TREND MICRO™

2.6 PortalProtect™

Administrator's Guide

Highly Effective Protection, Minimal IT Impact

for Microsoft™ SharePoint

Collaboration Security

Document Part No.: PPEM28661/190425

Release Date: March 2022

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

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp

Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that PortalProtect for SharePoint collects and provides detailed instructions on how to disable the specific features that feedback the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Notice:

https://www.trendmicro.com/privacy

Table of Contents

Preface

Chapter 1: Welcome to Trend Micro PortalProtect

Chapter 2: Getting Started with PortalProtect

Chapter 3: Configuring Scanning and Blocking

Chapter 4: Security Risk Scans

Chapter 5: File Blocking

Chapter 6: Content Filtering

Chapter 7: Data Loss Prevention

Chapter 8: Web Reputation

Chapter 9: Manual Scan

Chapter 10: Scheduled Scan

Chapter 11: Notifications, Alerts, Logs, and Reports

Chapter 12: Technical Support

Appendix A: Frequently Asked Questions (FAQs)

Appendix B: Using Control Manager with PortalProtect

Appendix C: About Regular Expressions

Index

Preface

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 on page x*
- *Audience on page x*
- *Document Conventions on page x*

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**: PDF documentation that can 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.

Note

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 Microsoft Windows SharePoint services. The Installation and Deployment Guide, Installation and Upgrade Guide, Administrator's Guide, and Online Help are designed for network administrators.

Document Conventions

The documentation uses the following conventions.

TABLE 1. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
Italics	References to other documents
`Monospace`	Sample command lines, program code, web URLs, file names, and program output
Navigation > **Path**	The navigation path to reach a particular screen For example, **File** > **Save** means, click **File** and then click **Save** on the interface
Note	Configuration notes
Tip	Recommendations or suggestions
Important	Information regarding required or default configuration settings and product limitations
WARNING!	Critical actions and configuration options

Chapter 1

Welcome to Trend Micro™ PortalProtect

Trend Micro™ PortalProtect™ is a server-based security solution for Microsoft SharePoint™ Server 2013/2016/2019/Subscription Edition. Trend Micro designed PortalProtect to provide protection against attacks from viruses and other security threats.

Trend Micro designed PortalProtect to integrate with Microsoft SharePoint Server and built it on proven enterprise security technology. It provides real-time background scanning of all content whenever it s checked-in, checked-out or published to a SharePoint Server. It also provides manual and scheduled scanning of content stored in the SharePoint Server 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 on page 1-3*

What's New

What's New in PortalProtect Version 2.6

This release of PortalProtect includes the following new features.

Feature	Description
SharePoint Server Subscription Edition Support	PortalProtect 2.6 provides full support for Microsoft SharePoint Server Subscription Edition.
Windows Server 2022 Desktop Experience Support	PortalProtect 2.6 supports Microsoft Windows Server 2022 Desktop Experience running Microsoft SharePoint Subscription Edition.
Windows Server 2022 Server Core Support	PortalProtect 2.6 supports Microsoft Windows Server 2022 Server Core running Microsoft SharePoint Subscription Edition.
SQL Server 2019 Support	PortalProtect 2.6 supports Microsoft SQL Server 2019 as the database server.
SharePoint Server 2019 Support	PortalProtect 2.6 provides full support for Microsoft SharePoint Server 2019.
Windows Server 2019 Support	PortalProtect 2.6 supports Microsoft Windows Server 2019 running Microsoft SharePoint Server.
SQL Server 2017 Support	PortalProtect 2.6 supports Microsoft SQL Server 2017 as the database server.
Using HTTPS to Connect to the Trend Micro ActiveUpdate Server	By default, PortalProtect 2.6 uses HTTPS to connect to the Trend Micro ActiveUpdate server.

Global Approved List

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

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 Loss Prevention
    - 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 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 URLs in files or 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 Server 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 you 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 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 Server 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 Server clients running applications such as Microsoft Office and Internet Explorer communicate with the SharePoint Server 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.

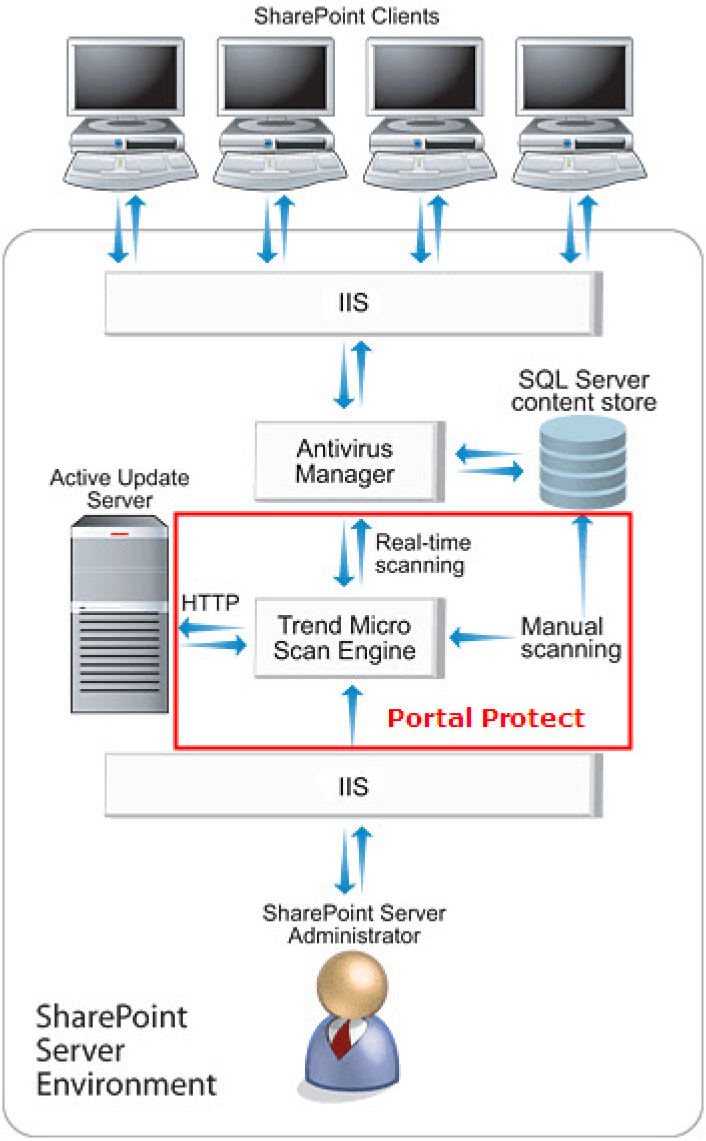


FIGURE 1-1. How PortalProtect interacts with SharePoint Server

Controlling Outbreaks

PortalProtect protects SharePoint Server 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:

- 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.
- 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.

- The traditional pattern file number is three-digits, in the format xxx, for example, 786.

- 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 protected information 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 1-22*.
- **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/.
- **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 1-22* and *About Unscannable Files on page 1-23*.

Possible Actions

During this scan	PortalProtect executes this action
Security Risk (real-time)	Clean, Block or Pass
File Blocking (real-time)	Block or Pass
Content Filtering (real-time)	Block or Pass

Web Reputation (real-time)	Block or Pass
Data Loss Prevention (real-time)	Block or Pass
Manual > Security Risk	Clean, Quarantine, Delete, Pass, or Rename
Manual > File Blocking	Quarantine, Delete, or Pass
Manual > Content Filtering	Quarantine, Delete, or Pass
Manual > Data Loss Prevention	Quarantine, Delete, or Pass
Scheduled > Security Risk	Clean, Quarantine, Delete, Pass, or Rename
Scheduled > File Blocking	Quarantine, Delete, or Pass
Scheduled > Content Filtering	Quarantine, Delete, or Pass
Scheduled > Data Loss Prevention	Quarantine, Delete, or Pass

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 1-1. Scan actions for encrypted and password protected files

During this scan...	PortalProtect executes this action...
Real-time	Block or Pass
Manual	Quarantine, Pass, Delete, or Rename
Scheduled	Quarantine, Pass, Delete, or Rename

Note

When PortalProtect quarantines encrypted, password protected, and Unscannable files, it reports to SharePoint Server 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 1-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 1-2. Scan actions for unscannable files

During this scan...	PortalProtect executes this action...
Real-time	Block or Pass
Manual	Quarantine, Pass, Delete, or Rename
Scheduled	Quarantine, Pass, Delete, or Rename

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

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 7.0 or above.

Procedure

1. Click the PortalProtect Management Console shortcut on the desktop.

2. Choose **Start** > **Programs** > **Trend Micro PortalProtect for Microsoft SharePoint** > **PortalProtect Management Console**.

   The Web Management Console appears.

3. Do either of the following:

   - **To view the Web Management Console for a local server**

     Type the following URL in the address box:

     `https://[localhost]:[port number]/PortalProtect/Login.htm`

     Note

     The port number depends on the user input during installation. The default port is 16373. SSL is enabled during installation, and there is no HTTP protocol for selection.

   - **To view the Web Management Console for a remote server:**

     Use Internet Explorer to access the following URL:

     `https://[server name]:[server port]/PortalProtect/Login.htm`

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

Main Elements

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.

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 either 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:

  https://olr.trendmicro.com/registration/us/en-us/login.aspx

  See *Technical Support on page 12-1*.

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, content filtering, and Web reputation; Using the PortalProtect suite AC, activates all the functions of thePortalProtect AC plus data loss prevention.

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 2-4*.

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 2-4*.
- If a proxy server handles Internet traffic on your network, you must type the proxy server information. See *Configuring Global Proxy Settings on page 2-8*.
- 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.

Selecting the Download Source

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

Important

The **Download Source** menu is only available when you upgrade PortalProtect from an older version where a download source other than the ActiveUpdate server is configured. For the fresh installation of PortalProtect, the **Download Source** menu is not available.

Procedure

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:

   https://<Server IP>:<Port>/PortalProtect/Activeupdate

3. Click **Save**.

   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
- Web Reputation filtering

Procedure

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 *Selecting the Download Source on page 2-6*.

Procedure

1. On the left menu, click **Updates** > **Manual**.

   The **Manual Update** screen appears.

2. Select the check box(es) of the component(s) you want to update.

3. Click **Update**.

   PortalProtect begins updating.

   Note

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

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 *Selecting the 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.

Procedure

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

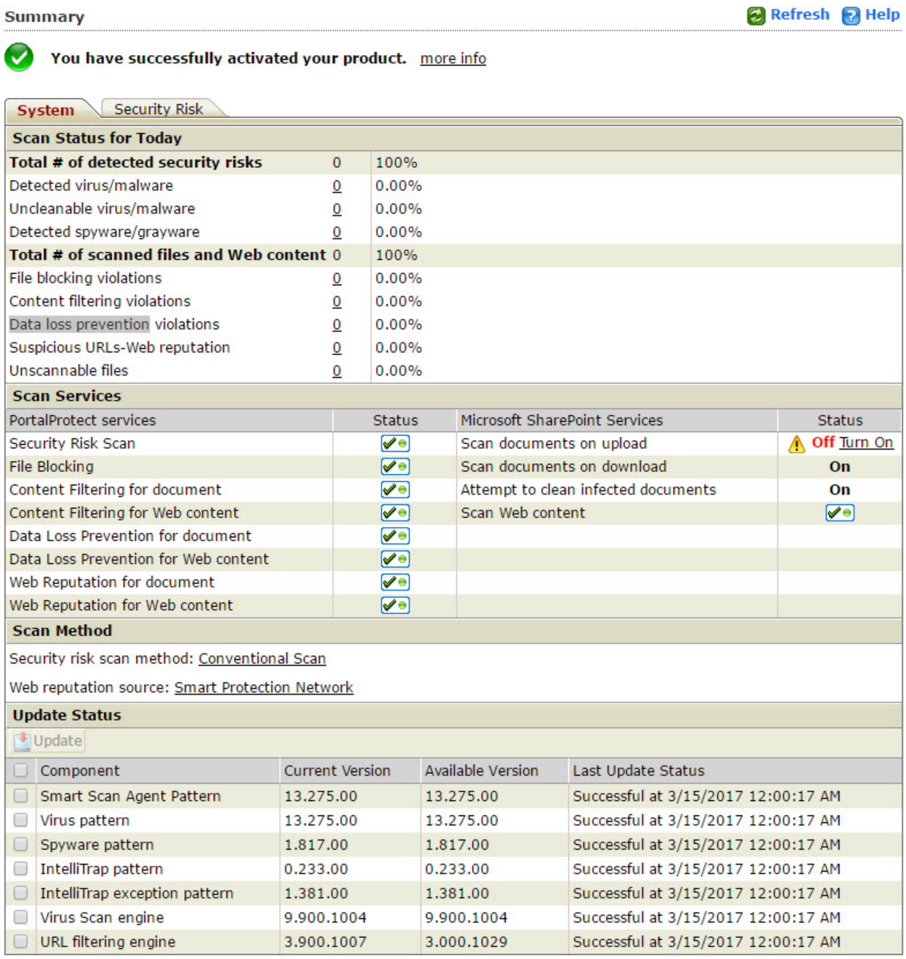
   Click **Reset** to change all download source settings to their default values.

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.



Summary

✓ You have successfully activated your product. more info

Scan Status for Today

Total # of detected security risks	0	100%
Detected virus/malware	0	0.00%
Uncleanable virus/malware	0	0.00%
Detected spyware/grayware	0	0.00%
Total # of scanned files and Web content	0	100%
File blocking violations	0	0.00%
Content filtering violations	0	0.00%
Data loss prevention violations	0	0.00%
Suspicious URLs-Web reputation	0	0.00%
Unscannable files	0	0.00%

Scan Services

PortalProtect services	Status	Microsoft SharePoint Services	Status
Security Risk Scan	✓	Scan documents on upload	⚠ Off Turn On
File Blocking	✓	Scan documents on download	**On**
Content Filtering for document	✓	Attempt to clean infected documents	**On**
Content Filtering for Web content	✓	Scan Web content	✓
Data Loss Prevention for document	✓		
Data Loss Prevention for Web content	✓		
Web Reputation for document	✓		
Web Reputation for Web content	✓		

Scan Method

Security risk scan method: Conventional Scan

Web reputation source: Smart Protection Network

Update Status

□	Component	Current Version	Available Version	Last Update Status
□	Smart Scan Agent Pattern	13.275.00	13.275.00	Successful at 3/15/2017 12:00:17 AM
□	Virus pattern	13.275.00	13.275.00	Successful at 3/15/2017 12:00:17 AM
□	Spyware pattern	1.817.00	1.817.00	Successful at 3/15/2017 12:00:17 AM
□	IntelliTrap pattern	0.233.00	0.233.00	Successful at 3/15/2017 12:00:17 AM
□	IntelliTrap exception pattern	1.381.00	1.381.00	Successful at 3/15/2017 12:00:17 AM
□	Virus Scan engine	9.900.1004	9.900.1004	Successful at 3/15/2017 12:00:17 AM
□	URL filtering engine	3.900.1007	3.000.1029	Successful at 3/15/2017 12:00:17 AM

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.

  Data loss prevention violations—total number of data loss prevention 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.

  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.

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 Loss Prevention for document**: click the icon in the status column to enable or disable data loss prevention for document.
- **Data Loss Prevention for Web content**: click the icon in the status column to enable or disable data loss prevention 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 Administration** > **Security** > **Antivirus** 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 *Choosing 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 *Choosing 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

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:

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

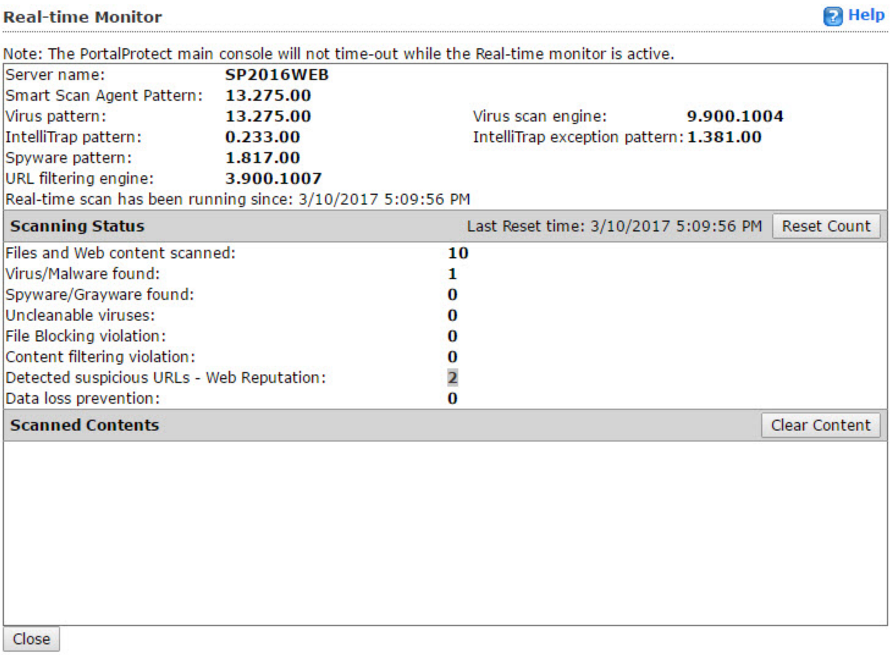
Scanning Status group

- 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 loss prevention

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



Real-time Monitor

Note: The PortalProtect main console will not time-out while the Real-time monitor is active.

Server name: **SP2016WEB**
Smart Scan Agent Pattern: **13.275.00**
Virus pattern: **13.275.00** Virus scan engine: **9.900.1004**
IntelliTrap pattern: **0.233.00** IntelliTrap exception pattern: **1.381.00**
Spyware pattern: **1.817.00**
URL filtering engine: **3.900.1007**
Real-time scan has been running since: 3/10/2017 5:09:56 PM

Scanning Status Last Reset time: 3/10/2017 5:09:56 PM

Files and Web content scanned: **10**
Virus/Malware found: **1**
Spyware/Grayware found: **0**
Uncleanable viruses: **0**
File Blocking violation: **0**
Content filtering violation: **0**
Detected suspicious URLs - Web Reputation: **2**
Data loss prevention: **0**

Scanned Contents

FIGURE 2-1. Real-time monitor screen

To view the real-time monitor:

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:

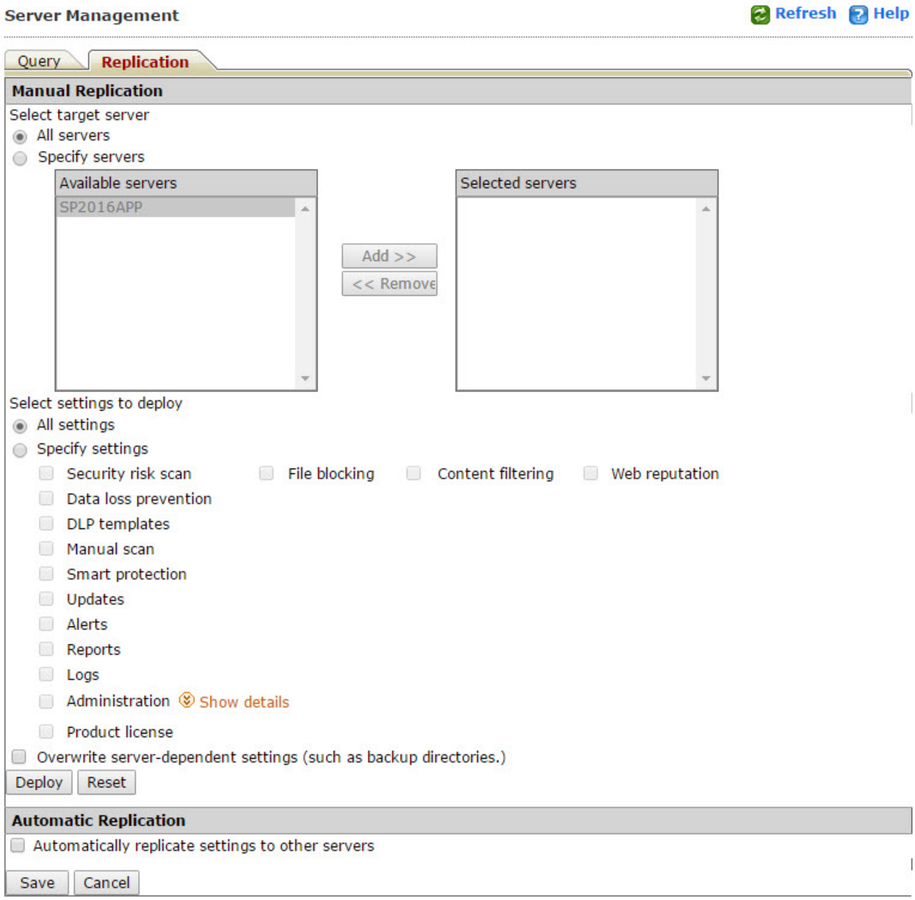
- **Pattern and engine version**: displays the current pattern/engine for each server
- **Scanning status**: displays the scanning status (On or Off) for Security Risk Scan, File Blocking, Content Filtering for files, Content Filtering for Web content, Data Loss Prevention for Files, Data Loss Prevention 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.

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.



Server Management

Manual Replication

Select target server

● All servers

○ Specify servers

Available servers: SP2016APP

Selected servers:

Select settings to deploy

● All settings

○ Specify settings

□ Security risk scan □ File blocking □ Content filtering □ Web reputation

□ Data loss prevention

□ DLP templates

□ Manual scan

□ Smart protection

□ Updates

□ Alerts

□ Reports

□ Logs

□ Administration

□ Product license

□ Overwrite server-dependent settings (such as backup directories.)

Automatic Replication

□ Automatically replicate settings to other servers

FIGURE 2-2. Server Management Replication tab

The following describes the available options:

- **Select target server**

  1. **All servers**: select to include all servers in the farm excluding the one being copied

2. **Specify servers**: select to choose specific target servers to send the replication

- Select settings to deploy

    1. **All Settings**: select to deploy all settings to the selected servers

    2. **Specify Settings**: Select to choose the following settings you want to deploy:

        Note

        These options are available only after selecting **Specify Settings**.

        - Security risk scan
        - File blocking
        - Content filtering
        - Web reputation
        - Data loss prevention
        - DLP templates
        - Manual scan
        - Smart protection
        - Updates
        - Alerts
        - Reports
        - Logs
        - Administration: Proxy, Notification settings, Access control, and Control manager
        - Product license
        - Overwrite server-dependent settings (such as backup directories). This option is enabled if **Security Risk Scan** or

Manual Scan is selected from **Specify Settings**. Can also be enabled when **All settings** is selected.

Note

The backup directories for **Real-time Security Risk Scan** and **Manual Scan for Security Risk** Scan have server dependent settings. See *Backing Up Files Before Taking Action on page 3-8* for more information.

- **Automatic Replication**

  Automatically replicate settings to other servers: select to automatically replicate settings to other servers

Chapter 3

Configuring Scanning and Blocking

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

- Real-time scan
- Manual scan
- Scheduled scan

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

- Security Risk Scan
- File Blocking
- Content Filtering
- Web Reputation
- Data Loss Prevention

Using advanced options, you can configure PortalProtect *for Microsoft SharePoint* to scan for malicious Macro code, and to block and scan compressed files.

In this chapter, you will find information about:

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 3-5*.

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.

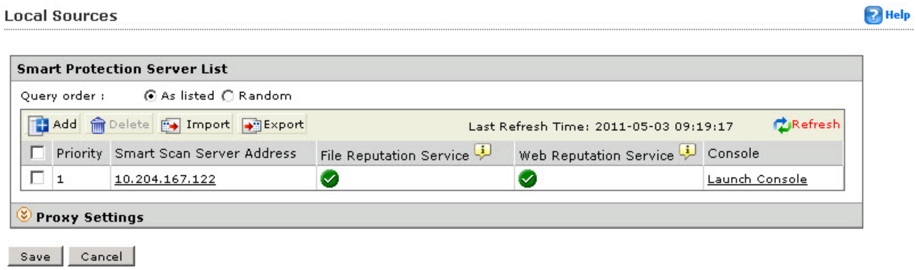
Note

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 11-32* for more information.



Query order : ● As listed ○ Random

Last Refresh Time: 2011-05-03 09:19:17

□	Priority	Smart Scan Server Address	File Reputation Service	Web Reputation Service	Console
□	1	10.204.167.122	✓	✓	Launch Console

FIGURE 3-1. Local Sources screen

Configuring Smart Protection Source

Procedure

1. Click **Smart Protection** > **Local Sources**. The **Local Sources** screen appears.

2. To add a smart protection server:

   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.

> **Note**
>
> 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**.

Backing Up 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:

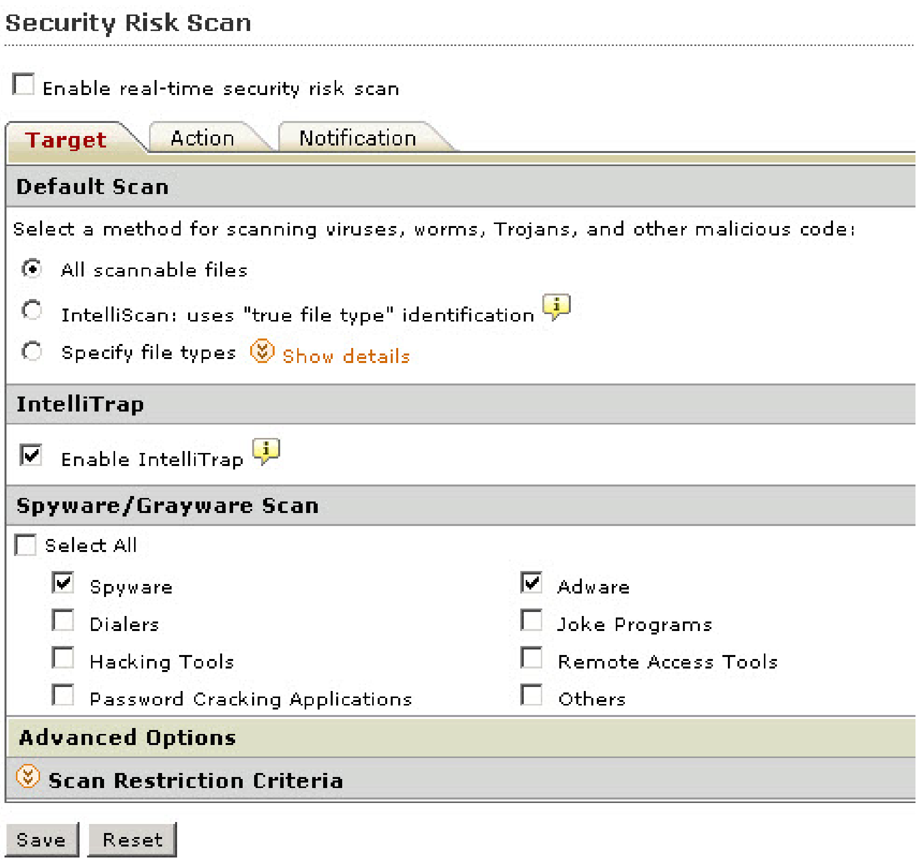
Specifying a Backup Folder for Security Risk Scan on page 3-8

Specifying a Backup Folder for Manual Scan on page 3-10

Specifying a Backup Folder for Scheduled Scan on page 3-13

Specifying a Backup Folder for Security Risk Scan

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



Security Risk Scan

□ Enable real-time security risk scan

Default Scan

Select a method for scanning viruses, worms, Trojans, and other malicious code:

● All scannable files

○ IntelliScan: uses "true file type" identification

○ Specify file types

IntelliTrap

☑ Enable IntelliTrap

Spyware/Grayware Scan

□ Select All

☑ Spyware

□ Dialers

□ Hacking Tools

□ Password Cracking Applications

☑ Adware

□ Joke Programs

□ Remote Access Tools

□ Others

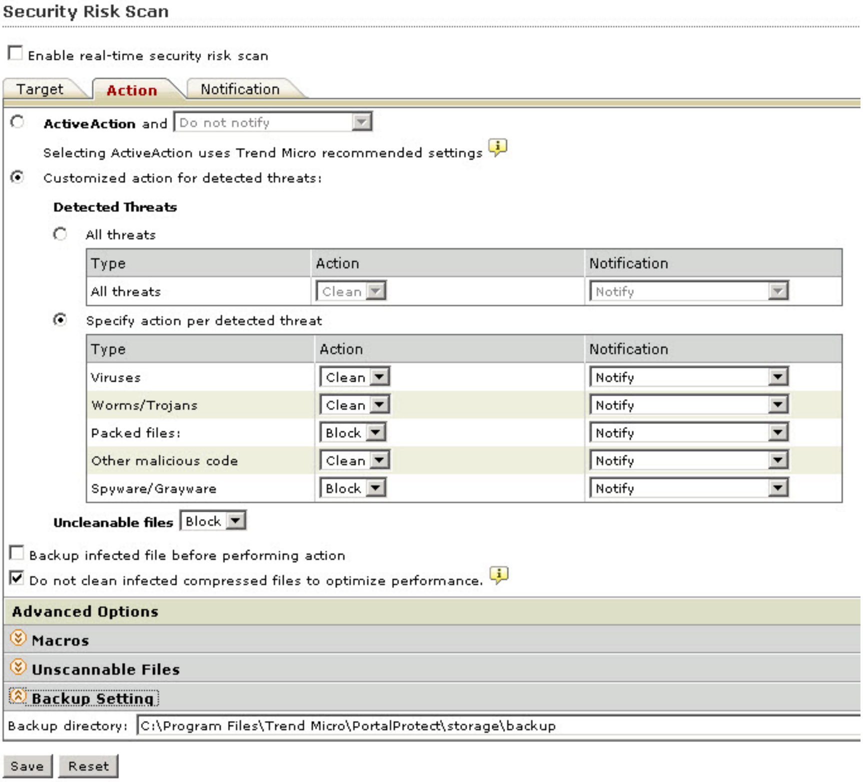
Advanced Options

FIGURE 3-2. Security risk scan screen (target tab)

Procedure

1. On the left menu, click **Security Risk Scan**. The **Security Risk Scan** screen appears.

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



Security Risk Scan

□ Enable real-time security risk scan

○ **ActiveAction** and Do not notify

Selecting ActiveAction uses Trend Micro recommended settings

● Customized action for detected threats:

Detected Threats

○ All threats

Type	Action	Notification
All threats	Clean	Notify

● Specify action per detected threat

Type	Action	Notification
Viruses	Clean	Notify
Worms/Trojans	Clean	Notify
Packed files:	Block	Notify
Other malicious code	Clean	Notify
Spyware/Grayware	Block	Notify

Uncleanable files Block

□ Backup infected file before performing action

☑ Do not clean infected compressed files to optimize performance.

Advanced Options

Macros

Unscannable Files

Backup Setting

Backup directory: C:\Program Files\Trend Micro\PortalProtect\storage\backup

FIGURE 3-3. Security risk scan (action tab)

3. 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.

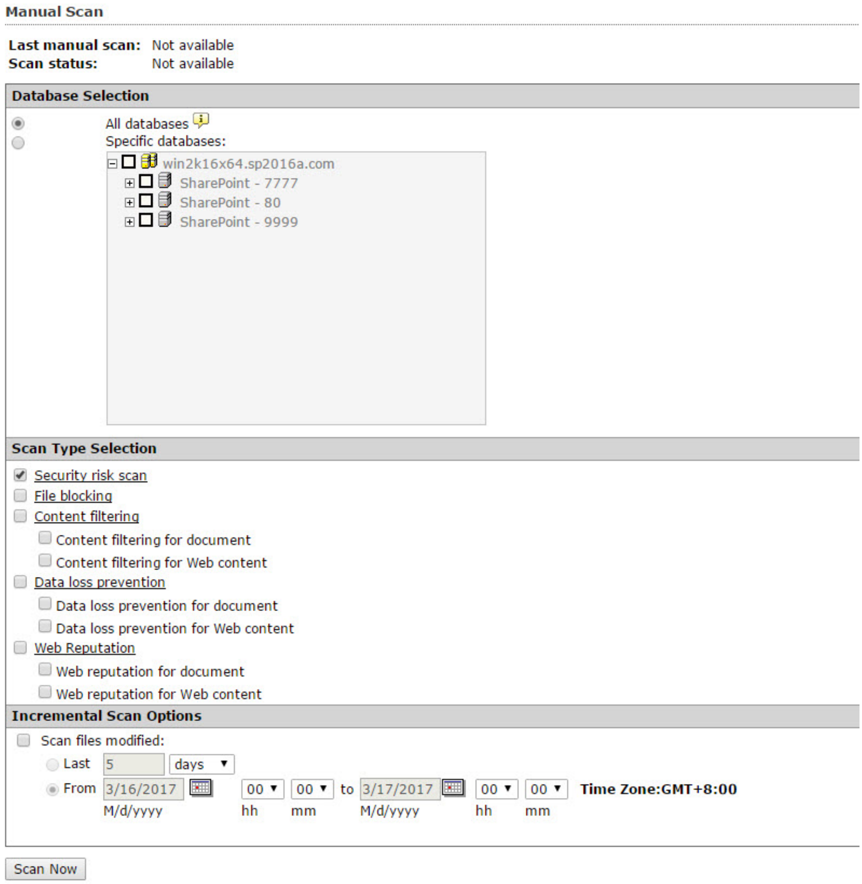
Specifying a Backup Folder for Manual Scan

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

Procedure

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.



Manual Scan

Last manual scan: Not available
Scan status: Not available

Database Selection

● All databases
○ Specific databases:

⊟ □ win2k16x64.sp2016a.com
⊞ □ SharePoint - 7777
⊞ □ SharePoint - 80
⊞ □ SharePoint - 9999

Scan Type Selection

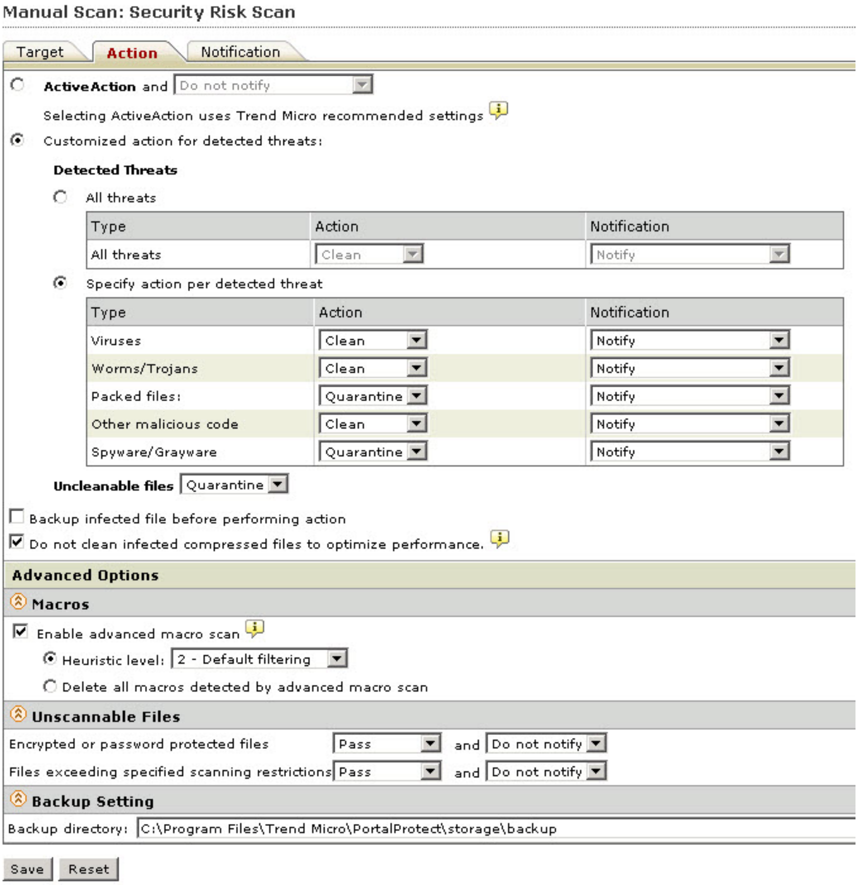
☑ Security risk scan
□ File blocking
□ Content filtering
□ Content filtering for document
□ Content filtering for Web content
□ Data loss prevention
□ Data loss prevention for document
□ Data loss prevention for Web content
□ Web Reputation
□ Web reputation for document
□ Web reputation for Web content

Incremental Scan Options

□ Scan files modified:
○ Last 5 days
● From 3/16/2017 (M/d/yyyy) 00 (hh) 00 (mm) to 3/17/2017 (M/d/yyyy) 00 (hh) 00 (mm) **Time Zone:GMT+8:00**

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.



Manual Scan: Security Risk Scan

○ **ActiveAction** and Do not notify

Selecting ActiveAction uses Trend Micro recommended settings

● Customized action for detected threats:

Detected Threats

○ All threats

Type	Action	Notification
All threats	Clean	Notify

● Specify action per detected threat

Type	Action	Notification
Viruses	Clean	Notify
Worms/Trojans	Clean	Notify
Packed files:	Quarantine	Notify
Other malicious code	Clean	Notify
Spyware/Grayware	Quarantine	Notify

Uncleanable files Quarantine

□ Backup infected file before performing action

☑ Do not clean infected compressed files to optimize performance.

Advanced Options

Macros

☑ Enable advanced macro scan

● Heuristic level: 2 - Default filtering

○ Delete all macros detected by advanced macro scan

Unscannable Files

Encrypted or password protected files	Pass	and	Do not notify
Files exceeding specified scanning restrictions	Pass	and	Do not notify

Backup Setting

Backup directory: C:\Program Files\Trend Micro\PortalProtect\storage\backup

FIGURE 3-4. 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.

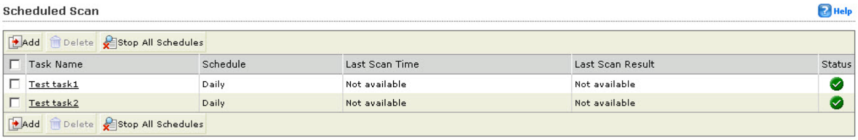
Specifying a Backup Folder for Scheduled Scan

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

Procedure

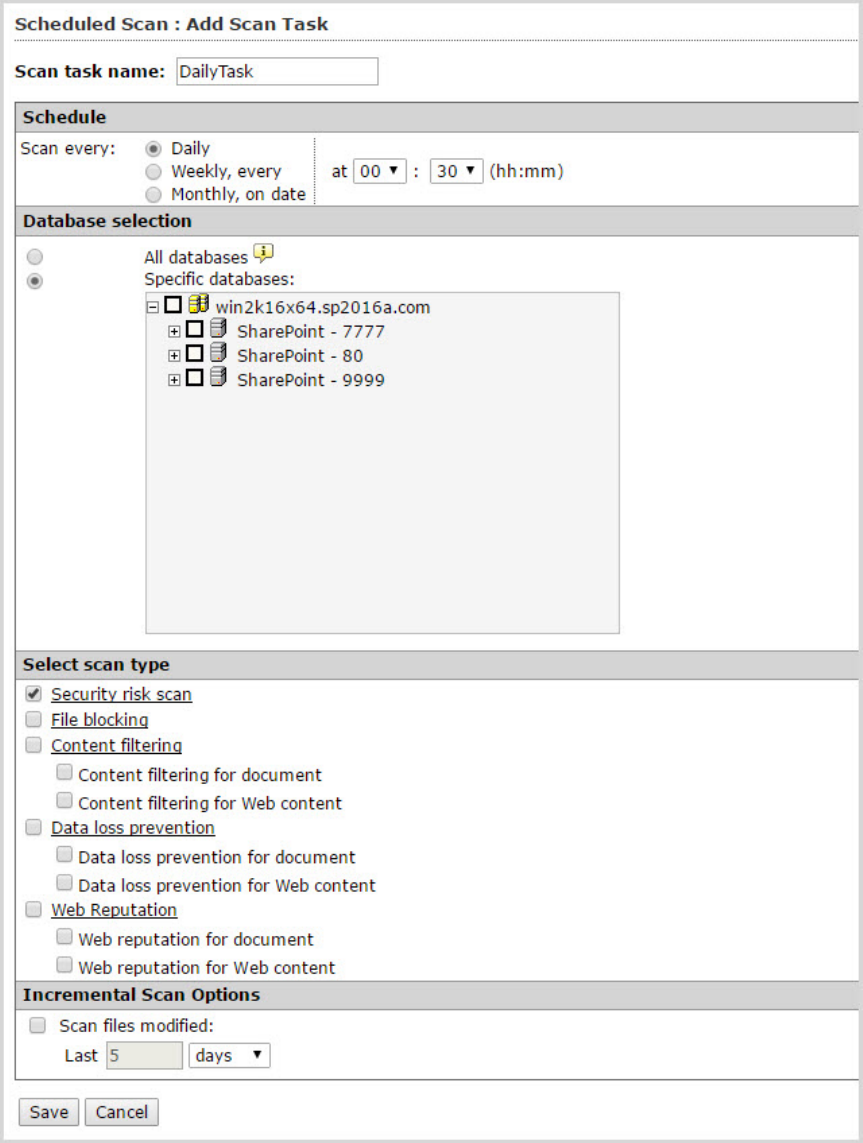
1. On the left menu, click **Scheduled Scan**. The **Scheduled Scan** screen then appears.

2. Add a new scheduled scan, or click an existing scheduled scan in the **Task Name** column.



□	Task Name	Schedule	Last Scan Time	Last Scan Result	Status
□	Test task1	Daily	Not available	Not available	✓
□	Test task2	Daily	Not available	Not available	✓

3. Depending on your previous selection, the **Scheduled Scan: Add Scan Task** or **Scheduled Scan: Edit Scan Task** screen appears.



Scheduled Scan : Add Scan Task

Scan task name: DailyTask

Schedule

Scan every: ● Daily ○ Weekly, every ○ Monthly, on date | at 00 ▼ : 30 ▼ (hh:mm)

Database selection

○ All databases

● Specific databases:

- ⊟ □ win2k16x64.sp2016a.com
  - ⊞ □ SharePoint - 7777
  - ⊞ □ SharePoint - 80
  - ⊞ □ SharePoint - 9999

Select scan type

- ☑ Security risk scan
- □ File blocking
- □ Content filtering
  - □ Content filtering for document
  - □ Content filtering for Web content
- □ Data loss prevention
  - □ Data loss prevention for document
  - □ Data loss prevention for Web content
- □ Web Reputation
  - □ Web reputation for document
  - □ Web reputation for Web content

Incremental Scan Options

□ Scan files modified:

Last 5 days ▼

FIGURE 3-5. 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:

- *Configuring Macro Scanning Options for Real-time Security Risk Scan on page 4-6*
- *Configuring Macro Scanning Options for Manual Scan on page 9-7*

- *Configuring Macro Scanning Options for Scheduled Scan on page 10-6*

Chapter 4

Security Risk Scans

This chapter 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.

In this chapter, you will find information about:

File Reputation

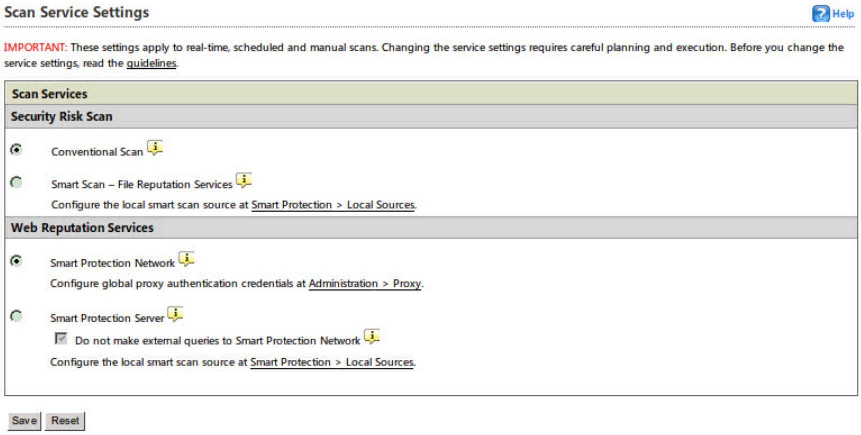
File reputation technology from Trend Micro checks the reputation of each file against an extensive in-the-cloud database before permitting user access. Since the malware information is stored in the cloud, it is available instantly to all users. High performance content delivery networks and local caching 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.

Choosing a Security Risk Scan Method

Procedure

1. Click **Smart Protection** > **Scan Service Settings** from the left menu.

   The **Scan Service Settings** screen appears.



Scan Service Settings

IMPORTANT: These settings apply to real-time, scheduled and manual scans. Changing the service settings requires careful planning and execution. Before you change the service settings, read the guidelines.

Scan Services

Security Risk Scan

● Conventional Scan

○ Smart Scan – File Reputation Services

Configure the local smart scan source at Smart Protection > Local Sources.

Web Reputation Services

● Smart Protection Network

Configure global proxy authentication credentials at Administration > Proxy.

○ Smart Protection Server

☑ Do not make external queries to Smart Protection Network

Configure the local smart scan source at Smart Protection > Local Sources.

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).

  Note

  See *Choosing a Web Reputation Source on page 8-3* for information on how to configure these settings.

3. Click **Save**.

Enabling or Disabling a Real-time Security Risk Scan

Procedure

1. On the left menu, click **Security Risk Scan**.

   The **Security Risk Scan** screen appears.

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 1-15*.
- **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.

Configuring Security Risk Scan: Target Settings

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

Procedure

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 the 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 1-100-MB.

If this option is not selected, files greater than 1-GB will not be scanned.

7. Under **Do not scan compressed files if**, type values according to the following:

   - **Decompressed file count exceeds [xxxxx]**—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**.

Configuring 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:

Procedure

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.

Procedure

1. Choose whether to set up a backup folder.

   When you set up a backup folder, PortalProtect sends a copy of the file to the backup directory before it performs the configured actions. See *Specifying a Backup Folder for Security Risk Scan on page 3-8*.

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 1-18*.

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.

Procedure

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**

     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**

      a. Block or Pass

         and...

b. Notify or Do not notify

- **Files exceeding specified scanning restrictions**

  a. Block or Pass

  and...

  b. Notify or Do not notify

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

13. Click **Save**.

> **Note**
>
> See *Configuring Security Risk Scan Notifications on page 11-4* for details on how to configure the notification settings.

Scanning 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 ScanAction** tab.

Procedure

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 1-100-MB.

4. Under **Do not scan compressed files if**, type values according to the following:

   - **Decompressed file count exceeds [xxxxx]**—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**.

Chapter 5

File Blocking

This chapter describes how to 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.

Topics include:

- *About File Blocking on page 5-2*
- *About File Blocking Action Settings on page 5-2*
- *Configuring File Blocking on page 5-3*
- *About Available File Types on page 5-15*

About 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 on page 11-42* for more information.

Possible Actions

During this scan	PortalProtect executes this action
File Blocking (real-time)	Block or Pass
Manual > File Blocking	Quarantine, Delete, or Pass
Scheduled > File Blocking	Quarantine, Delete, or Pass

Configuring File Blocking

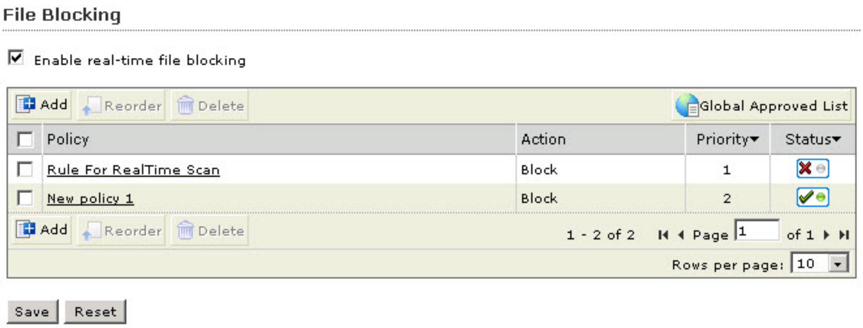
This section provides the information required to manage and configure File Blocking for PortalProtect. You can manage the following settings from the file blocking main screen:

- Enable or disable real-time file blocking
- 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

Procedure

1. On the left menu, click **File Blocking**.

The **File Blocking** screen appears.



File Blocking

☑ Enable real-time file blocking

□	Policy	Action	Priority▾	Status▾
□	Rule For RealTime Scan	Block	1	✗
□	New policy 1	Block	2	✓

1 - 2 of 2 Page 1 of 1

Rows per page: 10

2. Select **Enable real-time file blocking**.

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 File Blocking Policy

This section describes the steps required to add a new File Blocking policy.

Procedure

1. On the left menu, click **File Blocking**. The **File Blocking** screen appears.

2. Click **Add**. The **File Blocking: Add Policy > Step 1: Specify Rules** screen appears.

Step 1. File Blocking: Add Policy > Specify Rules

Procedure

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:

    a. 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.

    b. 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.

3. Select **Block compressed files containing the specific file types or names** to block compressed files if they contain any specified file types or names.

4. Select **Block OLE containers containing the specific file types or names**; click **Show details** to expand the content:

a. Select **Microsoft documents** to limit the Object Linking and Embedding (OLE) containers to Microsoft document files.

b. Select **Adobe Portable Document Format (.pdf)** to limit the OLE containers to PDF files.

c. Set the maximum number of OLE layers supported for blocking.

5. Click **Next**. The **File Blocking: Add Policy > Step 2: Exceptions** screen appears.

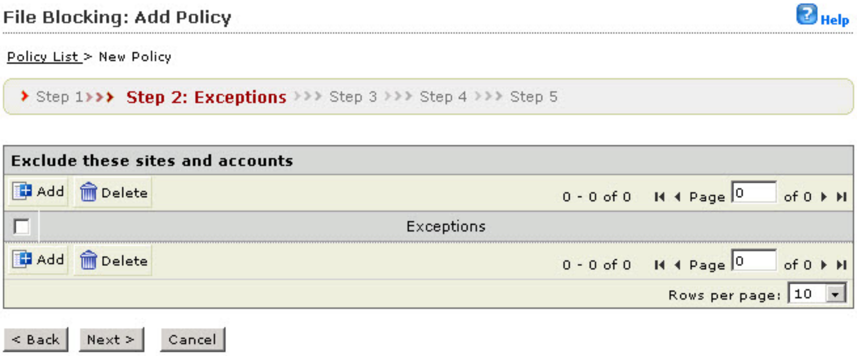
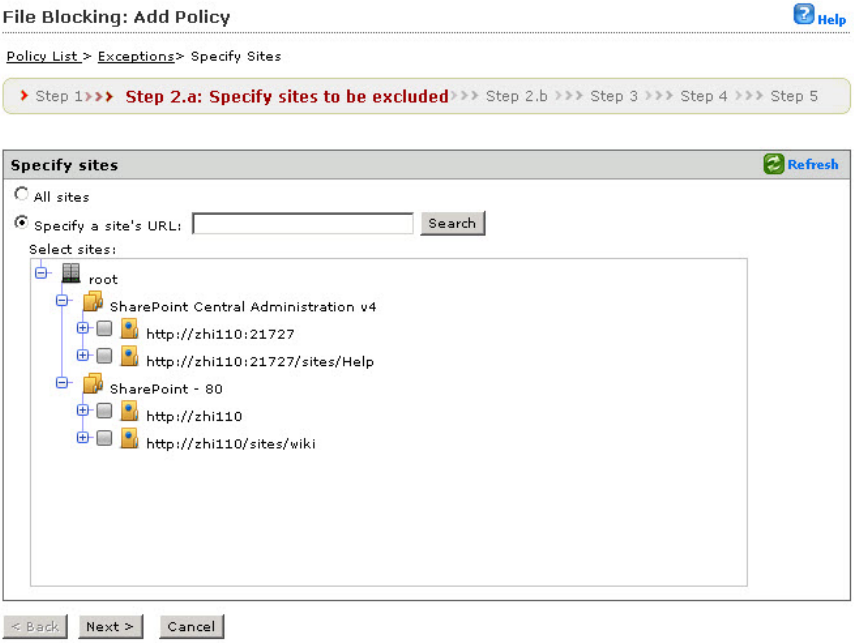


FIGURE 5-1. File Blocking: Add Policy > Step 2: Exceptions screen

Step 2. File Blocking: Add Policy > Exceptions

Procedure

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



File Blocking: Add Policy

Policy List > Exceptions> Specify Sites

› Step 1››› Step 2.a: Specify sites to be excluded››› Step 2.b ››› Step 3 ››› Step 4 ››› Step 5

Specify sites

○ All sites

● Specify a site's URL: [ ] Search

Select sites:

- root
  - SharePoint Central Administration v4
    - □ http://zhi110:21727
    - □ http://zhi110:21727/sites/Help
  - SharePoint - 80
    - □ http://zhi110
    - □ http://zhi110/sites/wiki

FIGURE 5-2. File Blocking: Add Policy > Step 2.a: Specify sites to be excluded screen

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 >**.

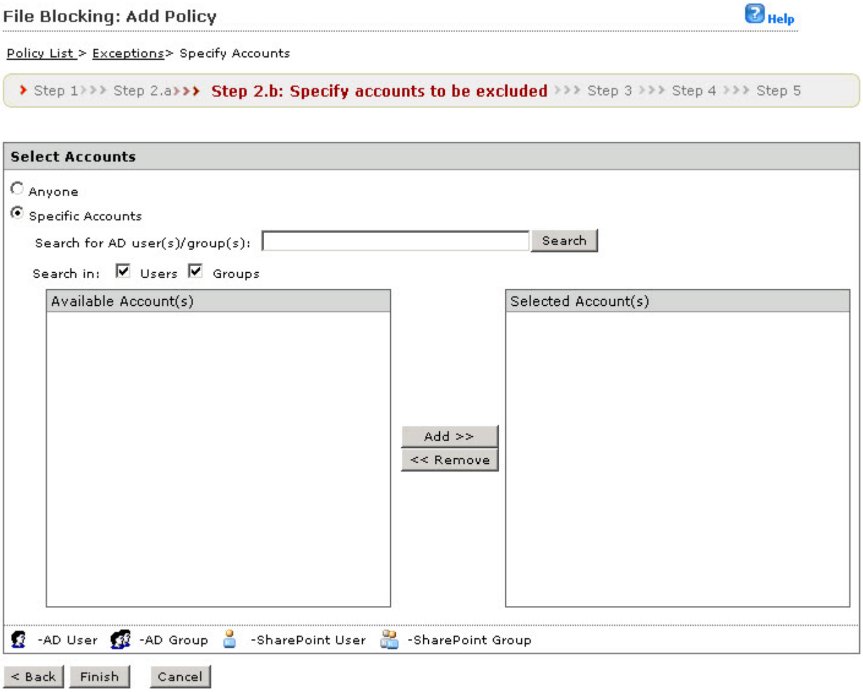
   - If you choose **Specify a site's URL...**

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.



File Blocking: Add Policy

Policy List > Exceptions> Specify Accounts

› Step 1››› Step 2.a››› **Step 2.b: Specify accounts to be excluded** ››› Step 3 ››› Step 4 ››› Step 5

Select Accounts

○ Anyone

● Specific Accounts

Search for AD user(s)/group(s): [   ] Search

Search in: ☑ Users ☑ Groups

Available Account(s)

Add >>

<< Remove

Selected Account(s)

-AD User -AD Group -SharePoint User -SharePoint Group

< Back Finish Cancel

FIGURE 5-3. File Blocking: 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.

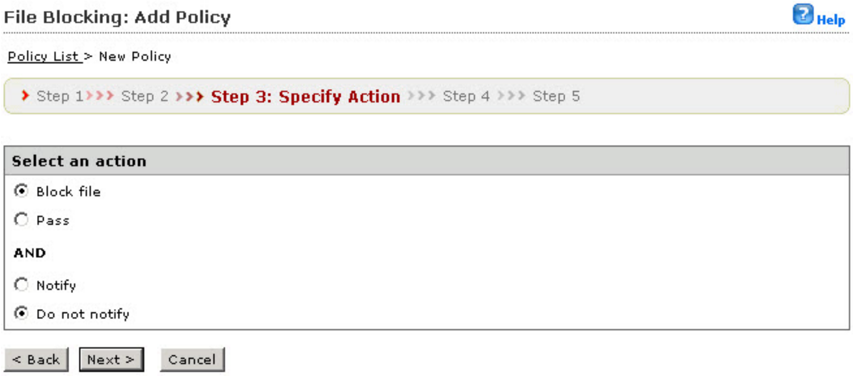
7. Click **Search**. Successful search results will then display in the **Available Account(s)** window.

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. After choosing your options, click **Finish**. The **File Blocking: Add Policy > Step 2: Exceptions** screen appears with the newly added exceptions.

11. Click **Next >**. The **File Blocking: Add Policy > Step 3: Specify Action** screen appears.



File Blocking: Add Policy

Policy List > New Policy

› Step 1 ››› Step 2 ››› **Step 3: Specify Action** ››› Step 4 ››› Step 5

Select an action

● Block file

○ Pass

AND

○ Notify

● Do not notify

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

Step 3. File Blocking: Add Policy > Specify Action

Procedure

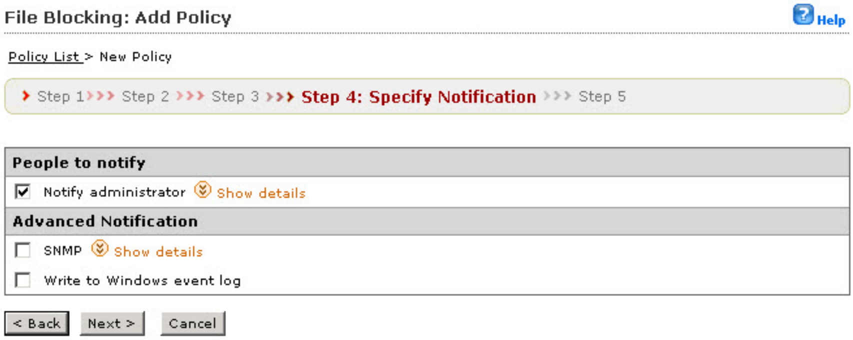
1. Select from the following options:

   - **Block** or **Pass**

     And...

- **Notify** or **Do not notify**

2. Click **Next >**. The **File Blocking: Add Policy > Step 4: Specify Notification** screen appears.



File Blocking: Add Policy

Help
Policy List > New Policy
› Step 1››› Step 2 ››› Step 3 ››› Step 4: Specify Notification ››› Step 5

People to notify

☑ Notify administrator Show details

Advanced Notification

☐ SNMP Show details

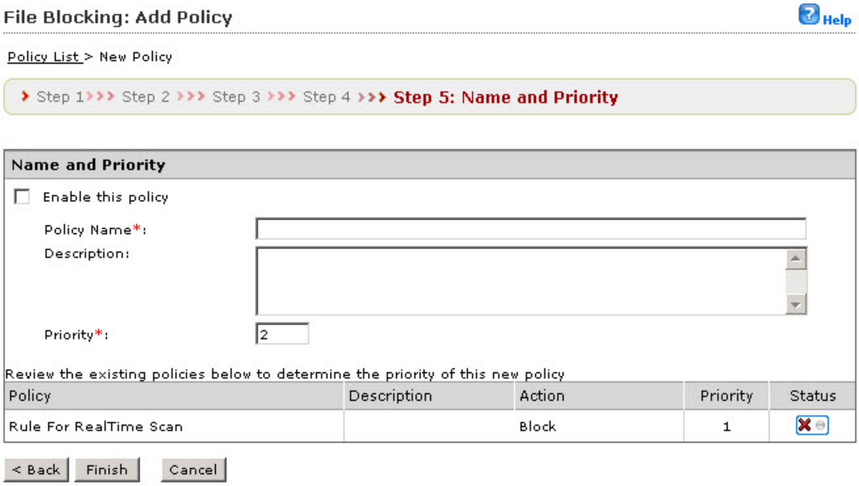
☐ Write to Windows event log

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

Step 4. File Blocking: Add Policy > Specify Notification

Procedure

1. Follow the basic steps explained in *Configuring File Blocking Notifications on page 11-5*. Click **Next >**. The **File Blocking: Add Policy > Step 5: Name and Priority** screen appears.



File Blocking: Add Policy

Policy List > New Policy

› Step 1››› Step 2 ››› Step 3 ››› Step 4 ››› Step 5: Name and Priority

Name and Priority

□ Enable this policy

Policy Name*:

Description:

Priority*: 2

Review the existing policies below to determine the priority of this new policy

Policy	Description	Action	Priority	Status
Rule For RealTime Scan		Block	1	✗

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

Step 5. File Blocking: Add Policy > Name and Priority screen

Procedure

1. Select **Enable this policy** to activate it.

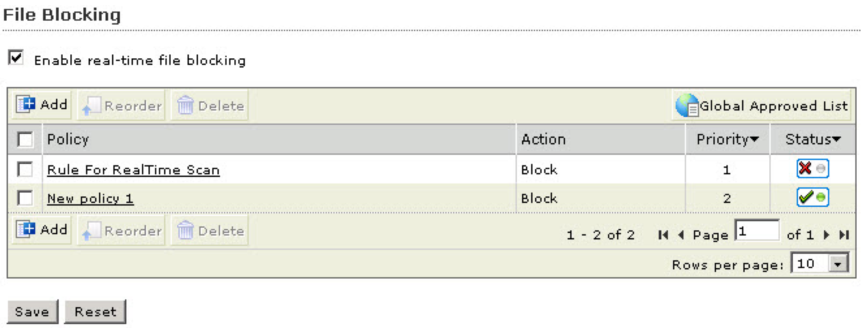
2. Type a name for your policy in the **Policy name** field.

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

☑ Enable real-time file blocking

Add Reorder Delete Global Approved List

□	Policy	Action	Priority	Status
□	Rule For RealTime Scan	Block	1	✗
□	New policy 1	Block	2	✓

Add Reorder Delete 1 - 2 of 2 Page 1 of 1

Rows per page: 10

Save Reset

FIGURE 5-7. File Blocking main screen

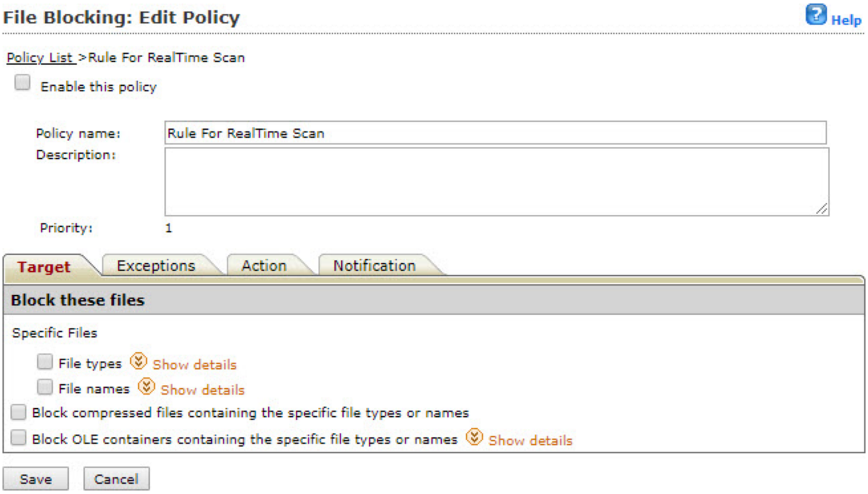
Editing a File Blocking Policy

This section describes the steps required to edit a File Blocking policy.

Procedure

1. On the left menu, click **File Blocking**.

The **File Blocking** screen appears.



File Blocking: Edit Policy

Policy List >Rule For RealTime Scan

□ Enable this policy

Policy name: Rule For RealTime Scan

Description:

Priority: 1

Block these files

Specific Files

□ File types Show details

□ File names Show details

□ Block compressed files containing the specific file types or names

□ Block OLE containers containing the specific file types or names Show details

FIGURE 5-8. File Blocking: Edit Policy screen (target tab)

2. From the **File Blocking** screen, click the policy name link you want to edit.

   The **File Blocking: Edit Policy** screen appears.

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.

6. In the **Block these files** section, under **Specific Files**, click **Show details** to expand the content and select **File types** and **File names**.

   See *Step 1. File Blocking: Add Policy > Specify Rules on page 5-5* for more information.

7. Click the **Exceptions** tab and add or edit any exceptions as required.

   See *Step 2. File Blocking: Add Policy > Exceptions on page 5-6* for more information.

8. Click the **Action** tab and choose from the following:

   - **Block file**
   - **Pass**
   - **Notify**
   - **Do not notify**

9. Click the **Notification** tab, and choose the appropriate settings.

   See *Step 4. File Blocking: Add Policy > Specify Notification on page 5-11* for more information.

10. Click **Save**.

About Available File Types

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

Application and Executables

TABLE 5-1. Application and executable file choices

FILE TYPE	ASSOCIATED EXTENSION(S)
Executable and linking format	`.elf`
Executable	`.exe`; `.dll`; `.vxd`
Java Applet	`.class`
Windows NT/95 shortcut	`.lnk`

File Type	Associated extension(s)
Windows Installer Package	.msi

Documents

Table 5-2. Document file choices

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

Images

Table 5-3. Image file choices

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

Video

Table 5-4. Video file choices

File Type	Associated extension(s)
Advanced Streaming Format	`.asf`; `.wmv`
Macromedia Flash	`.swf`
Moving Picture Experts Group video	`.mpg`; `.mpeg`
Microsoft Resource Interchange File Format	`.avi`; `.bnd`; `.wav`
Quicktime Movie	`.mov`; `.qt`; `.qtm`
Real Media	`.rm`

Audio

TABLE 5-5. Audio file choices

FILE TYPE	ASSOCIATED EXTENSION(S)
Musical Instrument Digital Interface	.mid
MPEG Audio Layer 3	.mp3
Real Audio	.ra; .ram

Compressed Files

TABLE 5-6. Compressed file choices

FILE TYPE	ASSOCIATED EXTENSION(S)
Archive created by LHA	`.lzh`
Archive created by Pkzip	`.zip`
Archive created by RAR	`.rar`
Archive created by Tar	`.tar`
ARJ Compressed archive	`.arj`
BINHEX	`.hqx`
GNU Zip	`.gz`; `.gzip`
LZW/Compressed 16-bits	`.Z`
MacBinary	`.bin`
Microsoft Cabinet	`.cab`
Microsoft Compressed	`.mscomp`
MIME	`.eml`; `.mht`
Teledisk format	`.td0`

File Type	Associated extension(s)
Unix BZ2 Bzip Comopressed file	`.bz2`
UUEncode	`.uu`
WinAce	`.ace`

Chapter 6

Content Filtering

This chapter describes how to configure PortalProtect to prevent the undesirable content from being posted to SharePoint.

Topics include:

- *About Content Filtering on page 6-2*
- *About Content Filtering Action Settings on page 6-3*
- *Content Filtering Policies on page 6-4*
- *Configuring Content Filtering on page 6-7*

About 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 the following table.

TABLE 6-1. Content Filtering actions

DURING THIS SCAN	PORTALPROTECT EXECUTES THIS ACTION
Content Filtering (real-time)	Block or Pass
Manual Scan > Content Filtering (for document)	Quarantine, Delete, or Pass
Manual Scan > Content Filtering (for Web)	Pass **Note** PortalProtect will pass and log the Web content that triggers the policy in manual scan.
Scheduled Scan > Content Filtering (for document)	Quarantine, Delete, or Pass

During this scan	PortalProtect executes this action
Scheduled Scan > Content Filtering (for Web)	Pass **Note** PortalProtect will pass and log the Web content that triggers the policy in manual scan.

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.

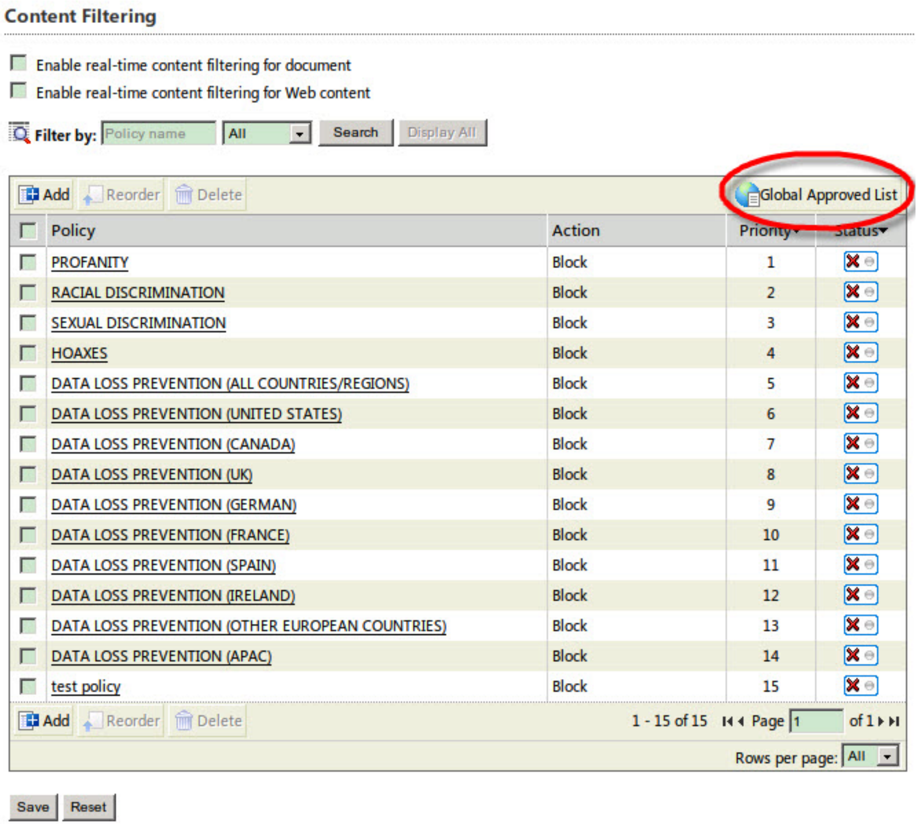
Note

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

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).

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 an approved 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 1-3*.



Content Filtering

☐ Enable real-time content filtering for document

☐ Enable real-time content filtering for Web content

☐	Policy	Action	Priority	Status
☐	PROFANITY	Block	1	✗ ⊖
☐	RACIAL DISCRIMINATION	Block	2	✗ ⊖
☐	SEXUAL DISCRIMINATION	Block	3	✗ ⊖
☐	HOAXES	Block	4	✗ ⊖
☐	DATA LOSS PREVENTION (ALL COUNTRIES/REGIONS)	Block	5	✗ ⊖
☐	DATA LOSS PREVENTION (UNITED STATES)	Block	6	✗ ⊖
☐	DATA LOSS PREVENTION (CANADA)	Block	7	✗ ⊖
☐	DATA LOSS PREVENTION (UK)	Block	8	✗ ⊖
☐	DATA LOSS PREVENTION (GERMAN)	Block	9	✗ ⊖
☐	DATA LOSS PREVENTION (FRANCE)	Block	10	✗ ⊖
☐	DATA LOSS PREVENTION (SPAIN)	Block	11	✗ ⊖
☐	DATA LOSS PREVENTION (IRELAND)	Block	12	✗ ⊖
☐	DATA LOSS PREVENTION (OTHER EUROPEAN COUNTRIES)	Block	13	✗ ⊖
☐	DATA LOSS PREVENTION (APAC)	Block	14	✗ ⊖
☐	test policy	Block	15	✗ ⊖

1 - 15 of 15 Page 1 of 1

Rows per page: All

FIGURE 6-1. Content Filtering Global Approved List

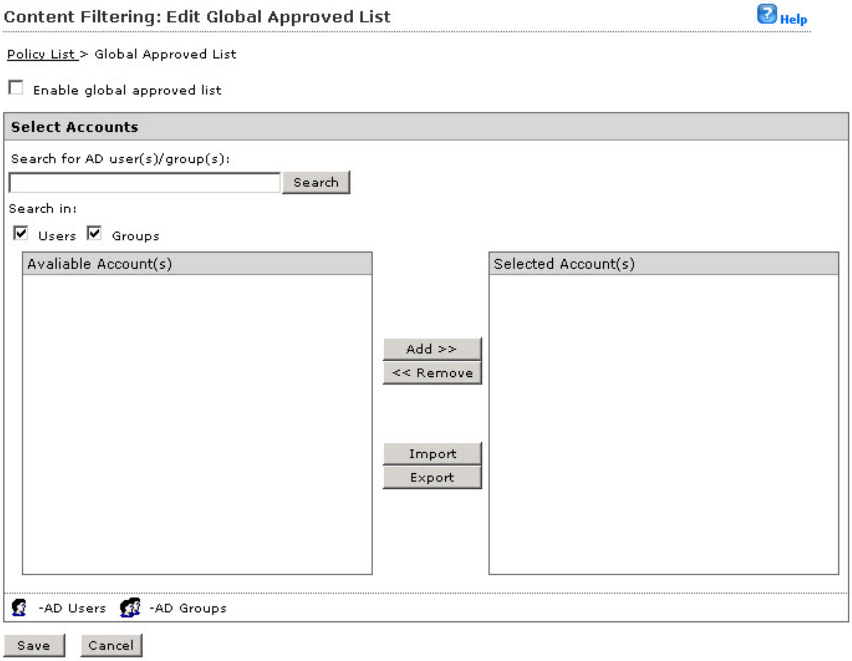
Procedure

1. Click **Content Filtering** on the left menu.

   The **Content Filtering** screen appears.

2. Click **Global Approved List**.

   The **Content Filtering: Edit Global Approved List** screen appears.



Content Filtering: Edit Global Approved List

Policy List > Global Approved List

□ Enable global approved list

Select Accounts

Search for AD user(s)/group(s):

Search in:

☑ Users ☑ Groups

Avaliable Account(s)

Selected Account(s)

-AD Users -AD Groups

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.

   Note

   You can also Import or Export AD users/groups from or to an external file.

9. Click **Save**.

Configuring Content Filtering

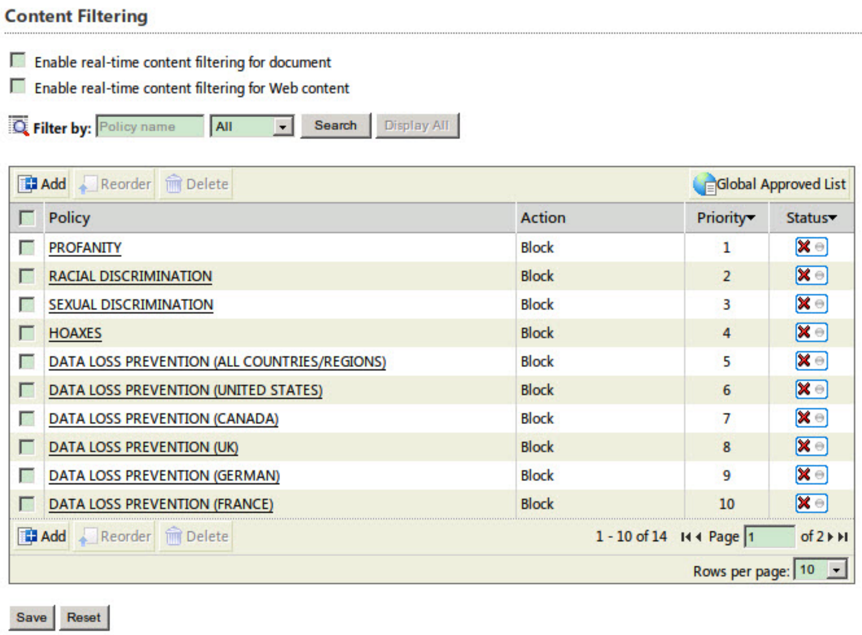
This section provides the information required to manage and configure Content Filtering for PortalProtect. You can manage the following settings from the content filtering main screen:

- Enable or disable real-time content filtering for document
- 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

Procedure

1. On the left menu, click **Content Filtering**.

The **Content Filtering** screen appears.



Content Filtering

□ Enable real-time content filtering for document

□ Enable real-time content filtering for Web content

Filter by: Policy name | All | Search | Display All

Add | Reorder | Delete | Global Approved List

□	Policy	Action	Priority	Status
□	PROFANITY	Block	1	✗ ⊖
□	RACIAL DISCRIMINATION	Block	2	✗ ⊖
□	SEXUAL DISCRIMINATION	Block	3	✗ ⊖
□	HOAXES	Block	4	✗ ⊖
□	DATA LOSS PREVENTION (ALL COUNTRIES/REGIONS)	Block	5	✗ ⊖
□	DATA LOSS PREVENTION (UNITED STATES)	Block	6	✗ ⊖
□	DATA LOSS PREVENTION (CANADA)	Block	7	✗ ⊖
□	DATA LOSS PREVENTION (UK)	Block	8	✗ ⊖
□	DATA LOSS PREVENTION (GERMAN)	Block	9	✗ ⊖
□	DATA LOSS PREVENTION (FRANCE)	Block	10	✗ ⊖

Add | Reorder | Delete — 1 - 10 of 14 Page 1 of 2

Rows per page: 10

Save | Reset

FIGURE 6-3. Content Filtering main screen

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

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

Step 1. Content Filtering: Add Policy > Specify Rules

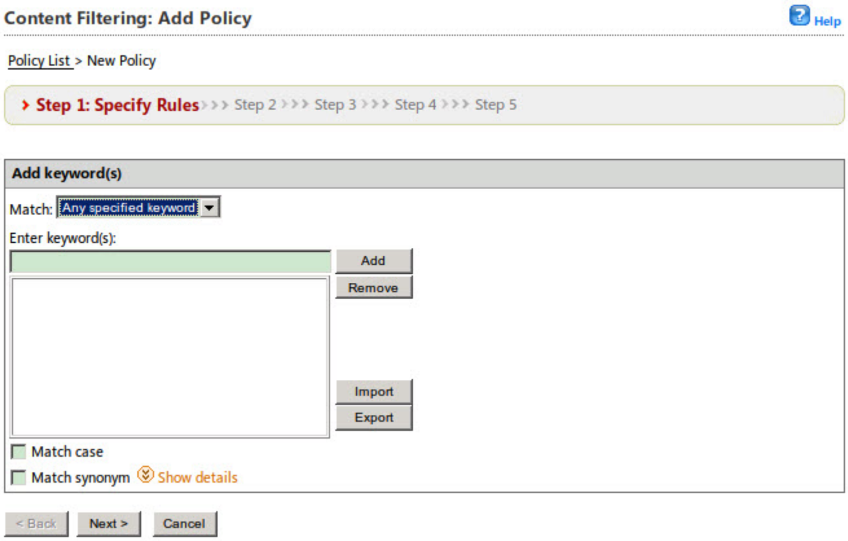
Procedure

1. On the left menu, click **Content Filtering**.

   The **Content Filtering** screen appears.

2. Click **Add**.

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


Content Filtering: Add Policy

Policy List > New Policy

› Step 1: Specify Rules››› Step 2 ››› Step 3 ››› Step 4 ››› Step 5

Add keyword(s)

Match: Any specified keyword

Enter keyword(s):

□ Match case

□ Match synonym

FIGURE 6-4. Content Filtering: Add Policy > Step 1: Specify Rules screen

3. From the **Match** drop-down list, 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, and then click **Add**.

Note

See *About Regular Expressions on page C-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.

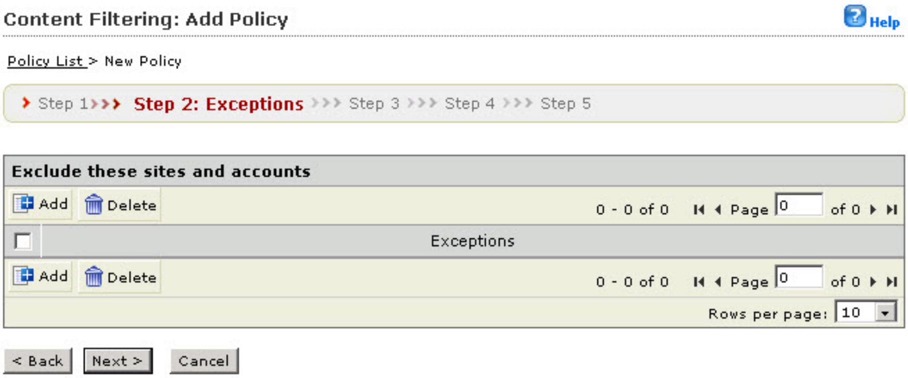
   b. Select a keyword from the keyword list to display its synonym(s) in the **Synonyms to exclude** window.

   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: Exceptions** screen appears.

Step 2. Content Filtering: Add Policy > Exceptions



Content Filtering: Add Policy

Policy List > New Policy

› Step 1››› **Step 2: Exceptions** ››› Step 3 ››› Step 4 ››› Step 5

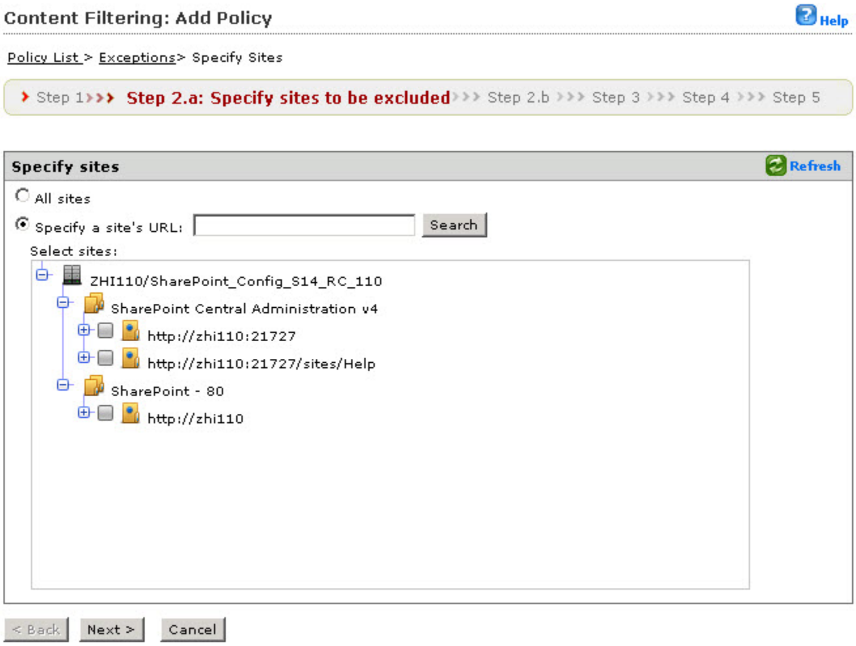
Exclude these sites and accounts

FIGURE 6-5. Content Filtering: Add Policy > Step 2: Exceptions screen

Procedure

1. Click **Add** from the **Step2: Exceptions** screen.

   The **Step 2a: Specify sites to be excluded** screen appears.



Content Filtering: Add Policy

Help

Policy List > Exceptions> Specify Sites

› Step 1››› Step 2.a: Specify sites to be excluded››› Step 2.b ››› Step 3 ››› Step 4 ››› Step 5

Specify sites

Refresh

○ All sites

● Specify a site's URL: Search

Select sites:

ZHI110/SharePoint_Config_S14_RC_110

SharePoint Central Administration v4

□ http://zhi110:21727

□ http://zhi110:21727/sites/Help

SharePoint - 80

□ http://zhi110

< Back | Next > | Cancel

Figure 6-6. Content Filtering: Add Policy > Step 2.a Specify sites to be excluded screen

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.

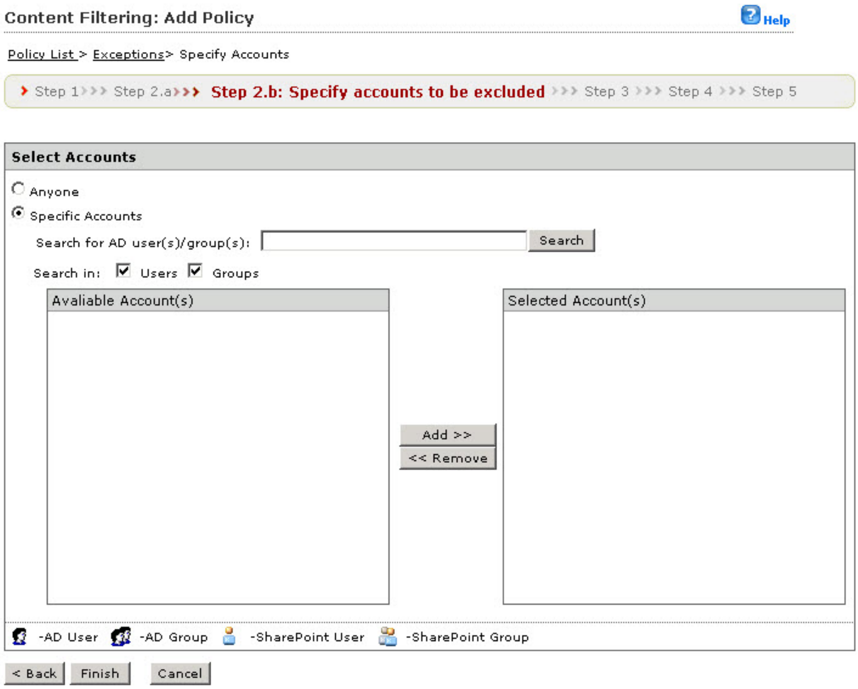
  a. Type the URL in the **Specify a site's URL** field and click **Search**.

  b. From the **Select sites** tree, choose the specific site(s) to exclude from this policy.

  c. Click **Next >** and go to Step 3.

3. Click **Next >**.

The **Step 2b: Specify accounts to be excluded** screen appears.



Content Filtering: Add Policy

Help

Policy List > Exceptions> Specify Accounts

› Step 1 ››› Step 2.a››› **Step 2.b: Specify accounts to be excluded** ››› Step 3 ››› Step 4 ››› Step 5

Select Accounts

○ Anyone

● Specific Accounts

Search for AD user(s)/group(s): [ ] Search

Search in: ☑ Users ☑ Groups

Avaliable Account(s)

Selected Account(s)

Add >>

<< Remove

-AD User -AD Group -SharePoint User -SharePoint Group

< Back Finish Cancel

FIGURE 6-7. Content Filtering: Add Policy > Step 2.b Specify accounts to be excluded screen

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.

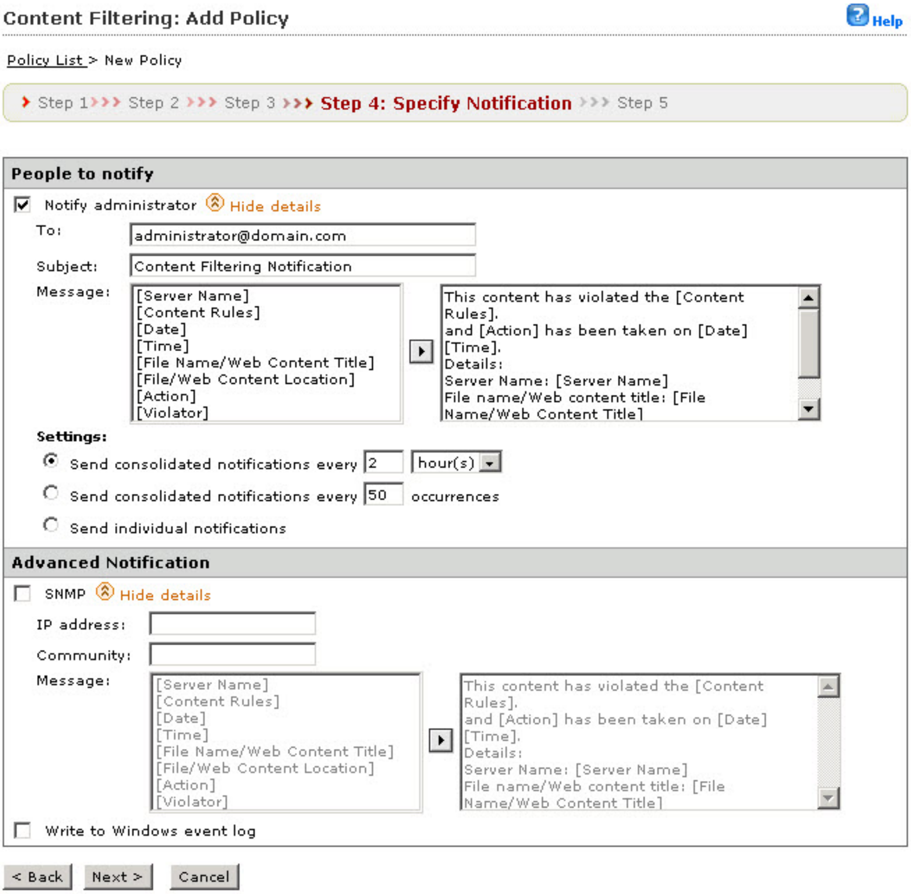
Step 3. Content Filtering: Add Policy > Specify Action

Procedure

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



Content Filtering: Add Policy

Policy List > New Policy

› Step 1 ››› Step 2 ››› Step 3 ››› **Step 4: Specify Notification** ››› Step 5

People to notify

☑ Notify administrator Hide details

To: administrator@domain.com

Subject: Content Filtering Notification

Message:

```
[Server Name]
[Content Rules]
[Date]
[Time]
[File Name/Web Content Title]
[File/Web Content Location]
[Action]
[Violator]
```

```
This content has violated the [Content
Rules].
and [Action] has been taken on [Date]
[Time].
Details:
Server Name: [Server Name]
File name/Web content title: [File
Name/Web Content Title]
```

Settings:

● Send consolidated notifications every 2 hour(s)

○ Send consolidated notifications every 50 occurrences

○ Send individual notifications

Advanced Notification

☐ SNMP Hide details

IP address:

Community:

Message:

```
[Server Name]
[Content Rules]
[Date]
[Time]
[File Name/Web Content Title]
[File/Web Content Location]
[Action]
[Violator]
```

```
This content has violated the [Content
Rules].
and [Action] has been taken on [Date]
[Time].
Details:
Server Name: [Server Name]
File name/Web content title: [File
Name/Web Content Title]
```

☐ Write to Windows event log

FIGURE 6-8. Content Filtering: Add Policy > Step 4: Specify Notification screen

Procedure

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.

   - **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**

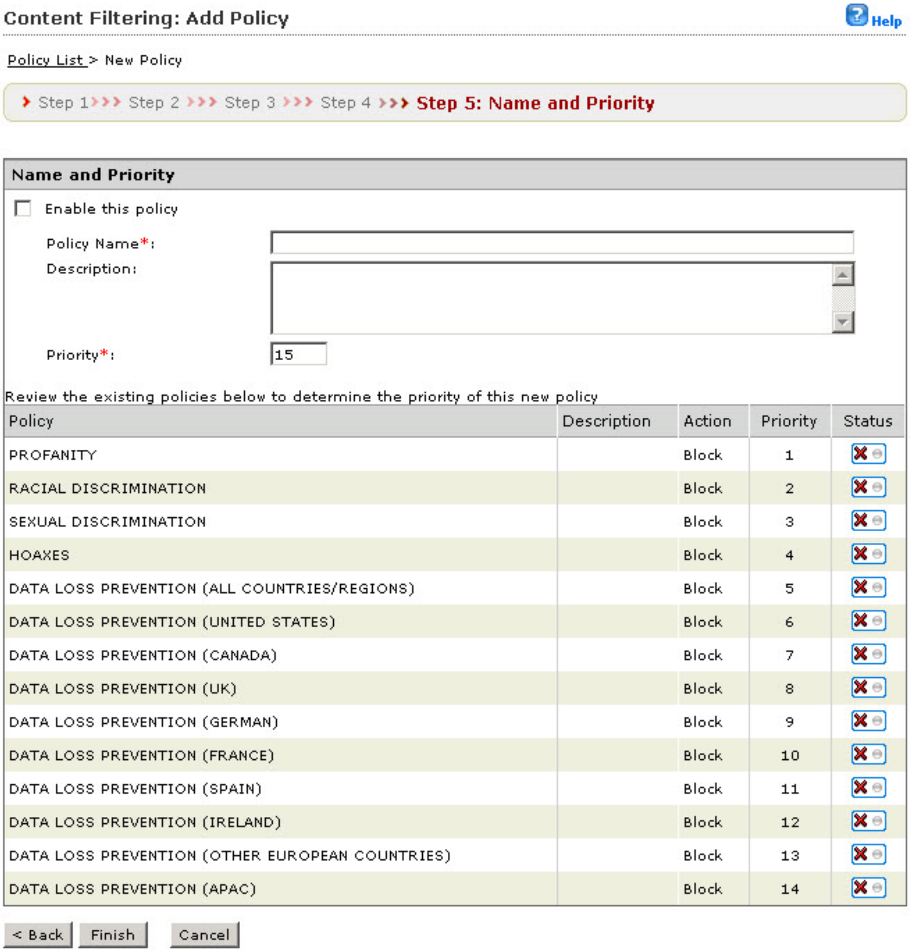
   - **Community**

- **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



Content Filtering: Add Policy

Policy List > New Policy

Step 1 >>> Step 2 >>> Step 3 >>> Step 4 >>> Step 5: Name and Priority

Name and Priority

□ Enable this policy

Policy Name*:

Description:

Priority*: 15

Review the existing policies below to determine the priority of this new policy

Policy	Description	Action	Priority	Status
PROFANITY		Block	1	☒
RACIAL DISCRIMINATION		Block	2	☒
SEXUAL DISCRIMINATION		Block	3	☒
HOAXES		Block	4	☒
DATA LOSS PREVENTION (ALL COUNTRIES/REGIONS)		Block	5	☒
DATA LOSS PREVENTION (UNITED STATES)		Block	6	☒
DATA LOSS PREVENTION (CANADA)		Block	7	☒
DATA LOSS PREVENTION (UK)		Block	8	☒
DATA LOSS PREVENTION (GERMAN)		Block	9	☒
DATA LOSS PREVENTION (FRANCE)		Block	10	☒
DATA LOSS PREVENTION (SPAIN)		Block	11	☒
DATA LOSS PREVENTION (IRELAND)		Block	12	☒
DATA LOSS PREVENTION (OTHER EUROPEAN COUNTRIES)		Block	13	☒
DATA LOSS PREVENTION (APAC)		Block	14	☒

FIGURE 6-9. Content Filtering: Add Policy > Step 5: Name and Priority screen

Procedure

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.

Editing a Content Filtering Policy

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

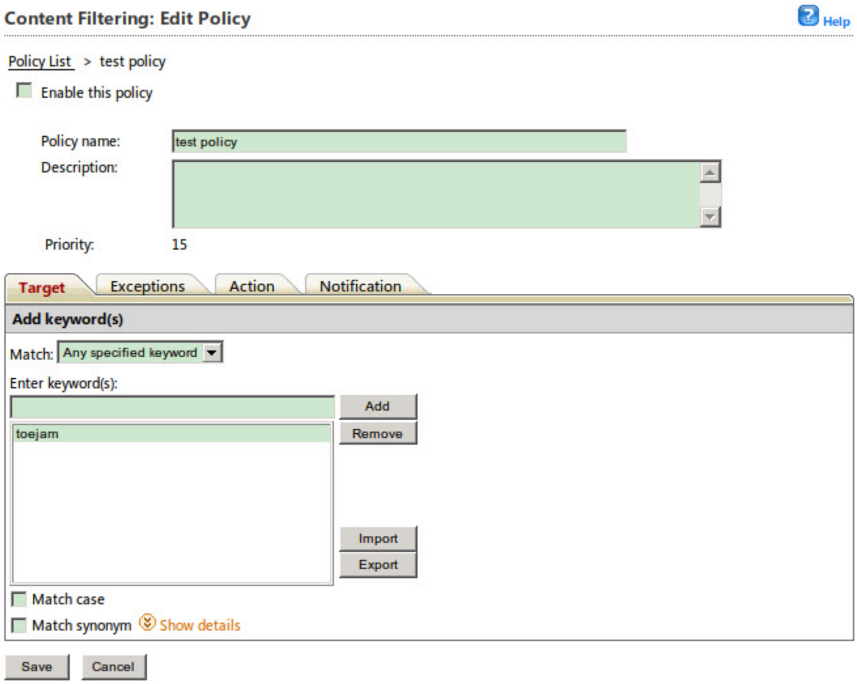
Procedure

1. On the left menu, click **Content Filtering**.

   The **Content Filtering** screen appears.

2. From the **Content Filtering** screen, click the policy name link you want to edit.

The **Content Filtering: Edit Policy** screen appears.



Content Filtering: Edit Policy

Policy List > test policy

□ Enable this policy

Policy name: test policy

Description:

Priority: 15

Add keyword(s)

Match: Any specified keyword

Enter keyword(s):

toejam

□ Match case

□ Match synonym

FIGURE 6-10. 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 on page C-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 *Step 2. Content Filtering: Add Policy > 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 *Step 4. Content Filtering: Add Policy > Specify Notification on page 6-16* for more information.

12. Click **Save**.

Chapter 7

Data Loss Prevention

This chapter explains how to configure Data Loss Prevention to protect your SharePoint environment.

Topics include:

About Data Loss Prevention

With the prevalence and damaging effects of data breaches, organizations now see digital asset protection as a critical component of their security infrastructure.

Data Loss Prevention safeguards an organization's sensitive data against accidental or deliberate leakage. Data Loss Prevention allows you to:

- Identify the sensitive information that requires protection using data identifiers
- Create policies that limit or prevent the transmission of digital assets through common transmission channels, such as email and external devices
- Enforce compliance to established privacy standards

Before you can monitor sensitive information for potential loss, you must be able to answer the following questions:

- What data needs protection from unauthorized users?
- Where does the sensitive data reside?
- How is the sensitive data transmitted?
- What users are authorized to access or transmit the sensitive data?
- What action should be taken if a security violation occurs?

This important audit typically involves multiple departments and personnel familiar with the sensitive information in your organization.

If you already defined your sensitive information and security policies, you can begin to define data identifiers and company policies.

Data Identifier Types

Digital assets are files and data that an organization must protect against unauthorized transmission. Administrators can define digital assets using the following data identifiers:

- Expressions: Data that has a certain structure.

  For details, see *Expressions on page 7-3*.

- Keyword lists: A list of special words or phrases.

  For details, see *Keywords on page 7-8*.

Note

Administrators cannot delete a data identifier that a Data Loss Prevention (DLP) template is using. Delete the template before deleting the data identifier.

Expressions

An expression is data that has a certain structure. For example, credit card numbers typically have 16 digits and appear in the format "nnnn-nnnn-nnnn-nnnn", making them suitable for expression-based detections.

Administrators can use predefined and customized expressions.

For details, see *Predefined Expressions on page 7-3* and *Customized Expressions on page 7-4*.

Predefined Expressions

Data Loss Prevention comes with a set of predefined expressions. These expressions cannot be modified or deleted.

Data Loss Prevention verifies these expressions using pattern matching and mathematical equations. After Data Loss Prevention matches potentially sensitive data with an expression, the data may also undergo additional verification checks.

For a complete list of predefined expressions, see the *Data Protection Lists* document at http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Customized Expressions

Create customized expressions if none of the predefined expressions meets the company's requirements.

Expressions are a powerful string-matching tool. Become comfortable with expression syntax before creating expressions. Poorly written expressions can dramatically impact performance.

When creating expressions:

- Refer to the predefined expressions for guidance on how to define valid expressions. For example, when creating an expression that includes a date, refer to the expressions prefixed with "Date".
- Note that Data Loss Prevention follows the expression formats defined in Perl Compatible Regular Expressions (PCRE). For more information on PCRE, visit the following website:

  http://www.pcre.org/
- Start with simple expressions. Modify the expressions if they are causing false alarms or fine tune them to improve detections.

Administrators can choose from several criteria when creating expressions. An expression must satisfy the chosen criteria before Data Loss Prevention subjects it to a DLP policy. For details about the different criteria options, see *Criteria for Customized Expressions on page 7-5*.

Criteria for Customized Expressions

TABLE 7-1. Criteria Options for Customized Expressions

CRITERIA	RULE	EXAMPLE
None	None	All - Names from US Census Bureau • Expression: [^\w]([A-Z][a-z]{1,12}(\s?,\s?|[\s]|\s([A-Z])\.\s)[A-Z][a-z]{1,12})[^\w]
Specific characters	An expression must include the characters you have specified. In addition, the number of characters in the expression must be within the minimum and maximum limits.	US - ABA Routing Number • Expression: [^\d]([0123678]\d{8})[^\d] • Characters: 0123456789 • Minimum characters: 9 • Maximum characters: 9
Suffix	Suffix refers to the last segment of an expression. A suffix must include the characters you have specified and contain a certain number of characters. In addition, the number of characters in the expression must be within the minimum and maximum limits.	All - Home Address • Expression: \D(\d+\s[a-z.]+\s([a-z]+\s){0,2} (lane|ln|street|st|avenue|ave|road|rd|place|pl|drive|dr|circle| cr|court|ct|boulevard|blvd)\.? [0-9a-z,#\s\.]{0,30}[\s|,][a-z]{2}\ s\d{5}(-\d{4})?)[^\d-] • Suffix characters: 0123456789- • Number of characters: 5 • Minimum characters in the expression: 25 • Maximum characters in the expression: 80

Criteria	Rule	Example
Single- character separator	An expression must have two segments separated by a character. The character must be 1 byte in length. In addition, the number of characters left of the separator must be within the minimum and maximum limits. The number of characters right of the separator must not exceed the maximum limit.	All - Email Address • Expression: [^\w.]([\w\.]{1,20}@[a-z0-9]{2,20}[\.][a-z]{2,5}[a-z\.]{0,10})[^\w.] • Separator: @ • Minimum characters to the left: 3 • Maximum characters to the left: 15 • Maximum characters to the right: 30

Creating a Customized Expression

Procedure

1. Go to **Data Loss Prevention** > **Data Identifiers**.
2. Click the **Expression** tab.
3. Click **Add**.

   A new screen displays.
4. Type an expression name that does not exceed 256 characters in length.
5. Type a description that does not exceed 256 characters in length.
6. Type the displayed data.

   For example, if you are creating an expression for ID numbers, type a sample ID number. This data is used for reference purposes only and will not appear elsewhere in the product.
7. Choose one of the following criteria and configure additional settings for the chosen criteria (see *Criteria for Customized Expressions on page 7-5*):

- None
- Specific characters
- Suffix
- Single-character separator

8. Optional: Select a validator for the expression.

   Note

   Data units follow semantic rules. Not every 9-digit number is a valid social security number and not every 15- or 16-digit number is a valid credit card number. To reduce false positives, expression validators check if the extracted data units follow these rules.

9. Test the expression against an actual data.

   For example, if the expression is for a national ID, type a valid ID number in the **Test data** text box, click **Test**, and then check the result.

10. Click **Save** if you are satisfied with the result.

    Note

    Save the settings only if the testing was successful. An expression that cannot detect any data wastes system resources and may impact performance.

Importing Customized Expressions

Use this option if you have a properly-formatted `.xml` file containing the expressions. You can generate the file by exporting the expressions from the PortalProtect administrator console.

Procedure

1. Go to **Data Loss Prevention** > **Data Identifiers**.

2. Click the **Expression** tab.

3. Click **Import** and then locate the `.xml` file containing the expressions.

4. Click **Open**.

   A message appears, informing you if the import was successful.

   > **Note**
   >
   > Every customized expression is identified by its **name** field in the `.xml` file. This name is a unique internal name that does not display on the administrator console.
   >
   > If the file contains a customized expression that already exists, PortalProtect overwrites the existing expression. If the file contains any predefined expression, PortalProtect skips the predefined expression while importing the remaining customized expressions.

Keywords

Keywords are special words or phrases. You can add related keywords to a keyword list to identify specific types of data. For example, "prognosis", "blood type", "vaccination", and "physician" are keywords that may appear in a medical certificate. If you want to prevent the transmission of medical certificate files, you can use these keywords in a DLP policy and then configure Data Loss Prevention to block files containing these keywords.

Commonly used words can be combined to form meaningful keywords. For example, "end", "read", "if", and "at" can be combined to form keywords found in source codes, such as "END-IF", "END-READ", and "AT END".

You can use predefined and customized keyword lists. For details, see *Predefined Keyword Lists on page 7-9* and *Customized Keyword Lists on page 7-9*.

Predefined Keyword Lists

Data Loss Prevention comes with a set of predefined keyword lists. These keyword lists cannot be modified or deleted. Each list has its own built-in conditions that determine if the template should trigger a policy violation.

For details about the predefined keyword lists in Data Loss Prevention, see the *Data Protection Lists* document at:

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

Customized Keyword Lists

Create customized keyword lists if none of the predefined keyword lists meets your requirements.

There are several criteria that you can choose from when configuring a keyword list. A keyword list must satisfy your chosen criteria before Data Loss Prevention subjects it to a policy. Choose one of the following criteria for each keyword list:

- **Any keyword**
- **All keywords**
- **All keywords within <x> characters**
- **Combined score for keywords exceeds threshold**

For details regarding the criteria rules, see *Customized Keyword List Criteria on page 7-9*.

Customized Keyword List Criteria

TABLE 7-2. Criteria for a Keyword List

CRITERIA	RULE
Any keyword	A file must contain at least one keyword in the keyword list.

Criteria	Rule
All keywords	A file must contain all the keywords in the keyword list.
All keywords within <x> characters	A file must contain all the keywords in the keyword list. In addition, each keyword pair must be within <x> characters of each other. For example, your 3 keywords are WEB, DISK, and USB and the number of characters you specified is 20. If Data Loss Prevention detects all keywords in the order DISK, WEB, and USB, the number of characters from the "D" (in DISK) to the "W" (in WEB) and from the "W" to the "U" (in USB) must be 20 characters or less. The following data matches the criteria: DISK####WEB############USB The following data does not match the criteria: DISK*******************WEB****USB(23 characters between "D" and "W") When deciding on the number of characters, remember that a small number, such as 10, usually results in a faster scanning time but only covers a relatively small area. This may reduce the likelihood of detecting sensitive data, especially in large files. As the number increases, the area covered also increases but scanning time might be slower.
Combined score for keywords exceeds threshold	A file must contain one or more keywords in the keyword list. If only one keyword was detected, its score must be higher than the threshold. If there are several keywords, their combined score must be higher than the threshold. Assign each keyword a score of 1 to 10. A highly confidential word or phrase, such as "salary increase" for the Human Resources department, should have a relatively high score. Words or phrases that, by themselves, do not carry much weight can have lower scores. Consider the scores that you assigned to the keywords when configuring the threshold. For example, if you have five keywords and three of those keywords are high priority, the threshold can be equal to or lower than the combined score of the three high priority keywords. This means that the detection of these three keywords is enough to treat the file as sensitive.

Creating a Keyword List

Procedure

1. Go to **Data Loss Prevention** > **Data Identifiers**.
2. Click the **Keyword** tab.
3. Click **Add**.

   A new screen displays.
4. Type a keyword list name that does not exceed 256 characters in length.
5. Type a description that does not exceed 256 characters in length.
6. Choose one of the following criteria and configure additional settings for the chosen criteria:
   - **Any keyword**
   - **All keywords**
   - **All keywords within <x> characters**
   - **Combined score for keywords exceeds threshold**
7. To manually add keywords to the list:

   a. Type a keyword that is 3 to 40 characters in length and specify whether it is case-sensitive.

   b. Click **Add**.
8. To edit a keyword, click a keyword in the list, edit it in the **Keyword** text box, and then click **Update**.
9. To delete keywords, select the keywords and click **Delete**.
10. Click **Save**.

Importing a Keyword List

Use this option if you have a properly-formatted `.xml` file containing the keyword lists. You can generate the file by exporting the keyword lists from the PortalProtect administrator console.

Procedure

1. Go to **Data Loss Prevention** > **Data Identifiers**.
2. Click the **Keyword** tab.
3. Click **Import** and then locate the `.xml` file containing the keyword lists.
4. Click **Open**.

   A message appears, informing you if the import was successful.

   Note

   Every customized keyword list is identified by its **name** field in the `.xml` file. This name is a unique internal name that does not display on the administrator console.

   If the file contains a customized keyword list that already exists, PortalProtect overwrites the existing keyword list. If the file contains any predefined keyword list, PortalProtect skips the predefined keyword list while importing the remaining customized keyword lists.

DLP Compliance Templates

A DLP compliance template combines DLP data identifiers and logical operators (And, Or, Except) to form condition statements. Only files or data that satisfy a certain condition statement will be subject to a DLP policy.

You can create your own templates if you have configured DLP data identifiers. You can also use predefined templates. For details, see *Customized DLP Templates on page 7-13* and *Predefined DLP Templates on page 7-13*.

Note

It is not possible to delete a template that is being used in a DLP policy. Remove the template from the policy before deleting it.

Predefined DLP Templates

Trend Micro comes with a set of predefined templates that you can use to comply with various regulatory standards. These templates cannot be modified or deleted.

For a detailed list on the purposes of all predefined templates, and examples of data being protected, see the *Data Protection Lists* document at http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Customized DLP Templates

Create your own templates if you have configured data identifiers. A template combines data identifiers and logical operators (And, Or, Except) to form condition statements.

For more information and examples on how condition statements and logical operators work, see *Condition Statements and Logical Operators on page 7-13*.

Condition Statements and Logical Operators

Data Loss Prevention evaluates condition statements from left to right. Use logical operators carefully when configuring condition statements. Incorrect usage leads to an erroneous condition statement that will likely produce unexpected results.

See the examples in the following table.

TABLE 7-3. Sample Condition Statements

CONDITION STATEMENT	INTERPRETATION AND EXAMPLE
[Data Identifier1] **And** [Data Identifier 2] **Except** [Data Identifier 3]	A file must satisfy [Data Identifier 1] and [Data Identifier 2] but not [Data Identifier 3]. For example: A file must be [an Adobe PDF document] and must contain [an email address] but should not contain [all of the keywords in the keyword list].
[Data Identifier 1] **Or** [Data Identifier 2]	A file must satisfy [Data Identifier 1] or [Data Identifier 2]. For example: A file must be [an Adobe PDF document] or [a Microsoft Word document].
Except [Data Identifier 1]	A file must not satisfy [Data Identifier 1]. For example: A file must not be [a multimedia file].

As the last example in the table illustrates, the first data identifier in the condition statement can have the "Except" operator if a file must not satisfy all of the data identifiers in the statement. In most cases, however, the first data identifier does not have an operator.

Creating a Template

Procedure

1. Go to **Data Loss Prevention** > **DLP Templates**.
2. Click **Add**.

   A new screen displays.
3. Type a template name that does not exceed 256 characters in length.
4. Type a description that does not exceed 256 characters in length.

5. Select data identifiers and then click the "add" icon.

6. If you selected an expression, type the number of occurrences, which is the number of times an expression must occur before Data Loss Prevention subjects it to a policy.

7. Choose a logical operator for each definition.

   Note

   Use logical operators carefully when configuring condition statements. Incorrect usage leads to an erroneous condition statement that will likely produce unexpected results. For examples of correct usage, see *Condition Statements and Logical Operators on page 7-13*.

8. To remove a data identifier from the list of selected identifiers, click the trash bin icon.

9. Click **Save**.

Importing Templates

Use this option if you have a properly-formatted `.xml` file containing the templates. You can generate the file by exporting the templates from the PortalProtect administrator console.

Procedure

1. Go to **Data Loss Prevention** > **DLP Templates**.

2. Click **Import** and then locate the `.xml` file containing the templates.

3. Click **Open**.

   A message appears, informing you if the import was successful.

Note

Every customized template is identified by its **name** field in the `.xml` file. This name is a unique internal name that does not display on the management console.

If the file contains a customized template that already exists, PortalProtect overwrites the existing template. If the file contains any predefined template, PortalProtect skips the predefined template while importing the remaining customized templates.

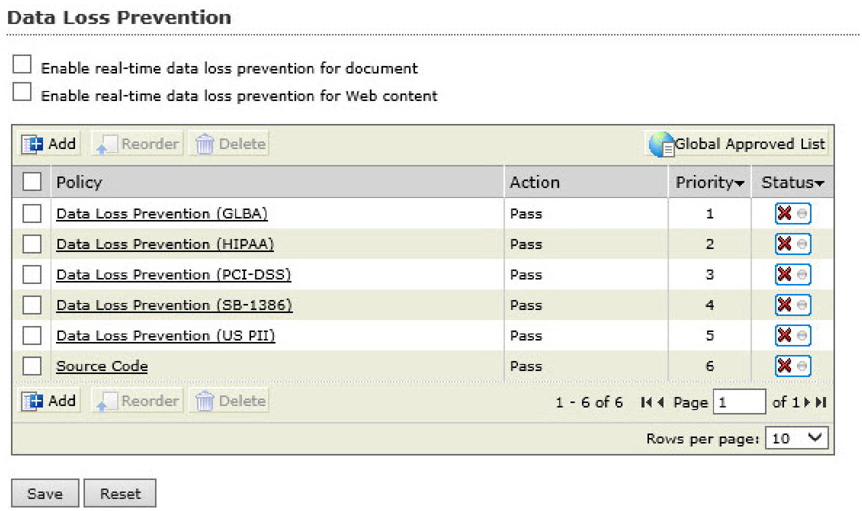
Data Loss Prevention Policies

This section explains the steps required to configure data loss prevention policies.

Procedure

1. On the left menu, click **Data Loss Prevention** > **Policy**.

The **Data Loss Prevention** screen appears.



Data Loss Prevention

□ Enable real-time data loss prevention for document

□ Enable real-time data loss prevention for Web content

□	Policy	Action	Priority	Status
□	Data Loss Prevention (GLBA)	Pass	1	✗ ⊖
□	Data Loss Prevention (HIPAA)	Pass	2	✗ ⊖
□	Data Loss Prevention (PCI-DSS)	Pass	3	✗ ⊖
□	Data Loss Prevention (SB-1386)	Pass	4	✗ ⊖
□	Data Loss Prevention (US PII)	Pass	5	✗ ⊖
□	Source Code	Pass	6	✗ ⊖

FIGURE 7-1. Data Loss Prevention main screen

2. Select one or both of the following options:

   - **Enable real-time data loss prevention for document**—performs real-time data loss prevention for documents

   - **Enable real-time data loss prevention for Web content**—performs data loss prevention for Web content

3. Click **Save**.

Adding a Data Loss Prevention Policy

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

Step 1. Data Loss Prevention: Add Policy > Specify Rules

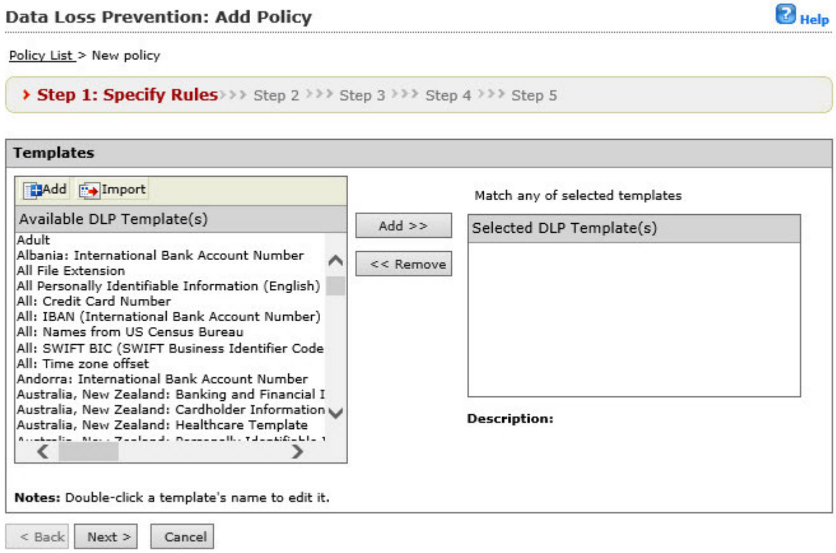
Procedure

1. On the left menu, click **Data Loss Prevention** > **Policy**.

   The **Data Loss Prevention** screen appears.

2. Click **Add**.

   The **Data Loss Prevention: Add Policy> Step 1: Specify Rules** screen appears.



Data Loss Prevention: Add Policy

Policy List > New policy

› Step 1: Specify Rules ››› Step 2 ››› Step 3 ››› Step 4 ››› Step 5

Templates

Match any of selected templates

Available DLP Template(s)

Adult
Albania: International Bank Account Number
All File Extension
All Personally Identifiable Information (English)
All: Credit Card Number
All: IBAN (International Bank Account Number)
All: Names from US Census Bureau
All: SWIFT BIC (SWIFT Business Identifier Code
All: Time zone offset
Andorra: International Bank Account Number
Australia, New Zealand: Banking and Financial I
Australia, New Zealand: Cardholder Information
Australia, New Zealand: Healthcare Template
Australia, New Zealand: Personally Identifiable I

Selected DLP Template(s)

Description:

Notes: Double-click a template's name to edit it.

FIGURE 7-2. Data Loss Prevention: Add Policy> Step 1: Specify Rules screen

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

Note

Press and hold the Ctrl key to select multiple DLP templates.

You can import a DLP template from an XML file by clicking the **Import** button.

4. To add a DLP template to the list of available DLP templates:

    a. Click the **Add** button, which is located next to the **Import** button.

       The **Add DLP Template** screen appears.

    b. Type a name for the new template in the **DLP template name** field.

    c. Type an optional description for the new template in the **Description** field.

5. To define a DLP template, select from the following:

    a. If you select **Expressions...**

       Choose an expression from the list, for example, **US: SSN (Social Security Number)**, **All: Credit Card Number**, or **US: Phone Number**.

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

    c. Click the "+" to add additional DLP template(s):

        i. Select the appropriate operator `And/Or`.

        ii. Repeat the previous process by choosing **Expressions** and select one of the available expressions from the list.

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

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

        i. Choose one of the keywords from the list of available keywords.

        ii. Click the "+" to add additional DLP template(s).

iii. Select the appropriate operator `And/Or`.

iv. Repeat the previous process by choosing **Keywords** and select one of the available keywords from the list.

6. After you finish adding your DLP template(s), click **Add**, then click **Save**.

   The **Data Loss Prevention: Add Policy > Step 1: Specify Rules** screen appears.

7. Click **Next >**.

   The **Data Loss Prevention: Add Policy > Step 2: Exceptions** screen appears.

Step 2. Data Loss Prevention: Add Policy > Step 2: Exceptions

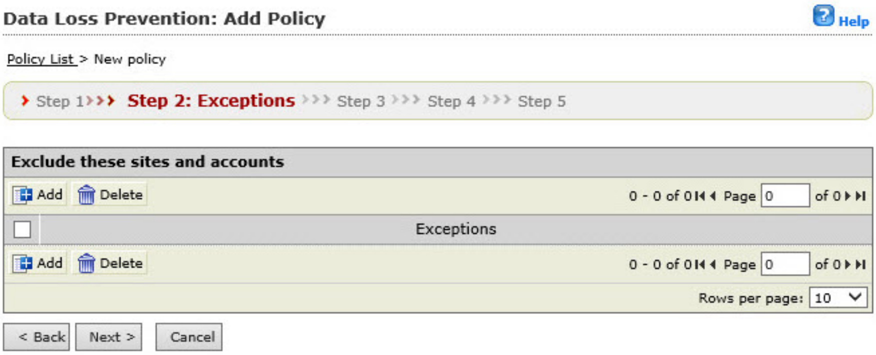
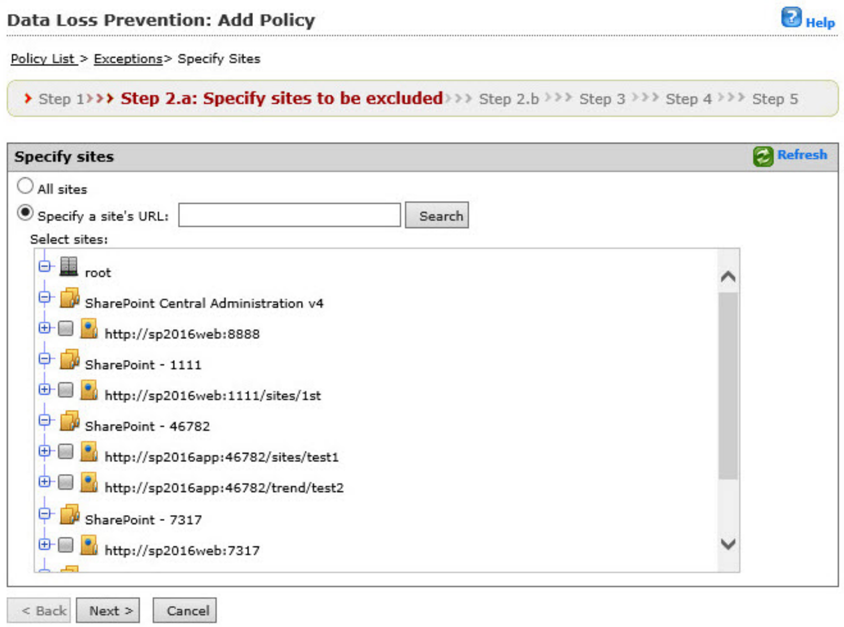


FIGURE 7-3. Data Loss Prevention: Add Policy > Step 2: Exceptions screen

Procedure

1. Click **Add** from the **Step2: Exceptions** screen.

The **Step 2a: Specify sites to be excluded** screen appears.



Data Loss Prevention: Add Policy

Policy List > Exceptions> Specify Sites

› Step 1››› **Step 2.a: Specify sites to be excluded** ››› Step 2.b ››› Step 3 ››› Step 4 ››› Step 5

Specify sites

○ All sites

● Specify a site's URL: [ ] Search

Select sites:

- root
  - SharePoint Central Administration v4
    - □ http://sp2016web:8888
  - SharePoint - 1111
    - □ http://sp2016web:1111/sites/1st
  - SharePoint - 46782
    - □ http://sp2016app:46782/sites/test1
    - □ http://sp2016app:46782/trend/test2
  - SharePoint - 7317
    - □ http://sp2016web:7317

FIGURE 7-4. Data Loss Prevention: New Policy> Step 2.a Specify sites to be excluded screen

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...**

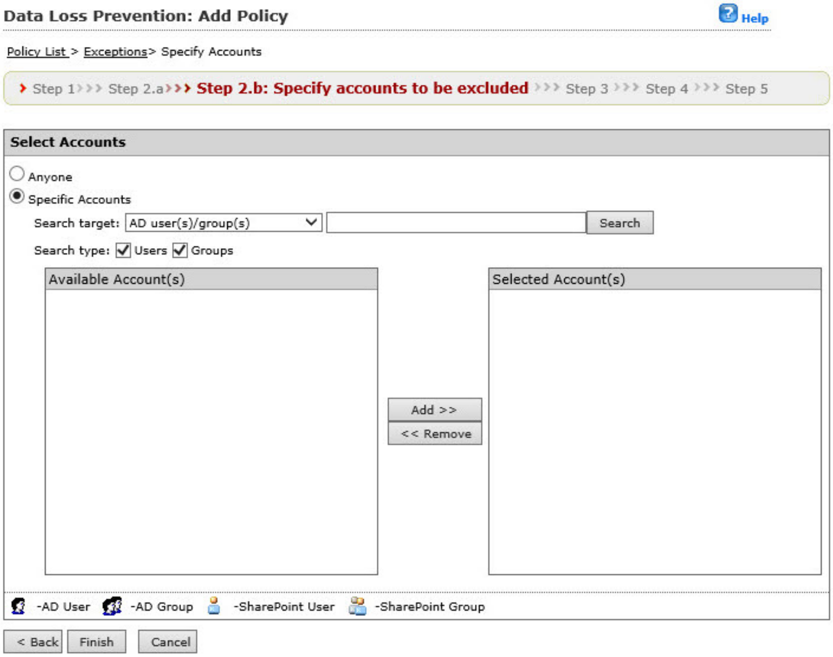
Note

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.



Data Loss Prevention: Add Policy

Policy List > Exceptions> Specify Accounts

› Step 1››› Step 2.a››› **Step 2.b: Specify accounts to be excluded** ››› Step 3 ››› Step 4 ››› Step 5

Select Accounts

○ Anyone
● Specific Accounts

Search target: AD user(s)/group(s)

Search type: ☑ Users ☑ Groups

FIGURE 7-5. Data Loss Prevention: 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.

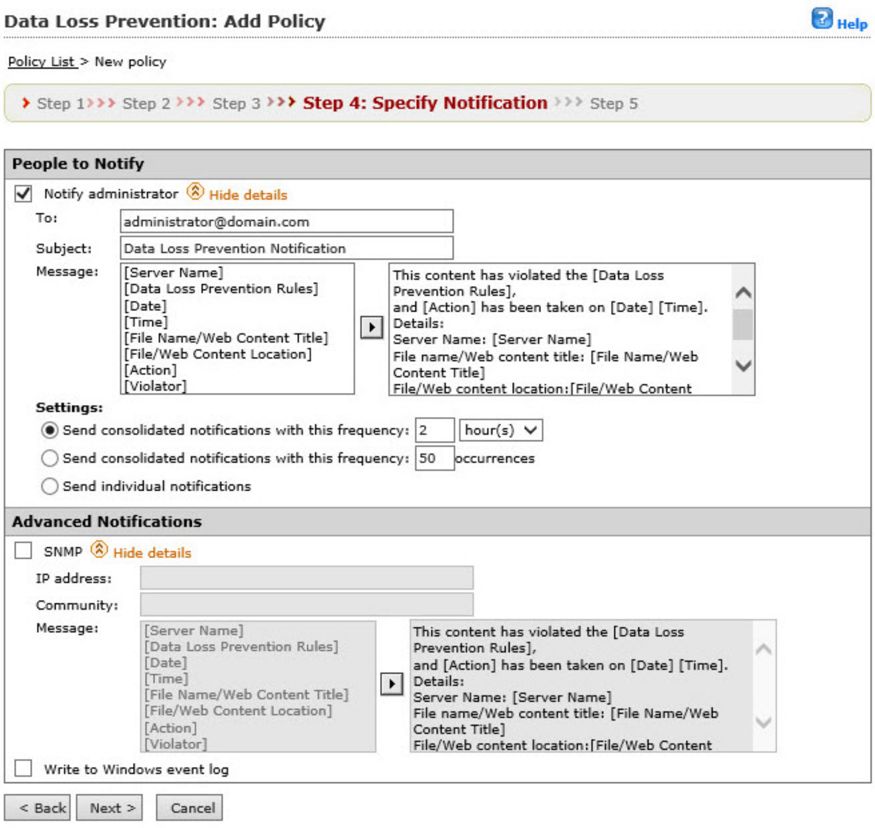
Step 3. Data Loss Prevention: Add Policy > Specify Action

Procedure

1. Select an action for the data loss prevention policy from the following options:

- **Block** or **Pass**
- **Notify** or **Do not notify**
- Click **Next >**.

Step 4. Data Loss Prevention: Add Policy > Specify Notification



Data Loss Prevention: Add Policy

Policy List > New policy

› Step 1 ››› Step 2 ››› Step 3 ››› **Step 4: Specify Notification** ››› Step 5

People to Notify

☑ Notify administrator Hide details

To: administrator@domain.com

Subject: Data Loss Prevention Notification

Message:

[Server Name]
[Data Loss Prevention Rules]
[Date]
[Time]
[File Name/Web Content Title]
[File/Web Content Location]
[Action]
[Violator]

This content has violated the [Data Loss Prevention Rules],
and [Action] has been taken on [Date] [Time].
Details:
Server Name: [Server Name]
File name/Web content title: [File Name/Web Content Title]
File/Web content location:[File/Web Content

Settings:

● Send consolidated notifications with this frequency: 2 hour(s)

○ Send consolidated notifications with this frequency: 50 occurrences

○ Send individual notifications

Advanced Notifications

□ SNMP Hide details

IP address:

Community:

Message:

[Server Name]
[Data Loss Prevention Rules]
[Date]
[Time]
[File Name/Web Content Title]
[File/Web Content Location]
[Action]
[Violator]

This content has violated the [Data Loss Prevention Rules],
and [Action] has been taken on [Date] [Time].
Details:
Server Name: [Server Name]
File name/Web content title: [File Name/Web Content Title]
File/Web content location:[File/Web Content

□ Write to Windows event log

FIGURE 7-6. Data Loss Prevention: Add Policy > Step 4: Specify Notification

Procedure

1. Select **Notify administrator** to enable notifications for this data loss prevention 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 Loss Prevention Notification).

   - **Message**—you can create a unique message using variables like: [Server Name], [Data Loss Prevention 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.

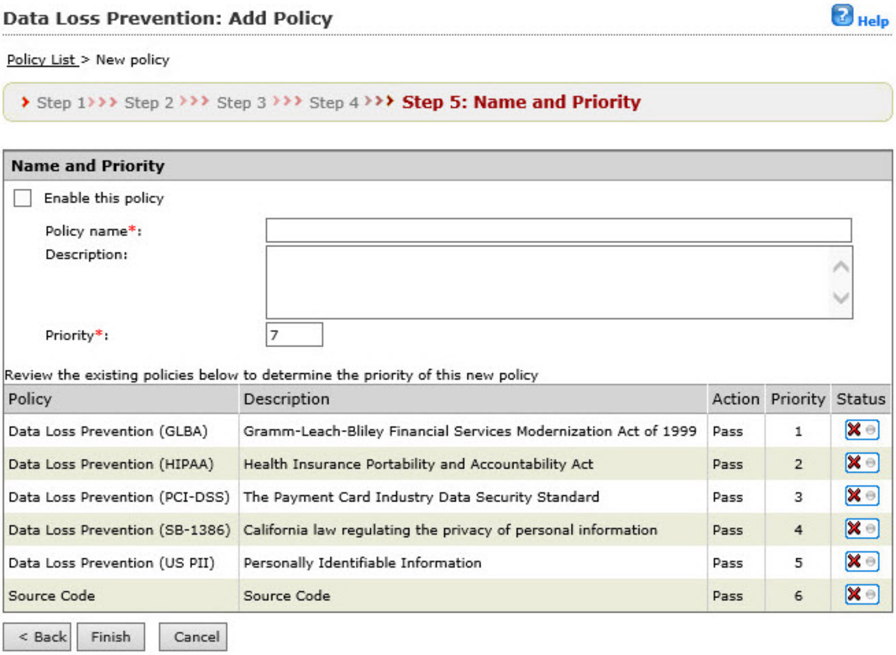
5. Click **Show details** to expand the options, and configure according to the following:

   - **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. Data Loss Prevention: Add Policy > Name and Priority



Data Loss Prevention: Add Policy

Policy List > New policy

› Step 1››› Step 2 ››› Step 3 ››› Step 4 ››› Step 5: Name and Priority

Name and Priority

☐ Enable this policy

Policy name*:

Description:

Priority*: 7

Review the existing policies below to determine the priority of this new policy

Policy	Description	Action	Priority	Status
Data Loss Prevention (GLBA)	Gramm-Leach-Bliley Financial Services Modernization Act of 1999	Pass	1	☒ ⊖
Data Loss Prevention (HIPAA)	Health Insurance Portability and Accountability Act	Pass	2	☒ ⊖
Data Loss Prevention (PCI-DSS)	The Payment Card Industry Data Security Standard	Pass	3	☒ ⊖
Data Loss Prevention (SB-1386)	California law regulating the privacy of personal information	Pass	4	☒ ⊖
Data Loss Prevention (US PII)	Personally Identifiable Information	Pass	5	☒ ⊖
Source Code	Source Code	Pass	6	☒ ⊖

FIGURE 7-7. Data Loss Prevention: Add Policy > Step 5: Name and Priority screen

Procedure

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.

   Note

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

4. Click **Finish**.

   The Data Loss Prevention main screen displays where your new policy will appear in the priority you selected.

Editing a Data Loss Prevention Policy

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

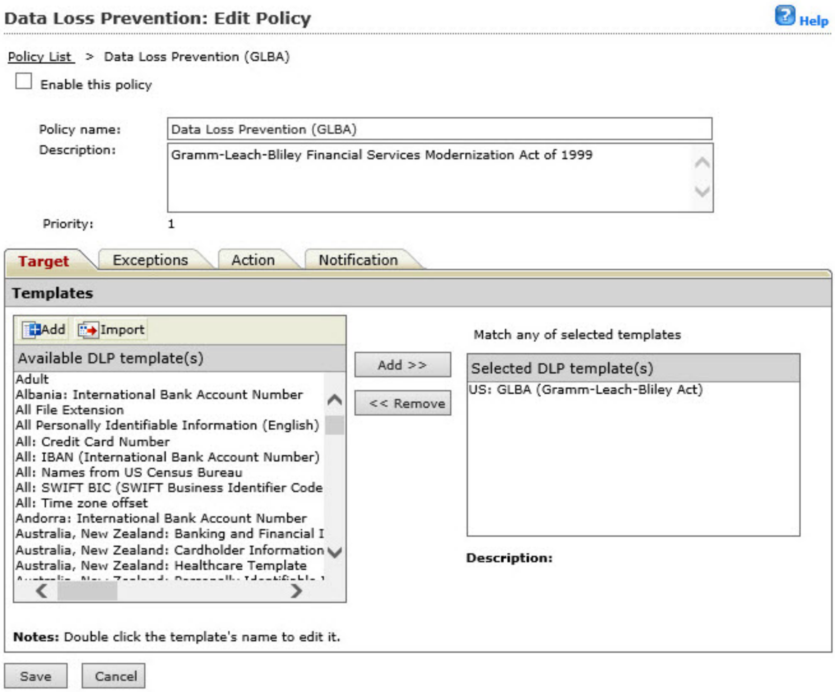
Procedure

1. On the left menu, click **Data Loss Prevention** > **Policy**.

   The **Data Loss Prevention** screen appears.

2. From the **Data Loss Prevention** screen, click the policy name link you want to edit.

The **Data Loss Prevention: Edit Policy** screen appears.



Data Loss Prevention: Edit Policy

Policy List > Data Loss Prevention (GLBA)

□ Enable this policy

Policy name: Data Loss Prevention (GLBA)

Description: Gramm-Leach-Bliley Financial Services Modernization Act of 1999

Priority: 1

Available DLP template(s)

Adult
Albania: International Bank Account Number
All File Extension
All Personally Identifiable Information (English)
All: Credit Card Number
All: IBAN (International Bank Account Number)
All: Names from US Census Bureau
All: SWIFT BIC (SWIFT Business Identifier Code
All: Time zone offset
Andorra: International Bank Account Number
Australia, New Zealand: Banking and Financial I
Australia, New Zealand: Cardholder Information
Australia, New Zealand: Healthcare Template
Australia, New Zealand: Personally Identifiable I

Match any of selected templates

Selected DLP template(s)

US: GLBA (Gramm-Leach-Bliley Act)

Description:

Notes: Double click the template's name to edit it.

FIGURE 7-8. Data Loss Prevention: 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.

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

Note

Press and hold the Ctrl key to select multiple DLP templates.

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

7. To add a DLP template to the list of available DLP templates:

    a. Click the **Add** button, which is located next to the **Import** button.

       The **Add DLP Template** screen appears.

    b. Type a name for the new template in the **DLP template name** field.

    c. Type an optional description for the new template in the **Description** field.

8. To define a DLP template, select from the following:

    a. If you select **Expressions...**

       Choose an expression from the list, for example, **US: SSN (Social Security Number)**, **All: Credit Card Number**, or **US: Phone Number**.

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

    c. Click the "+" to add additional DLP template(s).

        i. Select the appropriate operator **And/Or**.

        ii. Repeat the previous process by choosing **Expressions** and select one of the available expressions from the list.

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

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

        i. Choose one of the keywords from the list of available keywords.

        ii. Click the "+" to add additional DLP template(s).

   iii. Select the appropriate operator **And/Or**.

   iv. Repeat the previous process by choosing **Keywords** and select one of the available keywords from the list.

9. After you finish adding your DLP template(s), click **Add**, then click **Save**.

   The **Data Loss Prevention: Edit Policy > Target** tab appears.

10. Click the **Exceptions** tab and add or edit any exceptions as required.

    See *Step 2. Data Loss Prevention: Add Policy > Step 2: Exceptions on page 7-20* 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 *Step 4. Data Loss Prevention: Add Policy > Specify Notification on page 7-24* for more information.

13. Click **Save**.

Chapter 8

Web Reputation

This chapter describes how to configure PortalProtect to protect your network and computers from web-based threats.

Topics include:

About 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.

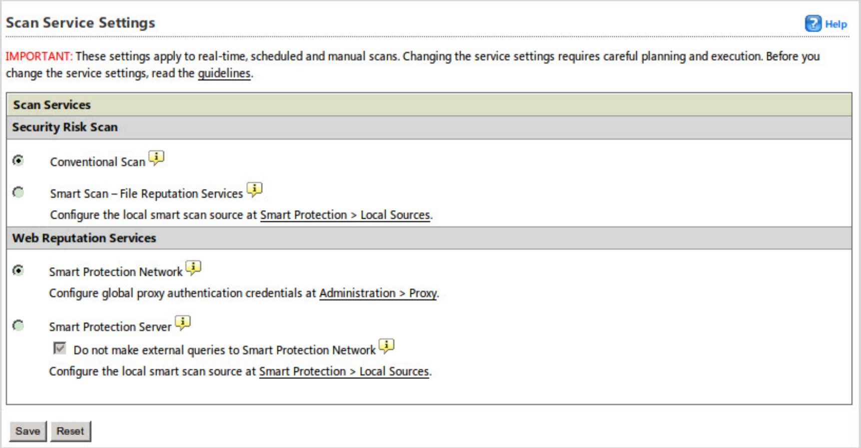
The Local Smart Protection Server uses the Trend Micro Smart Protection Network, which is your private next-generation cloud-client content security infrastructure designed to protect your SharePoint environment from security risks and Web threats. Protection is automatically updated and strengthened 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.

Choosing a Web Reputation Source

Procedure

1. Click **Smart Protection** > **Scan Service Settings** from the left menu.

   The **Scan Service Settings** screen appears.



Scan Service Settings

IMPORTANT: These settings apply to real-time, scheduled and manual scans. Changing the service settings requires careful planning and execution. Before you change the service settings, read the guidelines.

Scan Services

Security Risk Scan

● Conventional Scan

○ Smart Scan – File Reputation Services

Configure the local smart scan source at Smart Protection > Local Sources.

Web Reputation Services

● Smart Protection Network

Configure global proxy authentication credentials at Administration > Proxy.

○ Smart Protection Server

☑ Do not make external queries to Smart Protection Network

Configure the local smart scan source at Smart Protection > Local Sources.

FIGURE 8-1. Scan Service Settings screen

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 2-8* 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**, PortalProtect will only query the local smart scan server; if you clear the checkbox, PortalProtect 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 3-5* for instructions on how to configure this screen.

3. Click **Save**.

> **Note**
>
> Refer to *Alerts on page 11-32* for information on configuring your alerts when your smart servers are unavailable and/or come back online.

Enabling Real-time Web Reputation

Procedure

1. Log on to the product console.

2. Click **Web Reputation** from the main menu.

The **Web Reputation** screen displays.

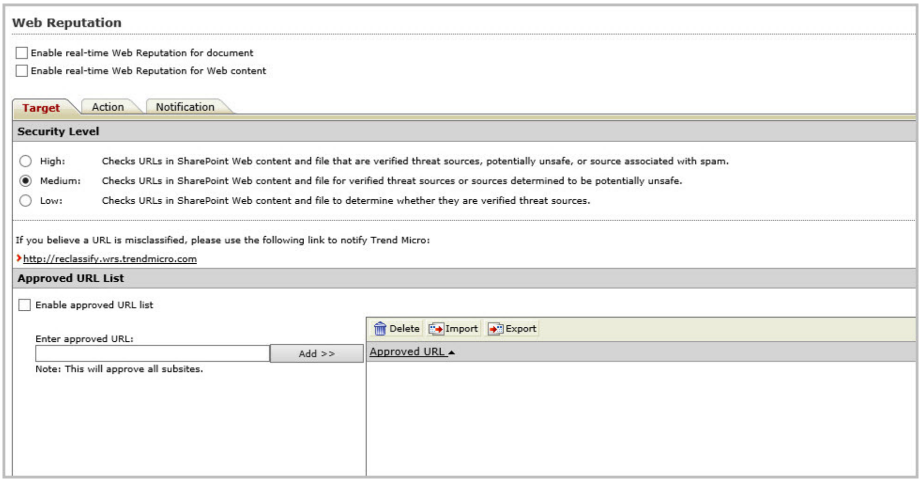
3. Select either or both of the following options:

- **Enable real-time Web Reputation for document**
- **Enable real-time Web Reputation for Web content**

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.



Web Reputation

□ Enable real-time Web Reputation for document

□ Enable real-time Web Reputation for Web content

Security Level

○ High: Checks URLs in SharePoint Web content and file that are verified threat sources, potentially unsafe, or source associated with spam.

● Medium: Checks URLs in SharePoint Web content and file for verified threat sources or sources determined to be potentially unsafe.

○ Low: Checks URLs in SharePoint Web content and file to determine whether they are verified threat sources.

If you believe a URL is misclassified, please use the following link to notify Trend Micro:

http://reclassify.wrs.trendmicro.com

Approved URL List

□ Enable approved URL list

Enter approved URL:

Note: This will approve all subsites.

FIGURE 8-2. Web Reputation target tab

- **Enable real-time Web Reputation for document**: 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 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.
- 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.

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.

Procedure

1. Log on to the product console.

2. Click **Web Reputation** from the main menu.

   The **Web Reputation** screen displays.

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.

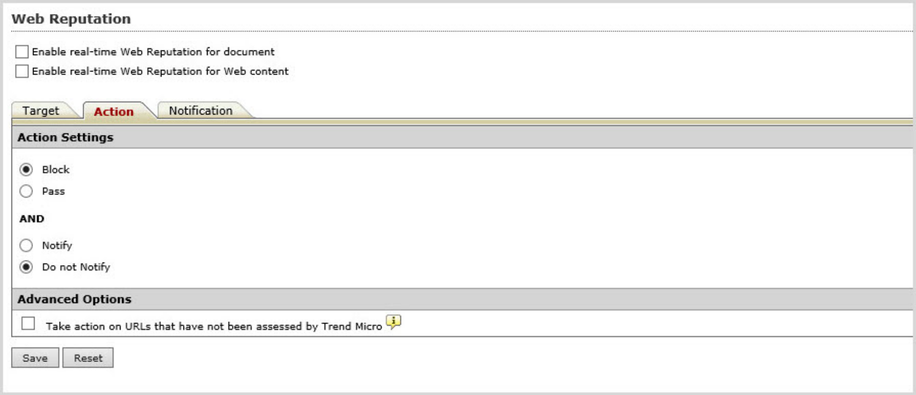
4. Select **Enable approved URL list** to avoid scanning URLs deemed safe under your security policy.

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.



Web Reputation

□ Enable real-time Web Reputation for document

□ Enable real-time Web Reputation for Web content

Action Settings

● Block

○ Pass

AND

○ Notify

● Do not Notify

Advanced Options

□ Take action on URLs that have not been assessed by Trend Micro

FIGURE 8-3. Web Reputation action tab

- **Block**
- **Pass**
- **Notify**: Select to send a notification
- **Do not notify**: Select to not send a notification
- **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.

Procedure

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.

Chapter 9

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.

In this chapter, you will find information about:

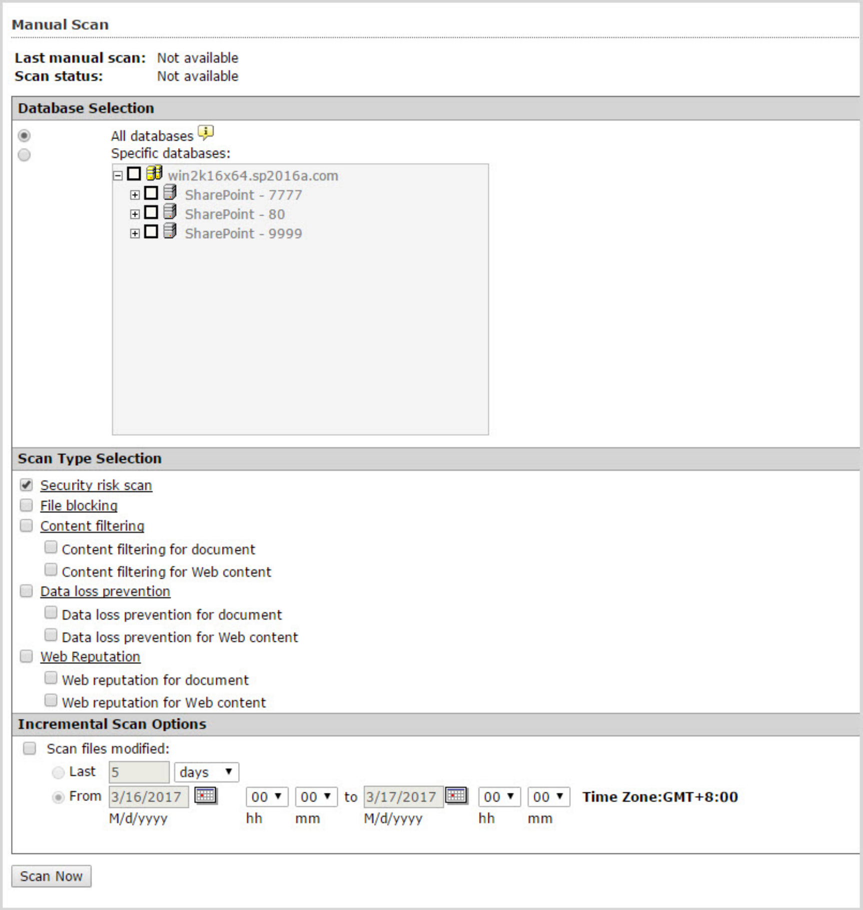
Configuring a Manual Scan

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

Procedure

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

The **Manual Scan** screen appears.



Manual Scan

Last manual scan: Not available
Scan status: Not available

Database Selection

● All databases
○ Specific databases:

- ⊟ □ win2k16x64.sp2016a.com
  - ⊞ □ SharePoint - 7777
  - ⊞ □ SharePoint - 80
  - ⊞ □ SharePoint - 9999

Scan Type Selection

- ☑ Security risk scan
- □ File blocking
- □ Content filtering
  - □ Content filtering for document
  - □ Content filtering for Web content
- □ Data loss prevention
  - □ Data loss prevention for document
  - □ Data loss prevention for Web content
- □ Web Reputation
  - □ Web reputation for document
  - □ Web reputation for Web content

Incremental Scan Options

□ Scan files modified:

○ Last 5 days

● From 3/16/2017 (M/d/yyyy) 00 (hh) 00 (mm) to 3/17/2017 (M/d/yyyy) 00 (hh) 00 (mm) Time Zone:GMT+8:00

FIGURE 9-1. Manual Scan main screen

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 loss prevention**, or **Web Reputation** links to configure the manual scan options. For more information, refer to:

About Content Filtering Action Settings on page 6-3

Configuring Manual Scan: Security Risk Scan on page 9-7

Configuring Manual Scan: File Blocking on page 9-12

Configuring Manual Scan: Content Filtering on page 9-19

Configuring Manual Scan: Data Loss Prevention on page 9-24

Configuring Manual Scan: Web Reputation on page 9-29

- **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.

  a. **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.

  b. **Content filtering for Web content**: select to scan Web content posted to SharePoint according to the content filtering options and policies you choose.

- **Data loss prevention**: select to perform a manual data loss prevention scan.

  a. **Data loss prevention for document**: select to scan documents according to the data loss prevention options and policies you choose.

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

- **Web Reputation**: select to perform a manual scan for Web Reputation.

   a. **Web reputation for document**: select to scan and block files containing URLs that are classified as unsafe. See *About Web Reputation on page 8-2* for more information.

   b. **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**.

Scanning Compressed Files for Manual Scan

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

Procedure

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 1-100-MB.

5. Select and type values for **Do not scan compressed files if**, according to the following:

   - **Decompressed file count exceeds [xxxxx]**—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**.

Configuring Macro Scanning Options for Manual Scan

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

Procedure

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**.

Configuring Manual Scan: Security Risk Scan

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

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

Procedure

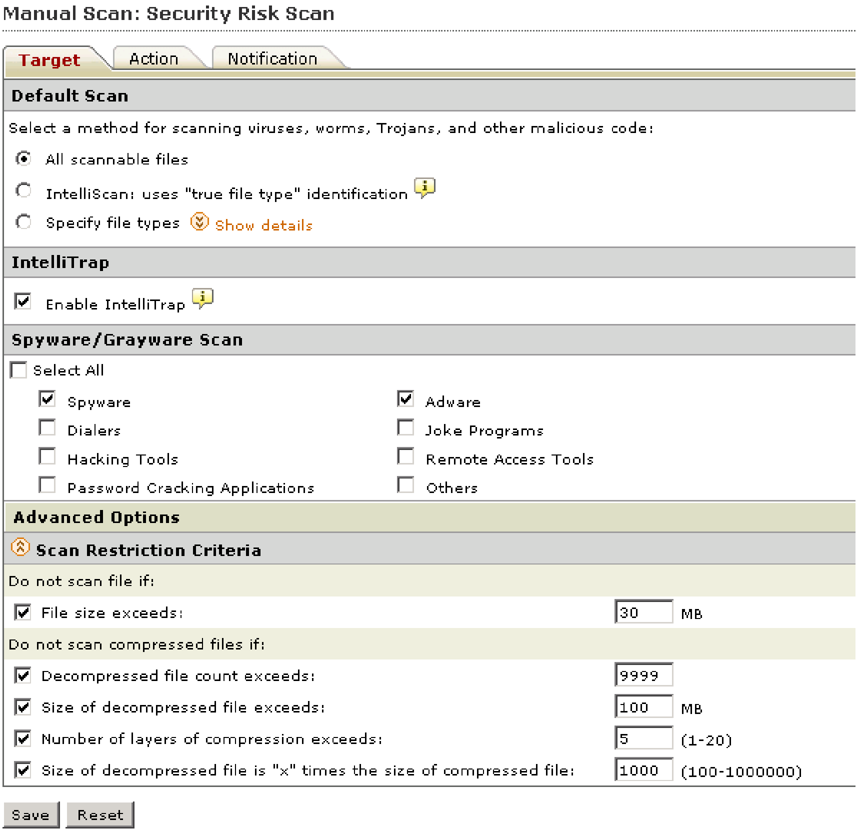
1. On the left menu, click **Manual Scan**.

   The **Manual Scan** screen appears.

2. As a prerequisite, be sure to configure the options as described in *Configuring a Manual Scan on page 9-2*.

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

The **Manual Scan: Security Risk Scan** screen appears.



Manual Scan: Security Risk Scan

Default Scan

Select a method for scanning viruses, worms, Trojans, and other malicious code:

● All scannable files

○ IntelliScan: uses "true file type" identification

○ Specify file types

IntelliTrap

☑ Enable IntelliTrap

Spyware/Grayware Scan

□ Select All

☑ Spyware	☑ Adware
□ Dialers	□ Joke Programs
□ Hacking Tools	□ Remote Access Tools
□ Password Cracking Applications	□ Others

Advanced Options

Scan Restriction Criteria

Do not scan file if:

☑ File size exceeds: 30 MB

Do not scan compressed files if:

☑ Decompressed file count exceeds: 9999

☑ Size of decompressed file exceeds: 100 MB

☑ Number of layers of compression exceeds: 5 (1-20)

☑ Size of decompressed file is "x" times the size of compressed file: 1000 (100-1000000)

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

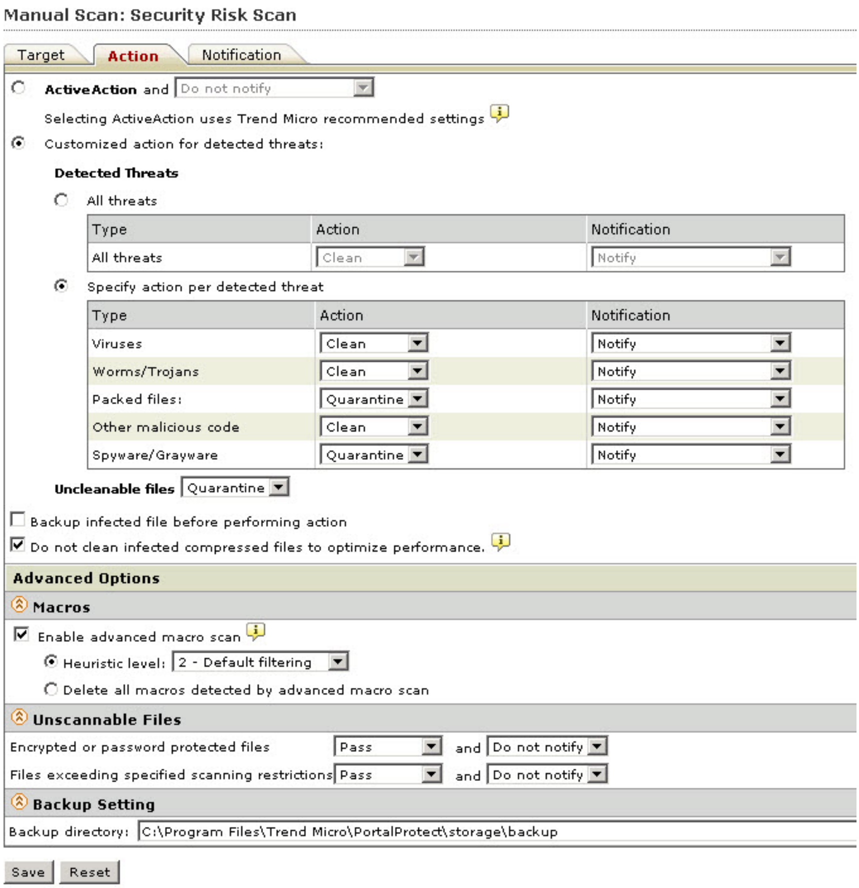
4. Configure the settings for the **Target** tab as described in *About Security Risk Scan Action Settings on page 4-7*.

Step 2. Configure Manual Scan: Security Risk Scan (Action tab)

Procedure

1. After completing the settings for the **Target** tab, click the **Action** tab.

   The **Manual Scan: Security Risk Scan** screen appears with the **Action** tab.



Manual Scan: Security Risk Scan

○ **ActiveAction** and Do not notify

Selecting ActiveAction uses Trend Micro recommended settings

● Customized action for detected threats:

Detected Threats

○ All threats

Type	Action	Notification
All threats	Clean	Notify

● Specify action per detected threat

Type	Action	Notification
Viruses	Clean	Notify
Worms/Trojans	Clean	Notify
Packed files:	Quarantine	Notify
Other malicious code	Clean	Notify
Spyware/Grayware	Quarantine	Notify

Uncleanable files Quarantine

□ Backup infected file before performing action

☑ Do not clean infected compressed files to optimize performance.

Advanced Options

Macros

☑ Enable advanced macro scan

● Heuristic level: 2 - Default filtering

○ Delete all macros detected by advanced macro scan

Unscannable Files

Encrypted or password protected files Pass and Do not notify

Files exceeding specified scanning restrictions Pass and Do not notify

Backup Setting

Backup directory: C:\Program Files\Trend Micro\PortalProtect\storage\backup

FIGURE 9-3. Manual Scan: Security Risk Scan (Action tab)

2. Choose from the available options for the Manual Security Risk Scan.

   Refer to *Configuring Security Risk Scan: Action Settings on page 4-8* and the following table.

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

THREAT TYPE	AVAILABLE ACTIONS
All threats	Clean, Quarantine, Delete, Pass or Rename
Viruses	Clean, Quarantine, Delete, Pass or Rename
Worms/Trojans	Quarantine, Delete, Pass or Rename
Packed files	Quarantine, Delete, Pass or Rename
Other malicious code	Clean, Quarantine, Delete, Pass, or Rename
Spyware/Grayware	Quarantine, Delete, Pass or Rename
Uncleanable files	Quarantine, Delete, Pass or Rename

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

Procedure

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

Configuring Manual Scan: File Blocking

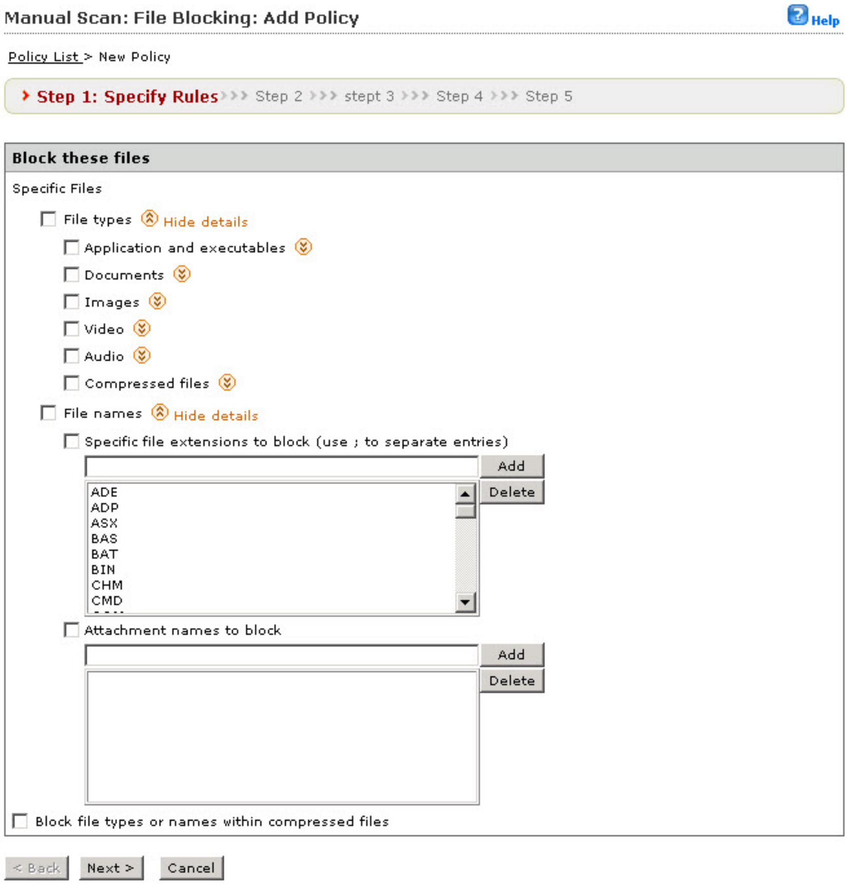
This section describes the steps required to configure File Blocking for Manual Scan.

Procedure

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.



Manual Scan: File Blocking: Add Policy

Policy List > New Policy

› Step 1: Specify Rules >>> Step 2 >>> stept 3 >>> Step 4 >>> Step 5

Block these files

Specific Files

- □ File types Hide details
  - □ Application and executables
  - □ Documents
  - □ Images
  - □ Video
  - □ Audio
  - □ Compressed files
- □ File names Hide details
  - □ Specific file extensions to block (use ; to separate entries)
    - ADE
    - ADP
    - ASX
    - BAS
    - BAT
    - BIN
    - CHM
    - CMD
  - □ Attachment names to block

□ Block file types or names within compressed files

FIGURE 9-4. Manual Scan: File Blocking: Add Policy > Step 1. Specify Rules screen

4. Continue through the steps that follow to complete the configuration for this new policy.

Step 1. Manual Scan: File Blocking: Add Policy > Specify Rules

Procedure

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 through Table 5-7 under *About Available File Types on page 5-15*.

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 **Manual Scan: File Blocking: Add Policy Step 2: Exceptions** screen appears.

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

Procedure

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.

8. Click **Next>**.

   The **Manual Scan: File Blocking: Add Policy Step 3: Specify Action** screen appears.

Step 3. Manual Scan: File Blocking: Add Policy > Specify Action

Procedure

1. Select an action from the following options:

   - **Quarantine**

   - **Delete**

- **Pass**

2. Select from the following:

   - **Notify**
   - **Do not notify**

3. Click **Next>**.

   The **Manual Scan: File Blocking: Add Policy Step 4: Specify Notification** screen appears.

Step 4. Manual Scan: File Blocking: Add Policy > Specify Notification

Procedure

1. Under People to notify, select from the following:

   - **Notify violator**
   - **Notify administrator**

   Note

   Refer to *Configuring File Blocking Notifications on page 11-5* for more information about setting up notifications.

2. Click **Next>**.

   The **Manual Scan: File Blocking: Add Policy Step 5: Name and priority** screen appears.

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

Procedure

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).

   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.

Importing File Blocking Rules

File Blocking for Manual Scan enables you to import rules from real-time scan for File Blocking, however the actions performed between real-time and manual scan differ and will be imported as illustrated in the following table.

TABLE 9-2. File Blocking Import Rule Mapping

Scan Type	Action in Real-time Scan	Action in Manual or Scheduled Scan
File Blocking for File	Block	Quarantine
	Pass	Pass

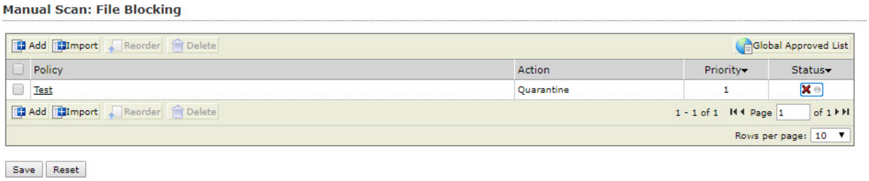
Procedure

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

   The **Manual Scan** screen appears.

2. Under **Scan Type Selection**, click the **File blocking** link.

   The **Manual Scan: File Blocking** screen appears.

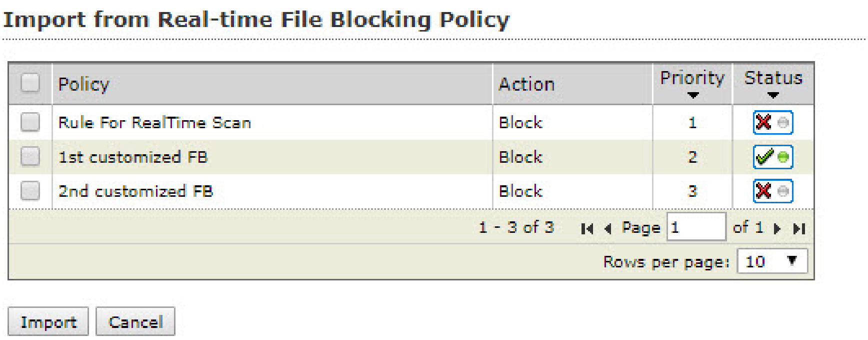


Manual Scan: File Blocking

□	Policy	Action	Priority▾	Status▾
□	Test	Quarantine	1	✗

3. Click **Import**.

The **Import from Real-time File Blocking Policy** screen appears.



Import from Real-time File Blocking Policy

□	Policy	Action	Priority	Status
□	Rule For RealTime Scan	Block	1	✗
□	1st customized FB	Block	2	✓
□	2nd customized FB	Block	3	✗

FIGURE 9-5. Import from Real-time File Blocking Policy screen

4. Select the policies you want to import, and click **Import**.

Configuring Manual Scan: Content Filtering

This section describes the steps required to configure Content Filtering for Manual Scan.

Importing Content Filtering Rules

Content Filtering for Manual 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 the following table.

TABLE 9-3. Content Filtering Import Rule Mapping

SCAN TYPE	ACTION IN REAL-TIME SCAN	ACTION IN MANUAL OR SCHEDULED SCAN
Content Filtering for File	Block	Quarantine
	Pass	Pass

Scan Type	Action in Real-time Scan	Action in Manual or Scheduled Scan
Content Filtering for Web Content	Block	Pass
	Pass	Pass

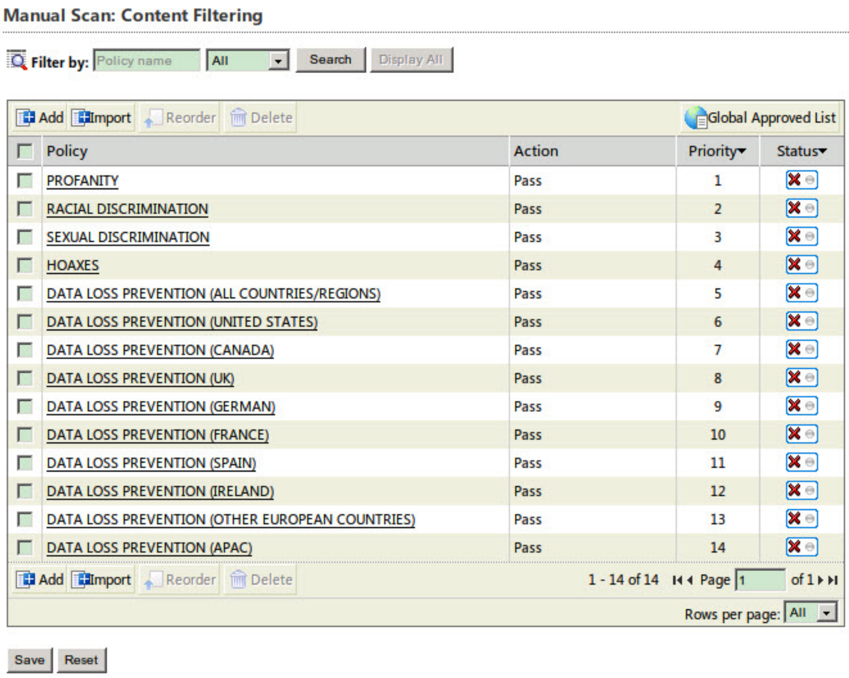
Procedure

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

   The **Manual Scan** screen appears.

2. Under **Select the scan type**, click the **Content filtering** link.

   The **Manual Scan: Content Filtering** screen appears.



Manual Scan: Content Filtering

Filter by: Policy name | All | Search | Display All

Add | Import | Reorder | Delete | Global Approved List

□	Policy	Action	Priority	Status
□	PROFANITY	Pass	1	✗ ⊖
□	RACIAL DISCRIMINATION	Pass	2	✗ ⊖
□	SEXUAL DISCRIMINATION	Pass	3	✗ ⊖
□	HOAXES	Pass	4	✗ ⊖
□	DATA LOSS PREVENTION (ALL COUNTRIES/REGIONS)	Pass	5	✗ ⊖
□	DATA LOSS PREVENTION (UNITED STATES)	Pass	6	✗ ⊖
□	DATA LOSS PREVENTION (CANADA)	Pass	7	✗ ⊖
□	DATA LOSS PREVENTION (UK)	Pass	8	✗ ⊖
□	DATA LOSS PREVENTION (GERMAN)	Pass	9	✗ ⊖
□	DATA LOSS PREVENTION (FRANCE)	Pass	10	✗ ⊖
□	DATA LOSS PREVENTION (SPAIN)	Pass	11	✗ ⊖
□	DATA LOSS PREVENTION (IRELAND)	Pass	12	✗ ⊖
□	DATA LOSS PREVENTION (OTHER EUROPEAN COUNTRIES)	Pass	13	✗ ⊖
□	DATA LOSS PREVENTION (APAC)	Pass	14	✗ ⊖

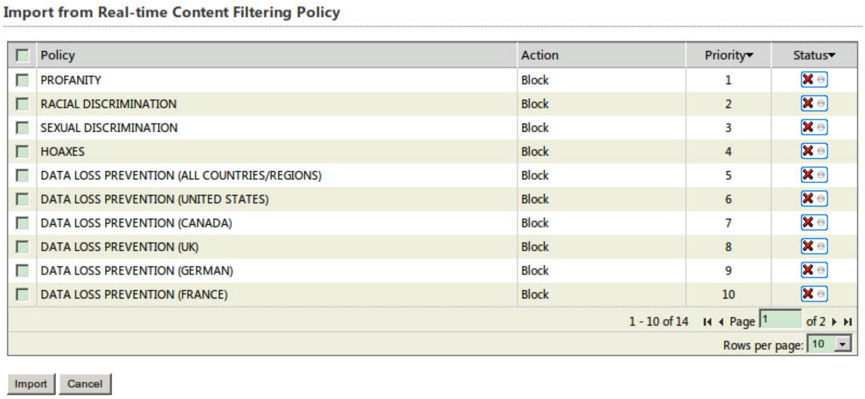
Add | Import | Reorder | Delete 1 - 14 of 14 Page 1 of 1

Rows per page: All

Save | Reset

3. Click **Import**.

   The **Import from Real-time Content Filtering Policy** screen appears.



Import from Real-time Content Filtering Policy

□	Policy	Action	Priority▾	Status▾
□	PROFANITY	Block	1	✖ ⊖
□	RACIAL DISCRIMINATION	Block	2	✖ ⊖
□	SEXUAL DISCRIMINATION	Block	3	✖ ⊖
□	HOAXES	Block	4	✖ ⊖
□	DATA LOSS PREVENTION (ALL COUNTRIES/REGIONS)	Block	5	✖ ⊖
□	DATA LOSS PREVENTION (UNITED STATES)	Block	6	✖ ⊖
□	DATA LOSS PREVENTION (CANADA)	Block	7	✖ ⊖
□	DATA LOSS PREVENTION (UK)	Block	8	✖ ⊖
□	DATA LOSS PREVENTION (GERMAN)	Block	9	✖ ⊖
□	DATA LOSS PREVENTION (FRANCE)	Block	10	✖ ⊖

1 - 10 of 14 ⏮ ◀ Page 1 of 2 ▶ ⏭

Rows per page: 10

FIGURE 9-6. Import from Real time Content Filtering Policy screen

4. Select the policies you want to import, and click **Import**.

Configuring a Manual Scan: Content Filtering scan

Procedure

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

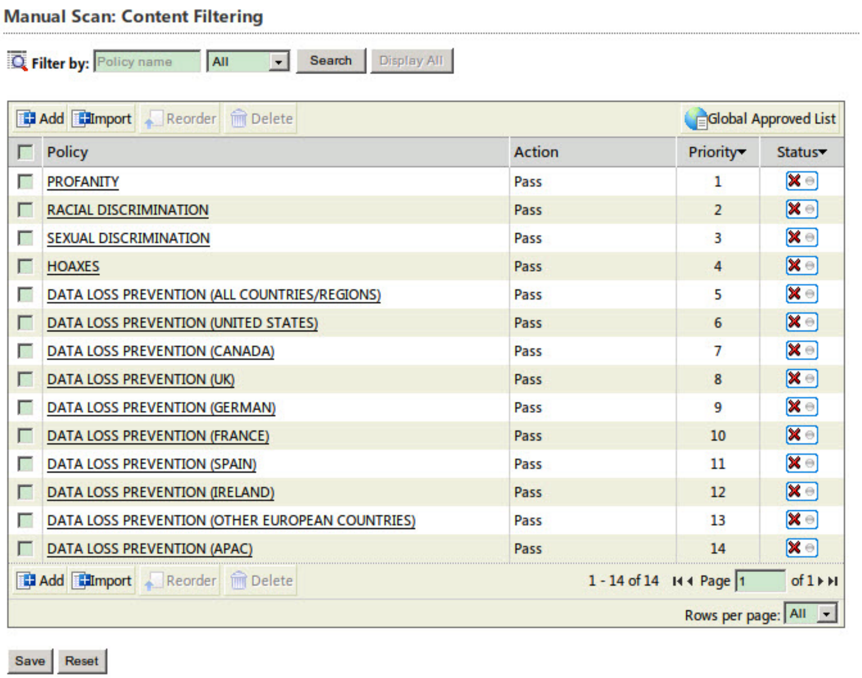
   The **Manual Scan** screen appears.

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.



Manual Scan: Content Filtering

Filter by: Policy name | All | Search | Display All

Add | Import | Reorder | Delete | Global Approved List

□	Policy	Action	Priority	Status
□	PROFANITY	Pass	1	✗
□	RACIAL DISCRIMINATION	Pass	2	✗
□	SEXUAL DISCRIMINATION	Pass	3	✗
□	HOAXES	Pass	4	✗
□	DATA LOSS PREVENTION (ALL COUNTRIES/REGIONS)	Pass	5	✗
□	DATA LOSS PREVENTION (UNITED STATES)	Pass	6	✗
□	DATA LOSS PREVENTION (CANADA)	Pass	7	✗
□	DATA LOSS PREVENTION (UK)	Pass	8	✗
□	DATA LOSS PREVENTION (GERMAN)	Pass	9	✗
□	DATA LOSS PREVENTION (FRANCE)	Pass	10	✗
□	DATA LOSS PREVENTION (SPAIN)	Pass	11	✗
□	DATA LOSS PREVENTION (IRELAND)	Pass	12	✗
□	DATA LOSS PREVENTION (OTHER EUROPEAN COUNTRIES)	Pass	13	✗
□	DATA LOSS PREVENTION (APAC)	Pass	14	✗

Add | Import | Reorder | Delete | 1 - 14 of 14 | Page 1 of 1

Rows per page: All

Save | Reset

FIGURE 9-7. Manual Scan: Content Filtering 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 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 on page 6-9*.

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 *Configuring Manual Scan Notifications—Content Filtering on page 11-16*.
21. Click **Save**.

Configuring Manual Scan: Data Loss Prevention

This section describes the steps required to configure Data Loss Prevention for Manual Scan.

Importing Data Loss Prevention Rules

Data Loss Prevention for Manual Scan enables you to import rules from real-time scan for Data Loss Prevention, however the actions performed between real-time and manual scan differ and will be imported as illustrated in the following table.

TABLE 9-4. Data Loss Prevention Import Rule Mapping

SCAN TYPE	ACTION IN REAL-TIME SCAN	ACTION IN MANUAL OR SCHEDULED SCAN
Data Loss Prevention for File	Block	Quarantine
	Pass	Pass
Data Loss Prevention for Web Content	Block	Pass
	Pass	Pass

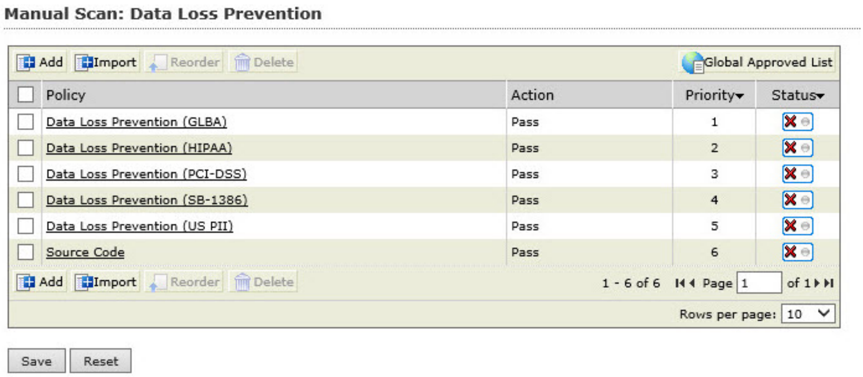
Procedure

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

   The **Manual Scan** screen appears.

2. Under **Select the scan type**, click the **Data loss prevention** link.

   The **Manual Scan: Data Loss Prevention** screen appears.



Manual Scan: Data Loss Prevention

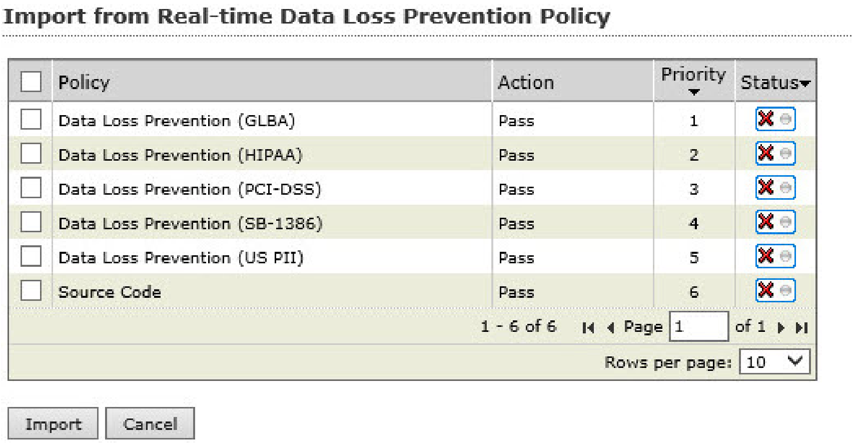
□	Policy	Action	Priority	Status
□	Data Loss Prevention (GLBA)	Pass	1	✗
□	Data Loss Prevention (HIPAA)	Pass	2	✗
□	Data Loss Prevention (PCI-DSS)	Pass	3	✗
□	Data Loss Prevention (SB-1386)	Pass	4	✗
□	Data Loss Prevention (US PII)	Pass	5	✗
□	Source Code	Pass	6	✗

1 - 6 of 6 Page 1 of 1

Rows per page: 10

3. Click **Import**.

The **Import from Real-time Data Loss Prevention Policy** screen appears.



Import from Real-time Data Loss Prevention Policy

□	Policy	Action	Priority	Status
□	Data Loss Prevention (GLBA)	Pass	1	✗ ⊖
□	Data Loss Prevention (HIPAA)	Pass	2	✗ ⊖
□	Data Loss Prevention (PCI-DSS)	Pass	3	✗ ⊖
□	Data Loss Prevention (SB-1386)	Pass	4	✗ ⊖
□	Data Loss Prevention (US PII)	Pass	5	✗ ⊖
□	Source Code	Pass	6	✗ ⊖

FIGURE 9-8. Import from Real time Data Loss Prevention Policy screen

4. Select the policies you want to import, and click **Import**.

Configuring a Manual Scan: Data Loss Prevention Scan

Procedure

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

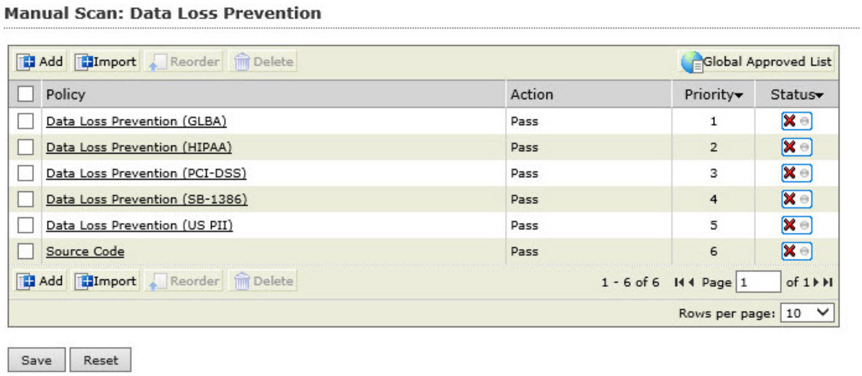
   The **Manual Scan** screen appears.

2. Under **Scan Type Selection**, select whether to perform content filtering for the following:

   - **Data loss prevention for document**
   - **Data loss prevention for Web content**

3. Click the **Data loss prevention** link.

The **Manual Scan: Data Loss Prevention** screen appears.



Manual Scan: Data Loss Prevention

□	Policy	Action	Priority	Status
□	Data Loss Prevention (GLBA)	Pass	1	✗
□	Data Loss Prevention (HIPAA)	Pass	2	✗
□	Data Loss Prevention (PCI-DSS)	Pass	3	✗
□	Data Loss Prevention (SB-1386)	Pass	4	✗
□	Data Loss Prevention (US PII)	Pass	5	✗
□	Source Code	Pass	6	✗

FIGURE 9-9. Manual Scan: Data Loss Prevention screen

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 loss 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 Loss Prevention Policy on page 7-17*.

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 Loss Prevention: 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**.

Configuring Manual Scan: Web Reputation

This section describes the steps required to configure Web Reputation for Manual Scan.

Procedure

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

   The **Manual Scan** screen appears.

2. As a prerequisite, be sure to configure the options as described in *Configuring a Manual Scan on page 9-2*.

3. Under **Select the scan type**, click the **Web Reputation** link.

   The **Manual Scan: Web Reputation** screen appears.

4. Refer to *Smart Protection Source on page 3-5*, *About Web Reputation on page 8-2*, and *Choosing 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.

Chapter 10

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.

In this chapter, you will find information about:

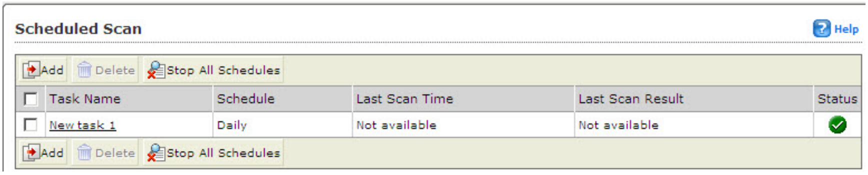
Configuring a Scheduled Scan

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

Procedure

1. On the left menu, click **Scheduled Scan**, to display the **Scheduled Scan** screen.

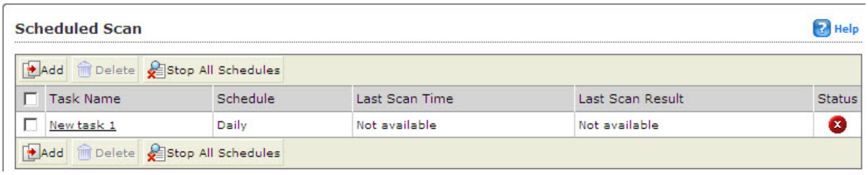
2. In the **Status** column, click the green checkmark to **disable** the scan; a red "X" then appears.



□	Task Name	Schedule	Last Scan Time	Last Scan Result	Status
□	New task 1	Daily	Not available	Not available	✓

FIGURE 10-1. Scheduled scan enabled

3. To enable a **Scheduled Scan**, click the red "X" in the **Status** column to display a green checkmark.



□	Task Name	Schedule	Last Scan Time	Last Scan Result	Status
□	New task 1	Daily	Not available	Not available	✗

FIGURE 10-2. Scheduled scan disabled

Note

Disabling the scan does not affect your configuration. When you decide to resume scheduled scanning, simply enable the scan again.

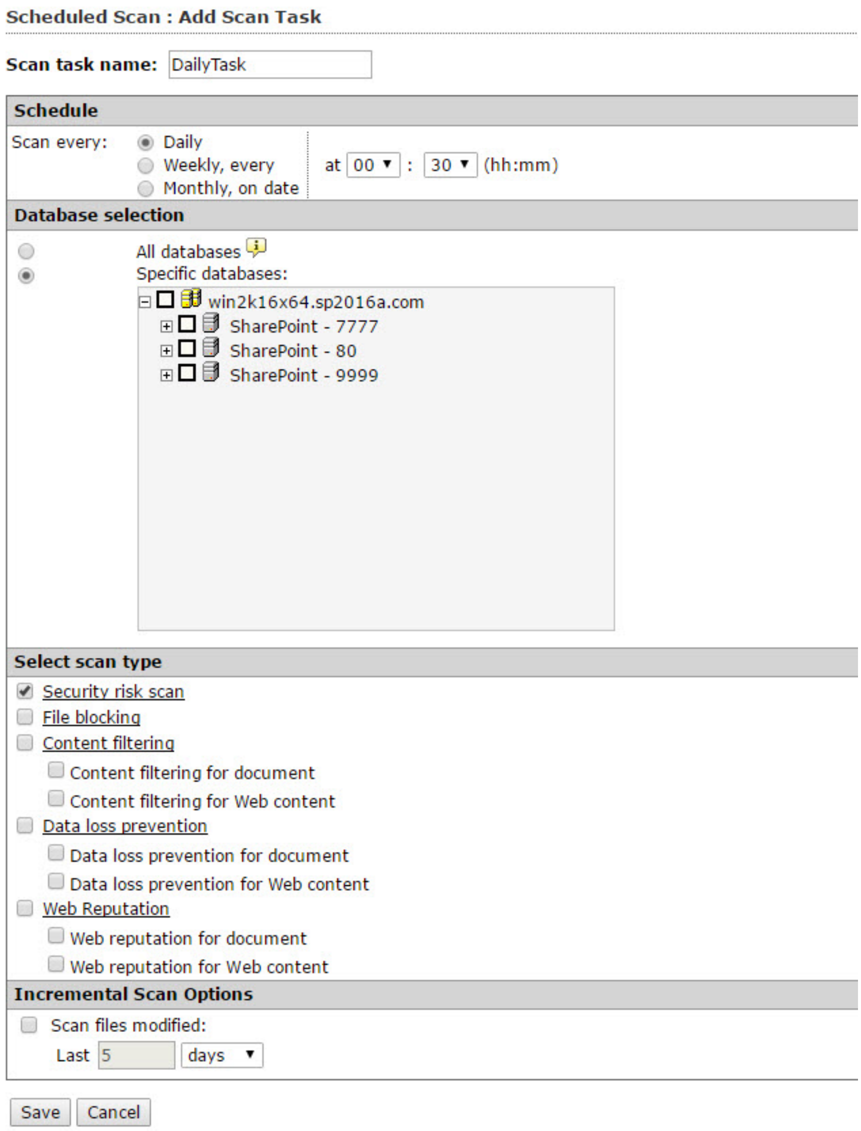
Adding or Editing a Scheduled Scan Task

This section explains the steps required to add or edit a scheduled scan task.

Procedure

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.



Scheduled Scan : Add Scan Task

Scan task name: DailyTask

Schedule

Scan every: ● Daily ○ Weekly, every ○ Monthly, on date at 00 : 30 (hh:mm)

Database selection

○ All databases

● Specific databases:

- □ win2k16x64.sp2016a.com
  - □ SharePoint - 7777
  - □ SharePoint - 80
  - □ SharePoint - 9999

Select scan type

- ☑ Security risk scan
- □ File blocking
- □ Content filtering
  - □ Content filtering for document
  - □ Content filtering for Web content
- □ Data loss prevention
  - □ Data loss prevention for document
  - □ Data loss prevention for Web content
- □ Web Reputation
  - □ Web reputation for document
  - □ Web reputation for Web content

Incremental Scan Options

□ Scan files modified:

Last 5 days

FIGURE 10-3. Scheduled Scan: Add Scan Task screen

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 loss prevention**, or **Web Reputation** links to configure the scheduled scan options. For more information, refer to:

   Configuring Scheduled Scan: Security Risk Scan on page 10-8

   Configuring Scheduled Scan: File Blocking Scan on page 10-11

   Configuring Scheduled Scan: Content Filtering on page 10-16

   Configuring Scheduled Scan: Data Loss Prevention on page 10-19

   Configuring Scheduled Scan: Web Reputation on page 10-22

   - **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 loss prevention**: select to perform a scheduled data loss prevention scan. Select or clear **Data loss prevention for document** or **Data loss prevention for Web content** as required

- **Web Reputation**: select to perform a manual scan for Web Reputation. Select or clear **Web Reputation for document** or **Web Reputation for Web content** as required.

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**.

Configuring Macro Scanning Options for Scheduled Scan

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

Procedure

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**.

Scanning Compressed Files for Scheduled Scan

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

Procedure

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 1-100-MB.

6. Select and type values for **Do not scan compressed files if**, according to the following:

   - **Decompressed file count exceeds [xxxxx]**—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**.

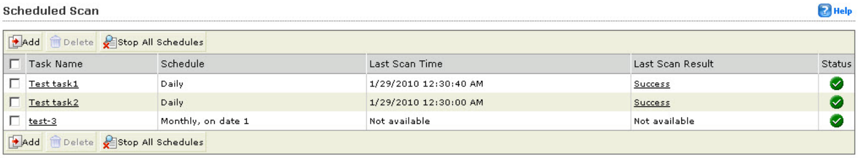
Configuring Scheduled Scan: Security Risk Scan

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

Procedure

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

The **Scheduled Scan** screen appears.



□	Task Name	Schedule	Last Scan Time	Last Scan Result	Status
□	Test task1	Daily	1/29/2010 12:30:40 AM	Success	✓
□	Test task2	Daily	1/29/2010 12:30:00 AM	Success	✓
□	test-3	Monthly, on date 1	Not available	Not available	✓

FIGURE 10-4. Scheduled Scan main screen

Note

As a prerequisite, 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.

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)

Procedure

1. Configure the settings for the **Target** tab as described in *About Security Risk Scan Action Settings on page 4-7*.

Step 2. Configure Scheduled Scan: Security Risk Scan (Action tab)

Procedure

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.

2. Choose from the available options for the Scheduled Security Risk Scan. Refer to *Step 2. Configure Manual Scan: Security Risk Scan (Action tab) on page 9-10* for more information.

3. Configure the **Advanced Options** as required. See *Configuring Macro Scanning Options for Scheduled Scan on page 10-6* for more information.

4. Configure the **Unscannable Files** settings as required. See *About Unscannable Files on page 1-23* for more information.

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

Procedure

1. Click the **Scheduled Scan: Security Risk Scan** > **Notification** tab.

2. Configure the **Notification** settings as required.

   Note

   Refer to *Configuring Scheduled Scan Notifications—Security Risk Scan on page 11-22* 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.

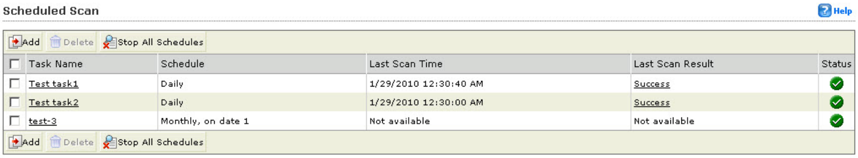
Configuring Scheduled Scan: File Blocking Scan

This section describes the steps required to configure a File Blocking Scan task for Scheduled Scan.

Procedure

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

   The **Scheduled Scan** screen appears.



Scheduled Scan

□	Task Name	Schedule	Last Scan Time	Last Scan Result	Status
□	Test task1	Daily	1/29/2010 12:30:40 AM	Success	✓
□	Test task2	Daily	1/29/2010 12:30:00 AM	Success	✓
□	test-3	Monthly, on date 1	Not available	Not available	✓

FIGURE 10-5. Scheduled Scan main screen

> **Note**
>
> As a prerequisite, 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.

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

Procedure

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 through Table 5-7 under *About Available File Types on page 5-15*.

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

Procedure

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.

8. Click **Next>**.

    The **Scheduled Scan: File Blocking: Add Policy Step 3: Specify Action** screen appears.

Step 3. Scheduled Scan: File Blocking: Add Policy > Specify Action

Procedure

1. Select an action from the following options:

- **Quarantine**
- **Delete**
- **Pass**

2. Select from the following:
    - **Notify**
    - **Do not notify**
3. Click **Next>**.

    The **Scheduled Scan: File Blocking: Add Policy Step 4: Specify Notification** screen appears.

Step 4. Manual Scan: File Blocking: Add Policy > Specify Notification

Procedure

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

    Note

    Refer to *Configuring Manual Scan Notifications—File Blocking on page 11-14* for details on setting notifications for this scan.

2. Click **Next>**.

    The **Scheduled Scan: File Blocking: Add Policy Step 5: Name and priority** screen appears.

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

Procedure

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.

Configuring 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:

- *About Content Filtering on page 6-2*
- *About Content Filtering Action Settings on page 6-3*
- *Content Filtering Policies on page 6-4*
- *Configuring Content Filtering on page 6-7*

Procedure

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 prerequisite, 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 > Specify Rules

Procedure

1. Add keywords and synonyms as described in *Adding a Content Filtering Policy 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

Procedure

1. Refer to *Step 2. Content Filtering: Add Policy > 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

Procedure

1. Select action and notification options. See *Step 3. Content Filtering: Add Policy > Specify Action on page 6-15* 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

Procedure

1. Select from the available options. See *Step 4. Content Filtering: Add Policy > Specify Notification on page 6-16* 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

Procedure

1. Configure the available options. See *Step 5. Content Filtering: Add Policy > Name and Priority on page 6-19* 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**.

Configuring Scheduled Scan: Data Loss Prevention

This section describes the steps required to configure Data Loss Prevention for Scheduled Scan.

For detailed background information on how to configure data loss prevention, refer to:

- *Data Loss Prevention on page 7-1*
- *Data Loss Prevention Policies on page 7-16*
- *DLP Compliance Templates on page 7-12*

Procedure

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 prerequisite, 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 loss prevention for the following:

- **Data loss prevention for document**
- **Data loss prevention for Web content**

5. Click the **Data loss prevention** link.

   The **Scheduled Scan: Data Loss Prevention** screen appears.

6. Click **Add** to create a new policy.

   The **Scheduled Scan: Data Loss Prevention: Add Policy > Step 1: Specify Rules** screen appears.

Step 1. Scheduled Scan: Data Loss Prevention: Add Policy > Specify Rules

Procedure

1. Configure as described in *Adding a Data Loss Prevention Policy on page 7-17*.

2. Click **Next>**.

   The **Scheduled Scan: Data Loss Prevention: Add Policy** screen appears.

Step 2. Scheduled Scan: Data Loss Prevention: Add Policy > Specify Sites to be Excluded

Procedure

1. Refer to *Step 2. Data Loss Prevention: Add Policy > Step 2: Exceptions on page 7-20* for details on how to configure this screen.

2. After completing any exceptions, click **Next>**.

   The **Scheduled Scan: Data Loss Prevention: Add Policy > Step 3: Specify Action** screen appears.

Step 3. Scheduled Scan: Data Loss Prevention: Add Policy > Specify Action

Procedure

1. Select action and notification options. See *Step 3. Data Loss Prevention: Add Policy > Specify Action on page 7-23* for details on how to configure this screen.

2. Click **Next>**.

   The **Scheduled Scan: Data Loss Prevention: Add Policy > Step 4: Specify Notification** screen appears.

Step 4. Scheduled Scan: Data Loss Prevention: Add Policy > Specify Notification

Procedure

1. Select from the available options. See *Step 4. Data Loss Prevention: Add Policy > Specify Notification on page 7-24* for details on how to configure this screen.

2. Click **Next>**.

   The **Scheduled Scan: Data Loss Prevention: Add Policy > Step 5: Name and Priority** screen appears.

Step 5. Scheduled Scan: Data Loss Prevention: Add Policy > Name and Priority

Procedure

1. Configure the available options. See *Step 5. Data Loss Prevention: Add Policy > Name and Priority on page 7-26* for details on how to configure this screen.

2. Click **Finish**.

   The **Scheduled Scan: Data Loss Prevention** screen appears with the new policy you just created.

3. Click **Save**.

Configuring 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:

- *About Web Reputation on page 8-2*
- *Local and Global Smart Protection on page 8-2*
- *Smart Protection Network on page 8-10*

Procedure

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

   The **Scheduled Scan** screen appears.

2. As a prerequisite, 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 *About Web Reputation on page 8-2* 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

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:

- *Configuring Security Risk Scan Notifications on page 11-4*
- *Configuring File Blocking Notifications on page 11-5*
- *Configuring Content Filtering Notifications on page 11-7*
- *Configuring Data Loss Prevention Notifications on page 11-8*
- *Configuring Web Reputation Notifications on page 11-10*
- *Configuring Manual Scan Notifications—Security Risk Scan on page 11-12*
- *Configuring Manual Scan Notifications—File Blocking on page 11-14*
- *Configuring Manual Scan Notifications—Content Filtering on page 11-16*
- *Configuring Manual Scan Notifications—Data Loss Prevention on page 11-18*
- *Configuring Manual Scan Notifications—Web Reputation on page 11-20*
- *Configuring Scheduled Scan Notifications—Security Risk Scan on page 11-22*
- *Configuring Scheduled Scan Notifications—File Blocking on page 11-24*
- *Configuring Scheduled Scan Notifications—Content Filtering on page 11-26*
- *Configuring Scheduled Scan Notifications—Data Loss Prevention on page 11-28*
- *Configuring Scheduled Scan Notifications—Web Reputation on page 11-30*

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 Loss Prevention.

Configuring Global Notification Settings

Procedure

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 Loss Prevention.

Configuring Security Risk Scan Notifications

The following explains the steps required to configure security risk scan notifications:

Procedure

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**.

Configuring File Blocking Notifications

The following explains the steps required to configure file blocking notifications:

Procedure

1. On the left menu, click **File Blocking**. The **File Blocking** screen appears.

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**.

Configuring Content Filtering Notifications

The following explains the steps required to configure content filtering notifications:

Procedure

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 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**.

Configuring Data Loss Prevention Notifications

The following explains the steps required to configure data loss prevention notifications:

Procedure

1. On the left menu, click **Data Loss Prevention** > **Policies**. The **Data Loss Prevention** screen appears.

2. Click **Add**, to add a new policy, or click an existing policy from the **Policy** column. The **Data Loss Prevention: Edit Policy** screen appears.

3. Click the **Notification** tab.

4. Under **People to notify**, select **Notify administrator** to enable data loss prevention 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 Loss Prevention Notification).

    - **Message**—you can create a unique message using variables like: [Server Name], [Data Loss Prevention 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**.

Configuring Web Reputation Notifications

The following explains the steps required to configure Web Reputation notifications:

Procedure

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.

Configuring Manual Scan Notifications—Security Risk Scan

The following explains the steps required to configure manual scan security risk scan notifications:

Procedure

1. On the left menu, click **Manual Scan**. The **Manual Scan** screen appears.
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].

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**.

Configuring Manual Scan Notifications—File Blocking

The following explains the steps required to configure manual scan file blocking notifications:

Procedure

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**.

Configuring Manual Scan Notifications—Content Filtering

The following explains the steps required to configure manual scan content filtering notifications:

Procedure

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**.

Configuring Manual Scan Notifications—Data Loss Prevention

The following explains the steps required to configure manual scan data loss prevention notifications:

Procedure

1. On the left menu, click **Manual Scan**. The **Manual Scan** screen appears.
2. Under, **Select the scan type**, click the **Data loss prevention** 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 Loss Prevention Notification).
    - **Message**—you can create a unique message using variables like: [Server Name], [Data Loss Prevention 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 Loss Prevention Notification).

    - **Message**—you can create a unique message using variables like: [Server Name], [Data Loss Prevention 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**.

Configuring Manual Scan Notifications—Web Reputation

The following explains the steps required to configure manual scan Web Reputation notifications:

Procedure

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.

Configuring Scheduled Scan Notifications—Security Risk Scan

The following explains the steps required to configure scheduled scan notifications for security risk scan:

Procedure

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**.

Configuring Scheduled Scan Notifications—File Blocking

The following explains the steps required to configure scheduled scan notifications for file blocking:

Procedure

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**.

Configuring Scheduled Scan Notifications—Content Filtering

The following explains the steps required to configure scheduled scan notifications for content filtering:

Procedure

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**.

Configuring Scheduled Scan Notifications—Data Loss Prevention

The following explains the steps required to configure scheduled scan notifications for data loss prevention:

Procedure

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 loss prevention** 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 Loss Prevention Notification).
- **Message**—you can create a unique message using variables like: [Server Name], [Data Loss Prevention 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**.

Configuring Scheduled Scan Notifications—Web Reputation

The following explains the steps required to configure scheduled scan notifications for Web reputation:

Procedure

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. 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]

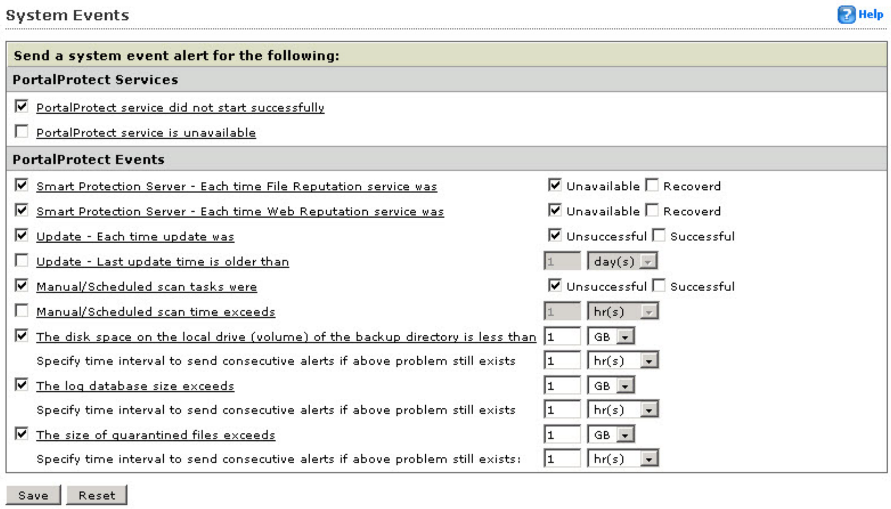
    Specify time interval to send consecutive alerts if above problem still exists [x] [min(s)/hr(s)]

- 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.



System Events

Help

Send a system event alert for 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 □ Recoverd

☑ Smart Protection Server - Each time Web Reputation service was — ☑ Unavailable □ Recoverd

☑ Update - Each time update was — ☑ Unsuccessful □ Successful

□ Update - Last update time is older than — 1 day(s)

☑ Manual/Scheduled scan tasks were — ☑ Unsuccessful □ Successful

□ Manual/Scheduled scan time exceeds — 1 hr(s)

☑ The disk space on the local drive (volume) of the backup directory is less than — 1 GB

Specify time interval to send consecutive alerts if above problem still exists — 1 hr(s)

☑ The log database size exceeds — 1 GB

Specify time interval to send consecutive alerts if above problem still exists — 1 hr(s)

☑ The size of quarantined files exceeds — 1 GB

Specify time interval to send consecutive alerts if above problem still exists: — 1 hr(s)

Save Reset

FIGURE 11-1. System Events configuration screen

Configuring System Events for PortalProtect Services

Procedure

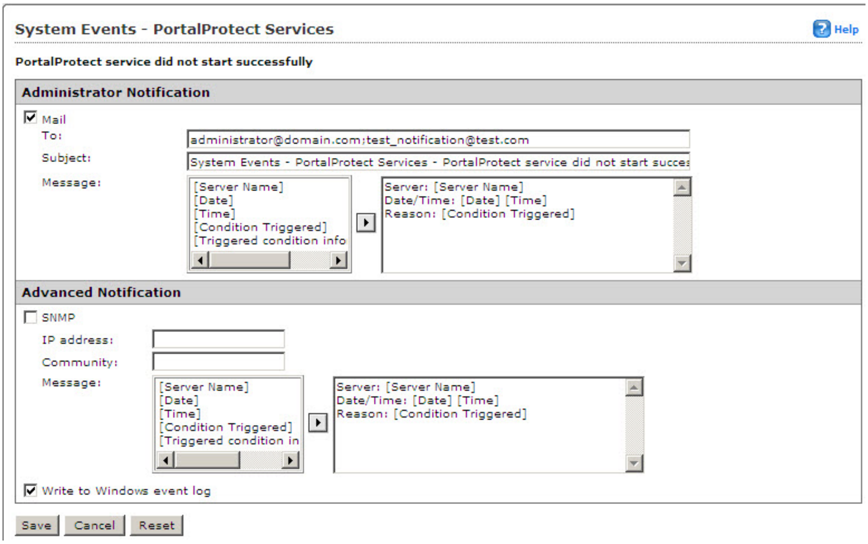
1. Click **Alerts** > **System Events**. The **System Events** screen appears.
2. Under PortalProtect Services, select from the following options:
   - **PortalProtect service did not start successfully**

- **PortalProtect service is unavailable**

3. After selecting an option, click the link to display the **Administrator Notification** screen.

4. Create a custom message and email list as explained in *Configuring Security Risk Scan Notifications on page 11-4*.

5. Click **Save**.



System Events - PortalProtect Services

PortalProtect service did not start successfully

Administrator Notification

☑ Mail

To: administrator@domain.com;test_notification@test.com

Subject: System Events - PortalProtect Services - PortalProtect service did not start succes

Message:

```
[Server Name]
[Date]
[Time]
[Condition Triggered]
[Triggered condition info
```

```
Server: [Server Name]
Date/Time: [Date] [Time]
Reason: [Condition Triggered]
```

Advanced Notification

☐ SNMP

IP address:

Community:

Message:

```
[Server Name]
[Date]
[Time]
[Condition Triggered]
[Triggered condition in
```

```
Server: [Server Name]
Date/Time: [Date] [Time]
Reason: [Condition Triggered]
```

☑ Write to Windows event log

FIGURE 11-2. System Events, administrator notification screen

Configuring System Events for PortalProtect Events

Procedure

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.

> **Note**
>
> 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.

4. Create a custom message and email list as explained in *Configuring Security Risk Scan Notifications on page 11-4*.

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

Configuring an Outbreak Alert

Procedure

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.

3. Configure the following options:

   - Select, **Virus detected reach the following number within the shown time:** [number] [time value] [hours/minutes]

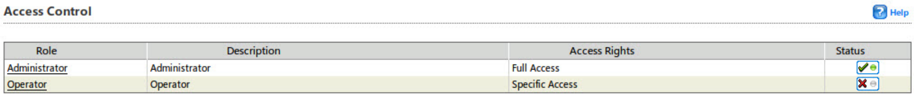
   - Select, **Uncleanable viruses reach the following number within the shown time:** [number] [time value] [hours/minutes]

   - Select, **Blocked files reach the following number within the shown time:** [number] [time value] [hours/minutes]

4. 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.



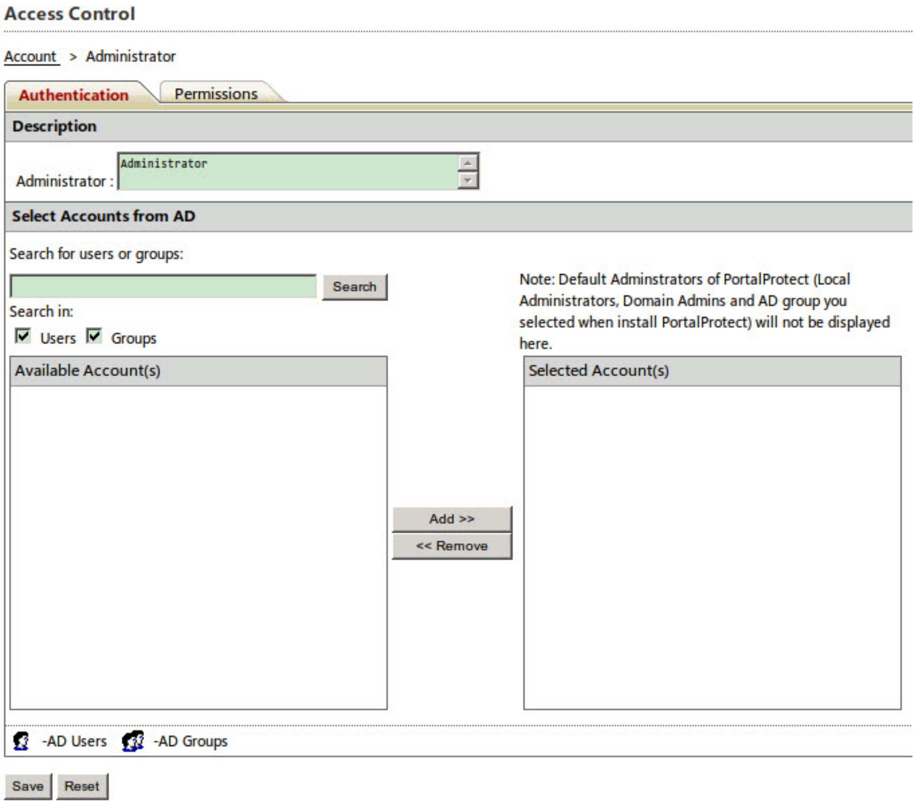
Access Control

Role	Description	Access Rights	Status
Administrator	Administrator	Full Access	✓
Operator	Operator	Specific Access	✗

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.



Access Control

Account > Administrator

Description

Administrator : Administrator

Select Accounts from AD

Search for users or groups:

Search in:

☑ Users ☑ Groups

Note: Default Adminstrators of PortalProtect (Local Administrators, Domain Admins and AD group you selected when install PortalProtect) will not be displayed here.

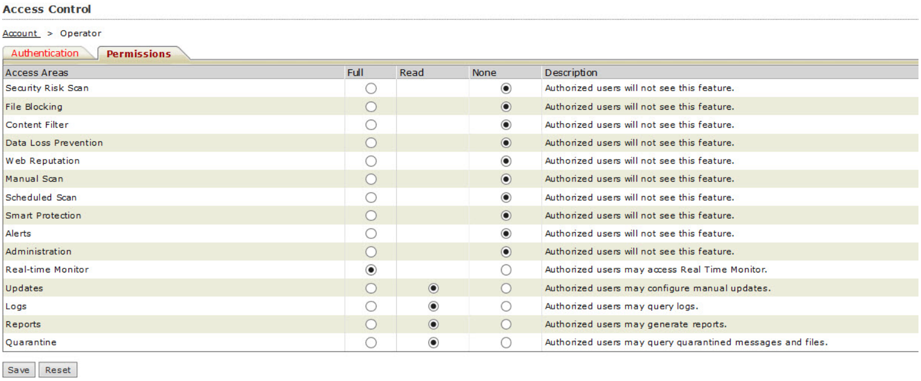
FIGURE 11-4. Access Control Authentication screen for administrator

The following provides a description of the various fields and functions found on the access control authentication screen:

- **Description**: this field enables you to modify the description for either the Administrator, or the Operator. The default descriptions are **Administrator** and **Operator**.
- **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.



Access Control

Account > Operator

Authentication | **Permissions**

Access Areas	Full	Read	None	Description
Security Risk Scan	○		●	Authorized users will not see this feature.
File Blocking	○		●	Authorized users will not see this feature.
Content Filter	○		●	Authorized users will not see this feature.
Data Loss Prevention	○		●	Authorized users will not see this feature.
Web Reputation	○		●	Authorized users will not see this feature.
Manual Scan	○		●	Authorized users will not see this feature.
Scheduled Scan	○		●	Authorized users will not see this feature.
Smart Protection	○		●	Authorized users will not see this feature.
Alerts	○		●	Authorized users will not see this feature.
Administration	○		●	Authorized users will not see this feature.
Real-time Monitor	●		○	Authorized users may access Real Time Monitor.
Updates	○	●	○	Authorized users may configure manual updates.
Logs	○	●	○	Authorized users may query logs.
Reports	○	●	○	Authorized users may generate reports.
Quarantine	○	●	○	Authorized users may query quarantined messages and files.

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:
  - **All**
  - **Detected virus/malware**
  - **Uncleanable virus/malware**
  - **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.
- **Data loss prevention** logs–contains information about the: Date & Time, Violator, Policy Name, Action, File Name/Web Content Title, Template(s), 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 Rick 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.

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.

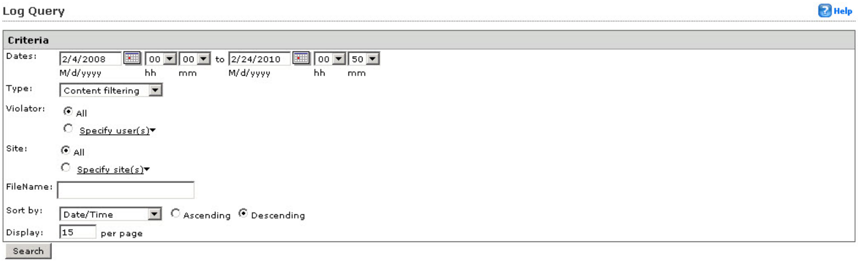
Performing a Log Query

Procedure

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.



Log Query

Criteria

Dates: 2/4/2008 (M/d/yyyy) 00 (hh) 00 (mm) to 2/24/2010 (M/d/yyyy) 00 (hh) 50 (mm)

Type: Content filtering

Violator: ● All ○ Specify user(s)

Site: ● All ○ Specify site(s)

FileName:

Sort by: Date/Time ○ Ascending ● Descending

Display: 15 per page

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 Deleting Logs

This procedure describes the steps required to manually delete logs for PortalProtect.

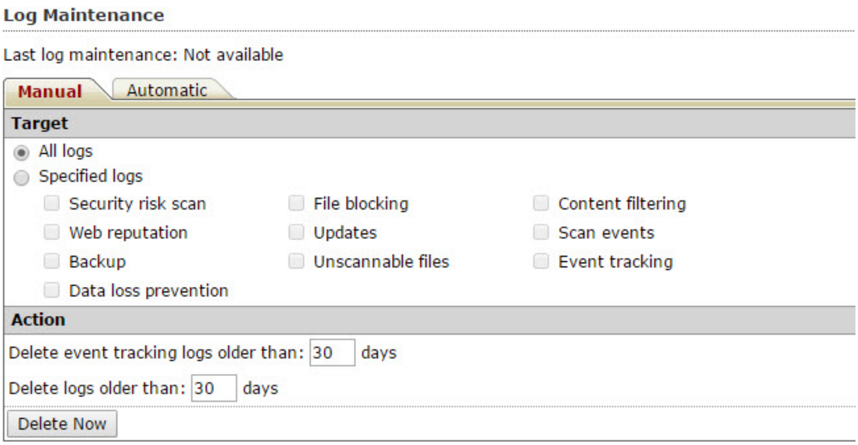
Procedure

1. From the left menu, click **Logs** > **Maintenance**, and select the **Manual** tab on the **Log Maintenance** screen.
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 loss prevention
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**.



Log Maintenance

Last log maintenance: Not available

Manual | Automatic

Target

● All logs

○ Specified logs

□ Security risk scan
□ Web reputation
□ Backup
□ Data loss prevention
□ File blocking
□ Updates
□ Unscannable files
□ Content filtering
□ Scan events
□ Event tracking

Action

Delete event tracking logs older than: 30 days

Delete logs older than: 30 days

Delete Now

FIGURE 11-7. Log Maintenance manual tab

Automatically Deleting 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.

Procedure

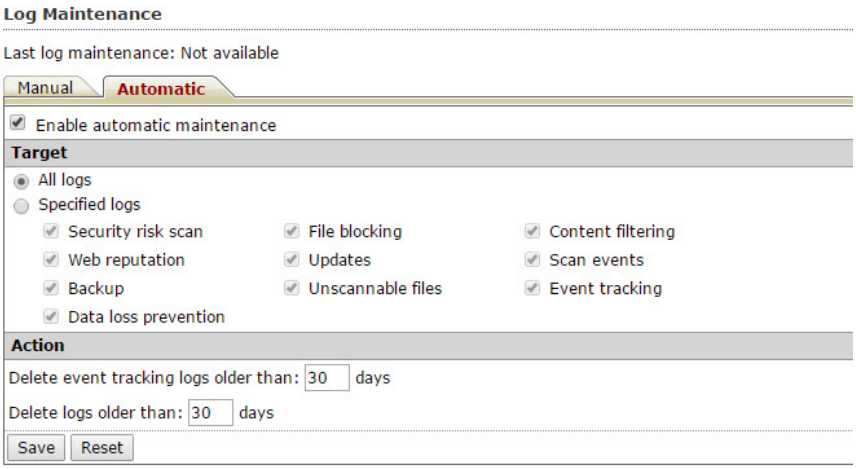
1. From the left menu, click **Logs** > **Maintenance**, and select the **Automatic** tab.

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 loss prevention
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

Last log maintenance: Not available

☑ Enable automatic maintenance

Target

● All logs

○ Specified logs

☑ Security risk scan ☑ File blocking ☑ Content filtering
☑ Web reputation ☑ Updates ☑ Scan events
☑ Backup ☑ Unscannable files ☑ Event tracking
☑ Data loss prevention

Action

Delete event tracking logs older than: 30 days

Delete logs older than: 30 days

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 functionality.

Quarantine Query

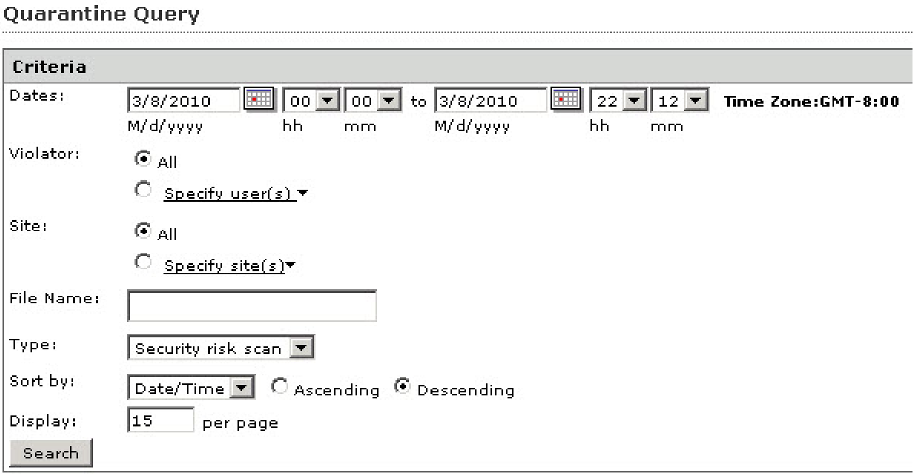
PortalProtect enables the administrator to query quarantined files using specific search criteria that includes:

- Date,
- Time,
- Violator (All or Specify user(s),

- Site (All or Specify site(s),
- File name, and
- Type (Security risk scan, File blocking, Content filtering, Data loss prevention, 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.



Quarantine Query

Criteria

Dates: 3/8/2010 M/d/yyyy 00 hh 00 mm to 3/8/2010 M/d/yyyy 22 hh 12 mm Time Zone:GMT-8:00

Violator: ● All ○ Specify user(s)

Site: ● All ○ Specify site(s)

File Name:

Type: Security risk scan

Sort by: Date/Time ○ Ascending ● Descending

Display: 15 per page

FIGURE 11-9. Quarantine Query main screen

TABLE 11-1. Default Quarantine Settings

SETTING NAME	DEFAULT SETTING
Date	One day
Violator	All **Note** Select specific violators from the Active Directory.
Sites	All **Note** Select specific sites from the site tree.
File Name	Null **Note** Type a specific file name, or leave blank to search all quarantined files according to the other search criteria.
Sort by	Date/Time Descending
Display	15 records per page

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 loss prevention can be downloaded after they are queried.

Performing a Quarantine Query

Procedure

1. From the left menu, click **Quarantine** > **Query**. The **Quarantine Query** screen appears.
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 loss prevention

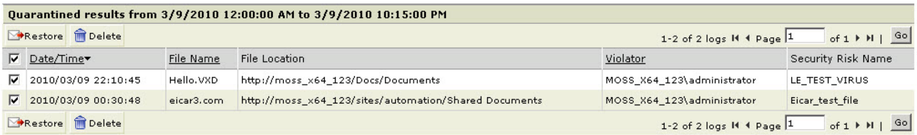
7. Select a sort option from the **Sort by** drop down; then, select **Ascending** or **Descending**.

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.



Quarantined results from 3/9/2010 12:00:00 AM to 3/9/2010 10:15:00 PM

☑	Date/Time	File Name	File Location	Violator	Security Risk Name
☑	2010/03/09 22:10:45	Hello.VXD	http://moss_x64_123/Docs/Documents	MOSS_X64_123\administrator	LE_TEST_VIRUS
☑	2010/03/09 00:30:48	eicar3.com	http://moss_x64_123/sites/automation/Shared Documents	MOSS_X64_123\administrator	Eicar_test_file

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 loss prevention 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)

Deleting, Restoring, or Downloading a Quarantined File

Procedure

1. Perform a quarantine query as described in *Quarantine Query on page 11-47*.

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

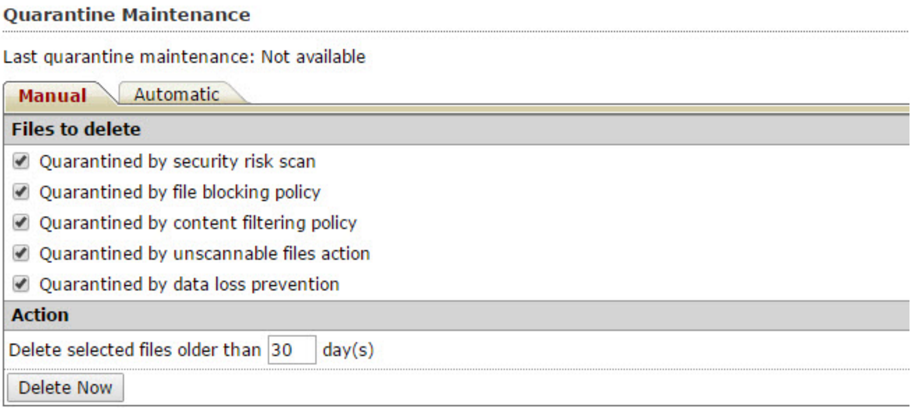
   For Content filtering, File blocking, Data loss prevention, and Unscannable files, you can click the File Name link to start a file download. You will have the option to open or save the file to the location you choose.

   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

Last quarantine maintenance: Not available

Files to delete

- ☑ Quarantined by security risk scan
- ☑ Quarantined by file blocking policy
- ☑ Quarantined by content filtering policy
- ☑ Quarantined by unscannable files action
- ☑ Quarantined by data loss prevention

Action

Delete selected files older than 30 day(s)

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.

Manually Deleting Quarantined Files

Procedure

1. Click **Quarantine** > **Maintenance** > **Manual** tab. The **Quarantine Maintenance** screen appears and displays the **Manual** tab.
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 loss prevention
3. Under **Action**, type a value in the **Delete selected files older than [xx] days** field.
4. Click **Delete Now**.

Automatically Deleting Quarantined Files

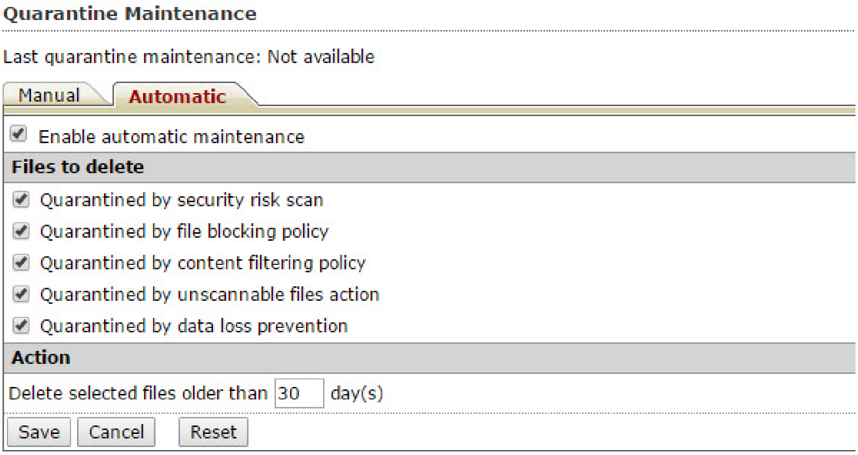
Procedure

1. Click **Quarantine** > **Maintenance** > **Automatic** tab. The **Quarantine Maintenance** screen appears and displays the **Automatic** tab.
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 loss prevention

4. Under **Action**, type a value in the **Delete selected files older than [xx] days** field.

5. Click **Save**.



Quarantine Maintenance

Last quarantine maintenance: Not available

☑ Enable automatic maintenance

Files to delete

☑ Quarantined by security risk scan

☑ Quarantined by file blocking policy

☑ Quarantined by content filtering policy

☑ Quarantined by unscannable files action

☑ Quarantined by data loss prevention

Action

Delete selected files older than 30 day(s)

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.

Generating a One-time Report

Procedure

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.
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

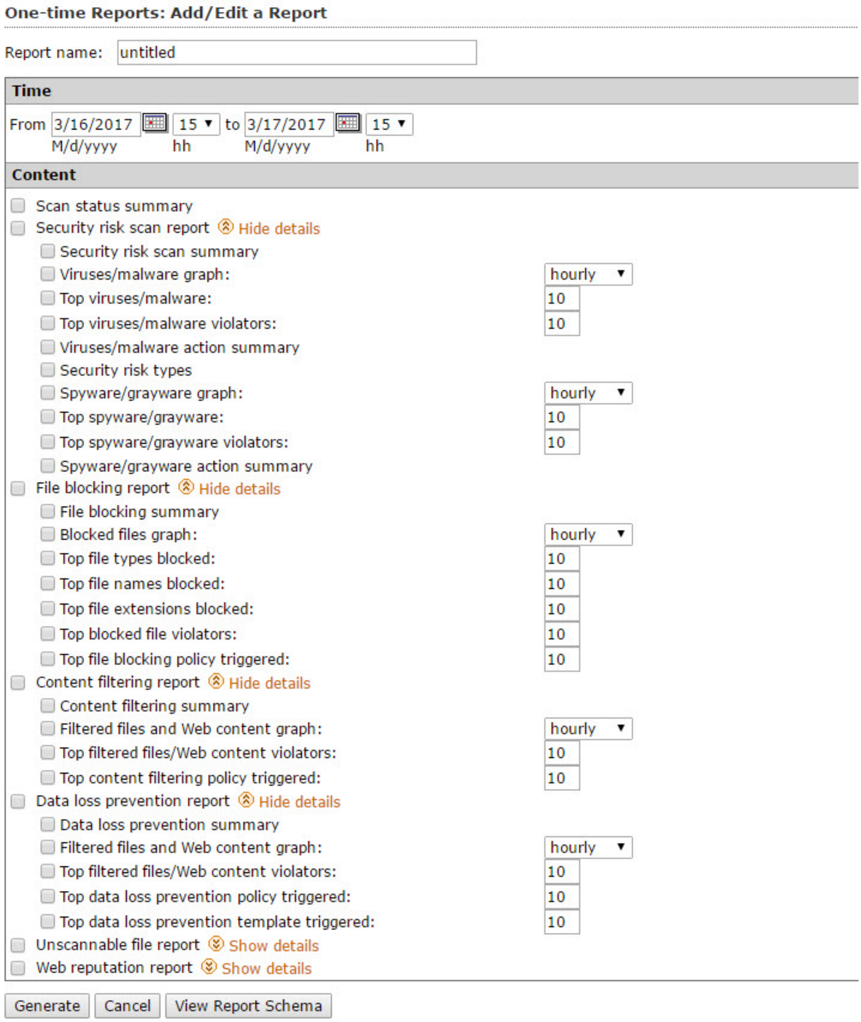
  - **Spyware/grayware graph**–from the drop down, choose whether the graph will display, hourly, daily, weekly or monthly data
  - **Top spyware/grayware**–select to display the top spyware/ grayware
  - **Top spyware/grayware violators**–select to display the top spyware/grayware violators
  - **Virus/grayware 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 loss prevention report**–select to enable and choose from the following:
    - **Data loss prevention 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 loss prevention policy triggered**–type the number of these top data loss prevention policies you want to appear in the report
    - **Top data loss prevention template triggered**–type the number of these top data loss prevention 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**.



One-time Reports: Add/Edit a Report

Report name: untitled

Time

From 3/16/2017 (M/d/yyyy) 15 ▾ (hh) to 3/17/2017 (M/d/yyyy) 15 ▾ (hh)

Content

- □ Scan status summary
- □ Security risk scan report
  - □ Security risk scan summary
  - □ Viruses/malware graph: hourly ▾
  - □ Top viruses/malware: 10
  - □ Top viruses/malware violators: 10
  - □ Viruses/malware action summary
  - □ Security risk types
  - □ Spyware/grayware graph: hourly ▾
  - □ Top spyware/grayware: 10
  - □ Top spyware/grayware violators: 10
  - □ Spyware/grayware action summary
- □ File blocking report
  - □ File blocking summary
  - □ Blocked files graph: hourly ▾
  - □ Top file types blocked: 10
  - □ Top file names blocked: 10
  - □ Top file extensions blocked: 10
  - □ Top blocked file violators: 10
  - □ Top file blocking policy triggered: 10
- □ Content filtering report
  - □ Content filtering summary
  - □ Filtered files and Web content graph: hourly ▾
  - □ Top filtered files/Web content violators: 10
  - □ Top content filtering policy triggered: 10
- □ Data loss prevention report
  - □ Data loss prevention summary
  - □ Filtered files and Web content graph: hourly ▾
  - □ Top filtered files/Web content violators: 10
  - □ Top data loss prevention policy triggered: 10
  - □ Top data loss prevention template triggered: 10
- □ Unscannable file report
- □ Web reputation report

FIGURE 11-13. Create one-time report screen

Creating a Scheduled Report

Procedure

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.
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

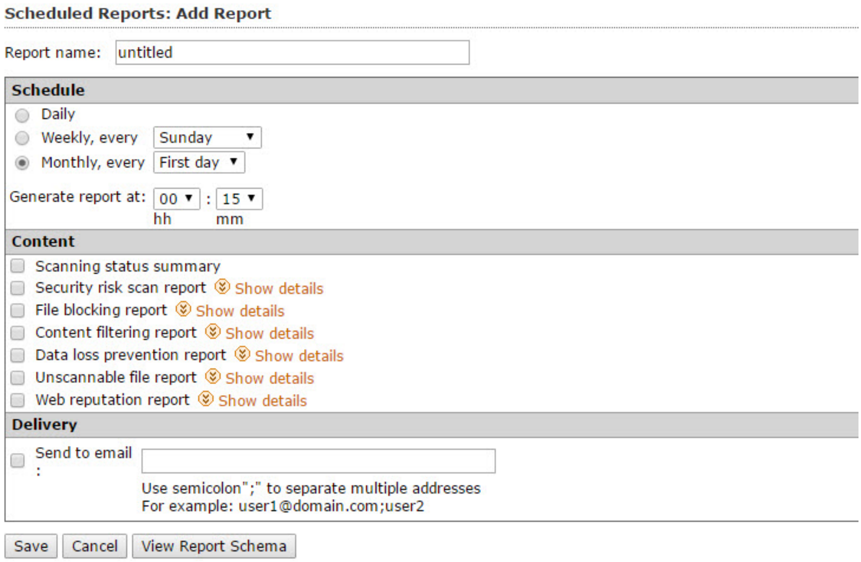
  - **Top viruses/malware violators**– type the number of top viruses/malware violators to display in the report
  - **Viruses/malware action summary**–select to display a summary of the action taken on all viruses and malware contained in the report
  - **Spyware/grayware graph**–from the drop down, choose 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 loss prevention report**–select to enable and choose from the following:
  - **Data loss prevention 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 loss prevention policy triggered**–type the number of these top policies you want to appear in the report
  - **Top data loss prevention 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

Report name: untitled

Schedule

○ Daily
○ Weekly, every Sunday ▾
● Monthly, every First day ▾

Generate report at: 00 ▾ : 15 ▾
hh mm

Content

□ Scanning status summary
□ Security risk scan report Show details
□ File blocking report Show details
□ Content filtering report Show details
□ Data loss prevention report Show details
□ Unscannable file report Show details
□ Web reputation report Show details

Delivery

□ Send to email :

Use semicolon";" to separate multiple addresses
For example: user1@domain.com;user2

FIGURE 11-14. Scheduled Reports: Add Report screen

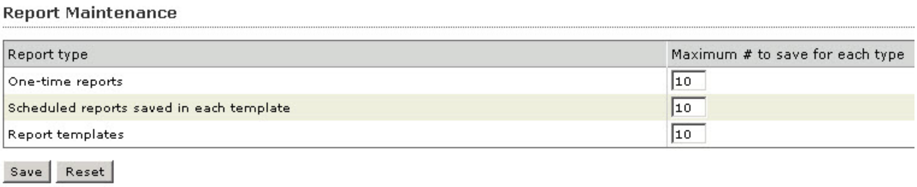
Tip

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



Report Maintenance

Report type	Maximum # to save for each type
One-time reports	10
Scheduled reports saved in each template	10
Report templates	10

FIGURE 11-15. Report Maintenance screen

Chapter 12

Technical Support

Learn about the following topics:

Troubleshooting Resources

Before contacting technical support, consider visiting the following Trend Micro online resources.

Using the Support Portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

1. Go to http://esupport.trendmicro.com.
2. Select from the available products or click the appropriate button to search for solutions.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Contact Support** and select the type of support needed.

   Tip

   To submit a support case online, visit the following URL:

   http://esupport.trendmicro.com/srf/SRFMain.aspx

   A Trend Micro support engineer investigates the case and responds in 24 hours or less.

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy.

The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to http://about-threats.trendmicro.com/us/threatencyclopedia#malware to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports

Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone or email:

Address	Trend Micro, Incorporated 225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A.
Phone	Phone: +1 (817) 569-8900 Toll-free: (888) 762-8736
Website	https://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:

  https://www.trendmicro.com/us/about-us/contact/index.html

- Trend Micro product documentation:

https://docs.trendmicro.com

Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional connected hardware or devices
- Amount of memory and free hard disk space
- Operating system and service pack version
- Version of the installed agent
- Serial number or Activation Code
- Detailed description of install environment
- Exact text of any error message received

Sending Suspicious Content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

https://ers.trendmicro.com/

Refer to the following Knowledge Base entry to send message samples to Trend Micro:

http://esupport.trendmicro.com/solution/en-US/1112106.aspx

File Reputation Services

Gather system information and submit suspicious file content to Trend Micro:

http://esupport.trendmicro.com/solution/en-us/1059565.aspx

Record the case number for tracking purposes.

Web Reputation Services

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and malware):

http://global.sitesafety.trendmicro.com/

If the assigned rating is incorrect, send a re-classification request to Trend Micro.

Other Resources

In addition to solutions and support, there are many other helpful resources available online to stay up to date, learn about innovations, and be aware of the latest security trends.

Download Center

From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to a specific product or service. To find out whether any patches are available, go to:

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

If a patch has not been applied (patches are dated), open the Readme file to determine whether it is relevant to your environment. The Readme file also contains installation instructions.

Documentation Feedback

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please go to the following site:

http://www.trendmicro.com/download/documentation/rating.asp

Appendix A

Frequently Asked Questions (FAQs)

This chapter covers some of the frequently asked questions and answers regarding PortalProtect features and functions.

In this chapter, you will find frequently asked questions and answers about:

Scanning

Content Filtering for Web Content or Web Reputation for Web Content is not working. Why?

Check the following:

1. Log on the PortalProtect Web console.
2. 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.
3. 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.
4. 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 Server 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 Server block list settings. SharePoint Server blocks files with the suffixes you specified. Use the SharePoint Server Central Management Page to modify the configuration.

To remove a file blocking configuration from SharePoint Server:

1. Select **Security Configuration**.
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 Server when it is uploaded or downloaded.

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 data loss prevention expression occurrences mean?

A data loss prevention (DLP) expression occurrence indicates that something from a document or Web content triggered an occurrence in a DLP expression. For example: A DLP policy contains an expression and the number of occurrences is set to “3”. For this scenario, when occurrences of the expression are less than “3”, documents and Web content posted to SharePoint sites will not trigger the corresponding DLP policy.

Why does PortalProtect not have Data Loss Prevention for documents or Data Loss Prevention for Web content?

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 loss prevention related features.

How can I skip some of the file type scans performed by Content Filtering, Data Loss Prevention, 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 Loss Prevention, Content Filtering and Web Reputation file scans.

When it is set to: "docx;pptx", PortalProtect will skip `.docx` and `.pptx` files in Data Loss Prevention, 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 Loss Prevention and URL in documents?

PortalProtect provides the following registry key to implement this function:

- Name: FileSizeThreshold
- Type: REG_DWORD

Description: Data Loss Prevention, 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.

ActiveUpdate

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:

https://<*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 PortalProtect for Microsoft SharePoint Master Service.
- **PortalProtect service is unavailable**: occurs if the PortalProtect_Master 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 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:
    - Remote Procedure Call (PRC)
    - Server
    - 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 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 HTTPS (default is 16373) port you specified during installation.
- Whether the Windows firewall on the PortalProtect server blocks the 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**. Scroll to **Security**, and clear the check box **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.

How does PortalProtect support IPv6?

PortalProtect provides IPv6 support in the following scenarios:

- Specifying target servers for installation
- Accessing the PortalProtect Web console
- Registering PortalProtect to Trend Micro Control Manager
- Specifying IP addresses for the download source
- Setting IP addresses for SNMP notifications
- Querying Web Reputation ratings

Appendix B

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 the Control Manager

Trend Micro Control Manager is a central management console that manages Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. Administrators can use the policy management feature to configure and deploy product settings to managed products and endpoints. 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 enables system administrators to monitor and report on activities such as infections, security violations, or virus/malware entry points. System administrators can download and deploy update components throughout the network, helping ensure that protection is consistent and up to date. Example update components include virus pattern files, scan engines, and anti-spam rules. Control Manager allows both manual and pre-scheduled updates. Control Manager allows the configuration and administration of products as groups or as individuals for added flexibility.

Configuring Control Manager Settings

The Control Manager Settings screen enables you to configure the settings for communication between the PortalProtect MCP Agent and the Control Manager servers.

Procedure

1. Click **Administration** > **Control Manager Settings** and configure the following options according to your requirements:

    - Top of Screen

        - Enable communication between the PortalProtect MCP agent and Control Manager: select to enable communication between the PortalProtect MCP agent and the Control manager

- Connection Status
  - Registered Control Manager server: indicates whether the Control Manager server is connected
- Connection Settings
  - Entity display name: shows the entity name that appears in the Control Manager product tree
- Control Manager Server Settings
  - Server FQDN or IP address: type the server FQDN or IP address
  - Port: type the port number, and select whether or not to use HTTPS
  - Web server authentication: type the Username and Password used for the IIS server

Note

Control Manager does not use the information provided for Web server authentication

- MCP Proxy Settings
  - **Use a proxy server for communication with the Control Manager server**: select to use a proxy server for communication with the Control Manager server
  - **Proxy protocol**: select whether to use HTTP or SOCKS 5
  - **Server FQDN or IP address**: type the server FQDN or IP address
  - **Port**: type the port number to use for the MCP proxy
  - **Proxy server authentication**: type the User ID and Password as required
- Two Way Communication Port Forwarding

- **Enable two-way communication port forwarding**: select to enable a real-time connection between the managed product and Control Manager
- **IP address**: type the IP address to use for port forwarding
- **Port**: type the port number to use for port forwarding

Note

Click **Test Connection**, to test the current connection settings, or **Register**, to register the current settings. Click **Cancel** to exit without saving changes.

Appendix C

About Regular Expressions

Regular expressions are used to perform string matching.

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.

See the following tables for some common examples of regular expressions:

- *Counting and Grouping on page C-2*
- *Character Classes (Shorthand) on page C-3*
- *Character Classes on page C-4*
- *Pattern Anchor Regular Expressions on page C-6*
- *Escape Sequences Regular Expressions on page C-6*

Counting and Grouping

TABLE C-1. Counting and Grouping

ELEMENT	WHAT IT MEANS	EXAMPLE
.	The dot or period character represents any character except new line character.	do. matches doe, dog, don, dos, dot, etc.d.r matches deer, door, etc.
*	The asterisk character means zero or more instances of the preceding element.	do* matches d, do, doo, dooo, doooo, etc.
+	The plus sign character means one or more instances of the preceding element.	do+ matches do, doo, dooo, doooo, etc. but not d
?	The question mark character means zero or one instances of the preceding element.	do?g matches dg or dog but not doog, dooog, etc.
( )	Parenthesis characters group whatever is between them to be considered as a single entity.	d(eer)+ matches deer or deereer or deereereer, etc. The + sign is applied to the substring within parentheses, so the regex looks for d followed by one or more of the grouping "eer."
[ ]	Square bracket characters indicate a set or a range of characters.	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.

Element	What It Means	Example
^	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.	d[^aeiouy] matches db, dc or dd, d9, d#. d followed by any single character except a vowel.
{ }	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.	da{3} matches daaa. d followed by 3 and only 3 occurrences of ”r;a”. da{2,4} matches daa, daaa, daaaa, and daaaa (but not daaaaa). d followed by 2, 3, or 4 occurrences of ”r;a”. da{4,} matches daaaa, daaaaa, daaaaaa, etc. d followed by 4 or more occurrences of ”r;a”.

Character Classes (Shorthand)

Table C-2. Character Classes (shorthand)

Element	What It Means	Example
\d	Any digit character; functionally equivalent to [0-9] or [[:digit:]]	\d matches 1, 12, 123, etc., but not 1b7. One or more of any digit characters.
\D	Any non-digit character; functionally equivalent to [^0-9] or [^[:digit:]]	\D matches a, ab, ab&, but not 1. One or more of any character but 0, 1, 2, 3, 4, 5, 6, 7, 8, or 9.
\w	Any "word" character. That is, any alphanumeric character; functionally equivalent to [_A-Za-z0-9] or [_[:alnum:]]	\w matches a, ab, a1, but not !&. One or more upper- or lower-case letters or digits, but not punctuation or other special characters.

Element	What It Means	Example
\W	Any non-alphanumeric character; functionally equivalent to [^_A-Za-z0-9] or [^_[:alnum:]]	\W matches *, &, but not ace or a1. One or more of any character but upper- or lower-case letters and digits.
\s	Any white space character; space, new line, tab, non-breaking space, etc.; functionally equivalent to [[:space]]	vegetable\s matches "vegetable" followed by any non-white space character. So the phrase "I like vegetables in my soup" would trigger the regex, but "I like a vegetable in my soup" would not.
\S	Any non-white space character; anything other than a space, new line, tab, non-breaking space, etc.; functionally equivalent to [^[:space]]	vegetable\S matches "vegetable" followed by any non-white space character. So the phrase "I like vegetables in my soup" would trigger the regex, but "I like a vegetable in my soup" would not.

Character Classes

Table C-3. Character Classes

Element	What It Means	Example
[: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 ~!@.

Element	What It Means	Example
[: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
[:lower:]	Any lowercase alphabetic characters (Note : ’r;Enable case sensitive matching’ must be enabled or else it will function as [:alnum:])	.REG. [[:lower:]] matches abc, Def, sTress, Do, etc., but not ABC, DEF, STRESS, DO, 123, !@#.
[:upper:]	Any uppercase alphabetic characters (Note : ’r;Enable case sensitive matching’ must be enabled or else it will function as [:alnum:])	.REG. [[:upper:]] matches ABC, DEF, STRESS, DO, Def, Stress, Do, etc., but not abc, 123, !@#.
[:xdigit:]	Digits allowed in a hexadecimal number (0-9a-fA-F)	.REG. [[:xdigit:]] matches 0a, 7E, 0f, etc.

Pattern Anchor Regular Expressions

TABLE C-4. Pattern Anchor Regular Expressions

ELEMENT	WHAT IT MEANS	EXAMPLE
^	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 C-5. Escape Sequences Regular Expressions

ELEMENT	WHAT IT MEANS	EXAMPLE
\	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.

Element	What It Means	Example
\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.
\r	Indicates a carriage return character.	(stress) \r matches any block of text that contained the substring "stress" followed immediately by one carriage return (ASCII 0x0D) character.
\b	Indicates a backspace character	(stress) \b matches any block of text that contained the substring ”r;stress” followed immediately by one backspace (ASCII 0x08) character.
\xhh	Indicates an ASCII character with given hexadecimal code (where hh represents any two-digit hex value).	\x7E(\w){6} matches any block of text containing a "word" 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.

Index

TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: PPEM28661/190425