuration. You can configure a scan task to scan all or some of the folders stored in the database. Manual scan provides an immediate way to secure the content on your SharePoint servers.

**Scheduled Scan**—Scans all or some of the files in your Document Library, depending on the configuration. You set the time and frequency of the scan. Scheduled Scan automates routine scans on your SharePoint servers, improves antivirus management efficiency, and gives you more control over your antivirus policy.
Trend Micro recommends you use a combination of scanning tasks to create a secure SharePoint environments. When you configure and perform a manual scan, it removes the threats from the content stored on the SQL Server content store. When you configure and enable real-time scanning, it protects your SharePoint servers from new threats as they arise. Finally, running regularly scheduled scans maintains a secure SharePoint environment.

PortalProtect Architecture

Trend Micro designed PortalProtect to work with SharePoint Services to provide comprehensive security for your SharePoint Server.

At the center of the PortalProtect security solutions is the Trend Micro patented scan engine. The scan engine integrates with the SharePoint Services Antivirus Manager (AVM). During real-time scanning, the Antivirus Manager calls the Trend Micro scan engine whenever content is checked-in, checked-out or published to a SharePoint server. The Trend Micro scan engine responds by scanning the content. During manual or scheduled scanning, the scan engine accesses and scans all content in the SharePoint Server SQL database.

SharePoint Services clients running applications such as Microsoft Office and Internet Explorer communicate with the SharePoint Services environment using Internet Information Services (IIS). The SharePoint administrator using the PortalProtect Web Management console also communicates with SharePoint environment using IIS.

PortalProtect is capable of receiving component updates through HTTP from the ActiveUpdate server or other Internet / intranet sources.
Controlling Outbreaks

PortalProtect protects SharePoint Server and SharePoint Services in many ways during a virus outbreak. The following is a list of methods you can use to protect your Portal environment:

- Use PortalProtect notifications to create an early warning for your administrator or IT professionals.
• Use **Update Now** to immediately download the latest virus pattern file and scan engine. Configure and run a manual scan and set PortalProtect to take action against any viruses. For fast and efficient action, select features such as IntelliScan and ActiveAction and PortalProtect will use Trend Micro recommended blocks and actions against viruses.

• Set the blocking options for manual or real-time scanning to detect a specific file type or name. Set an action like: block or quarantine for PortalProtect to take action on a file type or file name to prevent it from infecting your SharePoint servers.

---

**Note:** This method is very effective if you know the exact name of the virus. Virus alert information is available from TrendLabs at:

http://www.trendmicro.com/vinfo/

---

• Configure real-time scanning and set PortalProtect to take action against any viruses it detects. For fast and efficient action, select features such as IntelliScan and ActiveAction and PortalProtect will use Trend Micro recommended blocks and actions against viruses.

• Generate reports and make log queries to analyze the results of your counter-actions. Identify the sources and vectors of infection on your SharePoint servers.

---

**PortalProtect Technology**

The Trend Micro scan engines detect viruses/malware and other security threats to screen out unwanted content. This engine relies on the latest pattern files supplied by TrendLabs and delivered through ActiveUpdate servers or a user-configured update source.
About the Trend Micro Scan Engine

At the heart of all Trend Micro antivirus products lies a proprietary scan engine. Originally developed in response to the first computer viruses the world had seen, the scan engine today is exceptionally sophisticated. It is capable of detecting Internet worms, mass-mailers, Trojan horse threats, and network exploits, as well as viruses. The scan engine detects threats known to be:

- **IN THE WILD** or actively circulating
- **IN THE ZOO** or controlled viruses that are not in circulation

In addition to having a long history in the industry, the Trend Micro scan engine has also proven in test after test to be one of the fastest—whether checking a single file, scanning 100,000 files on a desktop machine, or scanning email traffic at the Internet gateway.

Rather than scan every byte of every file, the engine and pattern file work together to identify not only telltale characteristics of the virus code, but the precise location within a file where the virus would hide. When it detects a virus, the virus can be removed and the integrity of the file restored.

The scan engine includes an automatic clean-up routine for old virus pattern files (to help manage disk space), as well as incremental pattern updates (to help minimize bandwidth).

In addition, the scan engine is able to decrypt all major encryption formats (including MIME and BinHex). The scan engine recognizes and scans common compression formats including .Zip, .Arj, and .Cab. Most Trend Micro products also allow the product administrator to determine how many layers of compression to scan (up to a maximum of 20), for compressed files contained within a compressed file.

It is important that the scan engine remain current. Trend Micro ensures this in two ways:

1. Frequent updates to the scan engine's data-file, called the virus pattern file, can be downloaded and read by the engine without the need for any changes to the engine code itself.
2. Technological upgrades in the engine software prompted by a change in the nature of virus threats, such as the rise in mixed-threats like SQL Slammer. In both cases, updates can be automatically scheduled, or the security administrator can handle them manually. International computer security organizations, including the International Computer Security Association (ICSA) annually certify the Trend Micro scan engine.

About Scan Engine Updates

By storing the most time-sensitive virus information in the virus pattern file, Trend Micro is able to minimize the number of scan engine updates while at the same time keeping protection up-to-date. Nevertheless, Trend Micro periodically makes new scan engine versions available. New engines are released, for example, when:

- Trend Micro has incorporated new scanning and detection technologies into the software
- A new, potentially harmful, virus is discovered that cannot be handled by the current engine
- Scanning performance is enhanced
- Support is added for additional file formats, scripting languages, encoding, and/or compression formats

To view the version number for the most current version of the scan engine, visit:

http://www.trendmicro.com

About the Virus Pattern File

The Trend Micro scan engine uses an external data file, called the virus pattern file, to keep current with the latest viruses and other Internet threats such as Trojan horses, mass mailers, worms, and mixed attacks (for example, Bagle or NetSky).

All Trend Micro antivirus programs using the ActiveUpdate function can detect the availability of a new virus pattern on the Trend Micro server, and/or you can set it to automatically poll the server every week, day, or hour to get the latest file. Trend Micro recommends that you schedule automatic updates at least daily, which is the default setting for PortalProtect. Whether performed in the background or on-demand, the pattern file updates without interrupting users or network traffic.
You can manually download virus pattern files from the following Web site, where you can also find the current version, release date, and a list of all the new viruses definitions included in the file.

http://www.trendmicro.com/download/pattern.asp

How Scanning Works

The scan engine works together with the virus pattern file to perform the first level of detection, using a process called pattern matching. Since each virus contains a unique signature or string of telltale characters that distinguish it from any other code, the virus experts at TrendLabs capture inert snippets of this code in the pattern file. The engine then compares certain parts of each scanned file to the pattern in the virus pattern file, looking for a match. When it finds a match, it sends a notification through an email message to the system administrator.

Pattern File Numbering

To allow you to compare the current pattern file in your software products to the most current pattern file available from Trend Micro, pattern files have a version number.

There are two pattern file numbering systems currently in use at Trend Micro.

1. The traditional pattern file number is three-digits, in the format xxx, for example, 786.
2. The new pattern file numbering system, which came into use during 2003, uses six-digits, in the format x.xxx.xx.

For the file pattern number 1.786.01:

• The first digit (1) indicates the new numbering system.
• The next three digits (786) represent the traditional pattern file number.
• The last two digits (01) provide additional information about the pattern file release for Trend Micro engineers.

Be sure to keep your pattern file updated to the most current version to safeguard against the most current threats.
About ActiveUpdate

ActiveUpdate is a function common to many Trend Micro products. It connects to the Trend Micro Internet update server to enable downloads of virus pattern files, scan engines, anti-spam rules, and program files. ActiveUpdate does not interrupt network services, or require you to reboot your computers. Updates are available on a regularly scheduled interval, or on-demand.

Incremental Updates of the Virus Pattern File

ActiveUpdate supports incremental updates of the virus pattern file. Rather than download the entire pattern file each time, ActiveUpdate can download only the portion of the file that is new, and append it to the existing pattern file. This efficient update method can substantially reduce the bandwidth needed to update your antivirus software.

Using ActiveUpdate with PortalProtect

You can configure PortalProtect to use ActiveUpdate as a source for manual and scheduled component updates. When it is time for the component update, PortalProtect polls the ActiveUpdate server directly, ActiveUpdate determines if an update is available, and PortalProtect downloads it.

Note: New threats appear every day. Trend Micro recommends at least daily updates.

About Trend Micro IntelliScan™

Most antivirus solutions offer you two options for determining which files to scan for potential threats. PortalProtect will either scan all files—the safest approach—or true file types and those files with certain file extensions. It is important to note however, that there is an increasing number of attempts to disguise files by changing the extension, which renders the latter option less effective.

IntelliScan is a Trend Micro technology that identifies a file’s true file type, regardless of the file extension name. IntelliScan uses a method that can identify which files to scan and is more efficient than the Scan All files option.
Note: IntelliScan examines the header of every file, but based on certain indicators, selects only files that it determines are susceptible for security risk scanning.

Because IntelliScan scans only files that are vulnerable to infection it provides the following benefits:

• Performance optimization. IntelliScan uses fewer system resources than the Scan All option.
• Shorter scanning period. The scan time is shorter than when you Scan All files.

About Smart Protection Network

Trend Micro™ Smart Protection Network is a next-generation cloud-client content security infrastructure designed to protect customers from security risks and Web threats. It powers both on-premise and hosted solutions to protect users whether they are on the network, at home, or on the go. Trend Micro Smart Protection Network uses light-weight clients to access its unique in-the-cloud correlation of email, Web and file reputation technologies, as well as threat databases. Protection is automatically updated and strengthened as more products, services and users access the network, creating a real-time neighborhood watch protection service for those who use it. The smart scan solution uses the Smart Protection Network for in-the-cloud protection.

Smart Protection Services

Smart protection services provide anti-malware signatures, Web reputation, and threat databases that are stored in-the-cloud. Smart protection uses file reputation technology to detect security risks and Web reputation to proactively block malicious Web sites. File reputation technology works by off-loading a large number of anti-malware signatures that were previously stored on endpoint computers to the Smart Protection Network or Smart Protection Servers. Web reputation technology hosts URLs that were previously stored on the Smart Protection Network, to the Smart Protection Servers. Both technologies ensure smaller bandwidth consumption when updating patterns or querying URL validity.

Additionally, Trend Micro continues to harvest information anonymously sent from Trend Micro products worldwide to proactively determine each new threat.
Web Reputation

Web Reputation technology tracks the credibility of Web domains by assigning a reputation score based on factors such as a Web site’s age, historical location changes and indications of suspicious activities discovered through malware behavior analysis. It will then continue to scan sites and block users from accessing infected ones.

When a user accesses a URL, Trend Micro:
- Leverages the domain-reputation database to verify the credibility of the Web sites and pages
- Assigns reputation scores to Web domains and individual pages or links within sites
- Allows or blocks users from accessing sites

To increase accuracy and reduce false positives, Trend Micro Web Reputation technology assigns reputation scores to specific pages or links within sites instead of classifying or blocking entire sites since there are times that only portions of legitimate sites are hacked and reputations can change dynamically over time.

Smart Protection Sources

Smart protection sources download and host smart protection components that endpoints query when scanning or accessing Web sites. Clients can connect to either of the following smart protection sources:

- **Smart Protection Server**: Smart Protection Servers are for users who have access to their local corporate network. Local servers localize smart protection services to the corporate network to optimize efficiency.
- **Trend Micro Smart Protection Network**: A globally scaled, Internet-based, infrastructure that provides reputation services to users who do not have immediate access to their corporate network.

True File Types

When PortalProtect is set to scan true file types, the scan engine examines the file header rather than the file name to ascertain the actual file type. For example, if the scan engine is set to scan all executable files and it encounters a file named *family.gif*, the scan continues even though the file extension shows it to be a graphic. During scanning, the
scan engine opens the file header and examines the internally registered data type to
determine whether the file is indeed a graphic file, or, for example, an executable that
someone renamed to avoid detection.

True file type scanning works in conjunction with Trend Micro IntelliScan, to scan only
those file types known to pose a danger. These technologies reduce the overall number
of files that the scan engine examines—perhaps as much as a two-thirds—but may
create a greater risk.

For example, .gif and .jpg files make up a large volume of all Web traffic, but they
cannot harbor viruses, launch executable code, or carry out any known or theoretical
exploits. Therefore, does this mean they are safe? Not entirely. It is possible for a
malicious hacker to give a harmful file a safe file name to smuggle it past the scan engine
and onto the network. This file could cause damage if someone renamed it and ran it.

**Tip:** For the highest level of security, Trend Micro recommends scanning all files.

---

**About IntelliTrap**

Virus writers often attempt to circumvent virus filtering by using real-time compression
algorithms. IntelliTrap helps reduce the risk of such viruses entering your network by
blocking real-time compressed executable files and pairing them with other malware
characteristics. Because IntelliTrap identifies such files as security risks and may
incorrectly block safe files, Trend Micro recommends quarantining—rather than
deleting or cleaning—files when you enable IntelliTrap. You should disable IntelliTrap if
your users regularly use real-time compressed executable files.

IntelliTrap uses the following components:

- Virus Scan Engine
- IntelliTrap Pattern
- IntelliTrap Exception Pattern
Trend Micro™ ActiveAction™

ActiveAction identifies virus/malware types and provides suggested actions according to how each type invades a computer system or environment. ActiveAction categorizes malicious code, replication, and payload types as viruses/malware. When PortalProtect detects a virus/malware, it takes the recommended action (clean, quarantine, delete) on the virus/malware type to protect your environment's vulnerable points.

If you are not familiar with scan actions or if you are not sure which scan action is suitable for a certain type of virus/malware, Trend Micro recommends using ActiveAction.

Using ActiveAction provides the following benefits:

• **Time saving and easy to maintain**—ActiveAction uses scan actions recommended by Trend Micro. You do not have to spend time configuring the scan actions.

• **Updateable scan actions**—Virus/malware writers constantly change the way viruses/malware attack computers. Trend Micro updates ActiveAction settings in each new pattern file to protect clients against the latest threats and the latest methods of virus/malware attacks.

Customized Settings

Select *Customize action for detected threats* to instruct PortalProtect to execute a customized action according to the type of detected threat.

At the bottom of the screen you can configure PortalProtect to Backup infected files before performing an action. This is a safety precaution designed to protect the original file from damage.

Using Customized Scan Actions

Use these actions when you want to optimize scanning for your environment.

• When you want to configure PortalProtect to use the same action against all detected security risks. Select **All threats** and accept the default action or select a customized action.
When you want to configure an action for each type of threat detected by PortalProtect. Select **Specify action per detected threat**, and individually configure the action PortalProtect executes when it detects that threat type.

**Types of Threats**

- **Virus**–A computer virus is a program that replicates by attaching itself to other files (for example, .exe, .com, .dll) and executing whenever the file opens or runs.
- **Macros**–can contain malicious code. Macro viruses are application specific and target Microsoft Office applications. PortalProtect provides four (4) levels of heuristic scanning for these files, or provides the option to delete all detected macros. See *About Macro Viruses* on page 1-25.
- **Additional Threats**–additional threats include: Spyware, Dialers, Hacking Tools, Password Cracking Applications, Adware, Joke Programs, Remote Access Tools, and Others. The default action for additional threats is **Quarantine**. For more information about these kinds of threats, see the Trend Micro Web site for security information at [http://www.trendmicro.com/vinfo/](http://www.trendmicro.com/vinfo/).
- **Encrypted or password protected files**–PortalProtect does not scan these type of files. Instead, PortalProtect takes action to prevent these types of files from threatening your SharePoint server. The action it takes depends on the actions you have configured. The default action is **Pass**. Other options include: Quarantine, Delete, and Rename. For more information, see *About Encrypted and Password Protected Files* on page 1-25 and *About Unscannable Files* on page 1-26.

**Possible Actions**

If you select to use a customized action, you can set a scan action for each type of threat. PortalProtect automatically executes the action when it detects a threat with which the action is associated. Any scan action PortalProtect performs is recorded in the Virus logs.

Scan actions for viruses include the following:
• **Clean**—Removes virus code from infected files. When PortalProtect cannot clean the file, it takes the specified secondary action. Trend Micro recommends you use the default scan action: **Clean**, for viruses. Choose a secondary action for PortalProtect to execute when it cannot clean the file. The default secondary action is **Quarantine**.

During a manual or scheduled scan, PortalProtect updates the database and replaces the document content with the cleaned one.

---

**Note:** The **Clean** action is not available for **Additional threats** and **Packed files**.

---

• **Delete**—Deletes the file and logs an event.
• **Quarantine**—Moves the file to the PortalProtect database, thereby removing it as a security risk to the SharePoint environment.
• **Rename**—keeps the filename, but changes the file extension to `.vir` to prevent it from being opened or executed. For example: `virus.exe` will be renamed to `virus.exe.vir`.
• During real-time scanning PortalProtect allows the renamed file to enter the SharePoint server.
• **Block**—Blocks the file from accessing the SharePoint server and logs an event.
• **Pass**—Records a virus infection or malicious file in the virus log, but takes no action upon the file itself.

---

**Note:** PortalProtect performs a previous scan action specified while downloading a file, if that scan action is changed later. When a file is scanned with the first action specified, and you then change the scan action to another value, the file will not be sent to PortalProtect for re-scan. For example, if you change the scan action from **PASS** to **CLEAN** and then try to download the file, the resulting action for the file is **PASS** instead of **CLEAN**.
About Macro Viruses

Macro viruses are application-specific. They infect macro utilities that accompany such applications as Microsoft Word (.doc) and Microsoft Excel (.xls). Therefore, they can be detected in files with extensions common to macro capable applications such as .doc, .xls, and .ppt. Macro viruses travel between data files in the application and can eventually infect hundreds of files if undeterred.

About Encrypted and Password Protected Files

PortalProtect does not scan these types of files; instead, PortalProtect takes actions to prevent them from threatening your SharePoint server. The action it takes depends on the actions you have configured. The default action is Pass. Other options include: Quarantine, Delete, and Rename.

**TABLE 1-2. Scan actions for encrypted and password protected files**

<table>
<thead>
<tr>
<th>During this scan...</th>
<th>PortalProtect executes this action...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real-time</td>
<td>Block or Pass</td>
</tr>
<tr>
<td>Manual</td>
<td>Quarantine, Pass, Delete, or Rename</td>
</tr>
<tr>
<td>Scheduled</td>
<td>Quarantine, Pass, Delete, or Rename</td>
</tr>
</tbody>
</table>

**Note:** When PortalProtect quarantines encrypted, password protected, and Unscannable files, it reports to SharePoint Services that the files are infected. In some cases, PortalProtect may identify a file as being infected, when it actually is not. Trend Micro recommends that you review your quarantine logs from time to time for files that may have been identified with a false positive.
About Unscannable Files

PortalProtect cannot scan some types of files such as those over 4-GB. Instead, PortalProtect takes other actions to prevent these files from threatening your SharePoint servers. The action it takes depends on the actions you have configured. The default action is **Pass**; other options include: **Quarantine**, **Delete**, and **Rename**.

<table>
<thead>
<tr>
<th>During this scan...</th>
<th>PortalProtect executes this action...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real-time</td>
<td>Block or Pass</td>
</tr>
<tr>
<td>Manual</td>
<td>Quarantine, Pass, Delete, or Rename</td>
</tr>
<tr>
<td>Scheduled</td>
<td>Quarantine, Pass, Delete, or Rename</td>
</tr>
</tbody>
</table>

Scan Compressed Files

PortalProtect can scan and block compressed files according to how you configure the scanning options. When PortalProtect detects a virus, it blocks the file or executes a pre-configured action.

**Note:** PortalProtect cannot clean a virus if the compression layer is greater than 1. However, you can configure PortalProtect to block and quarantine or scan and delete compressed files.

Compression and archiving are among the most common methods of file storage, especially for file transfers - like email attachments, FTP, and HTTP. Compressed files must first be decompressed before any virus detection can occur.

Recognizing the importance of decompression for detecting viruses, Trend Micro is committed to supporting all major decompression routines, present and future.

PortalProtect currently supports the following compression types:
• Extraction—used when multiple files have been compressed or archived into a single file: PKZIP, LHA, LZH, ARJ, MIME, MSCF, TAR, GZIP, BZIP2, RAR, AMG, and ACE.

• Expansion—used when only a single file has been compressed or archived into a single file: PKLITE, PKLITE32, LZEXE, DIET, ASPACK, UPX, MSCOMP, LZW, MACBIN, Petite, PEPack, and WWPack.

• Decoding—used when a file has been converted from binary to ASCII, a method that is widely employed by email systems: UUCODE and BINHEX.

For other compression file types, PortalProtect scans the entire compressed file, rather than each individual file contained within the compressed file.

Maintenance Agreement

A Maintenance Agreement is a contract between your organization and Trend Micro, regarding your right to receive technical support and product updates in consideration for the payment of applicable fees. When you purchase a Trend Micro product, the License Agreement you receive with the product describes the terms of the Maintenance Agreement for that product.

Note: The Maintenance Agreement has an expiration date; your License Agreement does not.

A license to the Trend Micro software usually includes the right to product updates, pattern file updates, and basic technical support (“Maintenance”) for one (1) year from the date of purchase only. After the first year, Maintenance must be renewed on an annual basis at Trend Micro’s then-current Maintenance fees.

Typically, ninety (90) days before the Maintenance Agreement expires, you will start to receive email notifications, alerting you of the pending discontinuation.

When your Maintenance Agreement expires, you are entitled to a grace period of 30 days during which time PortalProtect is fully functional. After the grace period ends you will not be able to receive updated components or support from Trend Micro.
Renewing Your Maintenance Agreement

To purchase renewal maintenance, contact your reseller, Trend Micro sales, or on the Trend Micro Online Registration URL: https://olr.trendmicro.com/registration/.

A Maintenance Agreement, extending your protection for a year, will be sent by post to the primary company contact listed in your company’s Registration Profile.
Chapter 2

Getting Started with PortalProtect

This chapter discusses the basics you need to get started using PortalProtect to protect your SharePoint environments. Additionally, it describes how to get help, and tasks you should perform when you start to use PortalProtect. Completing these tasks ensures you are taking full advantage of PortalProtect features.

In this chapter, you will find information about:

• Viewing the PortalProtect Web Management Console starting on page 2-2
• Registering PortalProtect starting on page 2-3
• Activating PortalProtect starting on page 2-4
• Updating PortalProtect starting on page 2-5
• Managing PortalProtect starting on page 2-9
Viewing the PortalProtect Web Management Console

You can access and control PortalProtect through the intuitive Web Management Console. You can view the Web Management Console from any computer on your network that is running Internet Explorer 6.0 or above.

To view the Web Management Console for a local server

2. The URL in the Address box should be the following:
   http://[localhost]:[port number]/PortalProtect/Login.htm

   **Note:** The port number depends on the user input during installation. The default port is 16372. If SSL was enabled during installation, use **https** protocol.

To view the Web Management Console for a remote server:

Use Internet Explorer to access: http://[server name]:[server port]/PortalProtect/Login.htm

Where servername is the name of the server on which you installed PortalProtect and port number is the port number you use to access that computer.

The Web Management Console Consists of the Following Main Elements:

- The PortalProtect banner always appears at the top of the screen. It contains a drop-down list that you can use to access online assistance. You can also use the banner to log off.
- The sidebar is the menu on the left side of the Management Console. It provides quick access to all PortalProtect settings.
- Main display area is where you can view and set the different PortalProtect options.
- Screen tabs are a part of the main display area and provide access to a various topics and options.
• Help icons provide access to context sensitive help (❓) or pop-up information on various features (ℹ️).

Logging On and Off

Log on

You must log on to PortalProtect before you can configure any settings. By requiring PortalProtect administrators to log on, PortalProtect provides an extra layer of protection.

Log off

Click Log Off from the banner of the Web Management Console to log off.

Registering PortalProtect

When you purchase PortalProtect, you receive a Registration Key. You can use this Registration Key to register online. After you register, you receive an Activation Code that you can use to activate PortalProtect. When you use the Activation Code, you gain all the benefits of a fully licensed version of PortalProtect.

To register your product, do one of the following:

• During installation, you will be prompted to use your Registration Key to register online. Follow the link to the Trend Micro Web site, register your product, and then return to the installation program to complete your installation.

• Contact Trend Micro directly. Provide a Trend Micro representative with your Registration Key and he or she will give you an Activation Code. When you purchase PortalProtect, your vendor provides you with a Registration Key. You can register PortalProtect at:


See Contacting Trend Micro on page 12-2.
Activating PortalProtect

You must activate PortalProtect to gain the full benefits of the product. The full benefits include the right to download the most recent scan engine and virus pattern file updates. You are also entitled to download upgrades and hot fix patches. Without these key components, your SharePoint environment is not protected from the latest arising virus attacks.

PortalProtect has two types of activation codes (AC): PortalProtect, and PortalProtect Suite. Additionally, there are two types of maintenance agreements: evaluation and full. When you register PortalProtect, you receive one AC depending on whether you chose PortalProtect or PortalProtect Suite and the evaluation or fully licensed version.

Using the Portalprotect AC activates PortalProtect security risk scan, file blocking, Web reputation, and content filtering; Using the PortalProtect suite AC, activates all the functions of the PortalProtect AC plus data protection.

Activating PortalProtect is a two-step process: first, register your product and then activate it. Registration is accomplished with the use of your Registration Key that you received from your vendor when you purchased PortalProtect. You can use this Registration Key to register online. See Registering PortalProtect on page 2-3.

After you register, you receive an Activation Code. Use your Activation Code to activate PortalProtect during installation.

---

**Note:** You can use a trial activation code to activate a free trial period for PortalProtect. The trial period lasts for 30 days after which time you will no longer be able to use PortalProtect to scan files or receive updated components. To upgrade your trial period to a fully licensed version, contact Trend Micro or a licensed reseller to obtain a new activation code.

---

You receive the following benefits when you activate your product:

- The fully licensed version of PortalProtect. This includes the latest scan engine and virus pattern file updates. ActiveUpdate is available.
- Trend Micro technical support for the extent of your license.

To acquire a new activation code

- Use your Registration Key to register with Trend Micro. When you register online, you receive your Activation Code by email.
• When your Activation Code has expired, contact a Trend Micro reseller to renew your license. Trend Micro maintains a list of vendors at http://www.trendmicro.com/buy/partners/reseller.asp.

To activate your product from the management console:
1. From the sidebar, click **Administration > Product License**. The Product License screen appears.
2. Click **Enter New Activation Code**.
3. Type the new Activation Code in the space provided.
4. Click **Activate**.

### Updating PortalProtect

Antivirus software can only be effective if it is using the latest scan engine and pattern files. Since new viruses and other malicious code are constantly being released, it is crucial that you regularly update your scan engine, and pattern files to protect against new security threats.

Before you can update PortalProtect, you must complete the following tasks:

• Register your software. See **Registering PortalProtect** on page 2-3.

• If a proxy server handles Internet traffic on your network, you must type the proxy server information. See **Configuring Global Proxy Settings** on page 2-6.

• Configure your update method and source. Methods include **Manual Update** and **Scheduled Update**. Sources include the ActiveUpdate server, other update source, and the intranet UNC path.

---

**Note:** The management console contains three (3) update options: ActiveUpdate server, UNC path and Other Update source.
Select Download Source

Before updating your components the first time, you must select a download source.

To select a download source:

1. Click Updates > Download Source to select the download source. The Download Source screen appears.
   - **Trend Micro ActiveUpdate server**—ActiveUpdate downloads new components as soon as Trend Micro makes them available. Select ActiveUpdate as a source if you require frequent and timely updates.
   - **Intranet location containing a copy of the current file**—Type the Universal Naming Convention (UNC) path of another server on your network. Type the User name and Password as required.
   - **Other Update Source**—Download your components from an Internet source that receives updated components.

2. Select **Allow other servers to download updates from this server...** to create a component package on one server that can be accessed by the other servers on the same local network.

   Note: If selected, other servers can download the package from: http://<Server IP>:<Port>/PortalProtect/Activeupdate.

3. Click **Save**.

   Note: Click **Reset** to change all download source settings to their default values.

Configuring Global Proxy Settings

Most enterprises use proxy servers for added security and more efficiently use bandwidth. If your system uses a proxy server, configure the proxy settings to connect to the Internet and download updated components necessary to keep PortalProtect updated and check the license status online.

The following features use Proxy servers:
   - ActiveUpdate
• Product Registration
• World Virus Tracking
• Web Reputation filtering

To set the Internet proxy:
1. Open the PortalProtect Web console.
2. On the sidebar, click Administration > Proxy. The Proxy Settings screen appears.
3. Select Use a proxy server for Web Reputation, updates and product license notifications.
4. Enter the following to set the Proxy Server:
   • Server name or IP address
   • Port
   • Choose whether to use SOCKS 5 proxy protocol
5. For Proxy Authentication, if your proxy server requires a password, type the following in the fields provided:
   • User name
   • Password
6. Click Save to save your settings.

Manually Updating Your Components

Trend Micro recommends manually updating your components immediately after installing PortalProtect or whenever there is a virus outbreak. This establishes a baseline of security for your SharePoint environment.

Note: If you are updating components for the first time, be sure to select the Download Source before updating. See Select Download Source on page 2-6.

To manually install your components:
2. Select the check box(es) of the component(s) you want to update.
3. Click Update. PortalProtect begins updating.
Configuring Scheduled Updates

Configure PortalProtect to regularly check the update server and automatically download any available updates. This powerful function keeps PortalProtect and all its components updated, offering you maximum protection with minimal intervention.

Note: If you are updating components for the first time, be sure to select the Download Source before updating. See Select Download Source on page 2-6.

Tip: The virus pattern updates regularly, sometimes several times per day if there is a virus outbreak. Trend Micro recommends updating at least daily to help ensure PortalProtect has the current component versions.

To configure scheduled updates:

1. On the left menu, click Updates > Scheduled. The Scheduled Update screen appears.
2. Select Enable scheduled updates.
3. Select the check box(es) of the component(s) you want to update.
4. Under Update Schedule, select the options for the frequency of the update, whether, Minute(s), Hour(s), Day(s), or Weekly.
5. Use the drop down(s) to choose the appropriate starting schedule.
6. Click Save.

Note: Click Reset to change all download source settings to their default values.
Managing PortalProtect

This section describes the various features and functionalities available for managing PortalProtect.

The Summary Screen

The PortalProtect Summary screen contains two tabs: System, and Security Risk. This section provides a short description for the functionalities and displays found on these tabs.

Scan Status for Today

• Total # of detected security risks—displays the total number of detected security risks for today.
Detected virus/malware—number of virus/malware detections is not the number of unique viruses/malware, but rather the total number of virus/malware detections made by PortalProtect for today. This is accompanied by the percentage detected versus the total detected security risks for files and Web content. Click the numeric link to query and view the log.

Uncleanable virus/malware—total number of detected viruses/malware that could not be cleaned for today along with the percentage detected versus the total detected security risks for files and Web content. Click the numeric link to query and view the log.

Detected spyware/grayware—total number of detected spyware/grayware for today along with the percentage detected versus the total detected security risks for files and Web content. Click the numeric link to query and view the log.

• Total # of scanned files and Web content—displays the total number of files and Web content scanned.

File blocking violations—total number of detected file blocking violations for today along with the percentage detected versus the total files and Web content scanned. Click the numeric link to query and view the log.

Content filtering violations—total number of content filtering policy violations detected for today along with the percentage detected versus the total files and Web content scanned. Click the numeric link to query and view the log.

Suspicious URLs Web reputation—total number of suspicious URLs detected by Web reputation for today along with the percentage detected versus the total files and Web content scanned. Click the numeric link to query and view the log.

Data protection violations—total number of data protection violations for today with the percentage of detected versus the total files and Web content scanned. Click the numeric link to query and view the log.

Unscannable files—total number of unscannable files detected for today along with the percentage detected versus the total files and Web content scanned. Click the numeric link to query and view the log.

Scan Services—PortalProtect Services

• Security Risk Scan: click the icon in the status column to enable or disable security risk scan.

• File Blocking: click the icon in the status column to enable or disable file blocking.
• **Content Filtering for document**: click the icon in the status column to enable or disable content filtering for documents.

• **Content Filtering for Web content**: click the icon in the status column to enable or disable content filtering for Web content.

• **Data Protection for document**: click the icon in the status column to enable or disable data protection for document.

• **Data Protection for Web content**: click the icon in the status column to enable or disable data protection for Web content.

• **Web Reputation for document**: click the icon in the status column to enable or disable Web reputation for document.

• **Web Reputation for Web content**: click the icon in the status column to enable or disable Web reputation for Web content.

**Note**: A green checkmark indicates the service is enabled and a red “X” indicates the service is disabled.

---

**Scan Services—Microsoft SharePoint Services**

**Note**: Click the **Turn On** link to open the **Central SharePoint Administration > Antivirus server setting** window and choose the options you want to enable or disable. Click **OK**, close the window and refresh the **Summary** page to see the updated settings.

• **Scan documents on upload**: The status column displays **On**, when this service is enabled, and an exclamation icon, **Off**, and a **Turn On** link when it is disabled.

• **Scan documents on download**: The status column displays **On**, when this service is enabled, and an exclamation icon, **Off**, and a **Turn On** link when it is disabled.

• **Attempt to clean infected documents**: The status column displays **On**, when this service is enabled, and an exclamation icon, **Off**, and a **Turn On** link when it is disabled.

• **Scan Web content**: Click the icon in the status column to enable or disable Scanning for Web content. A green checkmark indicates the service is enabled and a red “X” indicates the service is disabled.
Scan Method

- **Security Risk Scan Method: Conventional Scan**—Click the link to select and configure conventional scan or smart scan. See *Choose a Security Risk Scan Method* on page 4-2.

- **Web Reputation Source: Smart Protection Network**—Click the link to select and configure scanning from the global smart protection network or a local smart protection server. See *Choose a Security Risk Scan Method* on page 4-2.

Smart Scan Server

**Note:** This section appears with the following ONLY if you have selected the Smart Scan option:

- **Smart Protection Service:** includes the server for Security Risk Scan and Web Reputation

- **Server Name:** for the smart scan server that handles PortalProtect scanning requests

- **Service Status:** shows the smart scan service status for this server

- **Console:** click the link to access the Web console for this smart scan server

Update Status

View the Current Version, Available Version, and Last Update Status for the following components. Select a component(s) and click **Update** to manually update, or query the update log for a complete history:

- Smart Scan Agent Pattern
- Virus pattern
- Spyware pattern
- IntelliTrap pattern
- IntelliTrap exception pattern
- Virus scan engine
- URL filtering engine
Understanding the Real-time Monitor (MOSS 2010/WSS 4.0 Only)

The Real-time Monitor displays information about the current PortalProtect server in real time. It shows PortalProtect scanning content as it is uploaded or posted. It also gives the current count of detected viruses/malware, spyware/grayware, and suspicious URLs on the server.

The Real-time Monitor displays the following information about the server (see Figure 2-1):

Top group
- Server name
- Smart Scan Agent Pattern
- Virus pattern
- IntelliTrap pattern
- Spyware pattern
- URL filtering engine
- Real-time scan has been running since: xxxx/xx/xx xx:xx:xx
- Virus scan engine
- IntelliTrap exception pattern

Scanning Status group
- Files and Web content scanned
- Virus/Malware found
- Spyware/Grayware found
- Uncleanable viruses
- File Blocking violation
- Content filtering violation
- Detected suspicious URLs - Web Reputation
- Data protection

The following is a list of the options available on the Real-time Monitor:
- **Reset Count**: resets all Scanning Status counts to zero and also clears the Scanned Contents list
• Clear Content: clears the lists under Scanned Contents
• Close: exits the screen

**FIGURE 2-1. Real-time monitor screen**

To view the real-time monitor (MOSS 2010/WSS 4.0 only):

**Note:** The Real-time Monitor is supported only for MOSS 2010/WSS 4.0 and Windows SharePoint Services 4.0.

1. Open the PortalProtect product console.
2. At the top of the screen, click the **Real-time monitor** link.

**Understanding the Server Management Console**

Server management provides the functionality to query information and replicate settings for all PortalProtect servers in a farm. The console provides information about engine/pattern version, scanning status, scanning result and last replication.

The following provides a brief description of the available options:

**Query tab**

Provides the latest information on the following:
• **Pattern and engine version:** displays the current pattern/engine for each server

• **Scanning status:** displays the scanning status (On or Off) for Security Risk Scan, File Blocking, Content Filtering for files, Content Filtering for Web content, Data Protection for Files, Data Protection for Web Content, Web Reputation for Files, and Web Reputation for Web Content.

• **Scanning result:** displays the latest scan results as listed on the Summary Page.

• **Last replication:** displays information relating to the last replication, including: Server Name, Last Replication Date, and Status.

**Replication tab**

Enables you to automatically replicate configurations from one PortalProtect server to another within the farm. To perform this action, select **Automatically replicate settings to other servers** at the bottom of the screen *(Figure 2-2)*.

---

**Note:** If you choose **All settings** and **Overwrite server-dependent settings (such as backup directories)**, the server-dependent settings will be replicated. If you select **All settings**, but clear **Overwrite server-dependent settings (such as backup directories)**, then the server-dependent settings will not be replicated.
The following describes the available options:

- **Select target server**
  a. **All servers**: select to include all servers in the farm excluding the one being copied
  b. **Specify servers**: select to choose specific target servers to send the replication

- **Select settings to deploy**
  a. **All Settings**: select to deploy all settings to the selected servers
b. **Specify Settings**: Select to choose the following settings you want to deploy:

<table>
<thead>
<tr>
<th>Note: These options are available only after selecting <strong>Specify Settings</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Security risk scan</td>
</tr>
<tr>
<td>- File blocking</td>
</tr>
<tr>
<td>- Content filtering</td>
</tr>
<tr>
<td>- Web reputation</td>
</tr>
<tr>
<td>- Data protection</td>
</tr>
<tr>
<td>- Compliance templates</td>
</tr>
<tr>
<td>- Manual scan</td>
</tr>
<tr>
<td>- Smart protection</td>
</tr>
<tr>
<td>- Updates</td>
</tr>
<tr>
<td>- Alerts</td>
</tr>
<tr>
<td>- Reports</td>
</tr>
<tr>
<td>- Logs</td>
</tr>
<tr>
<td>- Administration: Proxy, Notification settings, Access control, World virus tracking, and Control manager</td>
</tr>
<tr>
<td>- Product license</td>
</tr>
<tr>
<td>- Overwrite server-dependent settings (such as backup directories). This option is enabled if <strong>Security Risk Scan</strong> or <strong>Manual Scan</strong> is selected from <strong>Specify Settings</strong>. Can also be enabled when <strong>All settings</strong> is selected.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Note: The backup directories for <strong>Real-time Security Risk Scan</strong> and <strong>Manual Scan for Security Risk Scan</strong> have server dependent settings. See <strong>Backup Files Before Taking Action</strong> on page 3-6 for more information.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>- <strong>Automatic Replication</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>a. <strong>Automatically replicate settings to other servers</strong>: select to automatically replicate settings to other servers</td>
</tr>
</tbody>
</table>

2-17
Chapter 3

Configuring Scanning and Blocking

This chapter discusses the scanning and blocking options for PortalProtect. PortalProtect provides the following scanning functions for your SharePoint environment:

- Real-time scan,
- Manual scan,
- and Scheduled scan.

Each of these scanning options provides its own set of scan and blocking filters for:

- Security Risk Scan,
- File Blocking,
- Content Filtering,
- and Web Reputation
- Data Protection

Using advanced options, you can configure PortalProtect to scan for malicious Macro code, and to block and scan compressed files.
In this chapter, you will find information about:

- *About Scans* on page 3-2
- *Configuring Scan Options* on page 3-2

### About Scans

PortalProtect has the following three types of scans:

- Real-time
- Manual
- Scheduled

To protect your SharePoint environment, PortalProtect scans content searching for security risks and undesirable data. When PortalProtect makes a detection, it automatically takes action against the detection according to your configurations.

You can configure PortalProtect to scan specific targets and configure the actions it takes when it discovers a security risk or undesirable data. You can also configure PortalProtect to send notifications when it takes actions against security risks and undesirable data.

Additionally, you can configure PortalProtect to save files to the Backup folder before it takes action on it. This is a safety precaution designed to protect the original file from damage.

**Note:** Trend Micro recommends deleting backed up files once you have determined that the original file was not damaged and that it is usable after PortalProtect has executed an action on it. If the file becomes damaged or unusable, send it to Trend Micro for further analysis. Even if PortalProtect has completely cleaned and removed the virus itself, some viruses damage the original file code beyond repair.

### Configuring Scan Options

Use the scanning menus to setup scans and configure the options for those scans. You can set up real-time scans, manual scans, or scheduled scans. Additionally, you can configure each with different options. When you have configured and saved your scan
options, PortalProtect starts running the scans and taking actions based on your configurations. Disable scans to temporarily stop them without changing your configurations. See *Enabling and Disabling Real-time Security Risk Scan* on page 3-4.

**About Scanning**

Real-time scanning occurs whenever a file is saved to a SharePoint server (check-in) or retrieved from the SharePoint server (check-out). Manual scanning scans the SharePoint content database and occurs immediately after you manually choose Scan Now. Scheduled scans perform the same function as manual scans, but occur according to the schedule you set. The duration of the scan depends on the number of files and your hardware resources.

To optimize the performance of your SharePoint environment, Trend Micro recommends that you NOT perform a manual or scheduled scan during peak usage periods.

---

**Note:** When real-time scan is enabled and *scan documents on download* and *scan documents on upload* are also enabled on the SharePoint Anti-Virus options, then PortalProtect will scan the files while uploading, but *will not scan* the files while downloading. Since these files have already been scanned, PortalProtect will not scan them again during download. This is due to limitations of Microsoft SharePoint.

---

**Tip:** Refer to the Online Help for specific information about how to use the PortalProtect Management console to configure and perform scans.

---

PortalProtect secures your SharePoint environment by performing scans on all content that is either uploaded or downloaded. You can configure PortalProtect to run scans on-demand (manual scanning), according to a schedule (scheduled scanning), or in an ongoing and persistent manner (real-time scanning). Additionally, you configure scans using the Security Risk Scan screen, accessible from the sidebar, or from the Manual Scan and Scheduled Scan screens.
Note: Real-time Scanning protects your SharePoint environment in an ongoing manner. When you enable real-time scan, it continually runs in the background. You can configure only one real-time scan at a time.

WARNING! Trend Micro recommends that you always keep real-time scan enabled. However, if you must disable the real-time scan functionality, be sure to run regular manual scans.

Enabling and Disabling Real-time Security Risk Scan

When you enable real-time security risk scan, it continuously runs in the background of your Portal. Similarly, scheduled scans occur automatically according to the configured schedule. You can disable real-time and scheduled scans without affecting your scan configuration settings. When you decide to resume real-time scanning, simply re-enable the scan.

WARNING! If you disable real-time scanning, background scanning and file blocking will not occur, which will make your Portal vulnerable to infection. If you disable scheduled scanning, scanning and blocking of your SQL content store will not occur. Disabling scheduled scanning makes your system vulnerable to infected files being stored on your SharePoint servers.

Smart Protection Source

The Smart Protection Source option enables you to add, delete, import, and export smart scan servers according to your personal requirements. This section explains the various options and settings available to you, and how to configure them.

If your smart server becomes unavailable, PortalProtect will load local virus patterns for scanning your files. When Smart Protection becomes available again, PortalProtect will automatically unload the local virus pattern files and load smart scan patterns and
continue scanning files through your smart scan server. You can configure your system to send an email alert whenever the smart server becomes available or unavailable. See *System Events* on page 11-26 for more information.

To configure the smart protection source:

1. Click **Smart Protection > Local Sources**. The **Local Sources** screen appears.
2. To add a smart protection server:

   **Note:** You can click **Import** to import a server list and **Export** to export one.

   a. Click **Add**. The **Add Smart Protection Server** screen appears.

   b. Type the following information:
      - Server name or address
      - File Reputation Service Port
      - SSL
      - Web Reputation Service Port

   c. Click either the File or Web Reputation test button to test the connection.

3. Click **Add** to complete and save your settings.
If you have more than one Smart Protection Server listed, you can choose the order in which PortalProtect will query them. **As listed** will query according to the priority shown. **Random** will query the listed servers in a random fashion. Whenever the system is unable to connect to a Smart Protection Server, it will attempt to connect to next server according to the query order you choose.

4. Do the following to add or edit a proxy server for the Local Smart Protection network:
   a. From the **Local Sources** screen, click the icon next to **Proxy Settings** to expand the content.
   b. Select **Use a proxy server for PortalProtect and Local Smart Protection Server communication**.
   c. Type an IP or server name in the **Server name or IP address** field.
   d. Type a port number in the **Port** field.
   e. Type a User ID as required.
   f. Type a Password as required.
   g. Click **Save**.

   **Note:** These proxy settings affect only your Local Smart Protection Server(s) and do not affect the Global Proxy Server settings found in **Administration > Proxy**.

---

Backup Files Before Taking Action

You can set PortalProtect to backup a file to the Backup folder before it executes an action on it. This is a safety precaution designed to protect the original file from damage.

Backed up files should be deleted soon after you determine whether the modified file is usable and undamaged after PortalProtect executes an action on it. If the file is damaged or unusable, be sure to send it to Trend Micro for further analysis. It’s important to remember that even though PortalProtect may completely clean and remove a virus, the virus may have damaged the file code beyond repair.

See the following for information about how to set backup folder locations:
Specifying a Backup Folder for Security Risk Scan

The following explains the steps required to specify a backup folder for Security Risk Scan:

1. On the left menu, click Security Risk Scan. The Security Risk Scan screen appears (Figure 3-2).
2. Click the Action tab, and then expand the Backup Setting at the bottom of the screen (Figure 3-3).

**FIGURE 3-2.** Security risk scan screen (target tab)
In the Backup directory field, type the full path in which to save backup files. If the directory path does not exist, PortalProtect will create a folder for the specified path.

4. Click Save to accept and save the current setting.

Specify a Backup Folder for Manual Scan

The following explains the steps required to specify a backup folder for Manual Scan:
To specify a backup folder location for manual scan:

1. On the left menu, click Manual Scan. The Manual Scan screen then appears.
2. Under Select the scan type, click the Security risk scan link (Figure 3-4).

**FIGURE 3-4.** Configure manual scan
3. The Manual Scan > Security Risk Scan screen then appears.

4. Click the Action tab, and then expand Backup Setting at the bottom of the screen (Figure 3-5).

![Manual Scan: Security Risk Scan](image)

**FIGURE 3-5. Manual Scan > Security Risk Scan (action tab)**

5. In the Backup directory field, type the full path in which to save backup files. If the directory path does not exist, PortalProtect will create a folder for the specified path.

6. Click Save to accept and save the current setting.
Specify a Backup Folder for Scheduled Scan

The following explains the steps required to specify a backup folder for scheduled scan:

**To specify a backup folder location for scheduled scan:**

1. On the left menu, click **Scheduled Scan**. The **Scheduled Scan** screen then appears.
2. Add a new scheduled scan, or click an existing scheduled scan in the **Task Name** column (**Figure 3-6**).

**Figure 3-6.** Scheduled scan main screen
3. Depending on your previous selection, the Scheduled Scan: Add Scan Task or Scheduled Scan: Edit Scan Task screen appears (Figure 3-7).

**FIGURE 3-7.** Scheduled Scan: Add Scan Task screen
4. Under **Select scan type**, click the **Security risk scan** link. The **Scheduled Scan > Security Risk Scan** screen then appears.

5. Click the **Action** tab, and then expand **Backup Setting** at the bottom of the screen.

6. In the **Backup directory** field, type the full path in which to save backup files. If the directory path does not exist, PortalProtect will create a folder for the specified path.

7. Click **Save** to accept and save the current setting.

### About Advanced Macro Scan

Macro viruses/malware are application-specific. They infect macro utilities that accompany such applications as Microsoft Word (.doc) and Microsoft Excel (.xls). Therefore, they can be detected in files with extensions common to macro capable applications such as .doc, .xls, and .ppt. Macro viruses/malware travel between data files in the application and can eventually infect hundreds of files if undeterred.

PortalProtect prevents macro viruses/malware from infecting your server using the following methods:

- Detects malicious macro code using heuristic scanning
- Heuristic scanning is an evaluative method of detecting viruses/malware. This method excels at detecting undiscovered viruses/malware and threats that do not have a known virus signature
- Strips all macro code from scanned files

For more information see:

- *Configure Macro Scanning Options for Real-time Security Risk Scan* starting on page 4-5
- *Configure Macro Scanning Options for Manual Scan* starting on page 9-5
- *Configure Macro Scanning Options for Scheduled Scan* starting on page 10-5
Security Risk Scans

This section describes the background and configuration settings needed for Security Risk Scan. PortalProtect provides two options for Security Risk Scan: Conventional Scan, or Smart Scan. Conventional Scan sends request to the scan engine on your local machine. Smart Scan uses the Trend Micro Smart Protection Network, which is your private next-generation cloud-client content security infrastructure designed to protect your SharePoint environment from security risks and Web threats. Protection is automatically updated and strengthened as more products, services and users access the network, creating a real-time neighborhood watch protection service for those who use it. The smart scan solution uses the Smart Protection Network for in-the-cloud protection.

File Reputation

File reputation technology from Trend Micro checks the reputation of each file against an extensive in-the-cloud database before permitting user access. Since the malware information is stored in the cloud, it is available instantly to all users. High performance content delivery networks and local caching servers ensure minimum latency during the checking process. The cloud-client architecture offers more immediate protection and eliminates the burden of pattern deployment besides significantly reducing the overall client footprint.
Choose a Security Risk Scan Method

To choose a security risk scan method:

1. Click Smart Protection > Scan Service Settings from the left menu. The Scan Service Settings screen appears.

   ![Scan Service Settings screen](image)

   **FIGURE 4-1. Scan Service Settings screen**

2. Under Security Risk Scan, select from the following options:
   - **Conventional Scan**: performs the security risk scan for files using the scan engine on your local machine.
   - **Smart Scan - File Reputation Services**: performs security risk scan for files using your private smart scan server.

   Configure Smart Scan Source: if using Smart Scan, click the Smart Protection > Local Sources link to configure the Smart Protection Server(s).

   ![Configuring Smart Scan Source](image)

   **Configure Smart Scan Source**

   **Note:** Refer to Choose a Web Reputation Source on page 8-3 for information on how to configure these settings.

3. Click Save.
Enable or Disable Real-time Security Risk Scan

To enable or disable a real-time security risk scan:

1. On the left menu, click **Security Risk Scan**, to display the **Security Risk Scan** screen.
2. Select **Enable real-time security risk scan** to enable the scan, or clear the check box to disable the scan.
3. Click **Save**.

**Note:** You can also enable or disable real-time security risk scan from the **Summary** screen by clicking the Status icon under **Scan Services**.

About Security Risk Scan Target Settings

This section provides a brief description of the options available for the **Security Risk Scan > Target** tab. By default, PortalProtect scans all files on your SharePoint servers, which provides the maximum security. However, scanning every single file requires a lot of time and resources. Therefore, you may wish to consider limiting the number of files PortalProtect includes in its **Real-time**, **Manual**, and **Scheduled** scans.

You can configure PortalProtect to limit scanning to the following files:

- **All scannable files**—scans all content passing through or being stored on the SharePoint environment.
- **IntelliScan**—use Trend Micro IntelliScan to perform an efficient scan. See **About Trend Micro IntelliScan™** on page 1-18.
- **Specific file types**—PortalProtect provides a list of **file extensions** and **true file types** from which you can choose for scanning. You can add to this list by typing the file extension in the Specify file extensions configuration field.

Security Risk Scan Target Settings

The following lists the steps required to configure security risk scan settings for the target tab.
To configure security risk scan target settings:

1. Log on to the product console.
2. Click Security Risk Scan. The Security Risk Scan screen displays.
3. Select one of the following for security risk scan:
   - **All scannable files**: Select this option to have PortalProtect scan all scannable files.
   - **IntelliScan**: Uses true file type identification to perform efficient scans using Trend Micro recommended settings.
   - **Specify file types**: Click the Show details link to expand the list and select the files you want PortalProtect to scan. These files are "true file types." The scan engine examines the file header rather than the file name to ascertain the actual file type. Or, select to create a list of file extensions by selecting Specify file extensions.
     - For example: If you click Specify file types and then select Application and executables > Executable (.exe; .dll; .vxd), then PortalProtect will scan executable, DLL, and VXD file types—even when the file has a false file extension name; for example: the file extension is labeled .txt when it is actually an .exe. However, if you click Specify file extensions and type "exe", then PortalProtect will scan only .exe type files. PortalProtect does not recognize falsely labeled file types.
4. Select Enable IntelliTrap to use IntelliTrap technology.
5. For Spyware/Grayware Scan, choose Select All or select from the following:
   - Spyware
   - Dialers
   - Hacking Tools
   - Password Cracking Applications
   - Adware
   - Joke Programs
   - Remote Access Tools
   - Others
6. To modify or improve performance, click Scan Restriction Criteria to expand the contents. Under Do not scan file if...
   - **File size exceeds**—type a value between 1-30-MB.
7. Under **Do not scan compressed files if**, type values according to the following:
   - **Decompressed file count exceeds [xxxx]**—type the total decompressed file count (1-10000) that should not be exceeded. When PortalProtect encounters a number of files equal to or greater than this number it will not scan the files.
   - **Size of Decompressed file exceeds [xxxx]**—type a value in megabytes (1-2048) to set a limit for the size of the compressed files PortalProtect will scan. When PortalProtect encounters a compressed file that is equal to or greater than this size, it will not scan the file.
   - **Number of layers of compression exceeds [xx]**—type a number (1-20) to set a limit for the number of layers of compression to which PortalProtect will scan. When PortalProtect encounters a file of a compression layer equal to or greater than this number it will not scan the files.
   - **Size of decompressed file is "x" times the size of compressed file**—decompressed files must not exceed the multiple entered according to the compressed file size. Type a multiple (100-1000000) that the decompressed file must not exceed. Decompressed files that exceed the value: decompressed size is "x" times larger than the compressed size, will not be scanned.

8. Click **Save**.

**Note:** Office 2007 files are compressed files. If an office 2007 file exceeds the scan restriction criteria, PortalProtect will treat it as an **unscannable** file.

---

**Configure Macro Scanning Options for Real-time Security Risk Scan**

The following explains the steps required to configure macro scanning options for real-time security risk scan:

**To configure macro scanning options for real-time security risk scan:**

1. On the left menu, click **Security Risk Scan** and select the **Action** tab.
2. Under **Advanced Options**, click **Macros** to open the content.
3. Select, **Enable advanced macro scan**, to enable the functionality.
4. For **Heuristic level**, select an option according to the following:
   - 1 - Lenient filtering
• 2 - Default filtering
• 3 - Sensitive filtering
• 4 - Rigorous filtering

OR...

5. Select **Delete all macros detected by advanced macro scan.**
6. Click **Save.**

**About Security Risk Scan Action Settings**

When PortalProtect detects a file that matches your blocking or scanning configurations, it executes an action to protect your SharePoint environment. The type of action it executes depends on the type of scan it is performing (Real-time, Manual, or Scheduled) and the type of actions you have configured for that scan. Each time that PortalProtect executes an action, it logs an event. You can query these log events from the **Logs** menu.

**Before configuring security risk scan actions:**

1. Choose whether to set up a backup folder.
   
   When you setup a backup folder, PortalProtect sends a copy of the file to the backup directory before it performs the configured actions. See **Specify a Backup Folder for Security Risk Scan** on page 3-7.

2. Configure the action that PortalProtect executes when it detects viruses or malicious code. You can configure PortalProtect to use **ActiveAction** or configure a custom action. ActiveAction takes the most appropriate action based on the threat type. See **Trend Micro™ ActiveAction™** on page 1-22.

**Configuring Security Risk Scan Action Settings**

When PortalProtect detects a file that matches your scanning configurations, it executes an action to protect your SharePoint environment. The type of action it executes depends on the type of scan being performed (real-time, manual, or scheduled) and the type of actions you have configured for that scan.

The following provides a brief description of the options available:

- **ActiveAction**: Perform scan actions recommended by Trend Micro.
**Tip:** ActiveAction performs the primary and secondary scan actions recommended by Trend Micro. If the primary scan action is unsuccessful, the secondary action will be performed. ActiveAction uses pre-configured scan actions for viruses, Trojans, and joke programs.

- **Customized action for detected threats:** Select to perform an action over all security risks or specify an action for each threat.
- **Advanced Options:** Specify advanced options for Macros, Unscannable Files, and Backup Settings.

**To configure security risk scan action settings:**

1. Log on to the product console.
2. Click **Security Risk Scan**. The Security Risk Scan screen displays.
3. Click the **Action** tab. The Action screen displays.
4. Select one of the following:
   - **ActiveAction**
     1. Notify, Notify when uncleanable, or Do not notify
   - **Customized action for detected threats**:
5. To backup the infected file, select **Backup infected file before performing action**.
6. Select **Do not clean infected compressed files to optimize performance** if performance improvement is required.
7. Configure **Advanced Options** as necessary. Under **Advanced Options**, click **Macros** to expand the content.
8. Select **Enable advanced macro scan**, to enable the functionality.
9. For **Heuristic level**, select an option according to the following:
   - 1 - Lenient filtering
   - 2 - Default filtering
   - 3 - Sensitive filtering
   - 4 - Rigorous filtering
10. Select **Delete all macros detected by advanced macro scan**.
11. Click to expand **Unscannable Files** to specify actions for encrypted and password protected files, and files not in the scan restriction criteria. Select from the following options:

- **Encrypted or password protected files**
  - i. Block or Pass
  - and...
  - ii. Notify or Do not notify

- **Files exceeding specified scanning restrictions**
  - i. Block or Pass
  - and...
  - ii. Notify or Do not notify

12. Modify the **Backup Setting** if required.

13. Click **Save**.

---

**Note:** Refer to *Security Risk Scan Notifications* on page 11-3 for details on how to configure the notification settings.

---

**Scan Compressed Files**

This section explains the steps required to configure scanning for compressed files for Real-time, Manual, and Scheduled Security Risk Scan.

---

**Note:** To optimize scanning performance when scanning compressed files, clear **Do not clean infected compressed files to optimize performance** on the Security Risk Scan > Action tab.

---

**To scan compressed files for real-time security risk scan:**

1. On the left menu, click **Security Risk Scan** and select the **Target** tab.

2. From the **Target** tab, under **Advanced Options**, expand the **Scan Restrictions Criteria**.
Note: Select the checkbox for the items you want to scan and set the appropriate values.

3. Under **Do not scan file if...**
   - **File size exceeds**—type a value between 1-30-MB.

4. Under **Do not scan compressed files if**, type values according to the following:
   - **Decompressed file count exceeds [xxxx]**—type the total decompressed file count (1-10000) that should not be exceeded. When PortalProtect encounters a number of files equal to or greater than this number it will not scan the files.
   - **Size of Decompressed file exceeds [xxxx]**—type a value in megabytes (1-2048) to set a limit for the size of the compressed files PortalProtect will scan. When PortalProtect encounters a compressed file that is equal to or greater than this size, it will not scan the file.
   - **Number of layers of compression exceeds [xx]**—type a number (1-20) to set a limit for the number of layers of compression to which PortalProtect will scan. When PortalProtect encounters a file of a compression layer equal to or greater than this number it will not scan the files.
   - **Size of decompressed file is "x" times the size of compressed file**—decompressed files must not exceed the multiple entered according to the compressed file size. Type a multiple (100-1000000) that the decompressed file must not exceed. Decompressed files that exceed the value: decompressed size is "x" times larger than the compressed size, will not be scanned.

5. Click **Save**.

Note: Office 2007 files are compressed files. If an office 2007 file exceeds the scan restriction criteria, PortalProtect will treat it as an **unscannable** file.
File Blocking

You can configure PortalProtect to block files according to the file type and file name and select the action for all the files that match your configuration. When you enable file blocking, PortalProtect blocks the files according to your configurations. File blocking can occur during real-time, manual, and scheduled scanning according to the settings you choose.

**Note:** File blocking options vary according to the type of scan performed. Check the available actions for each scan type, whether Security Risk Scan, Manual Scan, or Scheduled Scan.

The extension of a file identifies the file type, for example .txt, .exe, or .dll. Many viruses are closely associated with certain types of files. Some virus writers have tried to disguise their files by using extension names that are known to be harmless, so true file type blocking scans the header of files to determine their actual type. By configuring PortalProtect to block according to file type, you can decrease the security risk to your SharePoint servers from those types of files. Similarly, specific attacks are often associated with a specific file name. If you learn the name of an infected file, you can use PortalProtect to screen that file out of your SharePoint. Blocking is an effective way to control virus outbreaks.
Tip: Administrators can also use file blocking to enforce their company’s policy restricting the sharing of non-work related files on their SharePoint servers.

About File Blocking Action Settings

When PortalProtect detects a file that matches your blocking configuration, it executes an action to protect your SharePoint environment. The type of action it executes depends on the type of scan it is performing (real-time, manual, or scheduled) and the type of actions you have configured for that scan (block or pass). Each time PortalProtect executes an action, it logs the event. You can view these from the Logs menu. See Query Logs starting on page 11-35 for more information.
Possible Actions

TABLE 5-1. Blocking actions for different scans

<table>
<thead>
<tr>
<th>During this scan</th>
<th>PortalProtect executes this action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Risk (real-time)</td>
<td>Clean, Block or Pass</td>
</tr>
<tr>
<td>File Blocking (real-time)</td>
<td>Block or Pass</td>
</tr>
<tr>
<td>Content Filtering (real-time)</td>
<td>Block or Pass</td>
</tr>
<tr>
<td>Web Reputation (real-time)</td>
<td>Block or Pass</td>
</tr>
<tr>
<td>Data Protection (real-time)</td>
<td>Block or Pass</td>
</tr>
<tr>
<td>Manual &gt; Security Risk</td>
<td>Clean, Quarantine, Delete, Pass, or Rename</td>
</tr>
<tr>
<td>Manual &gt; File Blocking</td>
<td>Quarantine, Delete, or Pass</td>
</tr>
<tr>
<td>Manual &gt; Content Filtering</td>
<td>Quarantine, Delete, or Pass</td>
</tr>
<tr>
<td>Manual &gt; Data Protection</td>
<td>Quarantine, Delete, or Pass</td>
</tr>
<tr>
<td>Scheduled &gt; Security Risk</td>
<td>Clean, Quarantine, Delete, Pass, or Rename</td>
</tr>
<tr>
<td>Scheduled &gt; File Blocking</td>
<td>Quarantine, Delete, or Pass</td>
</tr>
<tr>
<td>Scheduled &gt; Content Filtering</td>
<td>Quarantine, Delete, or Pass</td>
</tr>
<tr>
<td>Scheduled &gt; Data Protection</td>
<td>Quarantine, Delete, or Pass</td>
</tr>
</tbody>
</table>

- **Quarantine**—Move the file to the central quarantine database, removing it as a security risk from the SharePoint environment.
- **Pass**—No action taken. File is passed.
- **Block**—PortalProtect blocks the file from accessing the SharePoint server.
- **Delete**—During manual or scheduled scanning, PortalProtect deletes files that match the blocking options from the SharePoint environment.
- **Clean**—cleans the file of any potential threat.
• Rename—renames the file.

Configuring File Blocking for MOSS 2010/WSS 4.0

This section describes File Blocking configuration settings for MOSS 2010/WSS 4.0.

Adding a File Blocking Policy (MOSS 2010/WSS 4.0)

This section describes the steps required to add a new File Blocking policy for MOSS 2010/WSS4.0.

To add a new file blocking policy:


Step 1. File Blocking: Add Policy > Specify Rules

1. Under Block these files, select from the following options for Specific files > File Types; click Show details to expand the content:
   • Application and executables
   • Documents
   • Images
   • Video
   • Audio
   • Compressed files

2. For Specific files > File Names; click Show details to expand the content:
   • Select Specific file extensions to block to block the extensions that appear in the list. Type a new extension and click Add to include it on the list. Use a semicolon (;) to separate multiple entries.

  Note: To delete entries, select the entry and click Delete. Select multiple entries using Ctrl + click.

• Select File names to block to block files with the name that appears in the list. Type a new file name and click Add to include it on the list.
• Select **Block file type or name within compressed files.**
• Click **Next.** The **File Blocking: Add Policy > Step 2: Exceptions** screen appears.

![File Blocking: Add Policy](image)

**FIGURE 5-1.** File Blocking: Add Policy > Step 2: Exceptions screen
Step 2. File Blocking: Add Policy > Exceptions

1. To add an exception, click Add. The File Blocking: Add Policy > Step 2.a: Specify sites to be excluded screen appears.

2. Choose from the following:
   If you choose All sites...
   
   **Note:** The All sites option enables you to choose from AD user(s)/group(s) only.

   * Click Next >.

   If you choose Specify a site’s URL...

   **Note:** The Specify a site’s URL option enables you to choose from both AD user(s)/group(s) and SharePoint user(s)/group(s); use the Search for drop down to choose.
- Type the URL in the **Specify a site’s URL** field, and click **Search**.
- From the Select sites tree, choose the specific site(s) to exclude from this policy.
- Click **Next >**.

3. Click **Next >**. The **Step 2b: Specify accounts to be excluded** screen appears.

4. Select from the following options:
   - **Anyone**: to exclude all accounts. Click **Finish** and proceed to...
   - **Specific accounts**: select to choose the specific accounts to exclude and proceed to the next step.

5. Type an AD user or group name in the **Search for AD user(s)/group(s)** field.
Note: The Specify a site’s URL option enables you to choose from both AD user(s)/group(s) and SharePoint user(s)/group(s); use the Search for drop down to choose.

6. Next to Search in, select Users and/or Groups as appropriate.
7. Click Search. Successful search results will then display in the Available Account(s) window.
8. Repeat the search as required.
9. Select all the users/groups you want to add to exclude and click Add to move them to the Selected Account(s) window.

![Figure 5-4. File Blocking: Add Policy > Step 3: Specify Action screen](image)

**Figure 5-4.** File Blocking: Add Policy > Step 3: Specify Action screen

**Step 3. File Blocking: Add Policy > Specify Action**

1. Select from the following options:
   - Block or Pass
   - Notify or Do not notify
• Click Next >. The File Blocking: Add Policy > Step 4: Specify Notification screen appears.

**FIGURE 5-5.** File Blocking: Add Policy > Step 4: Specify Notification screen

**Step 4.** File Blocking: Add Policy > Specify Notification


**FIGURE 5-6.** File Blocking: Add Policy > Step 5: Name and Priority screen
Step 5. File Blocking: Add Policy > Name and Priority screen

1. Select Enable this policy to activate it.
2. Type a name for your policy in the Policy name field.
3. Type the priority for your policy in the Priority field.

Tip: You can review the priorities and settings for your other policies in the review existing policies window.

4. Click Finish. The File Blocking main screen displays where your new policy will appear in the priority you selected.

![File Blocking main screen](image)

FIGURE 5-7. File Blocking main screen

Configuring File Blocking for MOSS 2007/WSS 3.0

This section describes File Blocking configuration settings for MOSS 2007/WSS 3.0.

Configuring File Blocking: Target Settings

This section explains the steps required to configure real-time file blocking for the Target tab.

To configure real-time file blocking target settings:

2. Click the Target tab.
3. Select Enable real-time file blocking to enable this functionality.
4. Under **Block these files**, select from the following options for **Specific files > File Types**; click **Show details** to expand the content:
   - Application and executables
   - Documents
   - Images
   - Video
   - Audio
   - Compressed files

5. For **Specific files > File Names**; click **Show details** to expand the content:
   - Select **Specific file extensions to block** to block the extensions that appear in the list. Type a new extension and click **Add** to include it on the list. Use a semicolon (;) to separate multiple entries.

   **Note:** To delete entries, select the entry and click **Delete**. Select multiple entries using Ctrl + click.

   - Select **File names to block** to block files with the name that appears in the list. Type a new file name and click **Add** to include it on the list.
   - Select **Block file type or name within compressed files**.
   - Click **Save**.
Configuring File Blocking: Action Settings

This section explains the steps required to configure real-time file blocking for the Action tab.

To configure real-time file blocking action settings:
2. Click the Action tab.
3. Select Enable real-time file blocking to enable this functionality.
4. Select from the following options:
   • Block or Pass
     And...
   • Notify or Do not notify
   • Click Save.

Note: Refer to File Blocking Notifications on page 11-4 for details on how to configure the notification settings.

About Available File Types

This section describes the available file types from which you can choose.

Application and Executables

<table>
<thead>
<tr>
<th>File Type</th>
<th>Associated extension(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executable and linking format</td>
<td>.elf</td>
</tr>
<tr>
<td>Executable</td>
<td>.exe; .dll; .vxd</td>
</tr>
</tbody>
</table>
### Documents

**TABLE 5-3. Document file choices**

<table>
<thead>
<tr>
<th>File Type</th>
<th>Associated extension(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe Portable Document Format</td>
<td>.pdf</td>
</tr>
<tr>
<td>Compiled HTML Help</td>
<td>.chm</td>
</tr>
<tr>
<td>Macros in MS Office compressed by ActiveMime</td>
<td>.mso</td>
</tr>
<tr>
<td>Microsoft Access</td>
<td>.mdb; .accdb</td>
</tr>
<tr>
<td>Microsoft Excel</td>
<td>.xls; .xlt</td>
</tr>
<tr>
<td>Microsoft Office Excel 2007</td>
<td>.xlsx; .xslm; .xlsx; .xltx; .xltm; .xlsb; .xlam</td>
</tr>
<tr>
<td>Microsoft Office PowerPoint 2007</td>
<td>.pptx; .pptm; .potx; .ppam; .ppsx; .ppsm</td>
</tr>
<tr>
<td>Microsoft Office Word 2007</td>
<td>.docx; .docm; .dotx; .dotm</td>
</tr>
<tr>
<td>Microsoft OLE</td>
<td>.doc - Word 6.0-2003; .dot; vss; .shs</td>
</tr>
<tr>
<td>Microsoft PowerPoint</td>
<td>.pps; .ppt</td>
</tr>
<tr>
<td>Microsoft Project</td>
<td>.mpp</td>
</tr>
<tr>
<td>Microsoft Rich Text Format</td>
<td>.rtf</td>
</tr>
<tr>
<td>Microsoft WORD/DOS 4.0/5.0</td>
<td>.wri; .doc</td>
</tr>
<tr>
<td>File Type</td>
<td>Associated extension(s)</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Microsoft Help</td>
<td>.hlp</td>
</tr>
<tr>
<td>MSFT</td>
<td>.msft</td>
</tr>
<tr>
<td>WordPerfect</td>
<td>.wp</td>
</tr>
</tbody>
</table>
### Images

**TABLE 5-4. Image file choices**

<table>
<thead>
<tr>
<th>File Type</th>
<th>Associated extension(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compuserve</td>
<td>.gif</td>
</tr>
<tr>
<td>Corel PhotoPaint Image</td>
<td>.cpt</td>
</tr>
<tr>
<td>Corel Global Macro Storage</td>
<td>.gms</td>
</tr>
<tr>
<td>JPEG image</td>
<td>.jpg; .jpeg; .jpe</td>
</tr>
<tr>
<td>Macintosh MacPaint graphic</td>
<td>.mac</td>
</tr>
<tr>
<td>Portable Network Graphics</td>
<td>.png</td>
</tr>
<tr>
<td>Tagged image format</td>
<td>.tiff</td>
</tr>
<tr>
<td>Windows/OS/2 Bitmap</td>
<td>.bmp</td>
</tr>
<tr>
<td>Windows metafile</td>
<td>.wmf</td>
</tr>
</tbody>
</table>

### Video

**TABLE 5-5. Video file choices**

<table>
<thead>
<tr>
<th>File Type</th>
<th>Associated extension(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Streaming Format</td>
<td>.asf; .wmv</td>
</tr>
<tr>
<td>Macromedia Flash</td>
<td>.swf</td>
</tr>
<tr>
<td>Moving Picture Experts Group video</td>
<td>.mpg; .mpeg</td>
</tr>
</tbody>
</table>
## Audio

### TABLE 5-6. Audio file choices

<table>
<thead>
<tr>
<th>File Type</th>
<th>Associated extension(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Resource Interchange File Format</td>
<td>.avi; .bnd; .wav</td>
</tr>
<tr>
<td>Quicktime Movie</td>
<td>.mov; .qt; .qtm</td>
</tr>
<tr>
<td>Real Media</td>
<td>.rm</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>File Type</th>
<th>Associated extension(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Musical Instrument Digital Interface</td>
<td>.mid</td>
</tr>
<tr>
<td>MPEG Audio Layer 3</td>
<td>.mp3</td>
</tr>
<tr>
<td>Real Audio</td>
<td>.ra; .ram</td>
</tr>
</tbody>
</table>
## Compressed Files

**TABLE 5-7. Compressed file choices**

<table>
<thead>
<tr>
<th>File Type</th>
<th>Associated extension(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive created by LHA</td>
<td>.lzh</td>
</tr>
<tr>
<td>Archive created by Pkzip</td>
<td>.zip</td>
</tr>
<tr>
<td>Archive created by RAR</td>
<td>.rar</td>
</tr>
<tr>
<td>Archive created by Tar</td>
<td>.tar</td>
</tr>
<tr>
<td>ARJ Compressed archive</td>
<td>.arj</td>
</tr>
<tr>
<td>BINHEX</td>
<td>.hqx</td>
</tr>
<tr>
<td>GNU Zip</td>
<td>.gz; .gzip</td>
</tr>
<tr>
<td>LZW/Compressed 16-bits</td>
<td>.Z</td>
</tr>
<tr>
<td>MacBinary</td>
<td>.bin</td>
</tr>
<tr>
<td>Microsoft Cabinet</td>
<td>.cab</td>
</tr>
<tr>
<td>Microsoft Compressed</td>
<td>.mscomp</td>
</tr>
<tr>
<td>MIME</td>
<td>.eml; .mht</td>
</tr>
<tr>
<td>Teledisk format</td>
<td>.td0</td>
</tr>
<tr>
<td>Unix BZ2 Bzip Compressed file</td>
<td>.bz2</td>
</tr>
<tr>
<td>UUEncode</td>
<td>.uu</td>
</tr>
<tr>
<td>WinAce</td>
<td>.ace</td>
</tr>
</tbody>
</table>
Chapter 6

Content Filtering

When PortalProtect finds a word that matches a keyword in a content filter policy, it can take action to prevent the undesirable content from being posted to SharePoint. You can configure PortalProtect to send notifications whenever it takes an action against undesirable content.

Each PortalProtect Content filtering policy contains a list of keywords, phrases, or compliance patterns. Compliance patterns can be associated with credit card numbers, Social Security Numbers, and country specific identification information. PortalProtect is now fully integrated with Active Directory (AD) user(s)/group(s), and SharePoint user(s)/group(s). Policies can be applied to the following:

- Active Directory user(s)/group(s)
- SharePoint site(s)/SharePoint user(s)/group(s)

Content filtering can be enabled for:

- Real-time content filtering for documents—filters the content of documents uploaded or downloaded to SharePoint document libraries in real-time.
- Real-time content filtering for Web content—filters the Web content for SharePoint Lists when you create a new item or update an existing one (for example: Tasks, Links, Calendar, Announcements, and so forth).
PortalProtect applies the content filtering policies according to the order shown in the Content Filtering screen. You can configure the order in which the policies are applied. PortalProtect will perform filtering according to each policy until a content violation triggers an action that prevents further scanning (such as block or pass). You can change the order of these policies to optimize content filtering.

Additionally, the content filter provides a synonym checking feature that enables you to extend the reach of your policies.

---

**Note:** Content filtering for files scans during uploading and downloading, whereas content filtering for Web scans list items when they are added or modified.

Content filtering for files cannot scan the content of .eml files.

You can, for example, create policies to check for:

- Credit card numbers and country specific identification information
- Sexually harassing language
- Racist language
- Profanity

### About Content Filtering Action Settings

The available actions for Content Filtering are shown in *Table 6-1*:

<table>
<thead>
<tr>
<th><strong>During this scan</strong></th>
<th><strong>PortalProtect executes this action</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Filtering (real-time)</td>
<td>Block or Pass</td>
</tr>
<tr>
<td>Manual Scan &gt; Content Filtering (for document)</td>
<td>Quarantine, Delete, or Pass</td>
</tr>
</tbody>
</table>

---
Content Filtering Policies

This section provides background information about Content Filtering Policies to help you better configure these options.

Policy Exceptions

For Active Directory integrated policies, you can specify selected Active Directory User(s) and Group(s) as policy excluded accounts. For example, consider that AD Group1 contains an exclusion for ADUser1 and ADUser2. In this case, ADUser1 and ADUser2 will be excluded according to the AD Group1 policy.

Tip: Exclusion only works in an AD environment. The Exception list does not support AD users/groups across the forest and also does not support global AD groups.

For SharePoint user(s) and Group(s) integrated policies, you can specify selected SharePoint site(s) and user(s)/group(s) within the site(s).

---

TABLE 6-1. Content Filtering actions

<table>
<thead>
<tr>
<th>During this scan</th>
<th>PortalProtect executes this action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual Scan &gt; Content Filtering (for Web)</td>
<td>Pass</td>
</tr>
<tr>
<td></td>
<td>Note: PortalProtect will pass and log the Web content that triggers the policy in manual scan.</td>
</tr>
<tr>
<td>Scheduled Scan &gt; Content Filtering (for document)</td>
<td>Quarantine, Delete, or Pass</td>
</tr>
<tr>
<td>Scheduled Scan &gt; Content Filtering (for Web)</td>
<td>Pass</td>
</tr>
<tr>
<td></td>
<td>Note: PortalProtect will pass and log the Web content that triggers the policy in manual scan.</td>
</tr>
</tbody>
</table>
**Note:** PortalProtect and MOSS 2010/WSS 4.0 provides real-time policy exceptions. MOSS 2007/WSS 3.0 does not provide for this functionality. See *Adding a Content Filtering Policy (MOSS 2010/WSS 4.0)* on page 6-9 and *Adding a Content Filtering Policy (MOSS 2007/WSS 3.0)* on page 6-18 for more information.

---

**Global Approved List (Real-time)**

PortalProtect provides an additional real-time feature called the Global Approved List for both documents and Web content. This is a *white list* that enables the administrator to add Active Directory users and groups for which the Content Filtering policies will be excluded. See *Global Approved List* on page 1-7.
**Note:** Real-time functionality for the Global Approved list is supported only for the MOSS 2010 and WSS 4 platforms. See *Figure 6-1*.

---

**FIGURE 6-1.** Content Filtering Global Approved List (MOSS 2010/WSS 4.0 Only)

**Note:** The real-time Global Approved list for Content Filtering is available only for MOSS 2010/WSS 4.0. See *Global Approved List* on page 1-7 for more information.
To configure the real-time global approved list for content filtering:

1. Click **Content Filtering** on the left menu. The Content Filtering screen appears.
2. Click Global Approved List (see Figure 6-1). The Content Filtering: Edit Global Approved List screen appears (see Figure 6-2).

---

**FIGURE 6-2. Content Filtering: Edit Global Approved List screen**

3. Select **Enable global approved list** to enable to functionality.
4. Type an AD user or group name in the **Search for AD user(s)/group(s)** field.
5. Under **Search in**, select **Users** and/or **Groups** as appropriate.
6. Click **Search**. Successful search results will then display in the **Available Account(s)** window.
7. Repeat the search as required.
8. Select all the users/groups you want to add to the **Global Approved List** and click **Add** to move them to the **Selected Account(s)** window.
9. Click **Save**.

### Configuring Content Filtering

This section provides the information required to manage and configure Content Filtering for PortalProtect. You can manage the following settings from the content filtering main screen:

- Enable or disable real-time content filtering for documents
- Enable or disable real-time content filtering for Web content
- Filter the listed policies by policy name, or whether they are enabled or disabled
- Reorder the policy priority
- Delete a policy
- Enable or disable a policy
- Change the number rows that appear on the policy page
- Add a new policy or edit an existing policy
To enable or disable real-time content filtering for document or Web content:

1. On the left menu, click **Content Filtering**. The Content Filtering screen appears (Figure 6-3).

2. Select one or both of the following options:
   - **Enable real-time content filtering for document**—performs real-time content filtering for documents
   - **Enable real-time content filtering for Web content**—performs real-time content filtering for Web content

   **Note:** You can filter the listed policies by: **Policy name, All, Enabled**, or **Disabled**. After choosing your filter options, click **Search**; to display all search results click **Display All**.

3. Click **Save**.
Adding a Content Filtering Policy (MOSS 2010/WSS 4.0)

The section describes the various steps required to create a new content filtering policy.

Step 1. Content Filtering: Add Policy > Specify Rules

1. On the left menu, click Content Filtering. The Content Filtering screen appears (Figure 6-3).

2. Click Add. The Content Filtering: Add Policy > Step 1: Specify Rules screen appears.

![Content Filtering: Add Policy > Step 1: Specify Rules screen](Image)

3. From the Match drop down, select from the following options:

   - **Any specified keyword**—select this option if you want this rule to trigger when any keyword is found and matched
   - **All keywords**—select this option if you want this rule to trigger when all keywords are found and matched
Note: You can export or import a keyword list to or from a text file (.txt) using the Export or Import keys located next to the keyword list.

4. To add or remove keyword(s):
   a. Type a keyword or regular expression in the Enter keyword(s) field, then, click Add.
   
   Note: See About Regular Expressions starting on page B-1 for more information about using regular expressions with PortalProtect.

   b. To remove a keyword, select it from the existing list, and click Remove.

5. Select Match case if you want to match the case of the listed keywords.

6. Set Match synonym settings according to the following:
   a. Click Show details to expand the synonym settings section.
   b. Select a keyword from the keyword list to display its synonym(s) in the Synonyms to exclude window.
   c. Move one or more synonyms to the left Synonyms to include window. Multi-select using the Ctrl key.

Step 2. Content Filtering: Add Policy > Step 2: Exceptions

Content Filtering: Add Policy

Policy List > New Policy

![Step 2: Exceptions screen](image)

**FIGURE 6-5.** Content Filtering: Add Policy > Step 2: Exceptions screen
To add exceptions for the content filtering policy:

1. Click Add from the Step 2: Exceptions screen. The Step 2a: Specify sites to be excluded screen appears (Figure 6-6).

2. Choose from the following:
   - If you choose All sites...

   **Note:** The All sites option enables you to choose from AD user(s)/group(s) only.

   • Click Next > and go to Step 3.
   
   If you choose Specify a site’s URL...
**Note:** The **Specify a site’s URL** option enables you to choose from both **AD user(s)/group(s)** and **SharePoint user(s)/group(s)**; use the **Search for** drop down to choose.

- Type the URL in the **Specify a site’s URL** field, and click **Search**.
- From the Select sites tree, choose the specific site(s) to exclude from this policy.
- Click **Next >** and go to Step 3.

3. Click **Next >**. The **Step 2b: Specify accounts to be excluded** screen appears *(Figure 6-7)*.

---

**Content Filtering: Add Policy**

![Figure 6-7. Content Filtering: Add Policy > Step 2.b Specify accounts to be excluded screen](image-url)

---

6-13
4. Select from the following options:
   • **Anyone**: to exclude all accounts. Select, click Finish and proceed to...
   • **Specific accounts**: select to choose the specific accounts to exclude and proceed to the next step.

5. Type an AD user or group name in the **Search for AD user(s)/group(s)** field.

   **Note:** The **Specify a site’s URL** option enables you to choose from both AD user(s)/group(s) and SharePoint user(s)/group(s); use the Search for drop down to choose.

6. Next to **Search in**, select **Users** and/or **Groups** as appropriate.
7. Click **Search**. Successful search results will then display in the **Available Account(s)** window.
8. Repeat the search as required.
9. Select all the users/groups you want to add to exclude and click **Add** to move them to the Selected Account(s) window.
10. Click **Finish**. The **Step 2: Exceptions** screen appears.
11. Select the exception you added/edited to exclude it and click **Next >**. The **Step 3: Action** screen appears.

**Step 3. Content Filtering: Add Policy > Specify Action**

To specify an action for the content filtering policy:
1. Select an action for the content filtering policy from the following options:
   • **Block** or **Pass**
   • **Notify** or **Do not notify**
   • Click **Next >**.
Step 4. Content Filtering: Add Policy > Specify Notification

To configure notification settings:

1. Select Notify administrator to enable notifications for this content filtering policy.
2. Under People to notify, click Show details to expand and configure the following:
   - To—the global email address(es) appear in this field. You can enter additional email addresses, separated by a semicolon, to create unique notifications.

FIGURE 6-8. Content Filtering: Add Policy > Step 4: Specify Notification screen
- **Subject**—type a subject that will appear in the subject line of the email (for example: Content Filtering Notification).
- **Message**—you can create a unique message using variables like: [Server Name], [Content Rules], [Date], [Time], [File Name/Web Content Title], [File/Web Content Location], [Action], and [Violator].

**Note:** The available variables appear in the left window, and the message body in the right window.

3. Under **Settings**, choose the delivery options for this notification according to the following:
   - **Send consolidated notifications every [xx] [hours or days]**—select this option to send a notification according to the number of hours or days you type in the variable field.
   - **Send consolidated notifications every [xx] occurrences**—select this option to send a notification after a certain number of occurrences as you stipulate in the variable field.
   - **Send individual notifications**—select this option to send a notification each time an event occurs.

4. Under **Advanced Notification**, select SNMP to enable this option.

5. Click **Show details** to expand the options, and configure according to the following:
   - **IP Address**
   - **Community**
   - **Message**—create a message as stated in Step 2 of this procedure.

6. Select **Write to Windows event log** to write each notification to the Windows event log.

7. **Click Next >.**
Step 5. Content Filtering: Add Policy > Name and Priority

To configure the name and priority for the policy:

1. Select Enable this policy to activate it.
2. Type a name for your policy in the Policy name field.
3. Type the priority for your policy in the **Priority** field.

**Tip:** You can review the priorities and settings for your other policies in the review existing policies window.

4. Click **Finish**. The Content Filtering main screen displays where your new policy will appear in the priority you selected.

**Adding a Content Filtering Policy (MOSS 2007/WSS 3.0)**

The section describes the various steps required to create a new content filtering policy.

**Step 1. Content Filtering: Add Policy > Specify Rules**

1. On the left menu, click **Content Filtering**. The Content Filtering screen appears *(Figure 6-3)*.

2. Click **Add**. The **Content Filtering: Add Policy > Step 1: Specify Rules** screen appears.

**FIGURE 6-10. Content Filtering: Add Policy > Step 1: Specify Rules screen**
3. From the **Match** drop down, select from the following options:
   - **Any specified keyword**—select this option if you want this rule to trigger when any keyword is found and matched
   - **All keywords**—select this option if you want this rule to trigger when all keywords are found and matched

   **Note:** You can export or import a keyword list to or from a text file (.txt) using the **Export** or **Import** keys located next to the keyword list.

4. To add or remove keyword(s):
   a. Type a keyword or regular expression in the **Enter keyword(s)** field, then, click **Add**.

      **Note:** See *About Regular Expressions* starting on page B-1 for more information about using regular expressions with PortalProtect.

   b. To remove a keyword, select it from the existing list, and click **Remove**.

5. Select **Match case** if you want to match the case of the listed keywords.

6. Set **Match synonym** settings according to the following:
   a. Click **Show details** to expand the synonym settings section.
   b. Select a keyword from the keyword list to display its synonym(s) in the **Synonyms to exclude** window.
   c. Move one or more synonyms to the left **Synonyms to include** window. Multi-select using the **Ctrl** key.

7. Click **Next >**. The **Content Filtering: Add Policy > Step 2: Specify Action** screen appears.
Step 2. Content Filtering: Add Policy > Specify Action

To specify an action for the content filtering policy:

1. Select an action for the content filtering policy from the following options:
   - Block or Pass
   - Notify or Do not notify
   - Click Next >. The Content Filtering: Add Policy > Step 3: Specify Notification screen appears.
Step 3. Content Filtering: Add Policy > Specify Notification

Content Filtering: Add Policy

Policy List > New Policy

Step 1 >>> Step 2 >>> Step 3: Specify Notification >>> Step 4

To configure notification settings:

1. Select **Notify administrator** to enable notifications for this content filtering policy.
2. Under **People to notify**, click **Show details** to expand and configure the following:
   - **To**—the global email address(es) appear in this field. You can enter additional email addresses, separated by a semicolon, to create unique notifications.

**FIGURE 6-12. Content Filtering: Add Policy > Step 3: Specify Notification screen**
• **Subject**—type a subject that will appear in the subject line of the email (for example: Content Filtering Notification).

• **Message**—you can create a unique message using variables like: [Server Name], [Content Rules], [Date], [Time], [File Name/Web Content Title], [File/Web Content Location], [Action], and [Violator].

**Note:** The available variables appear in the left window, and the message body in the right window.

3. Under **Settings**, choose the delivery options for this notification according to the following:

   • **Send consolidated notifications every [xx] [hours or days]**—select this option to send a notification according to the number of hours or days you type in the variable field.

   • **Send consolidated notifications every [xx] occurrences**—select this option to send a notification after a certain number of occurrences as you stipulate in the variable field.

   • **Send individual notifications**—select this option to send a notification each time an event occurs.

4. Under **Advanced Notification**, select SNMP to enable this option.

5. Click **Show details** to expand the options, and configure according to the following:

   • **IP Address**

   • **Community**

   • **Message**—create a message as stated in Step 2 of this procedure.

6. Select **Write to Windows event log** to write each notification to the Windows event log.

7. Click **Next >**. The **Content Filtering: Add Policy > Step 4: Name and Priority** screen appears.
Step 4. Content Filtering: Add Policy > Name and Priority

To configure the name and priority for the rule:

1. Select Enable this policy to activate it.
2. Type a name for your policy in the Policy name field.
3. Type the priority for your policy in the Priority field.
Tip: You can review the priorities and settings for your other policies in the review existing policies window.

4. Click Finish. The Content Filtering main screen displays where your new policy will appear in the priority you selected.

Edit a Content Filtering Policy (MOSS 2010/WSS 4.0)

This section describes the steps required to edit a Content Filtering policy.

To edit a content filtering policy:

1. On the left menu, click Content Filtering. The Content Filtering screen appears (Figure 6-3).
2. From the Content Filtering screen, click the policy name link you want to edit. The **Content Filtering: Edit Policy** screen appears (Figure 6-14).

![Content Filtering: Edit Policy](image)

**FIGURE 6-14. Content Filtering: Edit Policy screen (target tab)**

3. Select or clear the **Enable this policy** checkbox to enable or disable the policy.

4. Edit the following as required:
   - **Policy name**
   - **Description**

5. Click the **Target** tab, and from the **Match** drop down, select from the following options:
   - **Any specified keyword**—select this option if you want this rule to trigger when **any** keyword is found and matched
• **All keywords**—select this option if you want this rule to trigger when all keywords are found and matched

---

**Note:** You can export or import a keyword list to or from a text file (.txt) using the **Export** or **Import** keys located next to the keyword list.

---

6. To add or remove keyword(s):
   a. Type a keyword or regular expression in the **Enter keyword(s)** field, then, click **Add**.
      
      **Note:** See *About Regular Expressions* starting on page B-1 for more information about using regular expressions with PortalProtect.

   b. To remove a keyword, select it from the existing list, and click **Remove**.

7. Select **Match case** if you want to match the case of the listed keywords.

8. Set **Match synonym** settings according to the following:
   a. Click **Show details** to expand the synonym settings section.
   b. Select a keyword from the keyword list to display its synonym(s) in the **Synonyms to exclude** window.
   c. Move one or more synonyms to the left **Synonyms to include** window. Multi-select using the **Ctrl** key.

9. Click the **Exceptions** tab and add or edit any exceptions as required. See *Content Filtering: Add Policy > Step 2: Exceptions* on page 6-11 for more information.

10. Click the **Action** tab and choose from the following:
    • **Block**
    • **Pass**
    • **Notify**
    • **Do not notify**

11. Click the **Notification** tab, and choose the appropriate settings. See *Content Filtering: Add Policy > Specify Notification* on page 6-21 for more information.

12. Click **Save**.
Edit a Content Filtering Policy (MOSS 2007/WSS 3.0)

This section describes the steps required to edit a Content Filtering policy.

To edit a content filtering policy:

1. On the left menu, click Content Filtering. The Content Filtering screen appears (Figure 6-3).
2. From the Content Filtering screen, click the policy name link you want to edit. The Content Filtering: Edit Policy screen appears (Figure 6-15).

3. Select or clear the Enable this policy checkbox to enable or disable the policy.
4. From the Match drop down, select from the following options:
   - Any specified keyword—select this option if you want this rule to trigger when any keyword is found and matched
• All keywords—select this option if you want this rule to trigger when all keywords are found and matched

**Note:** You can export or import a keyword list to or from a text file (.txt) using the Export or Import keys located next to the keyword list.

5. To add or remove keyword(s):
   a. Type a keyword or regular expression in the Enter keyword(s) field, then, click Add.

   **Note:** See *About Regular Expressions* starting on page B-1 for more information about using regular expressions with PortalProtect.

   b. To remove a keyword, select it from the existing list, and click Remove.

6. Select Match case if you want to match the case of the listed keywords.

7. Set Match synonym settings according to the following:
   a. Click Show details to expand the synonym settings section.
   b. Select a keyword from the keyword list to display its synonym(s) in the Synonyms to exclude window.
   c. Move one or more synonyms to the left Synonyms to include window. Multi-select using the Ctrl key.

8. Click the Action tab and choose from the following:
   • Block
   • Pass
   • Notify
   • Do not notify

9. Click the Notification tab, and choose the appropriate settings. See *Content Filtering: Add Policy > Specify Notification* on page 6-21 for more information.

10. Click Save.
Data Protection

This version of PortalProtect enables you to use data protection policies to detect sensitive data in both documents and Web content. Compliance Patterns are best used with structured content, like Social Security Numbers (SSN), credit card numbers (CCN) and telephone numbers.

For example, credit card numbers are typically presented in 16-digit format, “xxxx-xxxx-xxxx-xxxx”, making them good candidates for pattern-based detection. See *Adding a Data Protection Policy (MOSS 2010/WSS 4.0)* on page 7-2 for more information about how to configure these compliance patterns.

Configuring Data Protection Policies

This section explains the steps required to configure data protection policies.
To enable or disable real-time data protection for document or Web content:

1. On the left menu, click Data Protection > Policy. The Data Protection screen appears (Figure 7-1).

2. Select one or both of the following options:
   - Enable real-time data protection for document—performs real-time data protection for documents
   - Enable real-time data protection for Web content—performs data protection for Web content

   **Note:** You can filter the listed policies by: Policy name, All, Enabled, or Disabled. After choosing your filter options, click Search; to display all search results click Display All.

3. Click Save.

Adding a Data Protection Policy (MOSS 2010/WSS 4.0)

The section describes the various steps required to create a new data protection policy.
Step 1. Data Protection: Add Policy > Specify Rules

1. On the left menu, click Data Protection > Policy. The Data Protection screen appears (Figure 7-1).


3. Select the compliance template(s) you want to add from the list of Available compliance templates and click Add >>. Remove compliance templates by first selecting and then clicking << Remove.

   **Note:** Press and hold the Ctrl key to select multiple compliance templates.

   **Note:** You can import a compliance template from an XML file by clicking the Import button.
4. To add a compliance template to the list of available compliance templates:
   a. Click the Add button, which is located next to the Import button. The Add Compliance Template screen appears.
   b. Type a name for the new template in the Compliance template name field.
   c. Type an optional description for the new template in the Description field.

5. To define a compliance template, select from the following:
   a. If you select Expressions...
      • Choose an expression from the list (US SSN, Credit Card Number, Phone Number, and so on)
   b. Type the number of occurrences required to trigger the policy in the Occurrences field.
   c. Click the “+” to add additional compliance template(s)
      • Select the appropriate operator And/Or
      • Repeat the previous process by choosing Expressions and select one of the available expressions from the list.
      • Type the number of occurrences required to trigger the policy in the Occurrences field.
   d. If you select Keywords...
      • Choose one of the keywords from the list of available keywords.
      • Click the “+” to add additional compliance template(s)
      • Select the appropriate operator And/Or
      • Repeat the previous process by choosing Keywords and select one of the available keywords from the list.

6. After you finish adding your compliance template(s), click Add, then click Save. The Data Protection: Add Policy > Step 1: Specify Rules screen appears.

Step 2. Data Protection: Add Policy > Step 2: Exceptions

FIGURE 7-3. Data Protection: Add Policy > Step 2: Exceptions screen
To add exceptions for the data protection policy:

1. Click Add from the Step2: Exceptions screen. The Step 2a: Specify sites to be excluded screen appears (Figure 7-4).

2. Choose from the following:
   If you choose **All sites**...

   **Note:** The All sites option enables you to choose from AD user(s)/group(s) only.

   
   • Click **Next >** and go to Step 3.
   If you choose **Specify a site’s URL**...
Note: The **Specify a site’s URL** option enables you to choose from both **AD user(s)/group(s)** and **SharePoint user(s)/group(s)**; use the **Search for** drop down to choose.

- Type the URL in the **Specify a site’s URL** field, and click **Search**.
- From the Select sites tree, choose the specific site(s) to exclude from this policy.

3. Click **Next >**. The **Step 2b: Specify accounts to be excluded** screen appears (Figure 7-5).

**Figure 7-5.** Data Protection: Add Policy > Step 2.b Specify accounts to be excluded screen
4. Select from the following options:
   - **Anyone**: to exclude all accounts. Click **Finish** and proceed to...
   - **Specific accounts**: select to choose the specific accounts to exclude and proceed to the next step.

5. Type an AD user or group name in the **Search for AD user(s)/group(s)** field.

   **Note**: The **Specify a site’s URL** option enables you to choose from both AD user(s)/group(s) and SharePoint user(s)/group(s); use the **Search for** drop down to choose.

6. Next to **Search in**, select **Users** and/or **Groups** as appropriate.

7. Click **Search**. Successful search results will then display in the **Available Account(s)** window.

8. Repeat the search as required.

9. Select all the users/groups you want to add to exclude and click **Add** to move them to the **Selected Account(s)** window.

10. Click **Finish**. The **Step 2: Exceptions** screen appears.

11. Select the exception you added/edited to exclude it and click **Next >**. The **Step 3: Action** screen appears.

**Step 3. Data Protection: Add Policy > Specify Action**

**To specify an action for the data protection policy:**

1. Select an action for the data protection policy from the following options:
   - **Block** or **Pass**
   - **Notify** or **Do not notify**
   - Click **Next >**.
Step 4. Data Protection: Add Policy > Specify Notification

To configure notification settings:

1. Select Notify administrator to enable notifications for this data protection policy.
2. Under People to notify, click Show details to expand and configure the following:
   - To—the global email address(es) appear in this field. You can enter additional email addresses, separated by a semicolon, to create unique notifications.
• **Subject**—type a subject that will appear in the subject line of the email (for example: Data Protection Notification).

• **Message**—you can create a unique message using variables like: [Server Name], [Data Protection Rules], [Date], [Time], [File Name/Web Content Title], [File/Web Content Location], [Action], and [Violator].

**Note:** Note: The available variables appear in the left window, and the message body in the right window.

3. Under **Settings**, choose the delivery options for this notification according to the following:

   • **Send consolidated notifications every [xx] [hours or days]**—select this option to send a notification according to the number of hours or days you type in the variable field.

   • **Send consolidated notifications every [xx] occurrences**—select this option to send a notification after a certain number of occurrences as you stipulate in the variable field.

   • **Send individual notifications**—select this option to send a notification each time an event occurs.

4. Under **Advanced Notification**, select SNMP to enable this option.

5. Click **Show details** to expand the options, and configure according to the following:

   • **IP Address**

   • **Community**

   • **Message**—create a message as stated in Step 2 of this procedure.

6. Select **Write to Windows event log** to write each notification to the Windows event log.

7. Click **Next >**.
Step 5. Data Protection: Add Policy > Name and Priority

To configure the name and priority for the policy:

1. Select **Enable this policy** to activate it.
2. Type a name for your policy in the **Policy name** field.
3. Type the priority for your policy in the **Priority** field.

**Tip:** You can review the priorities and settings for your other policies in the review existing policies window.

4. Click **Finish**. The Data Protection main screen displays where your new policy will appear in the priority you selected.
Adding a Data Protection Policy (MOSS 2007/WSS 3.0)

The section describes the various steps required to create a new data protection policy.

Step 1. Data Protection: Add Policy > Specify Rules

1. On the left menu, click Data Protection > Policy. The Data Protection main screen appears (Figure 7-1).

![Data Protection: Add Policy](image)

**FIGURE 7-8.** Data Protection: Add Policy > Step 1: Specify Rules screen

3. Select the compliance template(s) you want to add from the list of Available compliance templates and click Add >>. Remove compliance templates by first selecting and then clicking << Remove.

**Note:** Press and hold the Ctrl key to select multiple compliance templates.
4. To add a compliance template to the list of available compliance templates:
   a. Click the Add button, which is located next to the Import button. The Add Compliance Template screen appears.
   b. Type a name for the new template in the Compliance template name field.
   c. Type an optional description for the new template in the Description field.

5. To define a compliance template, select from the following:
   a. If you select Expressions...
      • Choose an expression from the list (US SSN, Credit Card Number, Phone Number, and so on)
   b. Type the number of occurrences required to trigger the policy in the Occurrences field.
   c. Click the “+” to add additional compliance template(s)
      • Select the appropriate operator And/Or
      • Repeat the previous process by choosing Expressions and select one of the available expressions from the list.
      • Type the number of occurrences required to trigger the policy in the Occurrences field.
   d. If you select Keywords...
      • Choose one of the keywords from the list of available keywords.
      • Click the “+” to add additional compliance template(s)
      • Select the appropriate operator And/Or
      • Repeat the previous process by choosing Keywords and select one of the available keywords from the list.

6. After you finish adding your compliance template(s), click Add, then click Save. The Data Protection: New Policy > Step 1: Specify Rules screen appears.

Step 2.  Data Protection: Add Policy > Specify Action

To specify an action for the data protection policy:

1. Select an action for the data protection policy from the following options:
   - Block or Pass
   - Notify or Do not notify
   - Click Next >. The Data Protection: Add Policy > Step 3: Specify Notification screen appears.
Step 3. Data Protection: Add Policy > Specify Notification

To configure notification settings:

1. Select **Notify administrator** to enable notifications for this data protection policy.
2. Under **People to notify**, click **Show details** to expand and configure the following:
   - **To**—the global email address(es) appear in this field. You can enter additional email addresses, separated by a semicolon, to create unique notifications.
• **Subject**—type a subject that will appear in the subject line of the email (for example: Data Protection Notification).

• **Message**—you can create a unique message using variables like: [Server Name], [Data Protection Rules], [Date], [Time], [File Name/Web Content Title], [File/Web Content Location], [Action], and [Violator].

**Note:** The available variables appear in the left window, and the message body in the right window.

3. Under **Settings**, choose the delivery options for this notification according to the following:
   - **Send consolidated notifications every [xx] [hours or days]**—select this option to send a notification according to the number of hours or days you type in the variable field.
   - **Send consolidated notifications every [xx] occurrences**—select this option to send a notification after a certain number of occurrences as you stipulate in the variable field.
   - **Send individual notifications**—select this option to send a notification each time an event occurs.

4. Under **Advanced Notification**, select SNMP to enable this option.

5. Click **Show details** to expand the options, and configure according to the following:
   - **IP Address**
   - **Community**
   - **Message**—create a message as stated in Step 2 of this procedure.

6. Select **Write to Windows event log** to write each notification to the Windows event log.

7. Click **Next >**. The **Data Protection: New Policy > Step 4: Name and Priority** screen appears.
Step 4. Data Protection: Add Policy > Name and Priority

To configure the name and priority for the policy:

1. Select **Enable this policy** to activate it.
2. Type a name for your policy in the **Policy name** field.
3. Type the priority for your policy in the **Priority** field.

**Tip:** You can review the priorities and settings for your other policies in the review existing policies window.

4. Click **Finish**. The Data Protection main screen displays where your new policy will appear in the priority you selected.
Edit a Data Protection Policy (MOSS 2010/WSS 4.0)

This section describes the steps required to edit a Data Protection policy.

To edit a data protection policy:

1. On the left menu, click Data Protection > Policy. The Data Protection screen appears (Figure 7-1).
2. From the Data Protection screen, click the policy name link you want to edit. The Data Protection: Edit Policy screen appears (Figure 7-12).

3. Select or clear the Enable this policy checkbox to enable or disable the policy.
4. Edit the following as required:
   - Policy name
   - Description

**Figure 7-12.** Data Protection: Edit Policy screen (target tab)
5. Click the **Target** tab.

6. Select the compliance template(s) you want to add from the list of **Available compliance templates** and click **Add >>**. Remove compliance templates by first selecting and then clicking **<< Remove**.

---

**Note:** Press and hold the **Ctrl** key to select multiple compliance templates.

---

**Note:** You can import a compliance template from a text file (.txt) clicking the **Import** button.

---

7. To add a compliance template to the list of available compliance templates:
   a. Click the **Add** button, which is located next to the **Import** button. The **Add Compliance Template** screen appears.
   b. Type a name for the new template in the **Compliance template name** field.
   c. Type an optional description for the new template in the **Description** field.

8. To define a compliance template, select from the following:
   a. If you select **Expressions**...
      • Choose an expression from the list (US SSN, Credit Card Number, Phone Number, and so on)
   b. Type the number of occurrences required to trigger the policy in the **Occurrences** field.
   c. Click the “+” to add additional compliance template(s)
      • Select the appropriate operator **And/Or**
      • Repeat the previous process by choosing **Expressions** and select one of the available expressions from the list.
      • Type the number of occurrences required to trigger the policy in the **Occurrences** field.
   d. If you select **Keywords**...
      • Choose one of the keywords from the list of available keywords.
      • Click the “+” to add additional compliance template(s)
- Select the appropriate operator **And/Or**
- Repeat the previous process by choosing **Keywords** and select one of the available keywords from the list.

9. After you finish adding your compliance template(s), click **Add**, then click **Save**. The **Data Protection: Edit Policy > Target** tab appears.

10. Click the Exceptions tab and add or edit any exceptions as required. See **Data Protection: Add Policy > Step 2: Exceptions** on page 7-5 for more information.

11. Click the **Action** tab and choose from the following:
   - **Block**
   - **Pass**
   - **Notify**
   - **Do not notify**

12. Click the **Notification** tab, and choose the appropriate settings. See **Data Protection: Add Policy > Specify Notification** on page 7-15 for more information.

13. Click **Save**.

**Edit a Data Protection Policy (MOSS 2007/WSS 3.0)**

This section describes the steps required to edit a Data Protection policy.
To edit a data protection policy:

1. On the left menu, click Data Protection > Policy. The Data Protection screen appears (Figure 7-1).

2. From the Data Protection screen, click the policy name link you want to edit. The Data Protection: Edit Policy screen appears (Figure 7-13).

3. Select or clear the Enable this policy checkbox to enable or disable the policy.

4. Select the compliance template(s) you want to add from the list of Available compliance templates and click Add >>. Remove compliance templates by first selecting and then clicking << Remove.

Figure 7-13. Data Protection: Edit Policy screen (target tab)
Note: Press and hold the Ctrl key to select multiple compliance templates.

Note: You can import a compliance template from a text file (.txt) clicking the Import button.

5. To add a compliance template to the list of available compliance templates:
   a. Click the Add button, which is located next to the Import button. The Add Compliance Template screen appears.
   b. Type a name for the new template in the Compliance template name field.
   c. Type an optional description for the new template in the Description field.

6. To define a compliance template, select from the following:
   a. If you select Expressions...
      • Choose an expression from the list (US SSN, Credit Card Number, Phone Number, and so on)
   b. Type the number of occurrences required to trigger the policy in the Occurrences field.
   c. Click the “+” to add additional compliance template(s)
      • Select the appropriate operator And/Or
      • Repeat the previous process by choosing Expressions and select one of the available expressions from the list.
      • Type the number of occurrences required to trigger the policy in the Occurrences field.
   d. If you select Keywords...
      • Choose one of the keywords from the list of available keywords.
      • Click the “+” to add additional compliance template(s)
      • Select the appropriate operator And/Or
      • Repeat the previous process by choosing Keywords and select one of the available keywords from the list.

7. After you finish adding your compliance template(s), click Add, then click Save. The Data Protection: Edit Policy > Target tab appears.
8. Click the **Action** tab and choose from the following:
   - Block
   - Pass
   - Notify
   - Do not notify

9. Click the **Notification** tab, and choose the appropriate settings. See *Data Protection: Add Policy > Specify Notification* on page 7-15 for more information.

10. Click **Save**.

### Data Protection Compliance Templates

This version of PortalProtect includes five (5) new compliance templates, which are disabled by default (see *Figure 7-14*). Compliance templates combine digital assets and operators like: AND, OR, in condition statements.

These templates include:

1. **GLBA**: Gram-Leach-Bliley financial services modernization act of 1999
2. **HIPAA**: Health Insurance Portability and Accountability Act
3. **PCI-DSS**: The Payment Card Industry Data and Security Standard
4. **SB-1386**: California law regulating the privacy of personal information
5. **US PII**: Personally identifiable information

You cannot change priority, add keywords, or add entities to these compliance templates. However, you can add exceptions, select an action, or update notification settings. For more information see *Configuring Data Protection Policies* on page 7-1.

### Adding and Configuring Data Protection Compliance Templates

This section describes the steps and settings required to add or edit a data protection compliance template.
Compliance Templates

<table>
<thead>
<tr>
<th>Compliance Template Name</th>
<th>Description</th>
<th>Policy Instances</th>
</tr>
</thead>
<tbody>
<tr>
<td>GLBA</td>
<td>Gramm-Leach-Bliley Financial Services Modernization Act of 1999</td>
<td>2</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Health Insurance Portability and Accountability Act</td>
<td>2</td>
</tr>
<tr>
<td>PCI-DSS</td>
<td>The Payment Card Industry Data Security Standard</td>
<td>2</td>
</tr>
<tr>
<td>SB-1306</td>
<td>California law regulating the privacy of personal information</td>
<td>2</td>
</tr>
<tr>
<td>US PII</td>
<td>Personally Identifiable Information</td>
<td>2</td>
</tr>
<tr>
<td>Source Code</td>
<td>Source Code</td>
<td>2</td>
</tr>
</tbody>
</table>

**FIGURE 7-14. Compliance Templates Main screen**

- **Add:** Click to add and configure a new compliance template
- **Copy:** Select the existing compliance template(s) you want to copy, and click **Copy**.
- **Delete:** Select the existing compliance template(s) you want to delete, and click **Delete**.

**Note:** You cannot delete a default template, or a template that has a policy associated with it.

- **Import:** Click to import a template from an external file.
- **Export:** Click to export a selected template(s) to an external file.
To add a new compliance template:

1. Click Data Protection > Compliance Templates. The Compliance Templates main screen appears.
2. Click Add. The Add Compliance Template screen appears.

![Add Compliance Template Screen](image)

**FIGURE 7-15.  Compliance Template > Edit Template**

a. Type a name for the new template in the Compliance template name field.
b. Type an optional description for the new template in the Description field.

3. To define a compliance template, select from the following:
   a. If you select Expressions...
      • Choose an expression from the list of available expressions (US SSN, Credit Card Number, Phone Number, and so on)
   b. Type the number of occurrences required to trigger the policy in the Occurrences field.
   c. Click the “+” to add additional data protection definition(s)
      • Select the appropriate operator And/Or
Repeat the previous process by choosing **Expressions** and select one of the available expressions from the list.

Type the number of occurrences required to trigger the policy in the **occurrences** field.

d. If you select **Keywords**...

• Choose one of the keywords from the list of available keywords.
• Click the “+” to add additional data protection definition(s)
• Select the appropriate operator **And/Or**
• Repeat the previous process by choosing **Keywords** and select one of the available keywords from the list.

4. After you finish adding your data protection definition(s), click **Save**. The **Data Protection: Compliance Templates** main screen appears.

### Copy or Delete an Existing Compliance Template

This section explains the steps required to copy or delete an existing compliance template.

**To copy or delete an existing compliance template:**

1. Click **Data Protection > Compliance Templates**. The **Compliance Templates** main screen appears.

2. Select the existing compliance template(s) you want to copy or delete.

3. Click **Copy** or **Delete** as appropriate.

---

**Note:** You cannot delete a default compliance template, or a template that has a policy associated with it. You must first remove it from the policy and then delete it.

---

### Import or Export a Compliance Template

This section explains the steps required to import or export a compliance template.

**To import or export compliance template:**

1. Click **Data Protection > Compliance Templates**. The **Compliance Templates** main screen appears.

2. **To import a compliance template...**
a. Click Import.

**WARNING!** If the templates you import already exist, they will be overwritten by the imported template.

b. Browse for the template you want to import, select it, and click Import.

3. To export an existing compliance template...
   a. Select the template(s) you want to export.
   b. Click Export, and save the files to the appropriate location.
Web Reputation

This version of PortalProtect uses Web Reputation technology to evaluate the integrity of URLs contained in both Web content and files in your SharePoint server.

Web threats encompass a broad array of threats that originate from the Internet. Web threats are sophisticated in their methods, using a combination of various files and techniques rather than a single file or approach. For example, Web threat creators constantly change the version or variant used. Because the Web threat is in a fixed location of a Web site rather than on an infected computer, the Web threat creator constantly modifies its code to avoid detection.

Web reputation blocks both files and Web content based on their reputation ratings. It queries the Trend Micro Smart Protection Network for these ratings.

Files and Web content that contain a URL that has been classified by Trend Micro as unsafe will be blocked. You can also customize and add to your own approved URL list. To enable this functionality, select Enable real-time Web Reputation for documents and Enable real-time Web Reputation for Web content from the Web Reputation page.
Local and Global Smart Protection

This version of PortalProtect provides two options for determining the reputation and safety of URLs; these options are: the Global Smart Protection Network, and the Local Smart Protection Server. The Global Smart Protection Network sends requests to the Trend Micro Smart Protection Network to examine the reputation of URLs. The Local Smart Protection Server sends these requests to your local smart protection server. The Local Smart Protection Server will provide more privacy and perhaps improve the processing speed.

The Local Smart Protection Server uses the Trend Micro Smart Protection Network, which is your private next-generation cloud-client content security infrastructure designed to protect your SharePoint environment from security risks and Web threats. Protection is automatically updated and strengthened as more products, services and users access the network, creating a real-time neighborhood watch protection service for those who use it. The smart scan solution uses the Smart Protection Network for in-the-cloud protection.
Choose a Web Reputation Source

To choose a Web reputation scan source:

1. Click Smart Protection > Scan Service Settings from the left menu. The Scan Service Settings screen appears.

2. Under Web Reputation, select from the following options:
   a. **Smart Protection Network**: scans URLs via proxy from the Global Smart Protection Network.
   b. Click the Administration Proxy link and refer to Configuring Global Proxy Settings on page 2-6 for information on how to configure the settings.
   c. **Smart Protection Server**: scans URLs using your private smart scan server.

---

**Note:** If your Local Smart Protection Server is unable to determine a URLs reputation, you have the option of allowing your system to query the Smart Protection Network. If you select the checkbox, **Do not make external queries to Smart Protection Network**, PP will only query the local smart scan server; if you clear the checkbox, PP can query the Smart Protection Network.
d. Click the **Smart Protection > Local Sources** link to configure the Smart Protection Server(s). Refer to *Smart Protection Source* on page 3-4 for instructions on how to configure this screen.

3. Click **Save**.

---

**Note:** Refer to *Alerts* on page 11-26 for information on configuring your alerts when your smart servers are unavailable and/or come back online.

---

**Enabling Real-time Web Reputation**

**To enable real-time Web reputation:**

1. Log on the product console.
2. Click **Web Reputation** from the main menu. The Web Reputation screen displays.
3. Select **Enable real-time Web Reputation**.
4. Click **Save**.
About Web Reputation: Target Settings

The following provides a brief description of the options available for the Web Reputation screen Target tab (see Figure 8-2):

- **Enable real-time Web Reputation for documents**: Select to enable this feature.
- **Enable real-time Web Reputation for Web content**: Select to enable this feature.
- **High**: Checks Web content for URLs that are verified threat sources, potentially unsafe, or source associated with spam.
- **Medium**: Checks Web content for URLs that are verified threat sources or sources determined to be potentially unsafe.
- **Low**: Checks Web content for URLs that are verified threat sources.
- **http://reclassify.wrs.trendmicro.com**: Click to open a new page to notify Trend Micro of an incorrectly classified URL. You can also use this portal to check the reputation of a Web site.
- **Enable approved URL list**: Select to use a custom list of approved URLs.
- **Enter approved URL**: Type a URL.

**Figure 8-2. Web Reputation target tab**
Tip: To save network bandwidth, Trend Micro recommends adding the enterprise internal Web sites to the Web reputation approved URL list.

- Add>>: Click to add the URL to the list.
- Delete: Click to remove a URL from the list.
- Import: Click to import a URL list.
- Export: Click to export the URL list.
- Approved URL: Click to sort in ascending or descending order.
- Save: Click to save all settings.
- Reset: Click to revert to default settings.

Configuring Web Reputation: Target Settings

The following lists the procedure required to configure Web reputation for the Target tab:

To configure Web reputation target settings:

1. Log on to the product console.
2. Click Web Reputation from the main menu. The Web Reputation screen displays (see Figure 8-2).
3. Select one of the following security levels:
   - High: Checks Web content for URLs that are verified threat sources, potentially unsafe, or associated with spam.
   - Medium: Checks Web content for URLs that are verified threat sources or potentially unsafe.
   - Low: Checks Web content for URLs that are verified threat sources.
4. Select Enable approved URL list to avoid scanning URLs deemed safe under your security policy.
5. Add approved URLs to the list.
6. Click Save.
About Web Reputation: Action Settings

The following provides a brief description for the options available on the Web Reputation Action tab (Figure 8-3):

- Enable real-time Web Reputation for documents: Select to enable this feature.
- Enable real-time Web Reputation for Web content: Select to enable this feature.
- Block
- Pass
- Notify
- Do not Notify

- Take action on URLs that have not been assessed by Trend Micro: Select to treat URLs that have not been classified as suspicious URLs and perform the specified action
- Save: Click to save your settings
- Reset: Click to revert to default settings
Configuring Web Reputation: Action Settings

The following lists the procedure required to configure Web reputation action settings.

**To configure Web reputation action settings:**

1. Log on to the product console.
2. Click **Web Reputation** from the main menu. The Web Reputation screen displays.
3. Click the **Action** tab.
4. Select an action.
5. Select **Take action on URLs that have not been assessed by Trend Micro** to apply a strict Web reputation policy.
6. Select **Notify** or **Do not notify**.
7. Click **Save**.

Web Reputation: Notifications

A brief description of the options available on this screen is available below.

- **Notify administrator**: Select to send a notification to the administrator.
- **Show details**: Click to view additional options.
- **SNMP**: Select to send notifications by SNMP.
- **Write to Windows event log**: Select to record the notification to a Windows event log.
- **Save**: Click to save your settings.
- **Reset**: Click to revert to default settings.

Smart Protection Network

The Smart Protection Network consists of Trend Micro maintained servers and in-the-client technologies that provide unique in-the-cloud correlation of Web and file reputation technologies, as well as threat databases. Protection is automatically updated and strengthened as more products, services and users access the network, creating a real-time neighborhood watch protection service for its users.
Manual Scan

You can run a manual scan at any time. If you try to run a manual scan when PortalProtect is running a scheduled scan, the manual scan takes priority (Figure 9-1).
Manual Scan

Last manual scan:  Not available
Scan status:  Not available

Database Selection

- All databases
- Specific databases:
  - root
  - Central Administration
  - SharePoint - 8080
  - SharePoint - 8888

Scan Type Selection

- Security risk scan
- File blocking
- Content filtering
  - Content filtering for document
  - Content filtering for Web content
- Data protection
  - Data protection for document
  - Data protection for Web content
- Web Reputation
  - Web reputation for document
  - Web reputation for Web content

Incremental Scan Options

- Scan files modified:
  - Last 1 weeks
  - From: 2011/6/26 06:00 to 2011/6/25 06:00

Time Zone: GMT-8:00

Scan Now

**FIGURE 9-1.** Manual Scan main screen
Configuring a Manual Scan

This section explains the steps required to configure a manual scan.

To configure and perform a manual scan:

1. On the left menu, click Manual Scan. The Manual Scan screen appears (see Figure 9-1).
2. Select from the following options under Database selection:
   • All databases: select to scan all databases
   • Specific databases: select to enable the option to choose the specific databases you want to scan
3. Select from the following options under Select the scan type:
   
   Note: Click the Security risk scan, File blocking, Content filtering, Data protection, or Web Reputation links to configure the manual scan options. For more information, refer to:

   - About Content Filtering Action Settings on page 6-2
   - Configure Manual Scan: Security Risk Scan on page 9-6
   - Configure Manual Scan: File Blocking on page 9-10
   - Configure Manual Scan: Content Filtering on page 9-14
   - Configure Manual Scan: Data Protection on page 9-20
   - Configure Manual Scan: Web Reputation on page 9-24

   • Security risk scan: select to perform a manual security risk scan
   • File blocking: select to perform a manual file blocking scan
   • Content filtering: select to perform a manual content filtering scan.
     i. Content filtering for document: select to scan documents according to the content filtering options and policies you choose. See Configuring Content Filtering on page 6-7 for more information.
     ii. Content filtering for Web content: select to scan Web content posted to SharePoint according to the content filtering options and policies you choose.
   • Data protection: select to perform a manual data protection scan.
i. **Data protection for document:** select to scan documents according to the data protection options and policies you choose.

ii. **Data protection for Web content:** select to scan Web content posted to SharePoint according to the data protection options and policies you choose.

- **Web Reputation:** select to perform a manual scan for Web Reputation.
  
  i. **Web reputation for document:** select to scan and block files containing URLs that are classified as unsafe. See [Web Reputation](#) on page 8-1 for more information.

  ii. **Web reputation for Web content:** select to scan Web content posted to your SharePoint server.

4. To scan files modified within a certain date range, select **Scan files modified** to enable the following **Incremental Scan Options**:

   - Select **Last**, and type a number in the entry field that corresponds to the **Hours**, **Days**, or **Weeks** you want to scan.

   - Select **From**, and choose a date, hours, and minutes that corresponds to the **From** and **To** query you want to scan.

5. Click **Scan Now**.

**Scan Compressed Files for Manual Scan**

The following explains the steps required to scan compressed files for manual scan:

**To scan compressed files for manual scan:**

1. On the left menu, click **Manual Scan**.

2. Under **Select the scan type**, click the **Security risk scan** link.

3. Select the **Target** tab. Under **Advanced Options**, expand the **Scan Restrictions Criteria**.

   **Note:** Select the checkbox for the items you want to scan and set the appropriate values.

4. Under **Do not scan file if...**

   - **File size exceeds**—type a value between 1-30-MB.
5. Select and type values for **Do not scan compressed files if**, according to the following:
   - **Decompressed file count exceeds [xxxx]**—type the total decompressed file count (1-10000) that should not be exceeded. When PortalProtect encounters a number of files equal to or greater than this number it will not scan the files.
   - **Size of Decompressed file exceeds [xxxx]**—type a value in megabytes (1-2048) to set a limit for the size of the compressed files PortalProtect will scan. When PortalProtect encounters a compressed file that is equal to or greater than this size, it will not scan the file.
   - **Number of layers of compression exceeds [xx]**—type a number (1-20) to set a limit for the number of layers of compression to which PortalProtect will scan. When PortalProtect encounters a file of a compression layer equal to or greater than this number it will not scan the files.
   - **Size of decompressed file is "x" times the size of compressed file**—decompressed files must not exceed the multiple entered according to the compressed file size. Type a multiple (100-1000000) that the decompressed file must not exceed. Decompressed files that exceed the value: decompressed size is "x" times larger than the compressed size, will not be scanned.

6. Click **Save**.

**Configure Macro Scanning Options for Manual Scan**

The following explains the steps required to configure macro scanning options for manual scan:

**To configure macro scanning options for manual scan:**

1. On the left menu, click **Manual Scan**.
2. Under **Select the scan type**, click the **Security risk scan** link and select the **Action** tab.
3. Under **Advanced Options**, click **Macros** to open the content.
4. Select, **Enable advanced macro scan**, to enable the functionality.
5. For **Heuristic level**, select an option according to the following:
   - 1 - Lenient filtering
   - 2 - Default filtering
• 3 - Sensitive filtering
• 4 - Rigorous filtering

OR....

6. Select **Delete all macros detected by advanced macro scan**.

7. Click **Save**.

**Configure Manual Scan: Security Risk Scan**

This section describes the steps required to configure the Security Risk Scan for Manual Scan.

**Step 1. Configure Manual Scan: Security Risk Scan (Target tab)**

1. On the left menu, click **Manual Scan**. The **Manual Scan** screen appears (see **Figure 9-1**).

2. As a pre-requisite, be sure to configure the options as described in **Configuring a Manual Scan** on page 9-3.
3. Under Select the scan type, click the Security risk scan link. The Manual Scan: Security Risk Scan screen appears (Figure 9-2).

**FIGURE 9-2.** Manual Scan: Security Risk Scan screen (Target tab)

4. Configure the settings for the Target tab as described in About Security Risk Scan Action Settings on page 4-6.
Step 2. Configure Manual Scan: Security Risk Scan (Action tab)

1. After completing the settings for the Target tab, click the Action tab. The Manual Scan: Security Risk Scan appears with the Action tab.

TABLE 9-1.   Available Actions for Manual Scan: Security Risk Scan

<table>
<thead>
<tr>
<th>Threat Type</th>
<th>Available Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>All threats</td>
<td>Clean, Quarantine, Delete, Pass or Rename</td>
</tr>
<tr>
<td>Viruses</td>
<td>Clean, Quarantine, Delete, Pass or Rename</td>
</tr>
<tr>
<td>Worms/Trojans</td>
<td>Quarantine, Delete, Pass or Rename</td>
</tr>
<tr>
<td>Packed files</td>
<td>Quarantine, Delete, Pass or Rename</td>
</tr>
<tr>
<td>Other malicious code</td>
<td>Clean, Quarantine, Delete, Pass, or Rename</td>
</tr>
<tr>
<td>Spyware/Grayware</td>
<td>Quarantine, Delete, Pass or Rename</td>
</tr>
<tr>
<td>Uncleanable files</td>
<td>Quarantine, Delete, Pass or Rename</td>
</tr>
</tbody>
</table>

Step 3.  Configure Manual Scan: Security Risk Scan (Notification tab)

1.  Click the **Manual Scan: Security Risk Scan > Notification** tab.
2.  Set up the notifications for this Manual Security Risk scan as described in *Security Risk Scan Notifications* on page 11-3.
3.  Click **Save**.
4.  Click **Scan Now**, to perform the a manual scan using the saved settings.
Configure Manual Scan: File Blocking

This section describes the steps required to configure File Blocking for Manual Scan.

To add/edit a manual scan file blocking policy:

1. On the left menu, click Manual Scan.
2. Under Select the scan type, click the File blocking link. The Manual Scan: File Blocking screen appears.
3. Click **Add** to create a new policy. The **Manual Scan: File Blocking: Add Policy** screen appears *(Figure 9-4).* Continue through the steps that follow to complete the configuration for this new policy.

**Manual Scan: File Blocking: Add Policy**

- **Step 1: Specify Rules**

  - **Block these files**

    - **Specific File Extensions**
      - Hide details
      - **Add**
      - **Delete**

    - **Specific File Extensions**
      - *Add:*
        - .exe
        - .dll
        - .bat
        - .bin
        - .cmd

    - **Attachment names to block**

    - **Block file types or names within compressed files**


1. Under **Block these files > Specific Files**, select from the following options to determine which files you want to block for this rule:
   - **File types**: select to choose all file types, or click **Show details** to choose specific file types. Refer to *Table 5-2. Application and executable file choices on page 5-12 through Table 5-7. Compressed file choices on page 5-17.*

2. To add or remove specific filenames or extensions, click **Show details** next to **File names** to expand the content.

3. **Add** or **Delete** files and/or file extensions as required.

4. Select **Block file type or names within compressed files** to perform that action.


**Step 2. Manual Scan: File Blocking: Add Policy > Specify sites to be excluded**

1. To exclude any sites and accounts as exceptions to this new policy, click **Add**. The **Manual Scan: File Blocking: Add Policy (Step 2.a: Specify sites to be excluded** screen appears.

2. Select from the following options:
   - **All sites**...OR...
   - **Specify a site’s URL**: type a specific URL and click **Search**, and/or select the sites from the tree.

3. Click **Next**. The **Manual Scan: File Blocking: Add Policy (Step 2.b: Specify accounts to be excluded** screen appears.

4. Select from the following options:
   - **Anyone**...OR...
   - **Specific accounts**: from the **Search for** drop down, select **AD user(s)/groups** or **SharePoint user(s)/group(s)**

5. Select **Users, Groups**, or select both check boxes. Then, type the name and click **Search**.

6. After the search completes, select the items you want to include from the **Available Account(s) window and click Add.**
7. Continue to search and add items as required, and when complete, click **Finish**. The Manual Scan: File Blocking: Add Policy Step 2: Exceptions screen appears and displays the new sites/accounts you just added.


1. Select an action from the following options:
   - Quarantine
   - Delete
   - Pass

2. Select from the following:
   - Notify
   - Do not notify


1. Under People to notify, select from the following:
   - Notify violator
   - Notify administrator

   **Note:** Refer to *File Blocking Notifications* on page 11-4 for more information about setting up notifications.


**Step 5. Manual Scan: File Blocking: Add Policy > Name and priority**

1. Select **Enable this policy** to activate it for the manual scan; clear to deactivate it.

2. Type a name for this new policy in the **Policy Name** field (required).

3. Type a description for the policy in the **Description** field.

4. Type a number to indicate the processing priority in the **Priority** field (required).
Note: You can view the existing policies and status at the bottom of the screen to assist making a choice for the priority.

5. Click Finish. The Manual Scan: File Blocking screen appears and shows the policy just created with the following information:
   - **Policy**: name
   - **Action**: Quarantine, Block, and so on
   - **Priority**: 1, 2, 3, and so on
   - **Status**: enabled (green checkmark) or disabled (red X); click to change the status as needed

Note: Click Import to import a policy from Real-time Scan: File Blocking.

Configure Manual Scan: Content Filtering

This section describes the steps required to configure Content Filtering for Manual Scan. This scan enables you to import rules from real-time scan for Content Filtering, however the actions performed between real-time and manual scan differ and will be imported as illustrated in Table 9-2.
### TABLE 9-2. Content Filtering Import Rule Mapping

<table>
<thead>
<tr>
<th>Scan Type</th>
<th>Action in Real-time Scan</th>
<th>Action in Manual or Scheduled Scan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Filtering for File</td>
<td>Block</td>
<td>Quarantine</td>
</tr>
<tr>
<td></td>
<td>Pass</td>
<td>Pass</td>
</tr>
<tr>
<td>Content Filtering for Web Content</td>
<td>Block</td>
<td>Pass</td>
</tr>
<tr>
<td></td>
<td>Pass</td>
<td>Pass</td>
</tr>
</tbody>
</table>

To import content filtering rules from real-time content filtering

1. On the left menu, click **Manual Scan**. The **Manual Scan** screen appears (see *Figure 9-1*).
2. Under **Select the scan type**, click the **Content filtering** link. The **Manual Scan**:
**Content Filtering** screen appears.

### Manual Scan: Content Filtering

![Content Filtering Table]

3. Click **Import**. The **Import from Real-time Content Filtering Policy** screen appears.
4. Select the policies you want to import, and click **Import**.

**To configure a Manual Scan: Content Filtering scan**

1. On the left menu, click **Manual Scan**. The **Manual Scan** screen appears (see **Figure 9-1**).

2. Under **Select the scan type**, select whether to perform content filtering for the following:
   - Content filtering for document
   - Content filtering for Web content
3. Click the **Content filtering** link. The **Manual Scan: Content Filtering** screen appears *(Figure 9-6)*.

![Figure 9-6. Manual Scan: Content Filtering screen](image)

**Note:** You can filter the policies according to the **Policy name**, whether **Enabled**, **Disabled**, or **All** (both enabled and disabled).

4. From the list, select the policies that you want to **Delete** or **Reorder**. Click an existing policy to edit it.

5. In the **Status** column, click the red X, or green checkmark to enable or disable an existing content filtering policy for manual scan.

6. Select an existing policy and configure the following options:
   - **Enable this policy**: select to activate the policy
• **Policy name:** type the policy name
• **Description:** add a description to further describe the policy

7. Configure the **Target** tab settings as described in *Adding a Content Filtering Policy (MOSS 2010/WSS 4.0)* on page 6-9 or *Adding a Content Filtering Policy (MOSS 2007/WSS 3.0)* on page 6-18.

8. Click the **Exceptions** tab.

9. Click **Add** to create a new exception, or click an existing exception. The **Specify sites** screen appears.

10. Choose from the following options:
   - **All sites:** excludes all sites from this policy
   - **Specify a site’s URL:** choose the specific site(s) to exclude from this policy

11. Click **Next >**. The **Select Accounts** to be excluded screen appears.

12. Select from the following options:
   - **Anyone:** to exclude all accounts. Select, click Finish and proceed to...
   - **Specific accounts:** select to choose the specific accounts to exclude and proceed to the next step.

13. Type an AD user or group name in the **Search for AD user(s)/group(s)** field.

14. Next to **Search in,** select **Users** and/or **Groups** as appropriate.

15. Click **Search.** Successful search results will then display in the **Available Account(s)** window.

16. Repeat the search as required.

17. Select all the users/groups you want to add to exclude and click **Add** to move them to the Selected Account(s) window.

18. Click **Finish.** The **Manual Scan: Content Filtering: Edit Policy > Exceptions** screen appears.

19. Click the **Action** tab, and select an action for the content filtering policy from the following options:
   - **Quarantine, Delete, or Pass**
   - **Notify or Do not notify**

20. Click the **Notification** tab, and configure as described in *Manual Scan Notifications—Content Filtering* on page 11-13.

21. Click **Save.**
Configure Manual Scan: Data Protection

This section describes the steps required to configure Data Protection for Manual Scan. This scan enables you to import rules from real-time scan for Data Protection, however the actions performed between real-time and manual scan differ and will be imported as illustrated in Table 9-3.

### Table 9-3. Data Protection Import Rule Mapping

<table>
<thead>
<tr>
<th>Scan Type</th>
<th>Action in Real-time Scan</th>
<th>Action in Manual or Scheduled Scan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Protection for File</td>
<td>Block</td>
<td>Quarantine</td>
</tr>
<tr>
<td></td>
<td>Pass</td>
<td>Pass</td>
</tr>
<tr>
<td>Data Protection for Web Content</td>
<td>Block</td>
<td>Pass</td>
</tr>
<tr>
<td></td>
<td>Pass</td>
<td>Pass</td>
</tr>
</tbody>
</table>

To import data protection rules from real-time data protection

1. On the left menu, click Manual Scan. The Manual Scan screen appears (see Figure 9-1).
2. Under Select the scan type, click the Data protection link. The Manual Scan: Data Protection screen appears.
3. Click **Import**. The **Import from Real-time Data Protection Policy** screen appears.

![Import from Real-time Data Protection Policy screen](image)

**FIGURE 9-7. Import from Real-time Data Protection Policy screen**

4. Select the policies you want to import, and click **Import**.

**To configure a Manual Scan: Data Protection scan**

1. On the left menu, click **Manual Scan**. The **Manual Scan** screen appears (see *Figure 9-1*).

2. Under **Scan Type Selection**, select whether to perform content filtering for the following:
   - Data protection for document
   - Data protection for Web content
3. Click the **Data protection** link. The **Manual Scan: Data Protection** screen appears (**Figure 9-8**).

![Manual Scan: Data Protection screen](image)

**Figure 9-8. Manual Scan: Data Protection screen**

**Note:** You can filter the policies according to the **Policy name**, whether **Enabled**, **Disabled**, or **All** (both enabled and disabled).

4. From the list, select the policies that you want to **Delete** or **Reorder**. Click an existing policy to edit it.

5. In the **Status** column, click the red X, or green checkmark to enable or disable an existing data los prevention policy for manual scan.

6. Select an existing policy and configure the following options:
   - **Enable this policy**: select to activate the policy
   - **Policy name**: type the policy name
   - **Description**: add a description to further describe the policy

7. Configure the **Target** tab settings as described in *Adding a Data Protection Policy (MOSS 2010/WSS 4.0)* on page 7-2 or *Adding a Data Protection Policy (MOSS 2007/WSS 3.0)* on page 7-12.

8. Click the **Exceptions** tab.
9. Click **Add** to create a new exception, or click an existing exception. The **Specify sites** screen appears.

10. Choose from the following options:
    - **All sites**: excludes all sites from this policy
    - **Specify a site’s URL**: choose the specific site(s) to exclude from this policy

11. Click **Next >**. The **Select Accounts** to be excluded screen appears.

12. Select from the following options:
    - **Anyone**: to exclude all accounts. Select, click Finish and proceed to...
    - **Specific accounts**: select to choose the specific accounts to exclude and proceed to the next step.

13. Type an AD user or group name in the **Search for AD user(s)/group(s)** field.

14. Next to **Search in**, select **Users** and/or **Groups** as appropriate.

15. Click **Search**. Successful search results will then display in the **Available Account(s)** window.

16. Repeat the search as required.

17. Select all the users/groups you want to add to exclude and click **Add** to move them to the Selected Account(s) window.

18. Click **Finish**. The **Manual Scan: Data Protection: Edit Policy > Exceptions** screen appears.

19. Click the **Action** tab, and select an action for the content filtering policy from the following options:
    - **Quarantine, Delete, or Pass**
    - **Notify** or **Do not notify**

20. Click the **Notification** tab, and configure.

21. Click **Save**.
Configure Manual Scan: Web Reputation

This section describes the steps required to configure Web Reputation for Manual Scan.

To configure a Manual Scan: Web Reputation scan

1. On the left menu, click Manual Scan. The Manual Scan screen appears (see Figure 9-1).
2. As a pre-requisite, be sure to configure the options as described in Configuring a Manual Scan on page 9-3.
4. Refer to Smart Protection Source on page 3-4, Web Reputation on page 8-1, and Choose a Web Reputation Source on page 8-3 for more information about configuring Web Reputation settings.
5. After completing your settings, click Save. The Manual Scan screen appears.
6. Click Scan Now to perform the manual scan with the new settings.
Scheduled Scan

Scheduled scans automate routine antivirus maintenance procedures and improve the efficiency and control over security policies. Scheduled scans run according to the interval and time you set. At the configured time, scheduled scans automatically check for infected files on the SharePoint server(s). When you enable scheduled scans, all scans will run according to the schedule you set. You can disable any scheduled scan by clicking the green checkmark in the Scheduled Scan, Status column. When clicked, the green checkmark turns to a red X.
Configuring a Scheduled Scan

This section explains the steps required to configure a scheduled scan.

To enable or disable a scheduled scan:

1. On the left menu, click Scheduled Scan, to display the Scheduled Scan screen.
2. In the Status column, click the green checkmark to disable the scan; a red "X" then appears. (See Figure 10-9 and Figure 10-10).

Note: Disabling the scan does not affect your configuration. When you decide to resume scheduled scanning, simply enable the scan again.

Add or Edit a Scheduled Scan Task

This section explains the steps required to add or edit a scheduled scan task.

To add a scheduled scan task:

1. On the left menu, click Scheduled Scan, to display the Scheduled Scan screen.
2. Click Add on the Scheduled Scan toolbar. The Scheduled Scan: Add Scan Task screen appears (Figure 10-11).
3. In the **Scan task name** field, type a name for the new scan task.
4. Under **Schedule**, select a scan schedule from the following options:
• **Daily—at (hh:mm)**: select to perform a scan every day at the hour and minute you choose

• **Weekly, every—[day of week] at (hh:mm)**: select to perform a scan every week on the day, hour and minute you choose

• **Monthly, on date—[day of month] at (hh:mm)**: select to perform a scan every month on the day, hour and minute you choose

5. Under **Database selection**, select one of the following options:

   • **All databases**: includes databases added after you configure this setting

   • **Specific databases**: expand and choose which databases to scan from those listed in the window

6. Select from the following options under **Select the scan type**:

   **Note:** Click the **Security risk scan**, **File blocking**, **Content filtering**, **Data protection**, or **Web Reputation** links to configure the scheduled scan options. For more information, refer to:

   - *Configure Scheduled Scan: Security Risk Scan* on page 10-6
   - *Configure Scheduled Scan: File Blocking Scan* on page 10-8
   - *Configure Scheduled Scan: Content Filtering* on page 10-11
   - *Configure Scheduled Scan: Data Protection* on page 10-13
   - *Configure Scheduled Scan: Web Reputation* on page 10-15

   • **Security risk scan**: select to perform a scheduled security risk scan

   • **File blocking**: select to perform a scheduled file blocking scan

   • **Content filtering**: select to perform a scheduled content filtering scan. Select or clear **Content filtering for document** or **Content filtering for Web content** as required

   • **Data protection**: select to perform a scheduled data protection scan. Select or clear **Data protection for document** or **Data protection for Web content** as required

   • **Web Reputation**: select to perform a manual scan for Web Reputation

7. To scan files modified within a certain date range, select **Scan files modified** to enable the following **Incremental Scan Options**:
• Select Last, and type a number in the entry field that corresponds to the Hours, Days, or Weeks you want to scan.

8. Click Save.

Configure Macro Scanning Options for Scheduled Scan

The following explains the steps required to configure macro scanning options for scheduled scan:

To configure macro scanning options for scheduled scan:

1. On the left menu, click Scheduled Scan.
2. Click Add, to create a new scheduled scan, or click the Task Name to edit an existing one.
3. Under Select scan type, click the Security risk scan link and select the Action tab.
4. Under Advanced Options, click Macros to open the content.
5. Select, Enable advanced macro scan, to enable the functionality.
6. For Heuristic level, select an option according to the following:
   • 1 - Lenient filtering
   • 2 - Default filtering
   • 3 - Sensitive filtering
   • 4 - Rigorous filtering
   OR....
7. Select Delete all macros detected by advanced macro scan.
8. Click Save.

Scan Compressed Files for Scheduled Scan

The following explains the steps required to scan compressed files for scheduled scan:

To scan compressed files for scheduled scan:

1. On the left menu, click Scheduled Scan.
2. Click Add, to create a new scheduled scan, or click the Task Name to edit an existing one.
3. Under **Select scan type**, click the **Security risk scan** link.

4. Select the **Target** tab. Under **Advanced Options**, expand the **Scan Restrictions Criteria**.

   **Note:** Select the checkbox for the items you want to scan and set the appropriate values.

5. Under **Do not scan file if**...
   - **File size exceeds**—type a value between 1-30-MB.

6. Select and type values for **Do not scan compressed files if**, according to the following:
   - **Decompressed file count exceeds [xxxx]**—type the total decompressed file count (1-10000) that should not be exceeded. When PortalProtect encounters a number of files equal to or greater than this number it will not scan the files.
   - **Size of Decompressed file exceeds [xxxx]**—type a value in megabytes (1-2048) to set a limit for the size of the compressed files PortalProtect will scan. When PortalProtect encounters a compressed file that is equal to or greater than this size, it will not scan the file.
   - **Number of layers of compression exceeds [xx]**—type a number (1-20) to set a limit for the number of layers of compression to which PortalProtect will scan. When PortalProtect encounters a file of a compression layer equal to or greater than this number it will not scan the files.
   - **Size of decompressed file is "x" times the size of compressed file**—decompressed files must not exceed the multiple entered according to the compressed file size. Type a multiple (100-1000000) that the decompressed file must not exceed. Decompressed files that exceed the value: decompressed size is "x" times larger than the compressed size, will not be scanned.

7. Click **Save**.

### Configure Scheduled Scan: Security Risk Scan

This section describes the steps required to configure the Security Risk Scan task for Scheduled Scan.
To add a scheduled scan task for security risk scan

1. On the left menu, click Scheduled Scan. The Scheduled Scan screen appears (Figure 10-12).

   ![Scheduled Scan](image)

   **Figure 10-12. Scheduled Scan main screen**

   **Note:** As a pre-requisite, be sure to configure the options as described in Configuring a Scheduled Scan on page 10-2.

2. Click Add. The Scheduled Scan: Add Scan Task screen appears (see Figure 10-11. Scheduled Scan: Add Scan Task screen on page 10-3).

3. Type a new name in the Scan task name field.

4. Under Select the scan type, click the Security risk scan link. The Scheduled Scan: Security Risk Scan screen appears.

**Step 1. Scheduled Scan: Security Risk Scan (Target tab)**

1. Configure the settings for the Target tab as described in About Security Risk Scan Action Settings on page 4-6.

**Step 2. Configure Scheduled Scan: Security Risk Scan (Action tab)**

1. After completing the settings for the Target tab, click the Action tab. The Scheduled Scan: Security Risk Scan screen appears with the Action tab.


3. Configure the Advanced Options as required. See Configure Macro Scanning Options for Scheduled Scan on page 10-5 for more information.

4. Configure the Unscannable Files settings as required. See About Unscannable Files on page 1-26 for more information.
Step 3. Configure Scheduled Scan: Security Risk Scan (Notification tab)

1. Click the Scheduled Scan: Security Risk Scan > Notification tab.
2. Configure the Notification settings as required.

   **Note:** Refer to Scheduled Scan Notifications—Security Risk Scan on page 11-18 for details on how to configure notifications for this scan.

3. Click Save. The Scheduled Scan: Add Scan Task screen appears.
4. Click Save again. The newly created task appears in the Scheduled Scan task list.

Configure Scheduled Scan: File Blocking Scan

This section describes the steps required to configure a File Blocking Scan task for Scheduled Scan.

**To add a scheduled scan task for file blocking**

1. On the left menu, click Scheduled Scan. The Scheduled Scan screen appears (Figure 10-12).

   ![Scheduled Scan main screen](image)

   **FIGURE 10-13. Scheduled Scan main screen**

   **Note:** As a pre-requisite, be sure to configure the options as described in Configuring a Scheduled Scan on page 10-2.

2. Click Add. The Scheduled Scan: Add Scan Task screen appears (see Figure 10-11. Scheduled Scan: Add Scan Task screen on page 10-3).
3. Type a new name in the Scan task name field.
4. Under **Select the scan type**, click the **File Blocking** link. The **Scheduled Scan: File Blocking** screen appears.

5. From the **Scheduled Scan: File Blocking** screen, click **Add**. The **Scheduled Scan: File Blocking: Add Policy** screen appears. Continue through the steps that follow to complete the configuration for this new policy.

**Step 1. Scheduled Scan: File Blocking: Add Policy > Specify Rules**

1. Under **Block these files > Specific Files**, select from the following options to determine which files you want to block for this rule:
   - **File types**: select to choose all file types, or click **Show details** to choose specific file types. Refer to Table 5-2. Application and executable file choices on page 5-12 through Table 5-7. Compressed file choices on page 5-17.

2. To add or remove specific filenames or extensions, click **Show details** next to **File names** to expand the content.

3. **Add** or **Delete** files and/or file extensions as required.

4. Select **Block file type or names within compressed files** to perform that action.

5. Click **Next >**. The **Scheduled Scan: File Blocking: Add Policy > Step 2: Exceptions** screen appears.

**Step 2. Scheduled Scan: File Blocking: Add Policy > Exceptions**

1. To exclude any sites and accounts as exceptions to this new policy, click **Add**. The **Scheduled Scan: File Blocking: Add Policy (Step 2.a: Specify sites to be excluded)** screen appears.

2. Select from the following options:
   - **All sites...OR...**
   - **Specify a site’s URL**: type a specific URL and click **Search**, and/or select the sites from the tree.

3. Click **Next >**. The **Scheduled Scan: File Blocking: Add Policy (Step 2.b: Specify accounts to be excluded)** screen appears.

4. Select from the following options:
   - **Anyone...OR...**
   - **Specific accounts**: from the **Search for** drop down, select **AD user(s)/groups** or **SharePoint user(s)/group(s)**
5. Select Users, Groups, or select both check boxes. Then, type the name and click Search.

6. After the search completes, select the items you want to include from the Available Account(s) window and click Add.

7. Continue to search and add items as required, and when complete, click Finish. The Scheduled Scan: File Blocking: Add Policy Step 2: Exceptions screen appears and displays the new sites/accounts you just added.


1. Select an action from the following options:
   • Quarantine
   • Delete
   • Pass

2. Select from the following:
   • Notify
   • Do not notify


1. Under People to notify, select from the following:
   • Notify violator
   • Notify administrator

   **Note:** Refer to Manual Scan Notifications—File Blocking on page 11-11 for details on setting notifications for this scan.

Step 5. Scheduled Scan: File Blocking: Add Policy > Name and priority

1. Select Enable this policy to activate it for the manual scan; clear to deactivate it.
2. Type a name for this new policy in the Policy Name field (required).
3. Type a description for the policy in the Description field.
4. Type a number to indicate the processing priority in the Priority field (required).

Note: You can view the existing policies and status at the bottom of the screen to assist making a choice for the priority.

5. Click Finish. The Scheduled Scan: File Blocking screen appears and shows the policy just created with the following information:
   • Policy: name
   • Action: Quarantine, Block, and so forth
   • Priority: 1, 2, 3, and so on
   • Status: enabled (green checkmark) or disabled (red X); click to change the status as needed

Note: Click Import to import a policy from Real-time Scan: File Blocking.

Configure Scheduled Scan: Content Filtering

This section describes the steps required to configure Content Filtering for Scheduled Scan.

For detailed background information on how to configure content filtering, refer to:
   • Content Filtering on page 6-1
   • About Content Filtering Action Settings on page 6-2
   • Content Filtering Policies on page 6-3
   • Configuring Content Filtering on page 6-7

To configure a new Scheduled Scan task: Content Filtering scan

1. On the left menu, click Scheduled Scan. The Scheduled Scan screen appears.
2. Click Add. The Scheduled Scan: Add Scan Task screen appears.
3. Type a new task name in the **Scan task name** field.

   **Note:** As a pre-requisite, be sure to configure the options as described in *Configuring a Scheduled Scan* on page 10-2.

4. Under **Select the scan type**, select whether to perform content filtering for the following:
   - Content filtering for document
   - Content filtering for Web content

5. Click the **Content filtering** link. The **Scheduled Scan: Content Filtering** screen appears.

6. Click **Add** to create a new policy. The **Scheduled Scan: Content Filtering: Add Policy > Step 1: Specify Rules** screen appears.

**Step 1. Scheduled Scan: Content Filtering: Add Policy > Step 1: Specify Rules**

1. Add keywords and synonyms as described in *Adding a Content Filtering Policy (MOSS 2010/WSS 4.0)* on page 6-9.

2. Click **Next**. The **Scheduled Scan: Content Filtering: Add Policy** screen appears.

**Step 2. Scheduled Scan: Content Filtering: Add Policy > Specify Sites to be Excluded**

1. Refer to *Content Filtering: Add Policy > Step 2: Exceptions* on page 6-11 for details on how to configure this screen.

2. After completing any exceptions, click **Next**. The **Scheduled Scan: Content Filtering: Add Policy > Step 3: Specify Action** screen appears.

**Step 3. Scheduled Scan: Content Filtering: Add Policy > Specify Action**

1. Select action and notification options. See *Content Filtering: Add Policy > Specify Action* on page 6-14) for details on how to configure this screen.

2. Click **Next** (The **Scheduled Scan: Content Filtering: Add Policy > Step 4: Specify Notification** screen appears.)
Step 4. Scheduled Scan: Content Filtering: Add Policy > Specify Notification

1. Select from the available options. See Content Filtering: Add Policy > Specify Notification on page 6-15 for details on how to configure this screen.

2. Click Next>. The Scheduled Scan: Content Filtering: Add Policy > Step 5: Name and Priority screen appears.

Step 5. Scheduled Scan: Content Filtering: Add Policy > Name and Priority

1. Configure the available options. See Content Filtering: Add Policy > Name and Priority on page 6-17 for details on how to configure this screen.

2. Click Finish. The Scheduled Scan: Content Filtering screen appears with the new policy you just created.

3. Click Save.

Configure Scheduled Scan: Data Protection

This section describes the steps required to configure Data Protection for Scheduled Scan.

For detailed background information on how to configure data protection, refer to:

• Data Protection on page 7-1
• Configuring Data Protection Policies on page 7-1
• Data Protection Compliance Templates on page 7-23

To configure a new Scheduled Scan task: Data protection scan

1. On the left menu, click Scheduled Scan. The Scheduled Scan screen appears.

2. Click Add. The Scheduled Scan: Add Scan Task screen appears.

3. Type a new task name in the Scan task name field.

Note: As a pre-requisite, be sure to configure the options as described in Configuring a Scheduled Scan on page 10-2.

4. Under Select the scan type, select whether to perform data protection for the following:
• Data protection for document
• Data protection for Web content

5. Click the Data protection link. The Scheduled Scan: Data Protection screen appears.

6. Click Add to create a new policy. The Scheduled Scan: Data Protection: Add Policy > Step 1: Specify Rules screen appears.

Step 1. Scheduled Scan: Data Protection: Add Policy > Step 1: Specify Rules
1. Configure as described in Adding a Data Protection Policy (MOSS 2010/WSS 4.0) on page 7-2.
2. Click Next>. The Scheduled Scan: Data Protection: Add Policy screen appears.

Step 2. Scheduled Scan: Data Protection: Add Policy > Specify Sites to be Excluded
1. Refer to Data Protection: Add Policy > Step 2: Exceptions on page 7-5 for details on how to configure this screen.

Step 3. Scheduled Scan: Data Protection: Add Policy > Specify Action
1. Select action and notification options. See Data Protection: Add Policy > Specify Action on page 7-8) for details on how to configure this screen.

Step 4. Scheduled Scan: Data Protection: Add Policy > Specify Notification
1. Select from the available options. See Data Protection: Add Policy > Specify Notification on page 7-9 for details on how to configure this screen.
2. Click Next>. The Scheduled Scan: Data Protection: Add Policy > Step 5: Name and Priority screen appears.
Step 5. Scheduled Scan: Data Protection: Add Policy > Name and Priority

1. Configure the available options. See Data Protection: Add Policy > Name and Priority on page 7-11 for details on how to configure this screen.

2. Click Finish. The Scheduled Scan: Data Protection screen appears with the new policy you just created.

3. Click Save.

Configure Scheduled Scan: Web Reputation

This section describes the steps required to configure Web Reputation for Scheduled Scan. New functionality for Web Reputation in this release enables scanning for URLs in files. For detailed background information on how to configure Web Reputation, refer to:

- Web Reputation on page 8-1
- Local and Global Smart Protection on page 8-2
- Smart Protection Network on page 8-8

To configure a Scheduled Scan for Web Reputation

1. On the left menu, click Scheduled Scan. The Scheduled Scan screen appears.

2. As a pre-requisite, be sure to configure the options as described in Configuring a Scheduled Scan on page 10-2.

3. Under Select the scan type, click the Web Reputation link. The Scheduled Scan: Web Reputation screen appears.

4. Refer to Web Reputation on page 8-1 and the procedures that follow it for more information about configuring Web Reputation settings.

5. After completing your settings, click Save. The Scheduled Scan screen appears.

6. Click Save again.
Chapter 11

Notifications, Alerts, Logs, and Reports

This chapter discusses PortalProtect Notifications, Alerts, Logs, and Reports. Configure the type of notification and the method to send the notification. Configure system events to provide an alert in the event of an outbreak. View logs to understand what PortalProtect events occur. Logs are an important source of information that you can use for troubleshooting. Use daily, weekly, or monthly reports to share information about the security of your SharePoint environment.

Make notifications part of your proactive security strategy to predict attacks and assess risks. Make logs part of your reactive security strategy to assess and try to determine the causes of the damage. Use both notification and logs to identify vulnerabilities in your SharePoint environment and send reports to share information to other security team members.

In this chapter, you will find information about:

• Configuring Notifications starting on page 11-2
• Alerts starting on page 11-26
• About Access Control on page 11-32
• Working with Logs starting on page 11-34
• Viewing and Generating Reports starting on page 11-47
Configuring Notifications

Notifications may be sent to the administrator(s) or other specified recipients. With PortalProtect, you can configure notifications through email, Simple Network Management Protocol (SNMP) Trap, or the Windows Event Log. Setting Global notifications apply to all notifications. You can also make unique settings for each notification type, which include:

- **Security Risk Scan Notifications** on page 11-3
- **File Blocking Notifications** on page 11-4
- **Content Filtering Notifications** on page 11-6
- **Data Protection Notifications** on page 11-7
- **Web Reputation Notifications** on page 11-8
- **Manual Scan Notifications—Security Risk Scan** on page 11-10
- **Manual Scan Notifications—File Blocking** on page 11-11
- **Manual Scan Notifications—Content Filtering** on page 11-13
- **Manual Scan Notifications—Data Protection** on page 11-14
- **Manual Scan Notifications—Web Reputation** on page 11-16
- **Scheduled Scan Notifications—Security Risk Scan** on page 11-18
- **Scheduled Scan Notifications—File Blocking** starting on page 11-19
- **Scheduled Scan Notifications—Content Filtering** on page 11-21
- **Scheduled Scan Notifications—Data Protection** on page 11-23
- **Scheduled Scan Notifications—Web Reputation** starting on page 11-25

Global Notification Settings

You can also create global notification list under **Administration > Notification Settings**. If you add contact information in this area, and click **Apply All**, the email addresses will be applied to each of the unique notifications for Security Risk Scan, File Blocking, Manual Scan, Scheduled Scan, Content Filtering, Web Reputation, and Data Protection.
To configure global notification settings:

1. From the left menu, click **Administration > Notification Settings**.
2. Under **Administrator Notification**, type the email address for the administrator(s) you wish to receive all notifications. Separate multiple addresses using a semicolon (;). Click **Apply All**, to update the new settings.
3. Under **Sender Settings**, type the email address of the sender who sends alerts and notifications (for example: PortalProtect_Administrator@do.not.reply).
4. Under **Email Account Settings**, type the SMTP server settings that PortalProtect will use to send email-based notifications for the following:
   - **Display name**: unique identifier, for example: PortalProtect Notification
   - **SMTP Server**
   - **Port**
5. Under **SNMP**, type the following:
   - **IP address**
   - **Community**
6. Click **Save**.

**Event Notifications**

PortalProtect provides various options for sending unique event notifications for: Security Risk Scan, File Blocking, Content Filtering, Web Reputation, and Data Protection.

**Security Risk Scan Notifications**

The following explains the steps required to configure security risk scan notifications:

**To configure security risk scan notifications:**

1. On the left menu, click **Security Risk Scan**. The **Security Risk Scan** screen appears.
2. Click the **Notification** tab.
3. Under **People to notify**, select **Notify administrator** to enable security risk scan notifications.
4. Under **People to notify**, click **Show details** and configure the following:
• **To**—the global email address(es) appear in this field. You can enter additional email addresses, separated by a semicolon, to create unique notifications.

• **Subject**—type a subject that will appear in the subject line of the email (for example: Security Risk Scan Notification).

• **Message**—you can create a unique message using variables like: [Server Name], [Security Risk Name], [Date], [Time], [File Name], [File Location], [Action], and [Violator].

  **Note:** The available variables appear in the left window, and the message body in the right window.

5. Under **Settings**, choose the delivery options for this notification according to the following:

   • **Send consolidated notifications every [xx] [hours or days]**—select this option to send a notification according to the number of hours or days you type in the variable field.

   • **Send consolidate notifications every [xx] occurrences**—select this option to send a notification after a certain number of occurrences as you stipulate in the variable field.

   • **Send individual notifications**—select this option to send a notification each time an event occurs.

6. Under **Advanced Notification** (SNMP), select **SNMP** to enable this option.

7. Click **Show details** to expand the options, and configure according to the following:

   • **IP Address**

   • **Community**

   • **Message**—create a message as stated in Step 4 of this procedure.

8. Select **Write to Windows event log** to write each notification to the Windows event log.

9. Click **Save**.

**File Blocking Notifications**

The following explains the steps required to configure file blocking notifications:

11-4
To configure file blocking notifications:

1. On the left menu, click **File Blocking**. The **File Blocking** screen appears.

   **Note:** For MOSS 2007/WSS 3 continue the steps. For MOSS 2010/WSS 4, click an existing policy and continue the steps. To add a new policy, see **File Blocking** starting on page 5-1.

2. Click the **Notification** tab.
3. Under **People to notify**, select **Notify administrator** to enable file blocking notifications.
4. Under **People to notify**, click **Show details** and configure the following:
   - **To**—the global email address(es) appear in this field. You can enter additional email addresses, separated by a semicolon (;) to create unique notifications.
   - **Subject**—type a subject that will appear in the subject line of the email (for example: File Blocking Notification).
   - **Message**—you can create a unique message using variables like: [Server Name], [File Blocking Rules], [Date], [Time], [File Name], [File Location] [Action], and [Violator].

   **Note:** The available variables appear in the left window, and the message body in the right window.

5. Under **Settings**, choose the delivery options for this notification according to the following:
   - **Send consolidated notifications every [xx] [hours or days]**—select this option to send a notification according to the number of hours or days you type in the variable field.
   - **Send consolidate notifications every [xx] occurrences**—select this option to send a notification after a certain number of occurrences as you stipulate in the variable field.
   - **Send individual notifications**—select this option to send a notification each time an event occurs.

6. Under **Advanced Notification** (SNMP), select **SNMP** to enable this option.
7. Click Show details to expand the options, and configure according to the following:
   • IP Address
   • Community
   • Message
8. Select **Write to Windows event log** to write each notification to the Windows event log.
9. Click **Save**.

**Content Filtering Notifications**

The following explains the steps required to configure content filtering notifications:

**To configure content filtering notifications:**

1. On the left menu, click **Content Filtering**. The **Content Filtering** screen appears.
2. Click **Add**, to add a new policy, or click an existing policy from the **Policy** column. The **Content Filtering: Edit Policy** screen appears.
3. Click the **Notification** tab.
4. Under **People to notify**, select **Notify administrator** to enable content filtering notifications.
5. Under **People to notify**, click **Show details** and configure the following:
   • **To**—the global email address(es) appear in this field. You can enter additional email addresses, separated by a semicolon (;) to create unique notifications.
   • **Subject**—type a subject that will appear in the subject line of the email (for example: Content Filtering Notification).
   • **Message**—you can create a unique message using variables like: [Server Name], [Content Rules], [Date], [Time], [File Name/Web Content Title], [File/Web Content Location], [Action], and [Violator].

---

**Note:** The available variables appear in the left window, and the message body in the right window.

6. Under **Settings**, choose the delivery options for this notification according to the following:
• **Send consolidated notifications every [xx] hours or days**—select this option to send a notification according to the number of hours or days you type in the variable field.

• **Send consolidated notifications every [xx] occurrences**—select this option to send a notification after a certain number of occurrences as you stipulate in the variable field.

• **Send individual notifications**—select this option to send a notification each time an event occurs.

7. Under **Advanced Notification** (SNMP), select **SNMP** to enable this option.

8. Click Show details to expand the options, and configure according to the following:
   - **IP Address**
   - **Community**
   - **Message**

9. Select **Write to Windows event log** to write each notification to the Windows event log.

10. Click **Save**.

### Data Protection Notifications

The following explains the steps required to configure data protection notifications:

**To configure data protection notifications:**

1. On the left menu, click **Data Protection > Policies**. The **Data Protection** screen appears.

2. Click **Add**, to add a new policy, or click an existing policy from the **Policy** column. The **Data Protection: Edit Policy** screen appears.

3. Click the **Notification** tab.

4. Under **People to notify**, select **Notify administrator** to enable data protection notifications.

5. Under **People to notify**, click **Show details** and configure the following:
   - **To**—the global email address(es) appear in this field. You can enter additional email addresses, separated by a semicolon (;) to create unique notifications.
   - **Subject**—type a subject that will appear in the subject line of the email (for example: Data Protection Notification).
• **Message**—you can create a unique message using variables like: [Server Name], [Data Protection Rules], [Date], [Time], [File Name/Web Content Title], [File/Web Content Location], [Action], and [Violator].

**Note:** The available variables appear in the left window, and the message body in the right window.

6. Under **Settings**, choose the delivery options for this notification according to the following:
   • **Send consolidated notifications every [xx] [hours or days]**—select this option to send a notification according to the number of hours or days you type in the variable field.
   • **Send consolidate notifications every [xx] occurrences**—select this option to send a notification after a certain number of occurrences as you stipulate in the variable field.
   • **Send individual notifications**—select this option to send a notification each time an event occurs.

7. Under **Advanced Notification** (SNMP), select **SNMP** to enable this option.

8. Click **Show details** to expand the options, and configure according to the following:
   • **IP Address**
   • **Community**
   • **Message**

9. Select **Write to Windows event log** to write each notification to the Windows event log.

10. Click **Save**.

**Web Reputation Notifications**

The following explains the steps required to configure Web Reputation notifications:

**To configure Web reputation notifications:**

1. On the left menu, click **Web Reputation**. The **Web Reputation** screen appears.
2. Click the **Notification** tab.
3. Under **People to notify**, select **Notify administrator** to enable Web Reputation notifications.

4. Under **People to notify**, click **Show details** and configure the following:
   - **To**—the global email address(es) appear in this field. You can enter additional email addresses, separated by a semicolon (;) to create unique notifications.
   - **Subject**—type a subject that will appear in the subject line of the email (for example: Web Reputation Notification).
   - **Message**—you can create a unique message using variables like: [Server Name], [Suspicious URLs], [Date], [Time], [Web Content Title], [Web Content Location], [Action], and [Violator].

   **Note:** The available variables appear in the left window, and the message body in the right window.

5. Under **Settings**, choose the delivery options for this notification according to the following:
   - **Send consolidated notifications every [xx] [hours or days]**—select this option to send a notification according to the number of hours or days you type in the variable field.
   - **Send consolidate notifications every [xx] occurrences**—select this option to send a notification after a certain number of occurrences as you stipulate in the variable field.
   - **Send individual notifications**—select this option to send a notification each time an event occurs.

6. Under **Advanced Notification** (SNMP), select **SNMP** to enable this option.

7. Click **Show details** to expand the options, and configure according to the following:
   - **IP Address**
   - **Community**
   - **Message**

8. Select **Write to Windows event log** to write each notification to the Windows event log.

9. Click **Save**.
Manual Scan Notifications

This section discusses how to configure the various notification settings for Manual Scan.

Manual Scan Notifications—Security Risk Scan

The following explains the steps required to configure manual scan security risk scan notifications:

To configure security risk scan notifications:

2. Under, Select the scan type, click the Security risk scan link.
3. Click the Notification tab.
4. Under People to notify, select from the following:
   • Notify violator
   • Notify administrator

Note: The Notify violator option only includes a Subject and a Message. The consolidated message settings under Notify administrator do not apply to the violator.

5. Under People to notify, click Show details next to either Notify violator or Notify administrator and configure the following:

Note: The To field is not used for the Notify violator option.

• To—the global email address(es) appear in this field. You can enter additional email addresses, separated by a semicolon, to create unique notifications.
• Subject—type a subject that will appear in the subject line of the email (for example: Security Risk Notification).
• Message—you can create a unique message using variables like: [Server Name], [Security Risk Name], [Date], [Time], [File Name], [File Location], [Action], and [Violator].
6. Under Settings, choose the delivery options for this notification according to the following:
   - **Send consolidated notifications every [xx] [hours or days]**—select this option to send a notification according to the number of hours or days you type in the variable field.
   - **Send consolidate notifications every [xx] occurrences**—select this option to send a notification after a certain number of occurrences as you stipulate in the variable field.
   - **Send individual notifications**—select this option to send a notification each time an event occurs.

7. Under **Advanced Notification** (SNMP), select **SNMP** to enable this option.

8. Click **Show details** to expand the options, and configure according to the following:
   - IP Address
   - Community
   - Message

9. Select **Write to Windows event log** to write each notification to the Windows event log.

10. Click **Save**.

### Manual Scan Notifications—File Blocking

The following explains the steps required to configure manual scan file blocking notifications:

**To configure manual scan notifications for file blocking:**

1. On the left menu, click **Manual Scan**. The **Manual Scan** screen appears.
2. Under, **Select the scan type**, click the **File blocking** link.
3. Select an existing policy or click **Add** to create a new one.
4. Click the **Notification** tab.
5. Under **People to notify**, select from the following:
   - **Notify violator**
   - **Notify administrator**

   **Note:** The **Notify violator** option only includes a **Subject** and a **Message**. The consolidated message settings under **Notify administrator** do not apply to the violator.

6. Under **People to notify**, click **Show details** next to either **Notify violator** or **Notify administrator** and configure the following:
   - **To**—the global email address(es) appear in this field. You can enter additional email addresses, separated by a semicolon, to create unique notifications.
   - **Subject**—type a subject that will appear in the subject line of the email (for example: File Blocking Notification).
   - **Message**—you can create a unique message using variables like: [Server Name], [File Blocking Rules], [Date], [Time], [File Name], [File Location], [Action], and [Violator].

   **Note:** The available variables appear in the left window, and the message body in the right window.

7. Under **Settings**, choose the delivery options for this notification according to the following:
   - **Send consolidated notifications every [xx] hours or days**—select this option to send a notification according to the number of hours or days you type in the variable field.
   - **Send consolidate notifications every [xx] occurrences**—select this option to send a notification after a certain number of occurrences as you stipulate in the variable field.
   - **Send individual notifications**—select this option to send a notification each time an event occurs.

8. Under **Advanced Notification** (SNMP), select **SNMP** to enable this option.

9. Click **Show details** to expand the options, and configure according to the following:
• IP Address
• Community
• Message—create a message as stated in Step 6 of this procedure.

10. Select **Write to Windows event log** to write each notification to the Windows event log.

11. Click **Save**.

**Manual Scan Notifications—Content Filtering**

The following explains the steps required to configure manual scan content filtering notifications:

**To configure manual scan notifications for content filtering:**

1. On the left menu, click **Manual Scan**. The **Manual Scan** screen appears.
2. Under, **Select the scan type**, click the **Content filtering** link.
3. Select an existing policy or click **Add** to create a new one.
4. Click the **Notification** tab.
5. Under **People to notify**, select from the following:
   • Notify violator
   • Notify administrator

---

**Note:** The **Notify violator** option only includes a **Subject** and a **Message**. The consolidated message settings under **Notify administrator** do not apply to the violator.

---

6. Next to **Notify Violator**, click **Show details** and select from the following:
   • **Subject**—type a subject that will appear in the subject line of the email (for example: Content Filtering Notification).
   • **Message**—you can create a unique message using variables like: [Server Name], [Content Rules], [Date], [Time], [File Name/Web Content Title], [File/Web Content Location], [Action], and Violator.

7. Next to **Notify administrator**, click **Show details** and configure the following:
   • **To**—the global email address(es) appear in this field. You can enter additional email addresses, separated by a semicolon, to create unique notifications.
• **Subject**—type a subject that will appear in the subject line of the email (for example: Content Filtering Notification).

• **Message**—you can create a unique message using variables like: [Server Name], [Content Rules], [Date], [Time], [File Name/Web Content Title], [File/Web Content Location], [Action], and [Violator].

---

**Note:** The available variables appear in the left window, and the message body in the right window.

---

8. Under **Settings**, choose the delivery options for this notification according to the following:

   • **Send consolidated notifications every [xx] [hours or days]**—select this option to send a notification according to the number of hours or days you type in the variable field.

   • **Send consolidate notifications every [xx] occurrences**—select this option to send a notification after a certain number of occurrences as you stipulate in the variable field.

   • **Send individual notifications**—select this option to send a notification each time an event occurs.

9. Under **Advanced Notification (SNMP)**, select **SNMP** to enable this option.

10. Click **Show details** to expand the options, and configure according to the following:

    • **IP Address**
    • **Community**
    • **Message**

11. Select **Write to Windows event log** to write each notification to the Windows event log.

12. Click **Save**.

### Manual Scan Notifications—Data Protection

The following explains the steps required to configure manual scan data protection notifications:
To configure manual scan notifications for data protection:

2. Under, Select the scan type, click the Data protection link.
3. Select an existing policy or click Add to create a new one.
4. Click the Notification tab.
5. Under People to notify, select from the following:
   - Notify violator
   - Notify administrator

   **Note:** The Notify violator option only includes a Subject and a Message. The consolidated message settings under Notify administrator do not apply to the violator.

6. Next to Notify Violator, click Show details and select from the following:
   - **Subject**—type a subject that will appear in the subject line of the email (for example: Data Protection Notification).
   - **Message**—you can create a unique message using variables like: [Server Name], [Data Protection Rules], [Date], [Time], [File Name/Web Content Title], [File/Web Content Location], [Action], and Violator.

7. Next to Notify administrator, click Show details and configure the following:
   - **To**—the global email address(es) appear in this field. You can enter additional email addresses, separated by a semicolon, to create unique notifications.
   - **Subject**—type a subject that will appear in the subject line of the email (for example: Data Protection Notification).
   - **Message**—you can create a unique message using variables like: [Server Name], [Data Protection Rules], [Date], [Time], [File Name/Web Content Title], [File/Web Content Location], [Action], and [Violator].

   **Note:** The available variables appear in the left window, and the message body in the right window.

8. Under Settings, choose the delivery options for this notification according to the following:
• **Send consolidated notifications every [xx] [hours or days]**—select this option to send a notification according to the number of hours or days you type in the variable field.

• **Send consolidate notifications every [xx] occurrences**—select this option to send a notification after a certain number of occurrences as you stipulate in the variable field.

• **Send individual notifications**—select this option to send a notification each time an event occurs.

9. Under **Advanced Notification (SNMP)**, select **SNMP** to enable this option.

10. Click **Show details** to expand the options, and configure according to the following:
    • **IP Address**
    • **Community**
    • **Message**

11. Select **Write to Windows event log** to write each notification to the Windows event log.

12. Click **Save**.

**Manual Scan Notifications—Web Reputation**

The following explains the steps required to configure manual scan Web Reputation notifications:

**To configure manual scan notifications for Web Reputation:**

1. On the left menu, click **Manual Scan**. The **Manual Scan** screen appears.

2. Under, **Select the scan type**, click the **Web Reputation** link.

3. Click the **Notification** tab.

4. Under **People to notify**, select from the following:
    • **Notify violator**
    • **Notify administrator**
Note: The Notify violator option only includes a Subject and a Message. The consolidated message settings under Notify administrator do not apply to the violator.

5. Under People to notify, click Show details next to either Notify violator or Notify administrator and configure the following:
   - To—the global email address(es) appear in this field. You can enter additional email addresses, separated by a semicolon, to create unique notifications.
   - Subject—type a subject that will appear in the subject line of the email (for example: Web Reputation Notification).
   - Message—you can create a unique message using variables like: [Server Name], [Suspicious URLs], [Date], [Time], [Web Content Title], [Web Content Location], [Action], and [Violator].

Note: The available variables appear in the left window, and the message body in the right window.

6. Under Settings, choose the delivery options for this notification according to the following:
   - Send consolidated notifications every [xx] [hours or days]—select this option to send a notification according to the number of hours or days you type in the variable field.
   - Send consolidate notifications every [xx] occurrences—select this option to send a notification after a certain number of occurrences as you stipulate in the variable field.
   - Send individual notifications—select this option to send a notification each time an event occurs.

7. Under Advanced Notification (SNMP), select SNMP to enable this option.

8. Click Show details to expand the options, and configure according to the following:
   - IP Address
   - Community
   - Message
9. Select **Write to Windows event log** to write each notification to the Windows event log.
10. Click **Save**.

### Scheduled Scan Notifications

This section discusses how to configure the various notification settings for Scheduled Scan.

#### Scheduled Scan Notifications—Security Risk Scan

The following explains the steps required to configure scheduled scan notifications for security risk scan:

**To configure scheduled scan notifications for security risk scan:**

1. On the left menu, click **Scheduled Scan**. The **Scheduled Scan** screen appears.
2. Click **Add**, to add a new task, or click an existing task from the **Task Name** column. The **Scheduled Scan > Edit Scan Task** or **Scheduled Scan > Add Scan Task** screen appears.
3. Under **Select scan type**, click the **Security risk scan** link.
4. Click the **Notification** tab.
5. Under **People to notify**, select from the following:
   - Notify violator
   - Notify administrator

**Note:** The **Notify violator** option only includes a **Subject** and a **Message**. The consolidated message settings under **Notify administrator** do not apply to the violator.

6. Under **People to notify**, click **Show details** next to either **Notify violator** or **Notify administrator** and configure the following:
   - **To**—the global email address(es) appear in this field. You can enter additional email addresses, separated by a semicolon, to create unique notifications.
   - **Subject**—type a subject that will appear in the subject line of the email (for example: Security Risk Notification).
• **Message**—you can create a unique message using variables like: [Server Name], [Security Risk Name], [Date], [Time], [File Name], [File Location], [Action], and [Violator].

---

**Note:** The available variables appear in the left window, and the message body in the right window.

---

7. Under **Settings**, choose the delivery options for this notification according to the following:
   - **Send consolidated notifications every [xx] [hours or days]**—select this option to send a notification according to the number of hours or days you type in the variable field.
   - **Send consolidate notifications every [xx] occurrences**—select this option to send a notification after a certain number of occurrences as you stipulate in the variable field.
   - **Send individual notifications**—select this option to send a notification each time an event occurs.

8. Under **Advanced Notification** (SNMP), select **SNMP** to enable this option.

9. Click **Show details** to expand the options, and configure according to the following:
   - **IP Address**
   - **Community**
   - **Message**

10. Select **Write to Windows event log** to write each notification to the Windows event log.

11. Click **Save**.

---

**Scheduled Scan Notifications—File Blocking**

The following explains the steps required to configure scheduled scan notifications for file blocking:
To configure scheduled scan notifications for file blocking:

1. On the left menu, click Scheduled Scan. The Scheduled Scan screen appears.
2. Click an existing task from the Task Name column. The Scheduled Scan > Edit Scan Task screen appears.
3. Under Select scan type, click the File blocking link.
4. Select an existing policy.
5. Click the Notification tab.
6. Under People to notify, select from the following:
   - Notify violator
   - Notify administrator

   **Note:** The Notify violator option only includes a Subject and a Message. The consolidated message settings under Notify administrator do not apply to the violator.

7. Under People to notify, click Show details next to either Notify violator or Notify administrator and configure the following:
   - **To**—the global email address(es) appear in this field. You can enter additional email addresses, separated by a semicolon, to create unique notifications.
   - **Subject**—type a subject that will appear in the subject line of the email (for example: File Blocking Notification).
   - **Message**—you can create a unique message using variables like: [Server Name], [File Blocking Rules], [Date], [Time], [File Name], [File Location], [Action], and [Violator].

   **Note:** The available variables appear in the left window, and the message body in the right window.

8. Under Settings, choose the delivery options for this notification according to the following:
   - **Send consolidated notifications every [xx] [hours or days]**—select this option to send a notification according to the number of hours or days you type in the variable field.
• **Send consolidate notifications every [xx] occurrences**—select this option to send a notification after a certain number of occurrences as you stipulate in the variable field.

• **Send individual notifications**—select this option to send a notification each time an event occurs.

9. Under **Advanced Notification** (SNMP), select **SNMP** to enable this option.

10. Click **Show details** to expand the options, and configure according to the following:
    • IP Address
    • Community
    • Message

11. Select **Write to Windows event log** to write each notification to the Windows event log.

12. Click **Save**.

**Scheduled Scan Notifications—Content Filtering**

The following explains the steps required to configure scheduled scan notifications for content filtering:

**To configure scheduled scan notifications for content filtering:**

1. On the left menu, click **Scheduled Scan**. The **Scheduled Scan** screen appears.

2. Click an existing task from the **Task Name** column. The **Scheduled Scan > Edit Scan Task** screen appears.

3. Under **Select scan type**, click the **Content Filtering** link.

4. Select an existing policy.

5. Click the **Notification** tab.

6. Under **People to notify**, select from the following:
   • Notify violator
   • Notify administrator
Note: The Notify violator option only includes a Subject and a Message. The consolidated message settings under Notify administrator do not apply to the violator.

7. Under People to notify, click Show details next to either Notify violator or Notify administrator and configure the following:
   • To—the global email address(es) appear in this field. You can enter additional email addresses, separated by a semicolon, to create unique notifications.
   • Subject—type a subject that will appear in the subject line of the email (for example: Content Filtering Notification).
   • Message—you can create a unique message using variables like: [Server Name], [Content Rules], [Date], [Time], [File Name/Web Content Title], [File/Web Content Location], [Action], and [Violator].

   Note: The available variables appear in the left window, and the message body in the right window.

8. Under Settings, choose the delivery options for this notification according to the following:
   • Send consolidated notifications every [xx] [hours or days]—select this option to send a notification according to the number of hours or days you type in the variable field.
   • Send consolidate notifications every [xx] occurrences—select this option to send a notification after a certain number of occurrences as you stipulate in the variable field.
   • Send individual notifications—select this option to send a notification each time an event occurs.

9. Under Advanced Notification (SNMP), select SNMP to enable this option.
10. Click Show details to expand the options, and configure according to the following:
    • IP Address
    • Community
    • Message
11. Select **Write to Windows event log** to write each notification to the Windows event log.

12. Click **Save**.

### Scheduled Scan Notifications—Data Protection

The following explains the steps required to configure scheduled scan notifications for data protection:

**To configure scheduled scan notifications for data protection:**

1. On the left menu, click **Scheduled Scan**. The **Scheduled Scan** screen appears.
2. Click an existing task from the **Task Name** column. The **Scheduled Scan > Edit Scan Task** screen appears.
3. Under **Select scan type**, click the **Data protection** link.
4. Select an existing policy.
5. Click the **Notification** tab.
6. Under **People to notify**, select from the following:
   - **Notify violator**
   - **Notify administrator**

   **Note:** The **Notify violator** option only includes a **Subject** and a **Message**. The consolidated message settings under **Notify administrator** do not apply to the violator.

7. Under **People to notify**, click **Show details** next to either **Notify violator** or **Notify administrator** and configure the following:
   - **To**—the global email address(es) appear in this field. You can enter additional email addresses, separated by a semicolon, to create unique notifications.
   - **Subject**—type a subject that will appear in the subject line of the email (for example: Data Protection Notification).
   - **Message**—you can create a unique message using variables like: [Server Name], [Data Protection Rules], [Date], [Time], [File Name/Web Content Title], [File/Web Content Location], [Action], and [Violator].
**Note:** The available variables appear in the left window, and the message body in the right window.

8. Under **Settings**, choose the delivery options for this notification according to the following:
   - **Send consolidated notifications every [xx] [hours or days]**—select this option to send a notification according to the number of hours or days you type in the variable field.
   - **Send consolidate notifications every [xx] occurrences**—select this option to send a notification after a certain number of occurrences as you stipulate in the variable field.
   - **Send individual notifications**—select this option to send a notification each time an event occurs.

9. Under **Advanced Notification** (SNMP), select **SNMP** to enable this option.

10. Click **Show details** to expand the options, and configure according to the following:
    - **IP Address**
    - **Community**
    - **Message**

11. Select **Write to Windows event log** to write each notification to the Windows event log.

12. Click **Save**.
Scheduled Scan Notifications—Web Reputation

The following explains the steps required to configure scheduled scan notifications for Web reputation:

To configure scheduled scan notifications for Web reputation:

1. On the left menu, click Scheduled Scan. The Scheduled Scan screen appears.
2. Click an existing task from the Task Name column. The Scheduled Scan > Edit Scan Task screen appears.
3. Under Select scan type, click the Web Reputation link.
4. Click the Notification tab.
5. Under People to notify, select from the following:
   - Notify violator
   - Notify administrator

   **Note:** The Notify violator option only includes a Subject and a Message. The consolidated message settings under Notify administrator do not apply to the violator.

6. Under People to notify, click Show details next to either Notify violator or Notify administrator and configure the following:
   - **To**—the global email address(es) appear in this field. You can enter additional email addresses, separated by a semicolon, to create unique notifications.
   - **Subject**—type a subject that will appear in the subject line of the email (for example: Web Reputation Notification).
   - **Message**—you can create a unique message using variables like: [Server Name], [Suspicious URLs], [Date], [Time], [Web Content Title], [Web Content Location], [Action], and [Violator].

   **Note:** The available variables appear in the left window, and the message body in the right window.

7. Under Settings, choose the delivery options for this notification according to the following:
• **Send consolidated notifications every [xx] [hours or days]**—select this option to send a notification according to the number of hours or days you type in the variable field.

• **Send consolidate notifications every [xx] occurrences**—select this option to send a notification after a certain number of occurrences as you stipulate in the variable field.

• **Send individual notifications**—select this option to send a notification each time an event occurs.

8. Under **Advanced Notification** (SNMP), select **SNMP** to enable this option.

9. Click **Show details** to expand the options, and configure according to the following:
   - **IP Address**
   - **Community**
   - **Message**

10. Select **Write to Windows event log** to write each notification to the Windows event log.

11. Click **Save**.

## Alerts

The Alerts function provides notifications for System Events and Outbreaks. This section describes how to enable and configure these options.

### System Events

System events enables to send notifications regarding the status of various features in PortalProtect (see *Figure 11-1. System Events configuration screen*). These notifications include the following:

**PortalProtect Services**

- PortalProtect service did not start successfully
- PortalProtect service is unavailable

**PortalProtect Events**
• Smart Protection Server—Each time File Reputation service was **Unavailable** or **Recovered**

• Smart Protection Server—Each time Web Reputation service was **Unavailable** or **Recovered**

• Update—Each time update was **Unsuccessful** or **Successful**

• Update—Last update time is older than [x] [hour(s) or day(s)]

• Manual/Scheduled scan tasks were **Unsuccessful** or **Successful**

• Manual/Scheduled scan time exceeds [x] [hour(s) or day(s)]

• The disk space on the local drive (volume) of the backup directory is less than [x-GB/MB]
  
  Specify time interval to send consecutive alerts if above problem still exists [x] [min(s)/hr(s)]

• The log database size exceeds [x-GB/MB]
  
  Specify time interval to send consecutive alerts if above problem still exists [x] [min(s)/hr(s)]

• The size of quarantined files exceeds [x-GB/MB]
Additionally, you can configure a frequency for sending consecutive alerts when a problem continues to exist.

**FIGURE 11-1. System Events configuration screen**

**To configure system events for PortalProtect services:**

1. Click **Alerts > System Events**. The **System Events** screen appears.
2. Under **PortalProtect Services**, select from the following options:
   - PortalProtect service did not start successfully
   - PortalProtect service is unavailable
3. After selecting an option, click the link to display the Administrator Notification screen, similar to that shown in **Figure 11-2**.
4. Create a custom message and email list as explained in **Security Risk Scan Notifications** on page 11-3.
5. Click Save.

![System Events - PortalProtect Services](image)

**FIGURE 11-2. System Events, administrator notification screen**

*To configure system events for PortalProtect events:*

1. Click Alerts > System Events. The System Events screen appears.

2. Under PortalProtect Events, select from the following options:

   - **Smart Protection Server - Each time File Reputation service was Unavailable or Recovered**—select Unavailable to receive a single notification when the security risk scan service becomes unavailable. Select Recovered to receive a single notification when the security risk scan service becomes available.

   - **Smart Protection Server - Each time Web Reputation service was Unavailable or Recovered**—select Unavailable to receive a single notification when the Web reputation service becomes unavailable. Select Recovered to receive a single notification when the Web reputation service becomes available.
• **Update - each time update was [Unsuccessful] or [Successful]**—select the option according to whether send a notification if the update was successful or not.

• **Update - Last update is older than [x][hour(s) or day(s)]**—type a value in the field and choose **day(s)** or **hour(s)**. A notification will be sent after the last update time span reaches that value.

• **Manual/Scheduled scan tasks were Unsuccessful] or [Successful]**—select the option according to whether to send a notification if manual/scheduled scan task was successful or not.

• **Manual/Scheduled scan time exceeds [x][hour(s) or day(s)]**—type a value in the field and choose **day(s)** or **hour(s)**. A notification will be sent when the scan time exceeds that value.

• **The disk space on the local drive (volume) of the backup directory is less than [x-MB/GB]**—type a value in the field and choose **MB** (megabyte) or **GB** (gigabyte). A notification will be sent when the disk space for the specified areas is less than that value.

  **Specify time interval to send consecutive alerts if above problem available disk space still exists**—type a value in the field and choose **minute(s)** or **hour(s)**. Each time the specified time is reached, another notification will be sent.

• **Log database size exceeds [x-MB/GB]**—type a value in the field and choose **day(s)** or **hour(s)**.

  **Specify time interval to send consecutive alerts if above problem still exists**—type a value in the field and choose **minute(s)** or **hour(s)**. Each time the specified time is reached, another notification will be sent.

• **The size of quarantined files exceeds [x-GB/MB]**—type a value in the field and choose **day(s)** or **hour(s)**.

  **Specify time interval to send consecutive alerts if above problem still exists**—type a value in the field and choose **minute(s)** or **hour(s)**. Each time the specified time is reached, another notification will be sent.

---

**WARNING!** To prevent duplicate alerts in a farm environment, enable “The size of quarantined file exceeds” alert on only one PortalProtect server and disable the option on all other PortalProtect servers in the farm.
3. After selecting an option and setting the parameters to trigger the notification, click the link to display the Administrator Notification screen, similar to that shown in Figure 11-2.

4. Create a custom message and email list as explained in Security Risk Scan Notifications on page 11-3.

5. Click Save.

Outbreak Alert

Outbreak Alert enables you to configure settings to alert administrators when:

- Viruses detected reach a selected number within a selected time span
- Uncleanable viruses reach a selected number within a selected time span
- Blocked files reach a selected number within a selected time span

To configure an Outbreak Alert:

1. On the left menu, click Alerts > Outbreak Alert. The Outbreak Alert screen appears.

2. In the Number field, type a number that equals the number of Detected Viruses, Uncleanable Viruses, and Blocked Files that will trigger the alert. Then, type a value in the Time field, and choose whether that value should be expressed in Hours or Minutes.

Note: An Outbreak Alert will be triggered when the Number is reached within the specified time span. For example: for viruses detected, a value of 25 in the Number field with a Time of 24-hours, will trigger an Outbreak Alert if 25 or more viruses are detected within a 24-hour period.

Configure the following options:

- Select, **Virus detected reach the following number within the shown time**: [number] [time value] [hours/minutes]
- Select, **Uncleanable viruses reach the following number within the shown time**: [number] [time value] [hours/minutes]
- Select, **Blocked files reach the following number within the shown time**: [number] [time value] [hours/minutes]
3. Click Save.

About Access Control

Use the role based administration feature to grant and control access to PortalProtect product console menu and submenu items. This function also allows you to grant non-administrators view only access to the product console. PortalProtect provides two roles: Administrator and Operator. You can modify the permissions available to the Operator role to suit your organizational requirements.

![Access Control Main screen](image)

**FIGURE 11-3. Access Control Main screen**
Access Control Authentication

This section provides a description about the Access Control Authentication Settings screen. This screen enables you to select specific AD Users and AD Groups to add to either the Administrator or Operator roles.

The following provides a description of the various fields and functions found on the access control authentication screen:

- **Description**: this field enables you to modify the description for either the Administrator, or the Operator. The default descriptions are **Administrator** and **Operator**.

**FIGURE 11-4. Access Control Authentication screen for administrator**

The following provides a description of the various fields and functions found on the access control authentication screen:
• **Select Accounts from AD:** this section enables you to search for and add AD users and AD groups to apply to the Administrator or Operator role.

**Access Control Permissions**

PortalProtect enables you to customize permissions to allow or disallow access to certain features and functions. The Administrator role has full permission and access, and these permissions cannot be modified. However, you can customize the permissions available to the Operator according to your business needs. See *Figure 11-5.*

**Access Control**

<table>
<thead>
<tr>
<th>Access Areas</th>
<th>Full</th>
<th>Read</th>
<th>None</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Risk Scan</td>
<td>R</td>
<td>R</td>
<td>N</td>
<td>Authorized users will not see this feature.</td>
</tr>
<tr>
<td>File Blocking</td>
<td>R</td>
<td>R</td>
<td>N</td>
<td>Authorized users will not see this feature.</td>
</tr>
<tr>
<td>Content Filter</td>
<td>R</td>
<td>R</td>
<td>N</td>
<td>Authorized users will not see this feature.</td>
</tr>
<tr>
<td>Data Protection</td>
<td>R</td>
<td>R</td>
<td>N</td>
<td>Authorized users will not see this feature.</td>
</tr>
<tr>
<td>URL Reputation</td>
<td>R</td>
<td>R</td>
<td>N</td>
<td>Authorized users will not see this feature.</td>
</tr>
<tr>
<td>Manual Scan</td>
<td>R</td>
<td>R</td>
<td>N</td>
<td>Authorized users will not see this feature.</td>
</tr>
<tr>
<td>Scheduled Scan</td>
<td>R</td>
<td>R</td>
<td>N</td>
<td>Authorized users will not see this feature.</td>
</tr>
<tr>
<td>Smart Protection</td>
<td>R</td>
<td>R</td>
<td>N</td>
<td>Authorized users will not see this feature.</td>
</tr>
<tr>
<td>Alerts</td>
<td>R</td>
<td>R</td>
<td>N</td>
<td>Authorized users will not see this feature.</td>
</tr>
<tr>
<td>Administration</td>
<td>R</td>
<td>R</td>
<td>N</td>
<td>Authorized users will not see this feature.</td>
</tr>
<tr>
<td>Real-time Monitor</td>
<td>R</td>
<td>R</td>
<td>N</td>
<td>Authorized users may access Real Time Monitor.</td>
</tr>
<tr>
<td>Update</td>
<td>R</td>
<td>R</td>
<td>N</td>
<td>Authorized users may configure manual updates.</td>
</tr>
<tr>
<td>Logs</td>
<td>R</td>
<td>R</td>
<td>N</td>
<td>Authorized users may access logs.</td>
</tr>
<tr>
<td>Reports</td>
<td>R</td>
<td>R</td>
<td>N</td>
<td>Authorized users may generate reports.</td>
</tr>
<tr>
<td>Quarantine</td>
<td>R</td>
<td>R</td>
<td>N</td>
<td>Authorized users may access quarantined messages and files.</td>
</tr>
</tbody>
</table>

*Figure 11-5. Access control permissions for the Operator role*

**Working with Logs**

PortalProtect provides comprehensive information about various scans. It saves this information to a database. You can query the database and obtain logs for analysis. For example, you can analyze Security Risk scan logs to view the most common viruses and scan actions and see which users are introducing viruses to the network.

You can use this information to reduce system vulnerabilities and review the effectiveness of your security policies; then, if necessary, adjust the policies accordingly. Additionally, you can export the log data in `.csv` format for further analysis or to share the information.

The following is a listing of the information contained within the various log types:
• **Security risk scan** logs—contains information about the: Date & Time, Violator, Security Risk Name, Action, File Name, and Location. You can filter the Security risk scan logs for:
  a. All
  b. Detected virus/malware
  c. Uncleanable virus/malware
d. Detected spyware/grayware
• **File blocking** logs—contains information about the: Date & Time, Violator, Policy Name, Action, File Name, Triggered File Type/Name, and Location.
• **Content Filtering** logs—contains information about the: Date & Time, Violator, Policy Name, Action, File Name/Web Content Title, Triggered Keywords, and Location.
• **Web reputation** logs—contains information about the: Date & Time, Violator, Risk Level, Web Content Title, Suspicious URL, Action, and Location.
• **Update** logs—contains information about the: Date & Time, and Description.
• **Scan events** logs—contains information about the: Date & Time, and Description.
• **Backup** logs—contains information about the: Date & Time, Violator, Security Risk Name, File Name, Location, and Backup Path.
• **Unscannable files** logs—contains information about the: Date & Time, Location, Violator, Reason, File Name, and Action.
• **Event tracking** logs—contains information about the: Username, Event time, IP address, Event type, Source type, and Description.
• **Data protection** logs—contains information about the: Date & Time, Violator, Policy Name, Action, File Name/Web Content Title, Template(s), and Location.

**Query Logs**

PortalProtect enables you to view many types of logs, which you can export and print. Use the Query function to select the type of log you want PortalProtect to display. You can make queries about events, viruses detected, component updates, blocked files, and files placed in the backup folder. You can export or print the log information you obtain from a query.
To perform a log query:

1. From the left menu, click **Logs > Query**. The **Log Query** screen appears.
2. Select the log type from the **Type** drop-down.
3. To query using a date range:
   - Select a query date range from the **Dates** field. The date range includes a **from:** [MM/dd/yyyy] time of day [hh] and [mm] and **to:** [MM/dd/yyyy] time of day [hh] and [mm].
4. To query for **Violator**:
   - Select **All**, to search all users, or...
   - Select **Specify user(s)** and click the drop down to search for and add specific AD users.
5. To query a **Site**:
   - Select **All**, to search all sites, or...
   - Select **Specify site(s)** and click the drop down to search for and add specific site(s).
6. To query using a **File name**:
   - Type a full or partial filename in the **File name** field.
7. Select a sort option from the **Sort by** drop down; then, select **Ascending** or **Descending**.
8. In the **Display** field, type the number of log entries to display per page; the default is 15.
9. Click **Search** to display the query results.
10. Click **Export** to export the result of your query as a comma-separated value (CSV) file (Unicode standard).
11. Click **Print** to print the result of your query.

**FIGURE 11-6. Log Query screen**

**Log Maintenance**

The Log Maintenance screens enable you to set both manual and automatic options for deleting log histories. This functionality can be useful for saving disk space when it becomes an issue or if the information they provide is no longer useful. PortalProtect lets you delete logs both automatically and manually.

**Manually Delete Logs**

This procedure describes the steps required to manually delete logs for PortalProtect.

To **manually delete logs:**

1. From the left menu, click **Logs > Maintenance**, and select the **Manual** tab on the Log Maintenance screen (**Figure 11-7**).

2. Under the **Target** group, select whether to delete **All logs**, or select **Specified logs** from the following:
   - Security risk scan
   - Web reputation
   - Backup
   - File blocking
   - Updates
   - Unscannable files
   - Content filtering
• Scan events
• Event tracking
• Data protection

3. Under the **Action** group, type a value in days, in the **Delete event tracking logs older than** and the **Delete logs older than** fields.

**Note:** Event tracking logs will be deleted that are older than the number of days you enter in the **Delete event tracking logs older than** field. Other logs will be deleted that are older than the number of days you enter in **Delete logs older than** field.

4. Click, **Delete Now**.

**FIGURE 11-7. Log Maintenance manual tab**

**Automatically Delete Logs**

You can configure PortalProtect to automatically delete logs. You can set the number of days and/or the size of the logs that must be exceeded before PortalProtect automatically deletes them. If you only want to set one condition, do not specify a value for the other box.
To automatically delete logs:

1. From the left menu, click **Logs > Maintenance**, and select the **Automatic** tab *(Figure 11-8).*

2. Select **Enable automatic maintenance**.

3. Under the **Target** group, select whether to delete **All logs**, or select **Specified logs** from the following:
   - Security risk scan
   - Web reputation
   - Backup
   - File blocking
   - Updates
   - Unscannable files
   - Content filtering
   - Scan events
   - Event tracking
   - Data protection

4. Under the **Action** group, type a value in days, in the **Delete event tracking logs older than** and the **Delete logs older than** fields.

---

**Note:** Event tracking logs will be deleted that are older than the number of days you enter in the **Delete event tracking logs older than** field. Other logs will be deleted that are older than the number of days you enter in **Delete logs older than** field.
5. Click **Save**.

**Log Maintenance**

<table>
<thead>
<tr>
<th>Last log maintenance: 5/3/2011 2:30:00 AM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable automatic maintenance</strong></td>
</tr>
<tr>
<td><strong>Target</strong></td>
</tr>
<tr>
<td>• All logs</td>
</tr>
<tr>
<td>• Specified logs</td>
</tr>
<tr>
<td>• Security risk scan</td>
</tr>
<tr>
<td>• Web reputation</td>
</tr>
<tr>
<td>• Backup</td>
</tr>
<tr>
<td>• Data protection</td>
</tr>
<tr>
<td>• File blocking</td>
</tr>
<tr>
<td>• Updates</td>
</tr>
<tr>
<td>• Unscannable files</td>
</tr>
<tr>
<td>• Content filtering</td>
</tr>
<tr>
<td>• Scan events</td>
</tr>
<tr>
<td>• Event tracking</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Action</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete event tracking logs older than:</td>
</tr>
<tr>
<td>20 days</td>
</tr>
<tr>
<td>Delete logs older than:</td>
</tr>
<tr>
<td>50 days</td>
</tr>
</tbody>
</table>

**FIGURE 11-8. Log Maintenance automatic tab**

**Central Quarantine Management**

Quarantine Management enables you to manage all files that have been quarantined by manual scans and scheduled scans. The PortalProtect administrator can query, delete, restore and download the quarantined files quarantined by all PortalProtect systems in the farm. This section describes the quarantine query and maintenance functionalities.

**Quarantine Query**

PortalProtect 2.0 enables the administrator to query quarantined files using specific search criteria that includes the *(Figure 11-9)*:

- Date,
- Time,
- Violator (All or Specify user(s)),
- Site (All or Specify site(s)),
- File name,
• Type (Security risk scan, File blocking, Content filtering, Data protection, Unscannable files).

Additionally, you can sort and display the query results by:
• Date/Time,
• File Name,
• Violator,
• Sort by Ascending or Descending order, and
• Choose the number of results to Display per page.

**FIGURE 11-9. Quarantine Query main screen**
### Table 11-1. Default Quarantine Settings

<table>
<thead>
<tr>
<th>Setting name</th>
<th>Default setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>One day</td>
</tr>
<tr>
<td>Violator</td>
<td>All</td>
</tr>
<tr>
<td></td>
<td>Note: Select specific violators from the Active Directory.</td>
</tr>
<tr>
<td>Sites</td>
<td>All</td>
</tr>
<tr>
<td></td>
<td>Note: Select specific sites from the site tree.</td>
</tr>
<tr>
<td>File Name</td>
<td>Null</td>
</tr>
<tr>
<td></td>
<td>Note: Type a specific file name, or leave blank to search all quarantined files according to the other search criteria.</td>
</tr>
<tr>
<td>Sort by</td>
<td>Date/Time</td>
</tr>
<tr>
<td></td>
<td>Descending</td>
</tr>
<tr>
<td>Display</td>
<td>15 records per page</td>
</tr>
</tbody>
</table>

The following describes some of the functions available to the administrator for quarantined files:

- Quarantined files can be restored or deleted after they are queried.
- Files quarantined by file blocking, content filtering, or data protection can be downloaded after they are queried.
To perform a quarantine query:

1. From the left menu, click Quarantine > Query. The Quarantine Query screen appears (Figure 11-9).

2. To query using a date range:
   • Select a query date range from the Dates field. The date range includes a from: [MM/dd/yyyy] time of day [hh] and [mm] and to: [MM/dd/yyyy] time of day [hh] and [mm].

3. To query for Violator:
   • Select All, to search all users, or...
   • Select Specify user(s) and click the drop down to search for and add specific AD users.

4. To query a Site:
   • Select All, to search all sites, or...
   • Select Specify site(s) and click the drop down to search for and add specific site(s).

   **Note:** The default setting for Site is All. Users can select specified site(s) from site tree. A URL search produces the position of specified URL. All URLs must start with http or https.

5. To query using a File name:
   • Type a full or partial filename in the File name field.

6. To query using a scan Type, choose one of the following:
   • Security risk scan (default)
   • File blocking
   • Content filtering
   • Unscannable files
   • Data protection

7. Select a sort option from the Sort by drop down; then, select Ascending or Descending.

8. In the Display field, type the number of log entries to display per page; the default is 15.
9. Click Search to display the query results.

Delete, Restore, or Download Quarantined Files

After performing a quarantine query, you can delete, restore, or download the file as required. However, to protect your system, virus infected files cannot be downloaded. Figure 11-10 shows an example of the Quarantined Query results window.

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>File Name</th>
<th>File Location</th>
<th>Violator</th>
<th>Security Risk Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013/03/09 23:16:45</td>
<td>Hello.VID</td>
<td>http://mess_x64_1232/Documents</td>
<td>MOSS_x64_1232/administrator</td>
<td>LE_TEST_VIRUS</td>
</tr>
<tr>
<td>2013/03/09 00:06:49</td>
<td>siad0.com</td>
<td>http://mess_x64_1232/automation/Shared Documents</td>
<td>MOSS_x64_1232/administrator</td>
<td>Excel.text_file</td>
</tr>
</tbody>
</table>

**FIGURE 11-10. Quarantined Query results window**

The following describes the options available in the Quarantine Query results window:

- **Restore**—click to restore selected files to the location indicated under the File Location heading
- **Delete**—click to permanently delete selected files
- **Date/Time**—date and time the file was quarantined
- **File Name**—name of the quarantined file
- **File Location**—location of the quarantined file
- **Violator**—displays the user responsible for uploading the file
- **Security Risk Name** (for Security risk scan only)—displays the name of the virus/malware/spyware/grayware contained in the file
- **Policy Name** (for File blocking, Content filtering, and Data protection only)—displays the name of the policy responsible for the quarantine
- **Reason** (for Unscannable files only)—provides a brief explanation why the file was quarantined; for example: Over restriction (decompressed file count)

**To delete, restore, or download a quarantined file:**

1. Perform a quarantine query as described in Quarantine Query on page 11-40.
2. From the Quarantined results window, select the files you want to delete or restore and click:
   - Click **Delete** to permanently delete the selected file(s)
• Click **Restore** to restore the selected files to the original location

**Note:** For Content filtering, File blocking, Data protection, and Unscannable files, you can click the File Name link to start a file download. You will have the option to open or save the file to the location you choose.

**Tip:** Click the column headings to sort the quarantined results according to the heading label (Date/Time, File Name, and so on).

---

**Quarantine Maintenance**

Quarantine Maintenance enables you to configure manual and automatic settings to delete quarantined files according to the time period you choose.

![Quarantine Maintenance screen](image)

**FIGURE 11-11. Quarantine Maintenance screen Manual tab**

**WARNING!** Be sure to perform regular quarantine maintenance, and restore or delete files to prevent losing important documents and also free disk space.
**Tip:** In a farm environment, enable Automatic Quarantine Maintenance on only one PortalProtect server and disable it on all other Web front end servers in the same farm.

To manually delete quarantined files:
1. Click **Quarantine > Maintenance > Manual** tab. The Quarantine Maintenance screen appears and displays the Manual tab (*Figure 11-11*).
2. Under **Files to delete**, choose from the following options:
   - Quarantined by security risk scan
   - Quarantined by file blocking policy
   - Quarantined by content filtering policy
   - Quarantined by unscannable files action
   - Quarantined by data protection
3. Under **Action**, type a value in the **Delete selected files older than [xx] days** field.
4. Click **Delete Now**.

To automatically delete quarantined files:
1. Click **Quarantine > Maintenance > Automatic** tab. The Quarantine Maintenance screen appears and displays the Automatic tab (*Figure 11-12*).
2. Select **Enable automatic maintenance** to enable this functionality.
3. Under **Files to delete**, choose from the following options:
   - Quarantined by security risk scan
   - Quarantined by file blocking policy
   - Quarantined by content filtering policy
   - Quarantined by unscannable files action
   - Quarantined by data protection
4. Under **Action**, type a value in the **Delete selected files older than [xx] days** field.
5. Click **Save**.

![Quarantine Maintenance Automatic Tab](image)

**FIGURE 11-12.** Quarantine maintenance automatic tab

**Viewing and Generating Reports**

PortalProtect enables you to generate **One-time** or **Scheduled** reports. These reports are created using data from log events. You can view previously generated reports from the Management console.

**To generate a one-time report:**

1. From the left menu, click **Reports > One-time Reports**. The **One-time Reports** screen appears.

2. From the **One-time Reports screen**, click **Generate report**. The **One-time Reports > Add/Edit a report** screen appears (*Figure 11-13*).

3. Type a name for the report in the **Report name** field.

4. Select a time span to gather data for the report, in the **From** and **To** fields.

5. In the Content group, select the items you want to appear in your report from the following options:
   - **Scan status summary**—displays a summary of the scan status
   - **Security risk scan report**—select to enable and choose from the following:
     - **Security risk scan summary**
• **Viruses/malware graph**—from the drop down, choose whether the graph will display, hourly, daily, weekly or monthly data

• **Top viruses/malware**—type the number of top viruses/malware to display in the report

• **Top viruses/malware violators**—type the number of top viruses/malware violators to display in the report

• **Virus/malware action summary**—select to display a summary of the action taken on all viruses and malware contained in the report

• **Security risk types**—select to display the security risk types in the report

• **Spyware/grayware graph**—from the drop down, choose whether the graph will display, hourly, daily, weekly or monthly data

• **Top spyware/grayware**—select to display the top spyware/grayware

• **Top spyware/grayware violators**—select to display the top spyware/grayware violators

• **Virus/grayware action summary**—select to display a summary of the action taken on all viruses and grayware contained in the report

• **File blocking report**—select to enable and choose from the following:
  
  • **File blocking summary**—select to display in the report

  • **Blocked files graph**—from the drop down, choose whether the graph will display, hourly, daily, weekly or monthly data

  • **Top file types blocked**—type the number of top blocked file types to display in the report

  • **Top file names blocked**—type the number of top blocked file names to display in the report

  • **Top file extensions blocked**—type the number of top blocked file extensions to display in the report

  • **Top blocked file violators**—type the number of top blocked file violators to display in the report

  • **Top file blocking policy triggered**—type the number of top blocked file policy triggered to display in the report

• **Content filtering report**—select to enable and choose from the following:
  
  • **Content filtering summary**—select to display in the report
• **Filtered files and Web content graph**—from the drop down, choose whether the graph will display, hourly, daily, weekly or monthly data
• **Top filtered files/Web content violators**—type the number of these top violators you want to appear in the report
• **Top content filtering policy triggered**—type the number of these top policies you want to appear in the report

• **Data protection report**—select to enable and choose from the following:
  • **Data protection summary**—select to display in the report
  • **Filtered files and Web content graph**—from the drop down, choose whether the graph will display, hourly, daily, weekly or monthly data
  • **Top filtered files/Web content violators**—type the number of these top violators you want to appear in the report
  • **Top data protection policy triggered**—type the number of these top data protection policies you want to appear in the report
  • **Top data protection template triggered**—type the number of these top data protection templates you want to appear in the report

• **Unscannable file report**—select to enable and choose from the following:
  • **Unscannable file summary**—select to have this option appear in the report
  • **Unscannable file graph**—from the drop down, choose whether the graph will display, hourly, daily, weekly or monthly data

• **Web reputation report**—select to enable and choose from the following:
  • **Web reputation summary**—select to have this option appear in the report
  • **Suspicious URLs graph**—from the drop down, choose whether the graph will display, hourly, daily, weekly or monthly data
  • **Top malicious URLs**—type the number of top malicious URLs you want to appear in the report
  • **Top authors of Web content containing suspicious URLs**—type the number of top authors for this option you want to appear in the report

6. Click **Generate**.
FIGURE 11-13. Create one-time report screen
To create a scheduled report:

1. From the left menu, click Reports > Scheduled Reports. The Scheduled Reports screen appears.

2. From the Scheduled Reports screen, click Add. The Scheduled Reports > Add Report screen appears (Figure 11-14).

3. Type a name for the scheduled report in the Report name field.

4. Under the Schedule group, select from the following options:
   - **Daily**–select to generate a report every day
   - **Weekly, every**–select to generate a weekly report on the selected day of the week
   - **Monthly, every**–select to generate a monthly report on the First day, Last day, or 15th day, of the month

5. Select the time of day to generate the report from the Generate report at fields [hh] and [mm].

6. From the Content group, select from the following options:
   - **Scanning status summary**–displays a summary of the scan status
   - **Security risk scan report**–select to enable and choose from the following:
     - Security risk scan summary
     - Security risk types–select to display the security risk types in the report
     - Viruses/malware graph–from the drop down, choose whether the graph will display, hourly, daily, weekly or monthly data
     - Top viruses/malware–type the number of top viruses/malware to display in the report
     - Top viruses/malware violators– type the number of top viruses/malware violators to display in the report
     - Viruses/malware action summary–select to display a summary of the action taken on all viruses and malware contained in the report
     - Spyware/grayware graph–from the drop down, choose whether the graph will display, hourly, daily, weekly or monthly data
     - Top spyware/grayware–select to display the top spyware/grayware
     - Top spyware/grayware violators–select to display the top spyware/grayware violators
• **Virus/grayware action summary**—select to display a summary of the action taken on all viruses and grayware contained in the report

• **File blocking report**—select to enable and choose from the following:
  - **File blocking summary**—select to display in the report
  - **Blocked files graph**—from the drop down, choose whether the graph will display, hourly, daily, weekly or monthly data
  - **Top file types blocked**—type the number of top blocked file types to display in the report
  - **Top file names blocked**—type the number of top blocked file names to display in the report
  - **Top file extensions blocked**—type the number of top blocked file extensions to display in the report
  - **Top blocked file violators**—type the number of top blocked file violators to display in the report
  - **Top file blocking policy triggered**—type the number of top blocked file policy triggered to display in the report

• **Content filtering report**—select to enable and choose from the following:
  - **Content filtering summary**—select to display in the report
  - **Filtered files and Web content graph**—from the drop down, choose whether the graph will display, hourly, daily, weekly or monthly data
  - **Top filtered files/Web content violators**—type the number of these top violators you want to appear in the report
  - **Top content filtering policy triggered**—type the number of these top policies you want to appear in the report

• **Data protection report**—select to enable and choose from the following:
  - **Data protection summary**—select to display in the report
  - **Filtered files and Web content graph**—from the drop down, choose whether the graph will display, hourly, daily, weekly or monthly data
  - **Top filtered files/Web content violators**—type the number of these top violators you want to appear in the report
  - **Top data protection policy triggered**—type the number of these top policies you want to appear in the report
• **Top data protection template triggered**–type the number of these top templates you want to appear in the report

• **Unscannable file report**–select to enable and choose from the following:
  • **Unscannable file summary**–select to have this option appear in the report
  • **Unscannable file graph**–from the drop down, choose whether the graph will display, hourly, daily, weekly or monthly data

• **Web reputation report**–select to enable and choose from the following:
  • **Web reputation summary**–select to have this option appear in the report
  • **Suspicious URLs graph**–from the drop down, choose whether the graph will display, hourly, daily, weekly or monthly data
  • **Top malicious URLs**–type the number of top malicious URLs you want to appear in the report
  • **Top authors of Web content containing suspicious URLs**–type the number of top authors for this option you want to appear in the report

7. Under the **Delivery** group, type the email address where you want to have the reports delivered. Separate multiple email addresses using a semicolon.
8. Click **Save**.

![Scheduled Reports: Add Report](image)


**Tip:** To create a customized report, click **View Log Schema** to get a copy of the PortalProtect log schema.
Report Maintenance

Report Maintenance enables you to set the maximum number of reports to save for each of the following:

- **One-time reports**: specifies the maximum number of one-time reports PortalProtect will allow. One-time reports that exceed the set value will be purged, beginning with the oldest first.

- **Scheduled reports saved in each template**: specifies the maximum number of scheduled reports PortalProtect will allow. Scheduled reports that exceed the set value will be purged, beginning with the oldest first.

- **Report templates**: specifies the maximum number of report templates PortalProtect will allow. Report templates that exceed the set value will be purged, beginning with the oldest first.

<table>
<thead>
<tr>
<th>Report type</th>
<th>Maximum # to save for each type</th>
</tr>
</thead>
<tbody>
<tr>
<td>One-time reports</td>
<td>10</td>
</tr>
<tr>
<td>Scheduled reports saved in each template</td>
<td>10</td>
</tr>
<tr>
<td>Report templates</td>
<td>10</td>
</tr>
</tbody>
</table>

**FIGURE 11-15. Report Maintenance screen**
Getting Support and Contacting Trend Micro

This chapter discusses how to perform miscellaneous administrator tasks as well as how to get technical support.

In this chapter, you will find information about:

• *Contacting Trend Micro* starting on page 12-2
• *Contacting Technical Support* starting on page 12-3
• *TrendLabs* starting on page 12-4
• *Frequently Asked Questions (FAQ)* starting on page 12-5
Contacting Trend Micro

Trend Micro Incorporated has its world headquarters at:

Shinjuku MAYNDS Tower
2-1-1 Yoyogi, Shibuya-ku, Tokyo 151-0053 Japan.

In the United States, Trend Micro is located at:

10101 N. De Anza Blvd.
Cupertino, CA 95014-9985
Tel: +1-408-257-1500
Fax: +1-408-257-2003

Trend Micro has sales and corporate offices located in many cities around the globe. For global contact information, visit the Trend Micro Worldwide site:

http://www.us.trendmicro.com/us/about/contact/index.html

Note: The information on this Web site is subject to change without notice.

The Trend Micro Web site has a wealth of sales and corporate information available.
• Corporate information includes our company profile, international business office contacts, and partnering and alliance information.
• Sales information includes product evaluation information and trial downloads, reseller contacts, and virus research information.

Before Contacting Technical Support

While our basic technical support staff is always pleased to handle your inquiries, there are some things you can do to quickly find the answer you are seeking.
• Check the documentation: the manual and Online Help provide comprehensive information about PortalProtect. Search both documents to see if they contain your solution.

The documentation set for this product includes the following:
• Installation and Deployment Guide—This Guide helps you get “up and running” by introducing PortalProtect, assisting with installation planning and implementation, and also describes the main product functions. The latest version of the Guide is available in electronic form at:
   http://www.trendmicro.com/download/
• Administrator's Guide—This guide provides detailed information on how to configure PortalProtect.
• Online Help—The purpose of Online Help is to provide “how tos” for the main product tasks, usage advice, and field-specific information such as valid parameter ranges and optimal values. Online Help is accessible from the PortalProtect management console.
• Readme file—The Readme file contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, installation tips, known issues, and release history.
• Visit Knowledge Base at
   http://esupport.trendmicro.com/enterprise/default.aspx
   This site contains the most up-to-date information about all Trend Micro products. Other inquiries that were already answered are also posted and a dynamic list of the most frequently asked questions is also displayed.

• To speed up your problem resolution, when you contact our staff please provide as much of the following information as you can:
  • Product serial number
  • PortalProtect program, scan engine, pattern file, version number
  • OS name and version
  • Internet connection type
  • Exact text of any error message given
  • Steps to reproduce the problem

Contacting Technical Support

There is an abundance of security information and support available through the Web site. You can find the following:
• Downloadable product upgrades, component updates and hot fix patches
• Security advisories on the latest virus outbreaks
• Downloadable trial versions of Trend Micro products
• Expert advise on specific viruses in the wild and computer security in general
• An encyclopedia of computer security information, white papers, and virus statistics
• Free downloadable software for virus scanning, Web feeds, and security testing

To contact Trend Micro technical support:

1. Visit the following URL:
   http://esupport.trendmicro.com/default.aspx
2. Click the link for the region you want to contact and follow the instructions for contacting support in that region.

You can find Trend Micro contacts in the following regions:
• Asia/Pacific
• Australia and New Zealand
• Latin America
• United States and Canada.

TrendLabs

TrendLabs is Trend Micro’s global infrastructure of antivirus research and product support centers that provide up-to-the minute security information to Trend Micro customers.

The “virus doctors” at TrendLabs monitor potential security risks around the world, to ensure that Trend Micro products remain secure against emerging threats. The daily culmination of these efforts is shared with customers through frequent virus pattern file updates and scan engine refinements.

TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services. Dedicated service centers and rapid-response teams are located across the world to mitigate virus outbreaks and provide urgent support.

TrendLabs was one of the first antivirus research and support facilities to earn ISO 9002 certification for its quality management procedures. Trend Micro believes TrendLabs is the leading service and support team in the antivirus industry.
Frequently Asked Questions (FAQ)

This section covers some of the frequently asked questions and answers regarding PortalProtect features and functions.

Scanning

Content Filtering for Web Content or Web Reputation for Web Content is not working. Why?

Check the following:

a. Log on the PortalProtect Web console.

b. From the Summary screen, check whether Scan Web content is enabled. Click the icon in the Status column to enable or disable it. This option is a global hook switch for all the SharePoint servers in a farm.

c. If Web Content scanning is enabled and you create a new SharePoint list, you must first disable Scan Web content on the Summary Screen and then re-enable it. Otherwise, Web Content scanning for newly created SharePoint lists will be enabled 12 hours later.

d. From the Content Filtering or Web Reputation screens, ensure the scanning options are enabled. For Content Filtering, ensure that at least one rule is enabled.

Note: PortalProtect skips scanning files and Web content if the Web content author is the System account.

PortalProtect shows file “x.xxx” contains the following virus: “It has been blocked; final action is:[Block].” However, this file does not contain a virus. Why does the message tell me the file contains a virus?

Microsoft SharePoint Services provides this format and Trend Micro modifies the content within the quotation marks. Therefore, when the file is blocked by PortalProtect file blocking or content filtering it displays: contains the following virus, even though the file is not infected. To understand the message more clearly, disregard the message: contains the following virus, and note only the content inside the quotation marks.
I have not enabled “file blocking,” but some files are never uploaded or downloaded. Why?

Check SharePoint Services block list settings. SharePoint Server blocks files with the suffixes you specified. Use the SharePoint Services Central Management Page to modify the configuration.

To remove a file blocking configuration from SharePoint Services 2007:

1. Select the Operations tab.
2. Select Blocked file types from Security Configuration.
3. Check the extension names listed in the dialog box. Any extension name that is included will be blocked by SharePoint Services when it is uploaded or downloaded.

To remove a file blocking configuration from SharePoint Services 2010:

2. Select Define blocked file types from General Security configuration.
3. Check the extension names listed in the dialog box. Any extension name that is included will be blocked by SharePoint Services when it is uploaded or downloaded.

For MOSS 2007, it sometimes takes a long time to create a log file when I upload or download files. Why?

If you use an access method other than a Web browser, it may take a little longer to generate the log; sometimes more than one-minute. This also occurs if the action for the files is set to PASS. Additionally, when the log is generated, the Author and Location for the upload/download will appear as N/A.

When I upload file containing a virus to SharePoint Services, PortalProtect does not detect it. Why?

Check the following for SharePoint Services 2007:

- Check the SharePoint Services 2007 antivirus settings:
  a. Go to the SharePoint Central Administration page.
  b. Select the Operations tab.
  c. Select Configure antivirus settings in Security Configuration.
  d. If Scan documents on upload is disabled, PortalProtect will not perform a scan when the file is uploaded.
e. If **Scan documents on download** is disabled, SharePoint Services will not pass the file to PortalProtect when the file is downloaded.

f. If **Attempt to clean infected documents** is disabled, PortalProtect will only scan the file, and will not clean the file if it is infected by a virus.

Then, check the PortalProtect real-time Security Risk Scan options:

a. Log on the PortalProtect Web console and select **Security Risk Scan** from the left menu.

b. Select **Enable real-time security risk scan**.

**Check the following for SharePoint Services 2010:**

- Check the SharePoint Services 2010 antivirus settings:
  a. Go to the SharePoint Central Administration page.
  b. Select the **Security Configuration**.
  c. Select **Manage antivirus settings** from General Security Configuration.
  d. Same as SharePoint 2007.

**PortalProtect cannot block the files that exist in a compressed file. When an infected file exists in a compressed file, how can PortalProtect find it?**

Compressed files are regarded as a single file by PortalProtect for blocking operations. For Scan/Quarantine/Clean operation, PortalProtect deals with the files contained in the compressed file one by one. Therefore, infected files will not be omitted by PortalProtect.

**Does PortalProtect scan .zip and .lzh compressed files differently than other compressed files?**

PortalProtect uses VSAPI to deal with compressed files. VSAPI distinguishes compressed files by *true file type* rather than by file extension. That is, VSAPI can distinguish it even when a .zip file is renamed to .txt. VSAPI scans .zip and .lzh files in same way.

**Scans may be configured to have a primary and secondary action. Is the secondary action executed only after the primary action fails, or can PortalProtect execute both actions?**

The secondary action is executed only when the primary action fails. You can select a secondary action only when the primary action is **clean**.
Is there any record created when PortalProtect blocks a file?

Yes. When PortalProtect blocks a file, it sends out a notification (if you enabled that notification). When PortalProtect blocks a file in scanning, it creates a log.

What is considered to be an unscannable file?

Unscannable files are files that VSAPI cannot scan. For example, encrypted or password protected files.

Can PortalProtect scan encrypted files?

No. Encrypted files are an individual threat type covered in scan settings. Users can customize the action for encrypted files.

I can scan viruses from my PortalProtect server, but cannot update the engine and pattern file. Why?

It is possible that your Activation Code has expired. Please contact a reseller to renew your license. Refer to the Administrator’s Guide for more information.

What do compliance expression occurrences mean?

A compliance expression occurrence indicates that something from a document or Web content triggered an occurrence in a compliance expression. For example: A data protection policy contains a compliance expression and the number of occurrences is set to “3”. For this scenario, when occurrences of the compliance expression are less than “3”, documents and Web content posted to SharePoint sites will not trigger the corresponding data protection policy.

Why doesn’t Portal Protect have Data Protection for file or Data Protection for Web Content Filtering?

Carefully check your Activation Code (AC) for PortalProtect. The AC for PortalProtect Suite is the only code that provides these functionalities. If you change your AC from the PortalProtect Web console, you can log off and log on again to check your data protection related features.

How can I skip some of the file type scans performed by Content Filtering, Data Protection, and Web Reputation?

PortalProtect provides the following registry key to implement this capability:

- Name:FileTypeBypassMask
- Type:string
Description: This hidden key can be used to exclude specific file types for Data Protection, Content Filtering and Web Reputation file scans. When it is set to: “docx;pptx”, PortalProtect will skip docx and pptx files in Data Protection, Content Filter and Web Reputation file scans.

Note: Changes to this hidden key will take effect after you restart your service.

How can I customize the file scan size in Content Filtering, Data Protection and URL in documents?

PortalProtect provides the following registry key to implement this function:

- Name: FileSizeThreshold
- Type: REG_DWORD

Description: Data Protection, Content Filtering and Web Reputation File Scan Size Thresholds. This hidden key indicates the file scan threshold in Megabytes. The default value is 1000-MB. A key setting of zero (0) indicates no limitation.

Note: Changes to this hidden key will take effect after you restart your service.

Active Update

Why was the update unsuccessful from the Automatic Update server?

If your system requires a proxy to connect to Internet, check to ensure the settings are correct.

Does ActiveUpdate deliver the virus pattern file and the scan engine in the same way?

Yes. In fact, PortalProtect does not care about how ActiveUpdate downloads these files. PortalProtect sends the current engine/pattern version to ActiveUpdate module, ActiveUpdate checks if there is any more recent version available. It then downloads the files (in zip format), and unzips them automatically after a successful download. Finally, PortalProtect loads the new engine/pattern to use.
When PortalProtect uses an intranet source to receive updates, how is the central location updated?

ActiveUpdate supports downloading the latest components from an intranet machine. Put the update packages on that machine and enable the folder to be shared for other intranet machines to download.

How does the component package get updated?

After a successful download, ActiveUpdate extracts the packages and notifies PortalProtect to load new modules.

How do I update the engine or pattern using another PortalProtect server’s component package source?

Choose Updates > Download Source and select Other Update Source, then type the following URL:

http://<SERVERNAME>:<PORTNUMBER>/PortalProtect/activeupdate

where:

- **SERVERNAME** is the server hostname or IP address that contains the component package source.
- **PORTNUMBER** is the port number of PortalProtect Web console.

General Issues

Alert Issues

What the difference between the alert “PortalProtect service did not start successfully” and “PortalProtect service is unavailable?”

- **PortalProtect service did not start successfully**: occurs after an unsuccessful attempt to start the Trend Micro PortalProtect for Microsoft SharePoint Master Service.
- **PortalProtect service is unavailable**: occurs if the PortalProtect main service is already started and stops suddenly.
Why can I receive SNMP alerts but no email alerts?

PortalProtect sends email alerts to SMTP servers. If other alert types can be received, and only email alerts are missed, check that the SMTP server and port number are properly configured. If you have configured multiple email address to receive alerts, be sure to use a semicolon to separate them.

Notification Issues

I uploaded a file that triggered a file blocking rule and did not receive an email notification. Why?

Email notification settings for file blocking are set to provide consolidated notifications every two-hours by default. This means PortalProtect will send only one email notification for all files blocked within a two-hour time period. You can change this setting as per your requirement.

Other Issues

I am unable to query information from remote servers in Server Management console. What should I do?

- Make sure affected PortalProtect servers are all in the same farm.
- Make sure PortalProtect 2.1 is installed and started on your Web front end servers.
- Make sure the service PortalProtect_Master is started with the user who has local administrator and domain user privileges.
- Check the firewall of the remote PortalProtect servers and make sure port 139 and 445 for TCP are open.
- Make sure the following Windows services are running on remote servers:
  a. Remote Procedure Call (PRC)
  b. Server
  c. Workstation

I cannot automatically replicate configurations to other PortalProtect servers in the farm. Why?

Do the following:

- Ensure the check box Automatically replicate settings to other servers in Server Management is selected.
• Ensure the information for remote PortalProtect servers can be queried.
• Ensure PortalProtect licensing is current and fully activated (not trial or expired).
• Ensure all PortalProtect servers have same version.
• Ensure all PortalProtect servers are NOT in the OPP state (Outbreak Prevention Policy).

I cannot search AD user(s)/group(s) in PortalProtect. Why?
• PortalProtect only searches AD user(s)/group(s) from the current forest. Make sure the user exists in the current forest.
• PortalProtect only searches the AD user(s)/group(s) for the beginning characters in a search string.

Note: If your are searching for the string: “test”, then entering the characters “te” will produce a hit. However, a search using the characters: “es” will not produce a hit for the string “test”.

I cannot access the Web console. My browser displays a 404 error. What can I do to fix this problem?

Internet Explorer security settings on Windows 2003 does not include localhost or hostname as a trusted site when security level is set to high. Please add 127.0.0.1 or hostname to the list to solve this problem (http://127.0.0.1:16372).

1. Open Internet Explorer
2. Click Tools > Internet Options and select the Security tab.
3. Click Trusted Sites > Sites.
4. In the field for trusted zones, type the IP address: 127.0.0.1 or hostname.
5. Click Add.

I can access the PortalProtect Web console from the local server, but I cannot access it from a remote machine. Why?

Check the following:
• Whether there are network firewalls that block access to the PortalProtect Web Console through the HTTP (default is 16372) or HTTPS (default is 16373) port you specified during installation.
• Whether the Windows firewall on the PortalProtect server blocks the HTTP (default is 16372) or HTTPS (default is 16373) port you specified during installation.

Internet Explorer shuts down with a Data Execution Prevention alert when accessing the PortalProtect management console. What can I do to fix this problem?

• Select Tools > Internet Options > Advanced tab. Scroll to Security, and clear the checkbox Enable memory protection to help mitigate online attacks.

Which folders should I exclude for other Trend Micro Products?

The following four (3) folders should be excluded for other Trend Micro products:

• Backup folder
• Temp folder
• Sharedrespool folder

You can change the location of the Backup folders. The following indicates the default locations:

• Default Backup folder:
  Drive:\Program Files\Trend Micro\PortalProtect\storage\backup
• Temp folder:
  Drive:\Program Files\Trend Micro\PortalProtect\Temp
• Sharedrespool folder:
  Drive:\Program Files\Trend Micro\PortalProtect\SharedResPool

How does PortalProtect read a file to know if it has an extension?

When a user uploads a file to the SharePoint Server, SharePoint Server calls PortalProtect to detect whether the file has any virus in it. PortalProtect gets the file name and the extension from SharePoint Services.
After PortalProtect reads the extension, how does it determine whether there is a match; is there a database that contains all the user-configurations to which it compares the extensions?

All the user configurations are saved in a database. PortalProtect compares the file extension to see if there is a match.

Why does the Windows event log show: “Unable to connect to the PortalProtect database. Check your network settings and make sure the network connection between PortalProtect and the database server is available.”

PortalProtect monitors the database connection and will stop the PortalProtect service when it is unable to connect to it. When this happens, PortalProtect creates an entry in the Windows event log. PortalProtect will continue to monitor the database connection, and when the connection is restored, PortalProtect creates another entry in the Windows event log indicating that the database connection was restored.

The PortalProtect single sign on was unable to log on the Web console of a Windows 2003 server. Why?

If you use `mstsc` to connect to a remote server, try:

- Changing the connection mode to: `mstsc/admin` and re-connecting
- Or change the URL from localhost to hostname or use 127.0.0.1

What is the difference between the Smart Protection Server query order As Listed and Random?

The query order is only for available to the Smart Protection Server List. When the query order is As listed, PortalProtect will use the first available Smart Protection Server. When the query order is Random, PortalProtect will select from the available Smart Protection Server at random.

Accessing PortalProtect Web console is slow on Windows server 2008 R2 standalone. Why?

This occurs because IPv6 is enabled and there is only one line “::1 localhost” for localhost in the file “%windir%\system32\drivers\etc\hosts”. PortalProtect does not support IPv6. You can resolve this issue by adding the following new line in the previously mentioned file:

“127.0.0.1 localhost”
Using Control Manager with PortalProtect

Trend Micro Control Manager™ is a centralized system that unites Trend Micro antivirus products and services into a cohesive virus security and content management solution.

This chapter discusses the following topics:
- *Introducing Control Manager* on page A-2
- *Introducing the Control Manager Management Communication Protocol* on page A-3
- *Introducing Outbreak Prevention Services* on page A-4
- *Using Control Manager to Administrate PortalProtect* on page A-4
Introducing Control Manager

Trend Micro Control Manager is a central management console that manages Trend Micro and third-party antivirus and content security products and services at the gateway, mail server, file server, and corporate desktop levels. The Control Manager Web-based management console provides a single monitoring point for antivirus and content security products and services throughout the network.

Control Manager is available in Standard and Enterprise editions to better satisfy the needs of different enterprises.

- The Standard edition provides powerful management and configuration features that allow you to manage your corporate antivirus and content security.
- The Enterprise edition is for large enterprises and xSPs. This edition adds a variety of advanced features to the Standard edition—such as cascading console support and reporting functions.

Key Features

Key features of Control Manager include:

- Centralized management, which allows administrators to configure, monitor, and maintain Trend Micro software installed on the network from a single console—regardless of location or platform
- Flexible and scalable configuration, which simplifies the administration of a corporate virus and content security policy.
- A hierarchical structure for job delegation so administrators can determine access control—different users can be assigned separate access to individual branches of the hierarchy.
- Outbreak Prevention Services that provides proactive attack protection service and blocks malicious code by file name or specific file details while new pattern files are being developed that can detect and clean the new threat.
- Vulnerability Assessment, a service that assesses network security risk and scans for system vulnerabilities that are associated with known virus and malware attacks and recommends actions to take to eliminate the vulnerabilities.
• Agent-free Damage Cleanup Services (DCS), a comprehensive cleaning service that offers infection assessment and system repair for malicious remnants, such as Worms and Trojans. The service provides system administrators an easy approach for system cleaning without the use of any software locally installed on the client machines.

Using Control Manager with PortalProtect

Control Manager is a useful tool for organizations with multiple PortalProtect servers or for organizations using other Trend Micro products in addition to PortalProtect. The main advantages of using Control Manager with PortalProtect are:

• Centralized virus logging
• Powerful reporting and analysis options
• Faster response to virus outbreak prevention using Outbreak Prevention Services
• Centralized license management console
• Centralized distribution of components

Introducing the Control Manager Management Communication Protocol

The communication between PortalProtect and the Control Manager uses a new protocol called the Trend Micro Control Manager Management Communication Protocol (MCP). PortalProtect no longer supports the Trend Micro Management Infrastructure (TMI) protocol used by previous versions of PortalProtect and the Control Manager.

The Control Manager Agent can be registered after installing PortalProtect. PortalProtect supports single sign-on from the Control Manager. Access the PortalProtect product console directly from the Control Manager product console without typing a separate user name and password for the PortalProtect product console.
Introducing Outbreak Prevention Services

The Outbreak Prevention phase is the critical period when managed products have identified a virus outbreak and a pattern file is not yet available. During this crucial time, system administrators must endure a chaotic, time-consuming process of communication—often to global and decentralized groups within their organizations.

Outbreak Prevention Services delivers notification of new threats and continuous and comprehensive updates on system status as an attack progresses. The timely delivery of detailed virus data coupled with predefined, threat-specific action and scanning policies delivered immediately after a new threat identification allows enterprises to quickly contain viruses and prevent them from spreading.

Additionally, by centrally deploying and managing policy recommendations, Outbreak Prevention Services helps eliminate the potential for miscommunication, applies policies, and deploys information regarding attacks as they are occurring.

By providing automatic or manual download and deployment of policies via Trend Micro Control Manager, Outbreak Prevention Services import knowledge to critical access points on the network directly from experts at TrendLabs, Trend Micro’s global security research and support network.

This subscription-based service requires minimal up-front investment and provides enterprise-wide coordination and outbreak management via Trend Micro products, which reside across critical points on the network including the Internet gateway, mail server, file server, caching server, client, remote and broadband user, and third-party enterprise firewalls.

Using Control Manager to Administarte PortalProtect

Access the Control Manager management console to configure the PortalProtect managed product from any computer on the network.
Accessing the Control Manager Management Console

There are two ways to access the management console:

- Locally on the Control Manager server
- Remotely using any compatible browser

**Note:** PortalProtect 2.1 supports both TMCM 5.0 and TMCM 5.5 for remote access.

To access the management console locally from the Control Manager server:

1. Click **Start** > **Programs** > **Trend Micro Control Manager** > **Trend Micro Control Manager**.
2. Provide the **Username** and **Password** in the fields provided.
3. Click **Enter**.

To access the console remotely:

1. Type the following at your browser's address field to open the sign in page:
   
   For TMCM 5.0 or TMCM 5.5
   
   https://{host name}/webapp/login.aspx
   
   where {host name} is the Control Manager server’s fully qualified domain name (FQDN), IP address, or server name.
2. Type the **Username** and **Password** in the fields provided.
3. Click **Enter**.

Managing PortalProtect from the Control Manager Management Console

The Control Manager management console is a Web-based console that lets you use a compatible Web browser to administer the Control Manager network from any machine. For the list of compatible browsers, refer to the Control Manager Getting Started Guide or Online Help.

The Control Manager agent for PortalProtect accepts commands from the Control Manager server and instructs PortalProtect to perform them. For example, when you select **Tasks** > **Deploy scan engine** on the Control Manager management console, the Control Manager agent instructs PortalProtect to deploy the latest scan engine.
To manage PortalProtect from the management console:

1. Access the Control Manager management console.
2. From the main menu, click Products.
3. Under Product Directory, expand the PortalProtect folder to perform the following:

To check PortalProtect status:

1. From the working area, click Status, to update the currently displayed status.

   The Product Status screen displays the Product Information, Component Status, Operating System Information, Agent Environment Information, and Product License Information.

Viewing an Active Outbreak Prevention Policy

To view an active Outbreak Prevention Policy:

- Through the Control Manager management console > Services page
  a. Access the Control Manager management console.
  b. Click Services on the main menu.
  c. From the left menu under Services, click Outbreak Prevention.

This page automatically refreshes to ensure that the top threat and status information is current.

Create a Report Template

You can create custom report templates from within the Trend Micro Control Manager (TMCM). This section describes the steps required to create the following templates for PortalProtect:

- Top 10 Content Filtering Policies Triggered
- Top 10 File Blocking Policies Triggered
- Top 10 Filtered File/Web Content Authors
- Top 10 Blocked Files Authors
- Top 10 Authors of File/Web Content Containing Suspicious URLs
To create a new template:

1. Log on the TMCM Web console.

![Report Templates screen](image)

4. Type a name for the new template in the **Name** field, such as: Report Template for PortalProtect 2.1.

---

**Note:** After completing these steps, perform the steps in one of the five template procedures in this section to create that template. For example: **Top 10 Content Filtering Policies Triggered.**
To create bar chart for: "Top 10 Content Filtering Policies Triggered":

**Note:** Do To create a new template before performing this procedure.

1. Click **Bar Chart** in the **Working Panel**. You may have to click it three or four times to activate it.

![FIGURE A-6. Click Bar Chart from the Working Panel](image)

2. Drag and drop the bar chart to a blank row. The row will appear yellow in color *(Figure A-7)*.
3. After dropping the bar chart, click the **Edit** link (*Figure A-8*). The **Edit Bar Chart** > **Step 1: Data View** screen appears (*Figure A-9*).

---

**FIGURE A-7.** Blank row turns yellow during drag and drop

**FIGURE A-8.** Click Edit on the bar chart
FIGURE A-9. Edit Bar Chart > Step 1: Data View screen

5. Click Next >. The **Query Criteria > Step 2: Set Query Criteria** screen appears.
6. In the **Custom criteria** section, select **Filter type > is equal to > Content filter** from the three drop downs.

7. Click **Next >**. The **Edit Bar Chart > Step 3: Specify Design** screen appears.

*FIGURE A-12. Edit Bar Chart > Step 3: Specify Design screen*

8. Type the following in the **Name** field: "**Top 10 Content Filtering Policies Triggered.**"

9. From **Drag available Fields**, click and drag **Policy in violation** and drop it in the **Category Field**.
FIGURE A-13. Drag and drop Policy in Violation

10. From Drag available Fields, click and drag Policy Violation Detection Count and drop it in the Data Field.

11. Under Data Properties, type "Number of Detections" in the Value label field.
Using Control Manager with PortalProtect

12. Under **Category Properties**:
   - Type "Policy Name" in the **Label name** field
   - Select **Aggregation value**
   - Type 10 in the **Display top [xx] items** field
   - Select **Aggregate remaining items**

13. Click **Save**.

To create bar chart for: "Top 10 File Blocking Policies Triggered"

1. From the **Edit Report Template** screen, click **Insert row below** to add a new row.
2. Click **Bar Chart** in the **Working Panel**. You may have to click it three or four times to activate it.
3. Drag and drop the bar chart to a blank row. The row will appear yellow in color.
4. After dropping the bar chart, click the **Edit** link. The **Edit Bar Chart > Step 1: Data View** screen appears.
5. Select **Security Threat Information > Content Violation Information > Summary Information > Content Violation Policy Summary**.
6. Click **Next >**. The **Query Criteria > Step 2: Set Query Criteria** screen appears.
7. In the **Custom criteria** section, select **Filter type > is equal to > Attachment/File filter** from the three drop downs.

9. Type the following in the Name field: "Top 10 File Blocking Policies Triggered."

10. From Drag available Fields, click and drag Policy in violation and drop it in the Category Field.

11. From Drag available Fields, click and drag Policy Violation Detection Count and drop it in the Data Field.

12. Under Data Properties, type "Number of Detections" in the Value label field.

13. Under Category Properties:
   • Type "Policy Name" in the Label name field
   • Select Aggregation value
   • Type 10 in the Display top [xx] items field
   • Select Aggregate remaining items

14. Click Save.

To create bar chart for: "Top 10 Filtered Files/Web Content Authors":

1. From the Edit Report Template screen, click Insert row below to add a new row.
2. Click Bar Chart in the Working Panel. You may have to click it three or four times to activate it.
3. Drag and drop the bar chart to a blank row. The row will appear yellow in color.
4. After dropping the bar chart, click the Edit link. The Edit Bar Chart > Step 1: Data View screen appears.
5. Select Security Threat Information > Content Violation Information > Summary Information > Content Violation Sender/User in Violation Summary.
7. In the Custom criteria section, select Filter Type > is equal to > Content filter from the three drop downs.
9. Type the following in the Name field: "Top 10 Filtered Files/Web Content Authors."
10. From Drag available Fields, click and drag Sender/User in violation and drop it in the Category Field.
11. From **Drag available Fields**, click and drag **Policy Violation Detection Count** and drop it in the **Data Field**.

12. Under **Data Properties**, type "**Number of Detections**" in the **Value label** field.

13. Under **Category Properties**:
   - Type "**Violator**" in the **Label name** field
   - Select **Aggregation value**
   - Type 10 in the **Display top [xx] items** field

14. Click **Save**.

**To create bar chart for: "Top 10 Blocked Files Authors"**:

1. From the **Edit Report Template** screen, click **Insert row below** to add a new row.

2. Click **Bar Chart** in the **Working Panel**. You may have to click it three or four times to activate it.

3. Drag and drop the bar chart to a blank row. The row will appear yellow in color.

4. After dropping the bar chart, click the **Edit** link. The **Edit Bar Chart > Step 1: Data View** screen appears.

5. Select **Security Threat Information > Content Violation Information > Summary Information > Content Violation Sender/User in Violation Summary**.

6. Click **Next >**. The **Query Criteria > Step 2: Set Query Criteria** screen appears.

7. In the **Custom criteria** section, select **Filter Type > is equal to > Attachment/File filter** from the three drop downs.

8. Click **Next >**. The **Edit Bar Chart > Step 3: Specify Design** screen appears.

9. Type the following in the **Name** field: "**Top 10 Blocked Files Authors**."

10. From **Drag available Fields**, click and drag **Sender/User in violation** and drop it in the **Category Field**.

11. From **Drag available Fields**, click and drag **Policy Violation Detection Count** and drop it in the **Data Field**.

12. Under **Data Properties**, type "**Number of Detections**" in the **Value label** field.

13. Under **Category Properties**:
   - Type "**Violator**" in the **Label name** field
   - Select **Aggregation value**
• Type 10 in the **Display top [xx] items** field

14. Click **Save**.

**To create bar chart for: "Top 10 Authors of Files/Web Content Containing Suspicious URLs"**:

1. From the **Edit Report Template** screen, click **Insert row below** to add a new row.
2. Click **Bar Chart** in the **Working Panel**. You may have to click it three or four times to activate it.
3. Drag and drop the bar chart to a blank row. The row will appear yellow in color.
4. After dropping the bar chart, click the **Edit** link. The **Edit Bar Chart > Step 1: Data View** screen appears.
5. Select **Security Threat Information > Content Violation Information > Summary Information > Content Violation Sender/User in Violation Summary**.
6. Click **Next >.** The **Query Criteria > Step 2: Set Query Criteria** screen appears.
7. In the **Custom criteria** section, select **Filter Type > is equal to > URL reputation filter** from the three drop downs.
8. Click **Next >.** The **Edit Bar Chart > Step 3: Specify Design** screen appears.
9. Type the following in the **Name** field: **"Top 10 Authors of Files/Web Content Containing Suspicious URLs."**
10. From **Drag available Fields**, click and drag **Sender/User in violation** and drop it in the **Category Field**.
11. From **Drag available Fields**, click and drag **Policy Violation Detection Count** and drop it in the **Data Field**.
12. Under **Data Properties**, type **"Number of Detections"** in the **Value label** field.
13. Under **Category Properties**:
   • Type **"Violator"** in the **Label name** field
   • Select **Aggregation value**
   • Type 10 in the **Display top [xx] items** field
14. Click **Save**.
About Regular Expressions

Regular expressions are used to perform string matching. See the following tables for some common examples of regular expressions.

Note: Regular expressions are a powerful string matching tool. For this reason, it is recommended that an administrator who chooses to use regular expressions should be familiar and comfortable with regular expression syntax. Poorly written regular expressions can have a negative performance impact. Trend Micro’s recommendation is to start with simple regular expressions that do not use complex syntax. When introducing new rules, use the backup action and observe how PortalProtect applies your rule. When you are confident that the rule has no unexpected consequences, you can change the action.
**Counting and Grouping**

**TABLE B-2. Counting and Grouping**

<table>
<thead>
<tr>
<th>ELEMENT</th>
<th>WHAT IT MEANS</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>.</td>
<td>The dot or period character represents any character except new line character.</td>
<td>do. matches doe, dog, don, dos, dot, etc. d.r matches deer, door, etc.</td>
</tr>
<tr>
<td>*</td>
<td>The asterisk character means zero or more instances of the preceding element.</td>
<td>do* matches d, do, doo, dooo, dooooo, etc.</td>
</tr>
<tr>
<td>+</td>
<td>The plus sign character means one or more instances of the preceding element.</td>
<td>do+ matches do, doo, dooo, dooooo, etc. but not d</td>
</tr>
<tr>
<td>?</td>
<td>The question mark character means zero or one instances of the preceding element.</td>
<td>do?g matches dg or dog but not doog, doooog, etc.</td>
</tr>
<tr>
<td>( )</td>
<td>Parenthesis characters group whatever is between them to be considered as a single entity.</td>
<td>d(eer)+ matches deer or deer-eer or deereeer, etc. The + sign is applied to the substring within parentheses, so the regex looks for d followed by one or more of the grouping &quot;eer.&quot;</td>
</tr>
</tbody>
</table>
**Table B-2. Counting and Grouping**

<table>
<thead>
<tr>
<th>Element</th>
<th>What it means</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ]</td>
<td>Square bracket characters indicate a set or a range of characters.</td>
<td>d[aeiouy]+ matches da, de, di, do, du, dy, daa, dae, dai, etc. The + sign is applied to the set within brackets parentheses, so the regex looks for d followed by one or more of any of the characters in the set [aeioy]. d[A-Z] matches dA, dB, dC, and so on up to dZ. The set in square brackets represents the range of all upper-case letters between A and Z.</td>
</tr>
<tr>
<td>^</td>
<td>Carat characters within square brackets logically negate the set or range specified, meaning the regex will match any character that is not in the set or range.</td>
<td>d[^aeiouy] matches db, dc or dd, d9, d#. d followed by any single character except a vowel.</td>
</tr>
<tr>
<td>{ }</td>
<td>Curly brace characters set a specific number of occurrences of the preceding element. A single value inside the braces means that only that many occurrences will match. A pair of numbers separated by a comma represents a set of valid counts of the preceding character. A single digit followed by a comma means there is no upper bound.</td>
<td>da{3} matches daaa. d followed by 3 and only 3 occurrences of &quot;r;a&quot;. da{2,4} matches daa, daaa, daaaa, and daaaa (but not daaaaa). d followed by 2, 3, or 4 occurrences of &quot;r;a&quot;. da{4,} matches daaa, daaaa, daaaaa, etc. d followed by 4 or more occurrences of &quot;r;a&quot;.</td>
</tr>
</tbody>
</table>
## Character Classes (shorthand)

**TABLE B-3. Character Classes (shorthand)**

<table>
<thead>
<tr>
<th>EXAMPLE</th>
<th>WHAT IT MEANS</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>\d</td>
<td>Any digit character; functionally equivalent to [0-9] or [[:digit:]]</td>
<td>\d matches 1, 12, 123, etc., but not 1b7. One or more of any digit characters.</td>
</tr>
<tr>
<td>\D</td>
<td>Any non-digit character; functionally equivalent to [^0-9] or [^[[:digit:]]]</td>
<td>\D matches a, ab, ab&amp;, but not 1. One or more of any character but 0, 1, 2, 3, 4, 5, 6, 7, 8, or 9.</td>
</tr>
<tr>
<td>\w</td>
<td>Any &quot;word&quot; character. That is, any alphanumeric character; functionally equivalent to [<em>A-Za-z0-9] or [</em>[:alnum:]]</td>
<td>\w matches a, ab, a1, but not !&amp;. One or more upper- or lower-case letters or digits, but not punctuation or other special characters.</td>
</tr>
<tr>
<td>\W</td>
<td>Any non-alphanumeric character; functionally equivalent to [^_A-Za-z0-9] or [^[[:alnum:]]]</td>
<td>\W matches *, &amp;, but not ace or a1. One or more of any character but upper- or lower-case letters and digits.</td>
</tr>
<tr>
<td>\s</td>
<td>Any white space character; space, new line, tab, non-breaking space, etc.; functionally equivalent to [:space]</td>
<td>vegetable\s matches &quot;vegetable&quot; followed by any non-white space character. So the phrase &quot;I like vegetables in my soup&quot; would trigger the regex, but &quot;I like a vegetable in my soup&quot; would not.</td>
</tr>
<tr>
<td>\S</td>
<td>Any non-white space character; anything other than a space, new line, tab, non-breaking space, etc.; functionally equivalent to [^[[:space]]]</td>
<td>vegetable\S matches &quot;vegetable&quot; followed by any non-white space character. So the phrase &quot;I like vegetables in my soup&quot; would trigger the regex, but &quot;I like a vegetable in my soup&quot; would not.</td>
</tr>
</tbody>
</table>
## Character Classes

<table>
<thead>
<tr>
<th>Element</th>
<th>What it means</th>
<th>Example</th>
</tr>
</thead>
</table>
| [:alpha:] | Any alphabetic characters | .REG. [:alpha:] matches abc, def, xxx, but not 123 or @#$.
| [:digit:] | Any digit character; functionally equivalent to \d | .REG. [:digit:] matches 1, 12, 123, etc.
| [:alnum:] | Any "word" character. That is, any alphanumeric character; functionally equivalent to \w | .REG. [:alnum:] matches abc, 123, but not ~!@.
| [:space:] | Any white space character; space, new line, tab, non-breaking space, etc.; functionally equivalent to \s | .REG. (vegetable) [:space:] matches "vegetable" followed by any white space character. So the phrase "I like a vegetable in my soup" would trigger the regex, but "I like vegetables in my soup" would not.
| [:graph:] | Any characters except space, control characters or the like | .REG. [:graph:] matches 123, abc, xxx, >=", but not space or control characters.
| [:print:] | Any characters (similar with [:graph:]) but includes the space character | .REG. [:print:] matches 123, abc, xxx, >=", and space characters.
| [:cntrl:] | Any control characters (e.g. CTRL + C, CTRL + X) | .REG. [:cntrl:] matches 0x03, 0x08, but not abc, 123, !@#.
| [:blank:] | Space and tab characters | .REG. [:blank:] matches space and tab characters, but not 123, abc, !@#
| [:punct:] | Punctuation characters | .REG. [:punct:] matches ; : ? ! ~ @ # $ % & * 'r; "r; , etc., but not 123, abc
<table>
<thead>
<tr>
<th>ELEMENT</th>
<th>WHAT IT MEANS</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>[:lower:]</td>
<td>Any lowercase alphabetic characters (Note: 'r;Enable case sensitive matching’ must be enabled or else it will function as [:alnum:]))</td>
<td>.REG. [[:lower:]] matches abc, Def, sTress, Do, etc., but not ABC, DEF, STRESS, DO, 123, !@#.</td>
</tr>
<tr>
<td>[:upper:]</td>
<td>Any uppercase alphabetic characters (Note: 'r;Enable case sensitive matching’ must be enabled or else it will function as [:alnum:]))</td>
<td>.REG. [[:upper:]] matches ABC, DEF, STRESS, DO, Def, Stress, Do, etc., but not abc, 123, !@#.</td>
</tr>
<tr>
<td>[:xdigit:]</td>
<td>Digits allowed in a hexadecimal number (0-9a-fA-F)</td>
<td>.REG. [[:xdigit:]] matches 0a, 7E, 0f, etc.</td>
</tr>
</tbody>
</table>
### Pattern Anchor Regular Expressions

**TABLE B-5. Pattern anchor regular expressions**

<table>
<thead>
<tr>
<th>ELEMENT</th>
<th>WHAT IT MEANS</th>
<th>EXAMPLE</th>
</tr>
</thead>
</table>
| ^       | Indicates the beginning of a string. | ^
(notwithstanding) matches any block of text that began with "notwithstanding" So the phrase "notwithstanding the fact that I like vegetables in my soup" would trigger the regex, but "The fact that I like vegetables in my soup notwithstanding" would not. |
| $       | Indicates the end of a string. | $(notwithstanding) $ matches any block of text that ended with "notwithstanding" So the phrase "notwithstanding the fact that I like vegetables in my soup" would not trigger the regex, but "The fact that I like vegetables in my soup notwithstanding" would. |
## Escape Sequences Regular Expressions

### Table B-6. Escape sequences regular expressions

<table>
<thead>
<tr>
<th>ELEMENT</th>
<th>WHAT IT MEANS</th>
<th>EXAMPLE</th>
</tr>
</thead>
</table>
| \      | In order to match some characters that have special meaning in regular expression (for example, "+"). | (1) \.REG. \C\C\+\+ matches 'r;\C\C++'.
(2) \.REG. \* matches *.
(3) \.REG. \? matches ?. |
| \t     | Indicates a tab character. | (stress) \t matches any block of text that contained the substring "stress" immediately followed by a tab (ASCII 0x09) character. |
| \n     | Indicates a new line character. Note: Different platforms represent a new line character. On Windows, a new line is a pair of characters, a carriage return followed by a line feed. On Unix and Linux, a new line is just a line feed, and on Macintosh a new line is just a carriage return. | (stress) \n matches any block of text that contained the substring "stress" followed immediately by two new line (ASCII 0x0A) characters. |
### Table B-6. Escape sequences regular expressions

<table>
<thead>
<tr>
<th>Element</th>
<th>What it means</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>\r</td>
<td>Indicates a carriage return character.</td>
<td>(stress) \r matches any block of text that contained the substring &quot;stress&quot; followed immediately by one carriage return (ASCII 0x0D) character.</td>
</tr>
<tr>
<td>\b</td>
<td>Indicates a backspace character</td>
<td>(stress) \b matches any block of text that contained the substring &quot;r;stress&quot; followed immediately by one backspace (ASCII 0x08) character.</td>
</tr>
<tr>
<td>\xhh</td>
<td>Indicates an ASCII character with given hexadecimal code (where hh represents any two-digit hex value).</td>
<td>\x7E(\w){6} matches any block of text containing a &quot;word&quot; of exactly six alphanumeric characters preceded with a ~ (tilde) character. So, the words 'r;~ab12cd', 'r;~Pa3499' would be matched, but 'r;~oops' would not.</td>
</tr>
</tbody>
</table>
### A
- access control
  - about 11-32
  - authentication 11-33
  - permissions 11-34
  - what’s new version 2.1 1-6
- actions
  - possible 1-23
- activating PortalProtect 2-4
  - activation code 2-4
  - benefits received 2-4
  - from management console 2-5
- active action
  - about 1-22
- active update
  - using with PortalProtect 1-18
- activeupdate
  - about 1-18
- additional threats
  - types of threats 1-23
- advanced macro scan
  - about 3-13
- architecture
  - PortalProtect 1-12
- audience i-x
- automatic replication configuration
  - what’s new version 2.1 1-7

### B
- backup folder
  - manual scan 3-9
  - specifying 3-7–3-8, 3-11
- backup logs
  - deleting automatically 11-39
- benefits and capabilities
  - antivirus features 1-9
  - content filtering 1-9
  - data protection 1-9
  - easy management 1-10
  - fast and simple installation 1-9
  - file blocking 1-9
  - manual and scheduled scan 1-10
- PortalProtect 1-9
- quarantine 1-10
- updates 1-10

- Web reputation 1-9
  - blocked file logs
    - deleting automatically 11-39
  - blocking actions 5-12

### C
- central quarantine management 11-40
- compliance template
  - copy and delete existing 7-26
  - import/export 7-26
- compliance templates
  - adding/configuring 7-23
  - data protection 7-23
- compressed files
  - scanning 1-26
  - scheduled scan 10-5
- configuring
  - scheduled update 2-8
- configuring policies
  - data protection 7-1
- contacting technical support 12-3
- content filtering
  - about action settings 6-2
  - add policy, MOSS 2010/WSS 4.0 6-9
  - adding, MOSS 2007/WSS 3.0 6-18
  - benefits and capabilities 1-9
  - configuring 6-7
  - edit policy, MOSS 2007/WSS 3.0 6-27
  - edit policy, MOSS 2010/WSS 4.0 6-24
  - enable for document or Web content 6-8, 7-2
  - manual scan notifications 11-13
  - notifications 11-6
  - policy exceptions 6-3
  - scheduled scan notifications 11-21
  - what’s new version 2.0 1-2
- content filtering scans
  - what’s new version 2.0 1-4
- control manager
  - agent A-3
  - agent for ScanMail A-3
  - enterprise edition A-2
  - features A-2
  - manage ScanMail A-5
  - OPP A-6
  - outbreak prevention A-4
server A-2
standard edition A-2
using A-4
using ScanMail with A-2
controlling outbreaks 1-13
convention
document i-x
customized settings
about 1-22
custom scan actions 1-22

D
data protection
add policy, MOSS 2010/WSS4.0 7-2
adding, MOSS 2007/WSS 3.0 7-12
adding/configuring compliance templates 7-23
benefits and capabilities 1-9
compliance templates 7-23
configuring policies 7-1edit policy, MOSS 2007/WSS 3.0 7-20
edit policy, MOSS 2010/WSS 4.0 7-18
manual scan 9-20
notifications 11-7
scheduled scan 10-13
scheduled scan notifications 11-23
what’s new version 2.1 I-6
deleting automatically 11-39
document conventions i-x

E
easy management
benefits and capabilities 1-10
enabling real-time scan 3-4
encrypted and password protected files
about 1-25
encrypted or password protected files
types of threats 1-23
event logs
deleting automatically 11-39
event notifications 11-3
event tracking
what’s new 1-6
what’s new version 2.1 1-6

F
file blocking

I-2

about 5-1
actions for different scans 5-3
benefits and capabilities 1-9
configure scheduled scan 10-8
configuring action settings 5-12
configuring MOSS 2007/WSS 3.0 5-10
configuring MOSS 2010/WSS 4.0 5-4
configuring target settings 5-10
manual scan notifications 11-11
notifications 11-4
scheduled scan notifications 11-19

G
global approved list
about 1-7
available platforms 1-8
configuring 6-6
real-time 6-4
global notification
settings 11-2

H
how to 4-8

I
incremental updates
virus pattern file 1-18
installation
local and remote 1-4
installation enhancements
SharePoint versions 1-3
what’s new version 2.0 1-2
Windows versions 1-3
installaton enhancements
what’s new version 2.0 1-3
IntelliScan
about 1-18
intellitrap
about 1-21
ISO 9002 Certification-see TrendLabs 12-4

L
license agreement 1-27
logging
off 2-3
on 2-3
logs
delete automatically 11-38
delete manually 11-37
deleting automatically 11-39
maintenance 11-37
query 11-35
types of 11-35
working with 11-34

M
macro scanning
scheduled scan 10-5
macro viruses
about 1-25
macros
types of threats 1-23
maintenance
logs 11-37
maintenance agreement 1-27
renewing 1-28
management console A-5
management enhancements
quarantine management 1-5
real-time monitor 1-5
server management 1-5
single sign on (SSO) 1-5
what’s new version 2.0 1-3, 1-5
manual and scheduled scan
benefits and capabilities 1-10
manual scan 1-11, 3-8
configure content filtering 9-10
configure file blocking 9-10
configure macro scanning 9-5
configure Web reputation 9-10, 9-24
configuring 9-3
content filtering notifications 11-13
data protection 9-20
data protection notifications 11-14
notifications, file blocking 11-11
scan compressed files 9-4
security risk scan 9-6
Web reputation notifications 11-16
manual update 2-5
MS active directory integration
what’s new version 2.0 1-3

N
notifications
content filtering 11-6
data protection 11-7
file blocking 11-4
manual scan, security risk scan 11-10
outbreak alert 11-31
scheduled scan, content filtering 11-21
scheduled scan, Web reputation 11-25
security risk scan 11-3
Web reputation 11-8

O
online help 12-3
OPP. See Outbreak Prevention Policy
OPS. See Outbreak Prevention Services
outbreak alert 11-31
outbreak prevention A-4
outbreak prevention policy A-6
viewing A-6
outbreak prevention services A-4
outbreaks
controlling 1-13

P
pattern file
numbering 1-17
PortalProtect
architecture 1-12
benefits and capabilities 1-9
preface i-ix
protection
manual scan notifications 11-14

Q
quarantine
benefits and capabilities 1-10
maintenance 11-45
query 11-40
quarantine logs
deleting automatically 11-39
quarantine management
management enhancements 1-5
quarantine scan action 5-3
quarantined files
delete, restore, or download 11-44
query
quarantine 11-40

R
RBS support
what’s new version 2.1 1-6
readme file 12-3
real-time monitor
management enhancements 1-5
real-time scan 1-11
enabling 3-4
registering PortalProtect 2-3
how to 2-3
remote SQL installation
what’s new version 2.0 1-4
renewing maintenance agreement 1-28
report
maintenance 11-51
reports
create scheduled 11-51
maintenance 11-55
viewing and generating 11-47

S
scan
manual 1-11
real-time 1-11
scheduled 1-11
scan action
quarantine 5-3
scan engine updates
about 1-16
scan task
add or edit 10-2
scanning
compressed files 1-26
how it works 1-17
scheduled
update 2-8
scheduled scan 1-11, 3-11
about 10-1
add or edit a scan task 10-2
configure file blocking scan 10-8
configure macro scanning 10-5
configure Web reputation 10-15
configuring 10-2
data protection 10-13
data protection notifications 11-23
file blocking notifications 11-19
notifications 11-21
scan compressed files 10-5
security risk scan 10-6
security risk scan notifications 11-18
Web reputation notifications 11-25
scheduled update 2-8
security risk scan 3-7
about action settings 4-6
about target settings 4-3
action settings 4-6
background 4-1
before configuring 4-6
choose method 4-2
compressed files 4-8
configure action settings 4-7
enable or disable 4-3
file reputation 4-1
manual scan, notifications 11-10
notifications 11-3
scheduled scan 10-6
scheduled scan notifications 11-18
server
smart protection 1-20
server management
management enhancements 1-5
SharePoint environments
how viruses infect 1-10
SharePoint Servers
how PortalProtect protects 1-10
SharePoint users/groups integration
what’s new version 2.0 1-3
SharePoint versions
installation enhancements 1-3
single sign on (SSO)
management enhancements 1-5
smart protection
local and global 8-2
network 8-8
server 1-20
source 3-4
Index

sources 1-20
smart protection network 1-20
about 1-19
smart protection services
about 1-19
smart protection source
configuring 3-5
smart scan
what’s new version 2.1 1-5
sources
smart protection 1-20
specifying location 3-9
system events 11-26
configure PortalProtect events 11-29
configuring PortalProtect services 11-28

T
technical support
contacting 12-3
URL 12-4
Trend Micro
contact URL 12-2
Trend Micro control manager (TMCM) support 1-6
Trend Micro scan engine
about 1-15
TrendLabs 12-4
ture file types
about 1-20
types of threats 1-23
additional threats 1-23
encrypted or password protected files 1-23
macros 1-23
virus 1-23

U
unscannable files
about 1-26
update logs 11-39
updates
benefits and capabilities 1-10
updating
before you update 2-5
choosing components 2-7–2-8
pattern file 2-5
scan engine 2-5

scheduling 2-8
URLs
technical support 12-4
Trend Micro 12-2

V
viewing
Web management console 2-2
virus
types of threats 1-23
virus doctors-see TrendLabs 12-4
virus pattern file
about 1-16
incremental updates 1-18

W
Web management console
features 2-2
viewing 2-2
viewing on local server 2-2
viewing on remote server 2-2
viewing remote server 2-2
Web reputation
about 1-20
about action settings 8-7
about target settings 8-5
action settings 8-8
benefits and capabilities 1-9
choose source 8-3
configure target settings 8-6
document 1-6
enabling 8-4
manual scan notifications 11-16
notifications 8-8, 11-8
scheduled scan 10-15
scheduled scan notifications 11-25
Web reputation filtering
what’s new version 2.0 1-2
Web reputation for document
what’s new version 2.1 1-6
what’s new version 2.0 1-2
content filtering 1-2
content filtering scans 1-4
installation enhancements 1-2–1-3
local and remote installation 1-4
management enhancements 1-3, 1-5
MS active directory integration 1-3
remote SQL installation 1-4
SharePoint users/groups integration 1-3
Web reputation filtering 1-2
what’s new version 2.1 1-5
access control 1-6
automatic replication configuration 1-7
data protection 1-6
event tracking 1-6
RBS support 1-6
smart scan 1-5
Trend Micro control manager support 1-6
Web reputation for document 1-6
who should read this document
audience i-x
Windows versions
installation enhancements 1-3