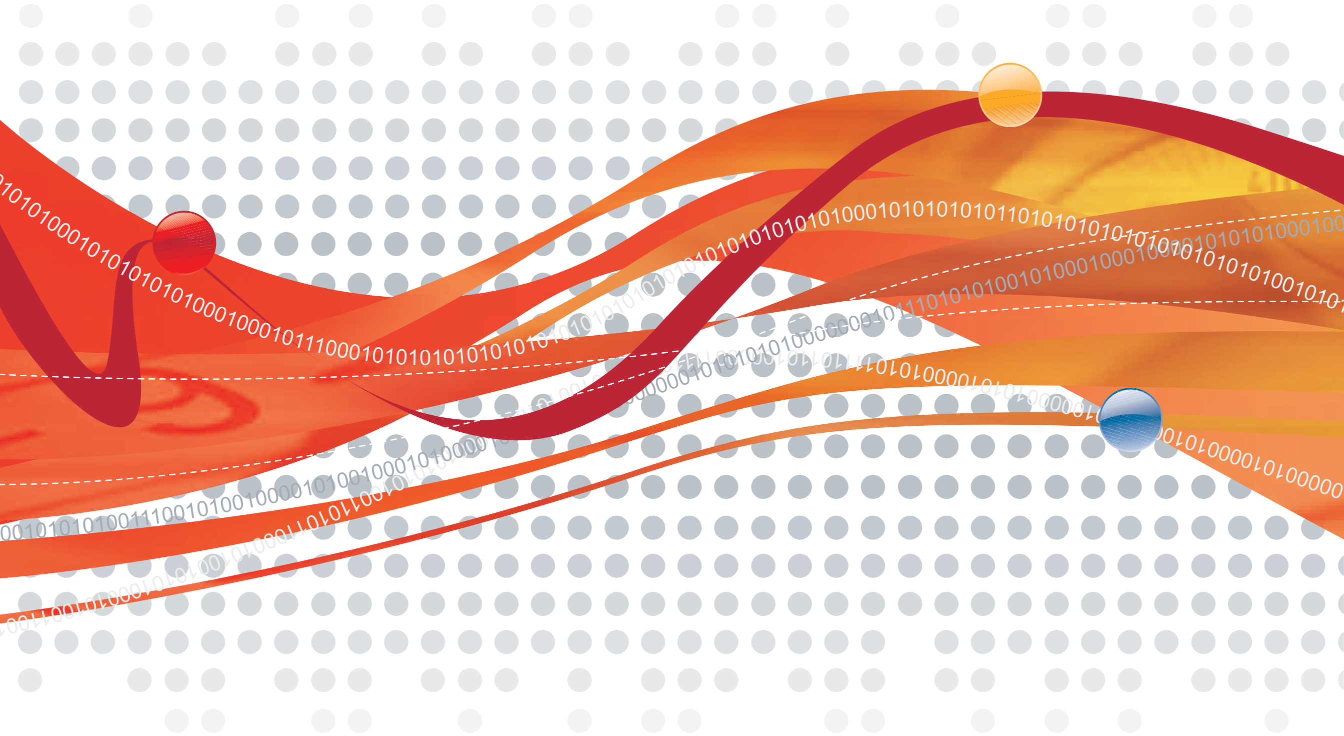
TREND MICRO™

PortalProtect^{1}

Highly Effective Protection, Minimal IT Impact

for Microsoft™ SharePoint

Getting Started Guide



Collaboration Security

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

www.trendmicro.com/download/

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

Document Part No. PPEM11964/40719

Release Date: June, 2009

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

The Getting Started Guide for Trend Micro PortalProtect is intended to introduce the main features of the software and installation instructions for your production environment. You should read it before installing or using the software.

For technical support, please refer to Contacting Trend Micro in this Getting Started Guide. Detailed information about how to use specific features within the software is available in the Online Help file and online Solution Bank at Trend Micro's Web site.

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

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

Contents

Chapter 1: Welcome to Trend Micro™ PortalProtect™

Chapter 2: Installing and Removing PortalProtect

Chapter 3: Getting Started with PortalProtect

Chapter 4: Configuring Scanning and File Blocking Options

Chapter 5: Notifications, Alerts, Logs, and Reports

Chapter 6: Getting Support and Contacting Trend Micro

Appendix A: Using Control Manager with PortalProtect

Appendix B: How to Configure PortalProtect to Use an External SQL Server Database

Chapter 1

Welcome to Trend Micro™ PortalProtect™

Trend Micro PortalProtect™ is a server-based security solution for Microsoft Windows™ SharePoint™ Services 3.0, including Microsoft™ SharePoint™ Server 2007. Trend Micro designed PortalProtect to provide protection against attacks from viruses and other security threats.

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

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

This chapter introduces PortalProtect, including its benefits and capabilities. It discusses the security threats to your SharePoint environments and how PortalProtect protects against these threats.

PortalProtect 1.8 integrates with Trend Micro Control Manager 3.5/5.0 with support for the following services:

- Centralized pattern file and scan engine deployment and updating
- Configuration replication
- Outbreak Prevention Service deployment

In this chapter, you will find information about:

- *What's New in PortalProtect 1.8* starting on page 1-2
- *Benefits and Capabilities* starting on page 1-2
- *How PortalProtect Protects SharePoint Servers* starting on page 1-3
- *PortalProtect Architecture* starting on page 1-5
- *Controlling Outbreaks* starting on page 1-7

What's New in PortalProtect 1.8

- Supports Windows 2008
- Supports x86 and x64 OS
- Silent Installation

Note: PortalProtect 1.8 protects SharePoint Server 2007 only.

Benefits and Capabilities

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

- Supports Windows 2008.
- 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.
- Uses proactive multi-threaded scanning to detect and clean viruses in real time from multiple access points, when authors check documents in and out or readers view documents.

- Uses Trend Micro IntelliScan™ to detect and scan true file types regardless whether the file extension was changed.
- 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.
- Uses file blocking during a virus outbreak to temporarily block all files types as designated by the administrator.
- Detects and removes potentially harmful macros viruses.
- Includes centralized configuration, reporting, logs, update, and real-time notification of customizable warning messages to administrators, workspace coordinators, and other recipients.
- Uses ActiveAction to sort threats into such categories such as viruses, malicious macro codes, and additional threats.
- 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 both SharePoint Server 2007 and SharePoint Services 3.0 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 block files based on the file extension, file name, or true file type. When it detects a file type, it takes an action like: quarantine or delete, as pre-configured by the administrator.
- Scanning employs the latest version of the Trend Micro scan engine to detect viruses and other malicious code. When PortalProtect detects a virus or malicious code, it performs a number of actions like: quarantine or delete, according to how the administrator has it configured. The scan engine can maintain multiple threads, thus processing many requests simultaneously. It can also prioritize requests.

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

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

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

Manual Scan (Scan Now)–Manual Scan occurs momentarily after you start it and scans all or some of the files in your Document Library, depending on the configuration. You can configure a scan task to scan all or some of the folders stored in the database. Manual scan provides an immediate way to secure the content on 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 work with SharePoint Services 3.0 to provide comprehensive security for your SharePoint Server.

At the center of the PortalProtect security solutions is the Trend Micro patented scan engine. The scan engine integrates with the SharePoint Services 3.0 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. To prevent redundant scanning, scan results are kept in the SQL store and made available to PortalProtect during subsequent scanning. Only files that have been modified will be scanned again.

SharePoint Services 3.0 clients running applications such as Microsoft Office and Internet Explorer communicate with the SharePoint Services 3.0 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.

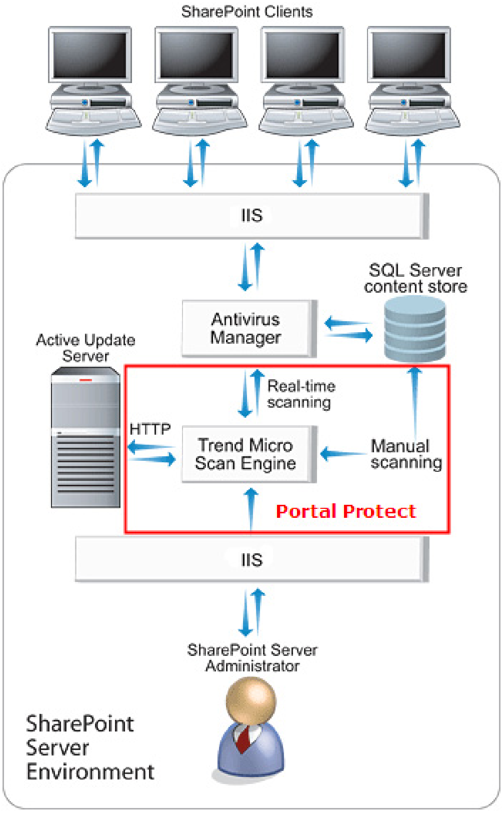


FIGURE 1-1. How PortalProtect interacts with SharePoint Server and SharePoint Services 3.0

Controlling Outbreaks

PortalProtect protects SharePoint Server and SharePoint Services 3.0 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.

  See *Alerts* on page 5-8.

- 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.

  See *Manually Updating Your Components* on page 3-7.

- 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.

Chapter 2

Installing and Removing PortalProtect

This section describes how to install and remove PortalProtect and lists the minimum system requirements. It also provides information about basic upgrading issues and suggestions about various PortalProtect features.

Administrators can easily install PortalProtect to multiple servers simultaneously. Likewise, if an administrator wants to remove PortalProtect from one or many servers, the process is simple and intuitive.

This chapter includes information about:

- *System Requirements* starting on page 2-2
- *Installation Scenarios Using Server Farms* starting on page 2-4
- *Silent Installation* starting on page 2-26
- *Testing Your Installation* starting on page 2-34
- *Uninstalling PortalProtect* starting on page 2-35

System Requirements

You need the following to effectively run PortalProtect 1.8:

Hardware/Software	Requirement	Recommended
Processor	Server with processor speed of 2.5-GHz (32-bit or 64-bit)	Dual processor, 3-GHz or greater (32-bit or 64-bit)
Memory	2-GB RAM	4-GB RAM
Disk Space	2-GB free disk space	5-GB free disk space
Windows Server	• Microsoft Windows Server 2008 Standard Edition x86/x64 • Microsoft Windows Server 2008 Enterprise Edition x86/x64 • Microsoft Windows Server 2008 Datacenter Edition x86/x64 • Microsoft Windows Web Server 2008 x86/x64 • Microsoft Windows Server HPC Edition x64	
SharePoint Service / Server	• Windows SharePoint Service 3.0 SP1 x86/x64 • Microsoft Office SharePoint Server 2007 Standard Edition SP1 x86/x64 • Microsoft Office SharePoint Server 2007 Enterprise Edition SP1 x86/x64	
Web Server	IIS 7.0 on Microsoft Windows Server 2008	
Browser	• Microsoft Internet Explorer 6.0 SP1, 7.0, 8.0 • Mozilla Firefox 2.0, 3.0	
JAVA Virtual Machine (JVM)	Sun™ Java Runtime Environment (JRE™) version 1.5.0	JRE™ version 6.0 update 12 (recommended)

You need the following to effectively run the CM agent:

- PortalProtect 1.8
- CM server 3.5 with Patch 5, or CM server 5.0 with Patch 3 + Hotfix 1760

Preparing for Installation

Consider the following to ensure a smooth deployment of PortalProtect to your network:

- Install PortalProtect 1.8 on a server with Microsoft Office SharePoint Server 2007, Microsoft SharePoint Services 3.0, and Windows 2008 installed. Microsoft Internet Information Services (IIS) is a required for a successful installation.
- **Registration Key/Activation Code**. During installation, the setup program prompts for an Activation Code. Use the Registration Key that came with PortalProtect to obtain an Activation Code online from the Trend Micro Web site. The setup program provides a link to the Trend Micro Web site. See *Registering PortalProtect* on page 3-5.
- **Privileges for Installation**. During installation, the account to launch the setup program must have the administrator privilege to where you launch the setup program and this account must have administrator privilege to all the target servers where you plan to install PortalProtect.
- **Proxy information**. During installation, the setup program prompts for proxy information. If a proxy server handles Internet traffic on your network, you must type the proxy server information, user name, and password to receive virus pattern file and scan engine updates. If you do not enter proxy information during installation, you can configure it later from the Administration menu. See *Configuring Proxy Settings* on page 3-6.
- **Management group**. During installation, the setup program prompts for management group selection. Select an existing Active Directory group for management and the setup program will grant this group permission to manage PortalProtect. Users in this group may log on to the PortalProtect Web management console. See *Logging On and Off* on page 3-3.

Note: PortalProtect 1.8 does not support upgrade from previous versions of PortalProtect such as: version 1.6 and 1.7.

Installation Scenarios Using Server Farms

You can configure PortalProtect to run on one stand-alone server or use a server farm configuration. Configure PortalProtect to use server farms according to one of the following models:

SharePoint Services 3.0 Small Server Farm

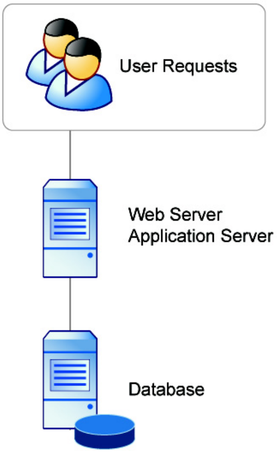


FIGURE 2-2. Small server farm configuration

SharePoint Services 3.0 Medium Server Farm

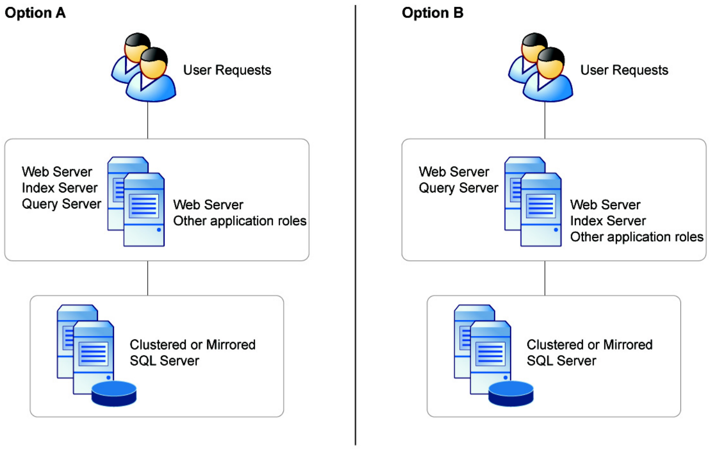


FIGURE 2-3. Medium server farm

SharePoint Services 3.0 Large Server Farm

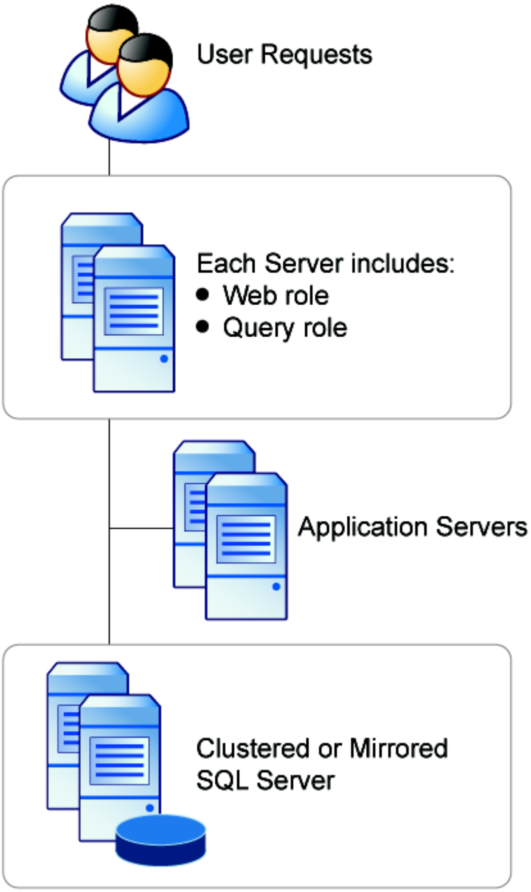


FIGURE 2-4. Large server farm configuration

Installing PortalProtect

You can install PortalProtect in two ways:

- Using an installation program called **setup.exe**
- Using a silent installation program

Setup.exe Installation

PortalProtect provides a user-friendly installation program, which can be used for both local and remote installation. The setup program enables you to install PortalProtect on one or many servers and rapidly deploy it to all SharePoint servers in your enterprise.

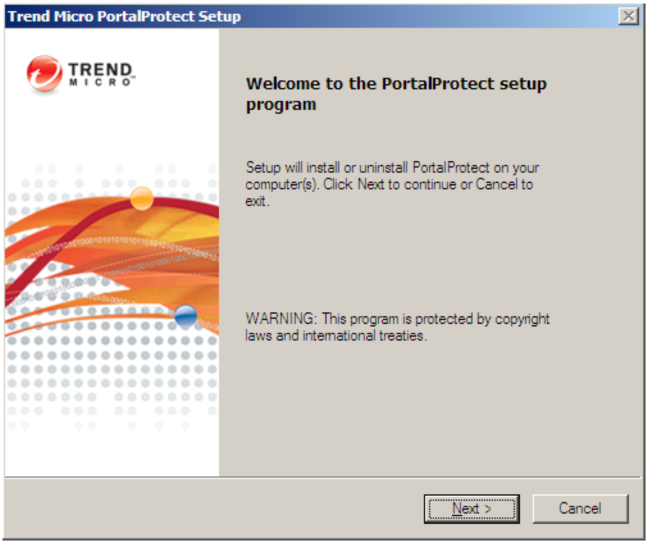
The target servers must be part of your network and you must have access with administrator privileges.

Note: You must install PortalProtect on a server with Microsoft Office SharePoint Server 2007 or Microsoft SharePoint service 3.0, and Windows Server 2008 installed. A successful installation also requires IIS 7.0 and Internet Explorer 6.0.

Note: PortalProtect 1.8 is compatible only with SharePoint Server 2007 and SharePoint Services 3.0.

To install PortalProtect:

1. Run `setup.exe` from the PortalProtect 1.8 CD to start the installation. The **Welcome to Trend Micro PortalProtect setup program** screen displays.



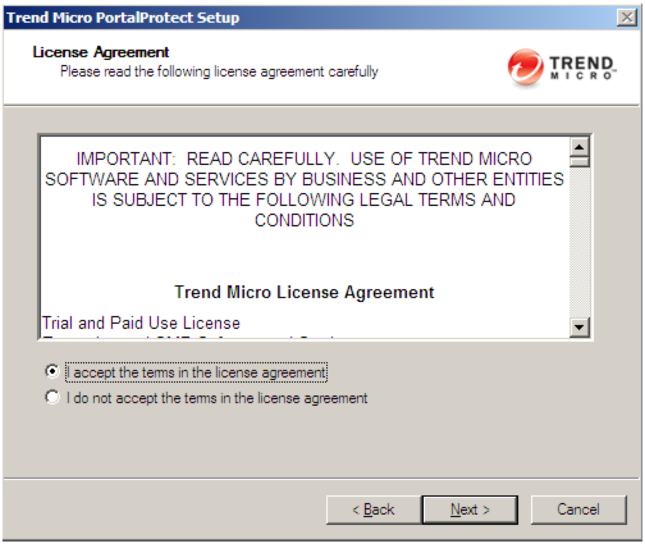
Trend Micro PortalProtect Setup

Welcome to the PortalProtect setup program

Setup will install or uninstall PortalProtect on your computer(s). Click Next to continue or Cancel to exit.

WARNING: This program is protected by copyright laws and international treaties.

2. Click **Next >**. The **License Agreement** screen displays.



Trend Micro PortalProtect Setup
License Agreement
Please read the following license agreement carefully
TREND MICRO

IMPORTANT: READ CAREFULLY. USE OF TREND MICRO SOFTWARE AND SERVICES BY BUSINESS AND OTHER ENTITIES IS SUBJECT TO THE FOLLOWING LEGAL TERMS AND CONDITIONS

Trend Micro License Agreement

Trial and Paid Use License

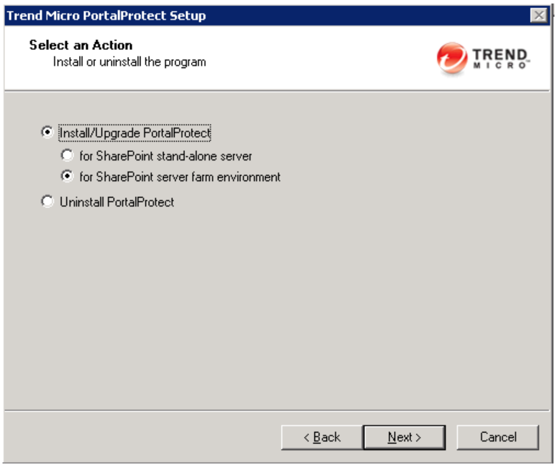
● I accept the terms in the license agreement
○ I do not accept the terms in the license agreement

Read the license agreement. If you accept the terms, select **I accept the terms in the license agreement** and click **Next**. The setup program begins checking your system requirements. If you do not accept the terms, click **Cancel** to exit the setup program.

3. The **Install/Upgrade** screen appears. Select **Install/Upgrade PortalProtect**, and choose from the following options:
   - for SharePoint stand-alone server
   - for SharePoint server farm environment

   After selecting the appropriate options, click **Next >**.

Note: Whether to select install **for SharePoint stand-alone server** or install **for SharePoint server farm environment** depends on your SharePoint deployment mode. If SharePoint will be deployed with farm mode, you must select **for SharePoint server farm environment**. Otherwise, if SharePoint will be deployed in the stand-alone mode (basic deployment) you should select **for SharePoint stand-alone server**.



Trend Micro PortalProtect Setup

Select an Action

Install or uninstall the program

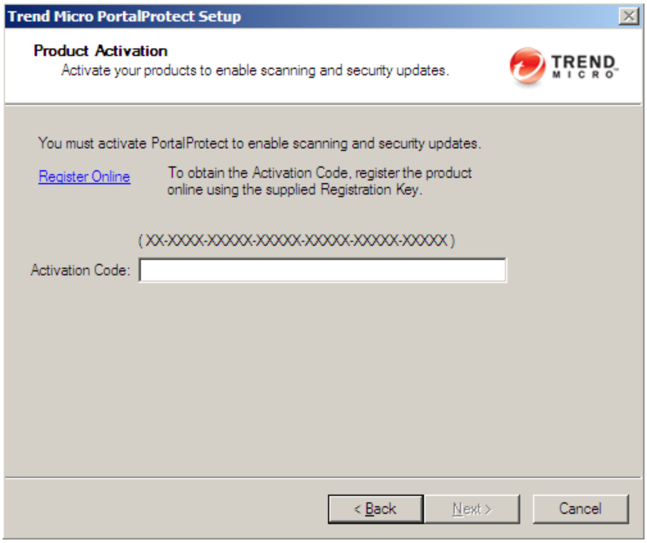
● Install/Upgrade PortalProtect

○ for SharePoint stand-alone server

● for SharePoint server farm environment

○ Uninstall PortalProtect

4. The **Product Activation** screen displays.



Trend Micro PortalProtect Setup

Product Activation

Activate your products to enable scanning and security updates.

You must activate PortalProtect to enable scanning and security updates.

Register Online — To obtain the Activation Code, register the product online using the supplied Registration Key.

(XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX)

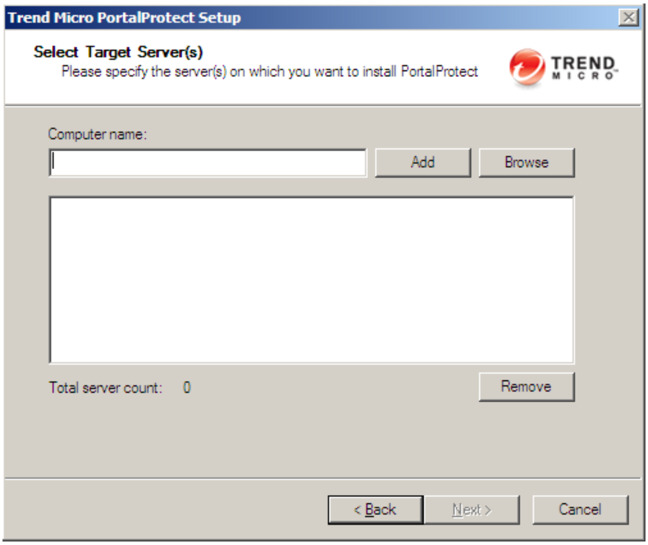
Activation Code:

Product Activation requires two steps:

a. You must register PortalProtect online to receive an Activation Code. Click **Register Online**. This opens the Trend Micro online registration Web page in your browser. Follow the prompts to complete the registration. When you have registered, Trend Micro sends you an Activation Code via e-mail.

b. Type the Activation Code and click **Next** > to proceed with the installation.

5. The **Select Target Server(s)** screen displays.



Trend Micro PortalProtect Setup

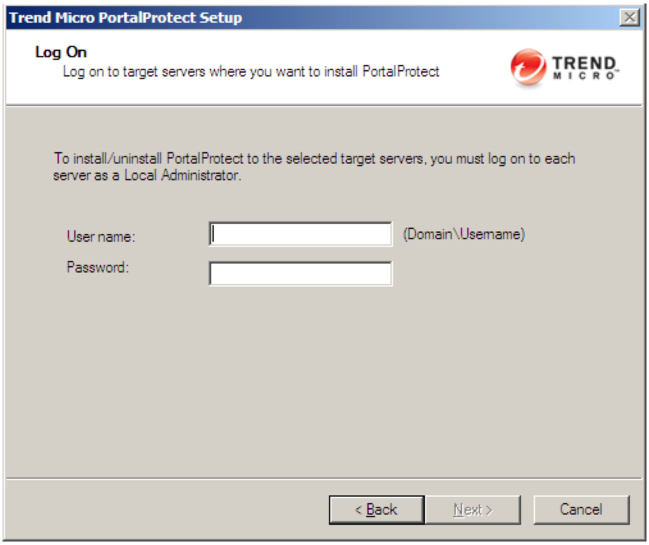
Select Target Server(s)

Please specify the server(s) on which you want to install PortalProtect

Total server count: 0

Use this screen to choose the target servers to which you want to install PortalProtect. Type or Browse for the **Computer name**, and **Add** one or more servers. When you are satisfied with the list of target servers, click **Next** > to continue the installation.

6. The target **Log On** screen displays.



Trend Micro PortalProtect Setup

Log On

Log on to target servers where you want to install PortalProtect

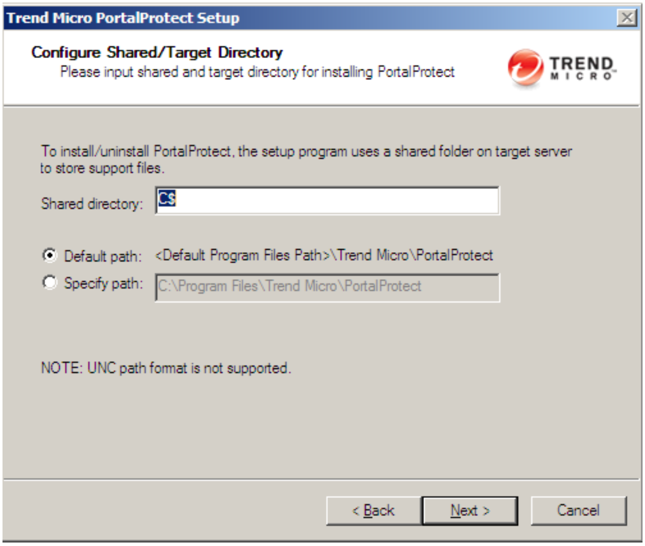
To install/uninstall PortalProtect to the selected target servers, you must log on to each server as a Local Administrator.

User name: (Domain\Username)

Password:

Type the server **User name** [Domain\Username] and **Password** and click **Next >**.

7. The **Configure Shared/Target Directory** screen displays.



Configure Shared/Target Directory

Please input shared and target directory for installing PortalProtect

To install/uninstall PortalProtect, the setup program uses a shared folder on target server to store support files.

Shared directory: C$

● Default path: <Default Program Files Path>\Trend Micro\PortalProtect

○ Specify path: C:\Program Files\Trend Micro\PortalProtect

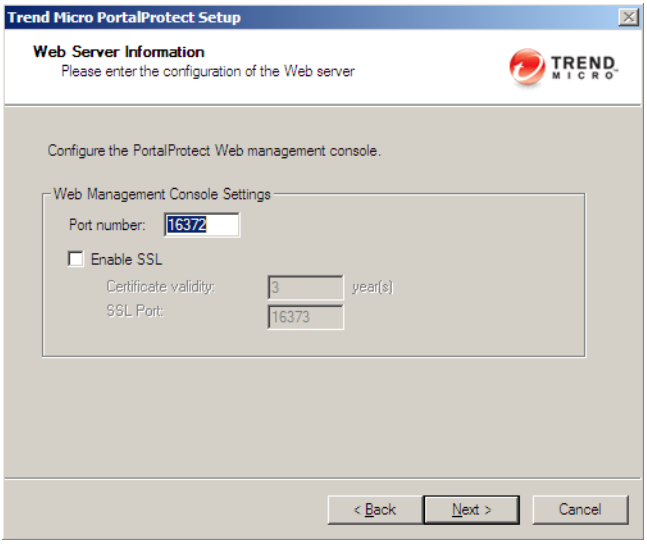
NOTE: UNC path format is not supported.

Accept the default path for the shared folder on the target server, or type a new path in the **Specify path** field. Click **Next >**.

Note: PortalProtect only accepts Windows default shares for Shared directories, such as C$, D$ and so on.

Note: To use the Shared directory, File and Printer Sharing must be enabled for Windows firewall on each of the target servers where PortalProtect will be installed.

8. The **Web Server Information** screen displays.



Trend Micro PortalProtect Setup

Web Server Information

Please enter the configuration of the Web server

Configure the PortalProtect Web management console.

Web Management Console Settings

Port number: 16372

□ Enable SSL

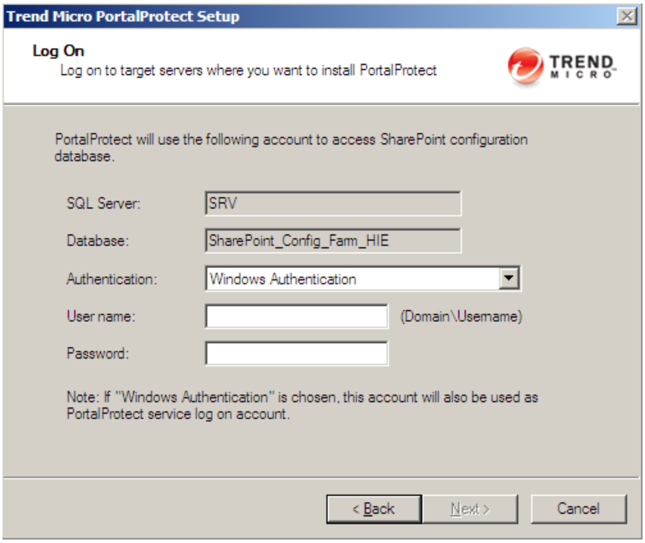
Certificate validity: 3 year(s)

SSL Port: 16373

Type the port number for the Web Management Console in the **Port number** field. **Click Next >**.

Note: Enable or Disable SSL as required. If enabling, type the number of years of **Certificate validity** and also the **SSL Port** number.

9. The **Log On** screen displays.



Trend Micro PortalProtect Setup
Log On
Log on to target servers where you want to install PortalProtect
TREND MICRO

PortalProtect will use the following account to access SharePoint configuration database.

SQL Server: SRV

Database: SharePoint_Config_Farm_HIE

Authentication: Windows Authentication

User name: (Domain\Username)

Password:

Note: If "Windows Authentication" is chosen, this account will also be used as PortalProtect service log on account.

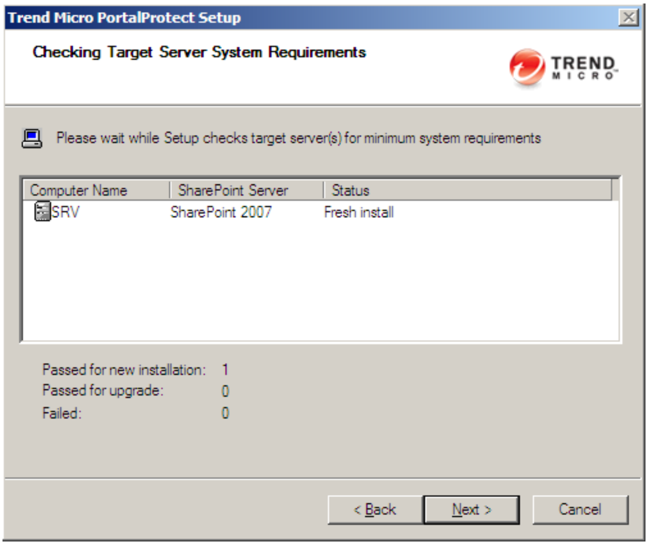
Select or type the following and click **Next >**.

- **Windows Authentication** or **SQL Server Authentication**
- **User name** (Domain\User name)
- **Password**

Note: Trend Micro highly recommends that you specify the same database account as the one used to deploy SharePoint. If you choose a database account different than the one used to deploy SharePoint, the database account must be configured as db_datareader role to SharePoint configDB and db_owner role to all the SharePoint content databases.

Note: If you selected Install/Upgrade PortalProtect for SharePoint stand-alone server in Step 3 page 2-10, the screen shown in Step 9 will not display because SharePoint stand-alone server bundles the SharePoint database in the same server.

10. The **Checking Target Server System Requirements** screen displays.



Trend Micro PortalProtect Setup

Checking Target Server System Requirements

Please wait while Setup checks target server(s) for minimum system requirements

Computer Name	SharePoint Server	Status
SRV	SharePoint 2007	Fresh install

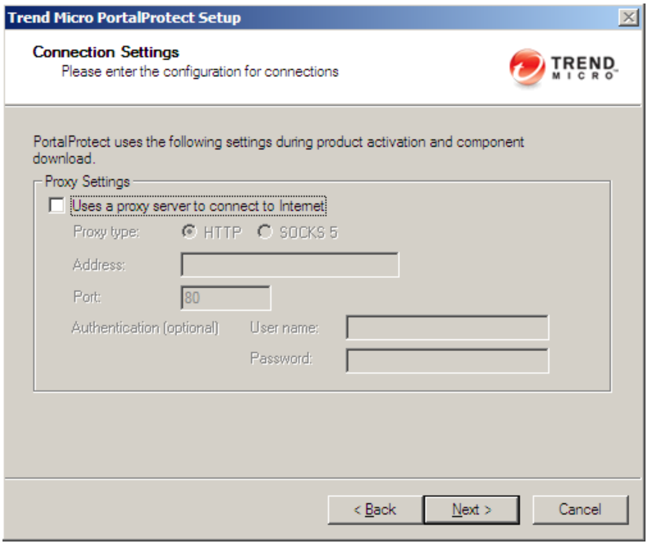
Passed for new installation:	1
Passed for upgrade:	0
Failed:	0

The installation program will analyze the systems to ensure the following on each of the target servers where PortalProtect will be installed:

- Whether the target server is running Windows 2008
- Whether the target server is running correct SharePoint version with Web application
- Whether the correct privileges have been provided to logon the target server
- Whether the correct SharePoint DB access account is specified to access the SharePoint configDB

Verify the Status reads **Fresh Install**, and click **Next >**.

11. The **Connection Settings** screen displays.



Trend Micro PortalProtect Setup

Connection Settings

Please enter the configuration for connections

PortalProtect uses the following settings during product activation and component download.

Proxy Settings

□ Uses a proxy server to connect to Internet

Proxy type: ● HTTP ○ SOCKS 5

Address:

Port: 80

Authentication (optional) User name:

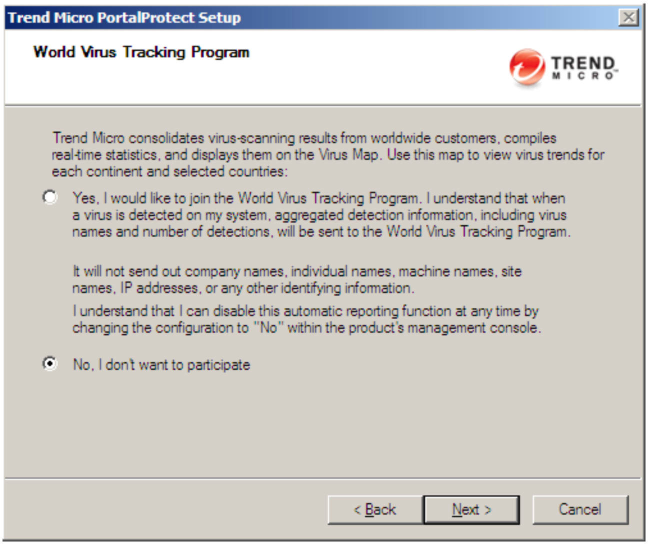
Password:

If you use a proxy server, select **Uses a proxy server to connect to Internet**, and enter the following:

- Proxy type (HTTP or SOCKS 5)
- Address (IP)
- Port (Port number)
- If your proxy server requires a password, type the **User name** and **Password** in the fields provided. See *Configuring Proxy Settings* on page 3-6 for more information.

Click **Next >**.

12. The **World Virus Tracking Program** screen displays.



World Virus Tracking Program

Trend Micro consolidates virus-scanning results from worldwide customers, compiles real-time statistics, and displays them on the Virus Map. Use this map to view virus trends for each continent and selected countries:

○ Yes, I would like to join the World Virus Tracking Program. I understand that when a virus is detected on my system, aggregated detection information, including virus names and number of detections, will be sent to the World Virus Tracking Program.

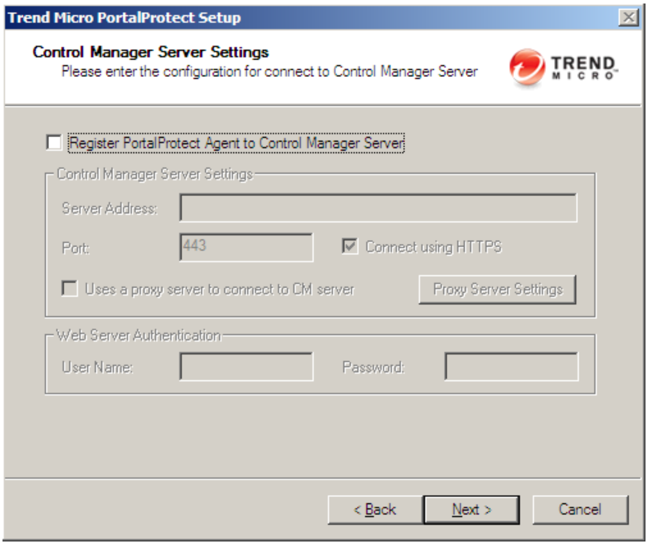
It will not send out company names, individual names, machine names, site names, IP addresses, or any other identifying information.

I understand that I can disable this automatic reporting function at any time by changing the configuration to "No" within the product's management console.

● No, I don't want to participate

Select **Yes**, if you would like to participate in the World Virus Tracking Program, or **No**, if you do not. Click **Next >**.

13. The **Control Manager Server Settings** screen displays.



Trend Micro PortalProtect Setup

Control Manager Server Settings

Please enter the configuration for connect to Control Manager Server

□ Register PortalProtect Agent to Control Manager Server

Control Manager Server Settings

Server Address:

Port: 443

☑ Connect using HTTPS

□ Uses a proxy server to connect to CM server

Web Server Authentication

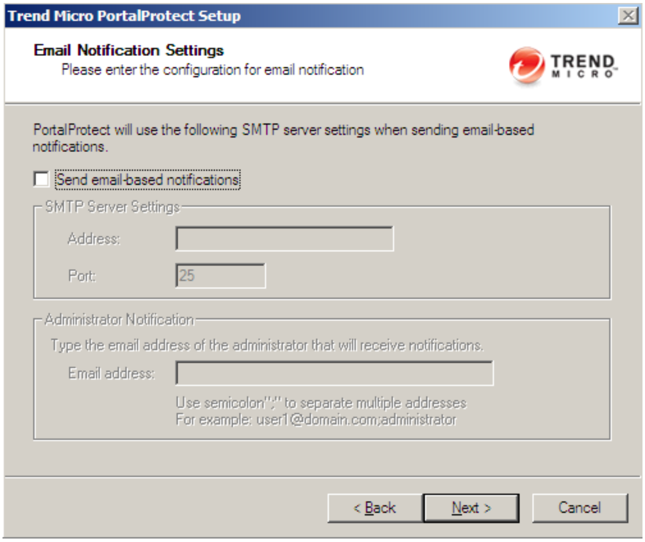
User Name:

Password:

Click **Next >** to accept the default settings, or select **Register PortalProtect Agent to Control Manager Server** and enter the following:

- Server Address.
- **Port** (Port number).
- **Connect using HTTPS** (if desired).
- If a proxy server is used, select **Uses a proxy server to connect to CM server**, and click **Proxy Server Settings** to modify. See *Configuring Proxy Settings* on page 3-6 for more information.
- If **Web Server Authentication** is required, type the User Name and Password.
- Click **Next >**.

14. The **Email Notification Settings** screen displays.



Trend Micro PortalProtect Setup

Email Notification Settings

Please enter the configuration for email notification

PortalProtect will use the following SMTP server settings when sending email-based notifications.

□ Send email-based notifications

SMTP Server Settings

Address:

Port: 25

Administrator Notification

Type the email address of the administrator that will receive notifications.

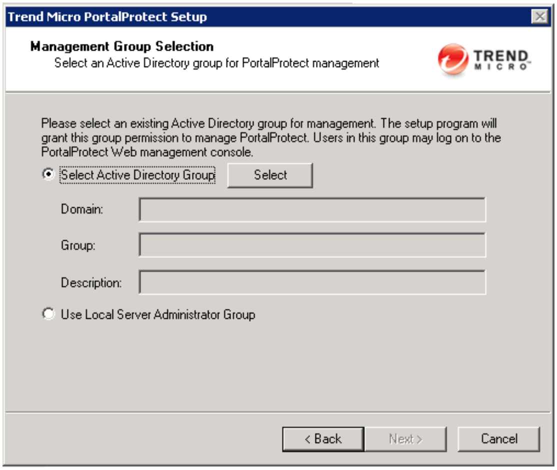
Email address:

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

If you wish to send email based notifications, enter the following:

- Select, **Send email-based notifications.**
- Type the SMTP server **Address** and **Port.**
- To enable Administrator email notification, type the administrator(s) email address(es) in the **Email address** field. Use a semicolon to separate multiple addresses.
- Click **Next >**.

15. The **Management Group Selection** screen displays.



Trend Micro PortalProtect Setup

Management Group Selection

Select an Active Directory group for PortalProtect management

Please select an existing Active Directory group for management. The setup program will grant this group permission to manage PortalProtect. Users in this group may log on to the PortalProtect Web management console.

● Select Active Directory Group [Select]

Domain:

Group:

Description:

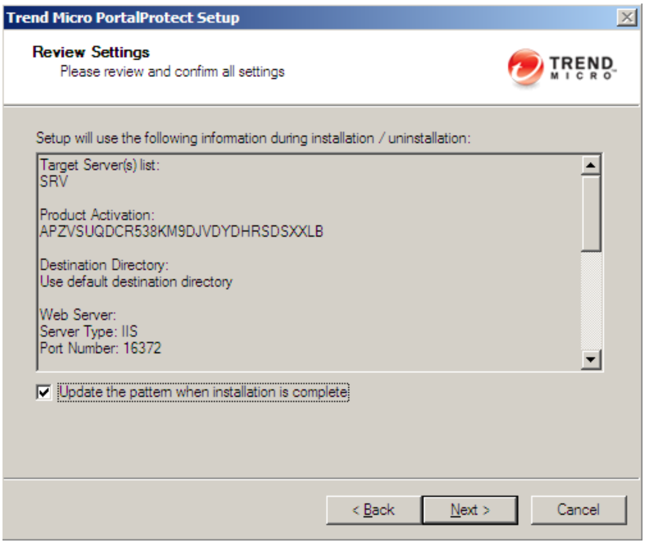
○ Use Local Server Administrator Group

Note: You must use an existing Active Directory group, or create a new one before you complete this step. If you select **Use Local Server Administrator Group**, accounts with administrator privilege on each target server can logon its own PortalProtect Management Console locally.

Select **Use Local Server Administrator Group**, if you do not wish to select an active directory group now, or do the following to choose an active directory group:

- Choose **Select Active Directory Group** and click **Select** to choose a pre-existing group; the **Domain**, **Group**, and **Description** fields then populate accordingly.
- Click **Next >**.

16. The **Review Settings** screen displays.



Review Settings
Please review and confirm all settings

Setup will use the following information during installation / uninstallation:

Target Server(s) list:
SRV

Product Activation:
APZVSUQDCR538KM9DJVDYDHRSDSXXLB

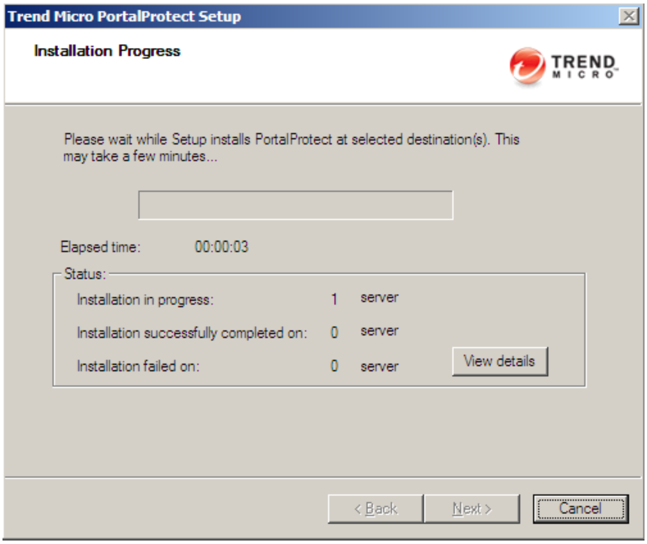
Destination Directory:
Use default destination directory

Web Server:
Server Type: IIS
Port Number: 16372

☑ Update the pattern when installation is complete

Check the settings as they are displayed on screen, and go back to make any changes if needed. Click **Update the pattern when installation is complete**, if you wish to do so; then, click **Next >**.

17. The **Installation Progress** screen displays.



Trend Micro PortalProtect Setup

Installation Progress

Please wait while Setup installs PortalProtect at selected destination(s). This may take a few minutes...

Elapsed time: 00:00:03

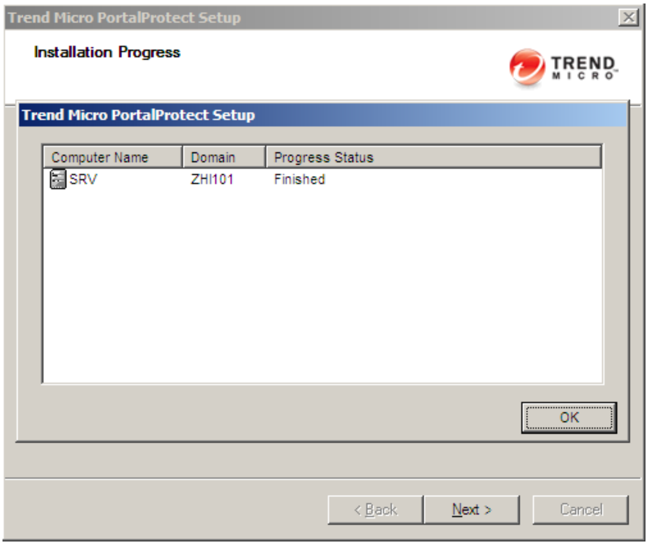
Status:

Installation in progress: 1 server

Installation successfully completed on: 0 server

Installation failed on: 0 server

While the installation is active, click **View details** to check the status (see Figure 2-5.

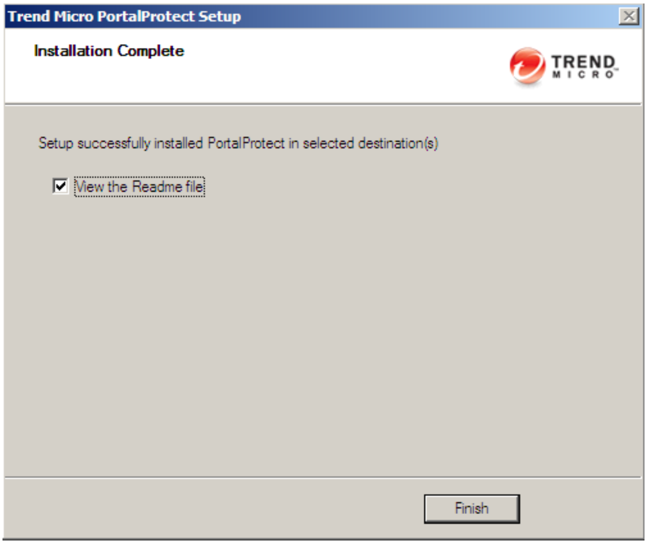

Trend Micro PortalProtect Setup
Installation Progress
TREND MICRO
Trend Micro PortalProtect Setup

Computer Name	Domain	Progress Status
SRV	ZHI101	Finished

FIGURE 2-5. Installation progress status (Finished)

18. After the installation status displays **Finished**, click **Next >**.

19. The **Installation Complete** screen displays.



Trend Micro PortalProtect Setup

Installation Complete

Setup successfully installed PortalProtect in selected destination(s)

☑ View the Readme file

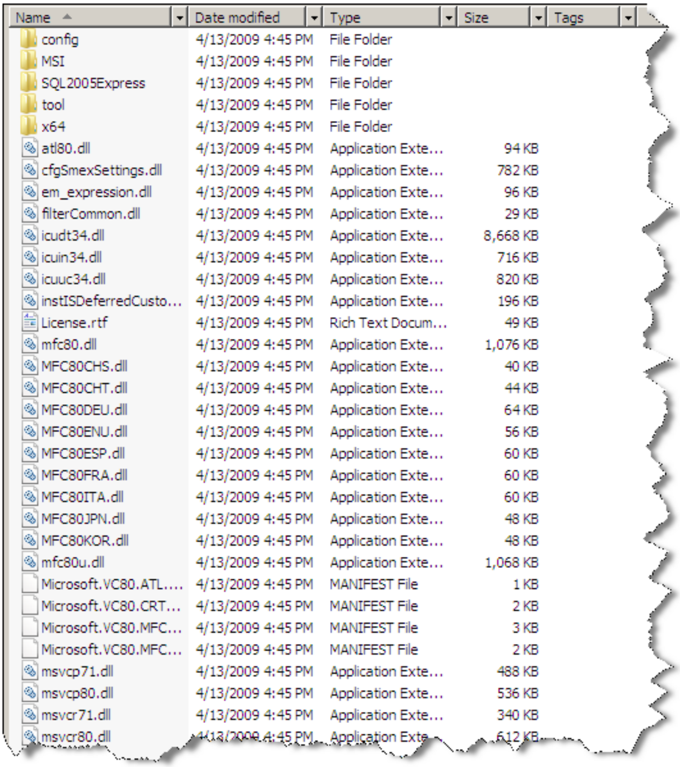
Select **View the Readme file**, if you wish to view it, and **Finish** to complete the installation.

Silent Installation

Silent installation pre-populates an INI file with installation parameters and installs PortalProtect without the need for administrator intervention. You need to have a PortalProtect setup package or build to run silent installation.

To install PortalProtect using Silent Install:

1. Go to **/PP setup package/PP/** where you can see a list of executable files.

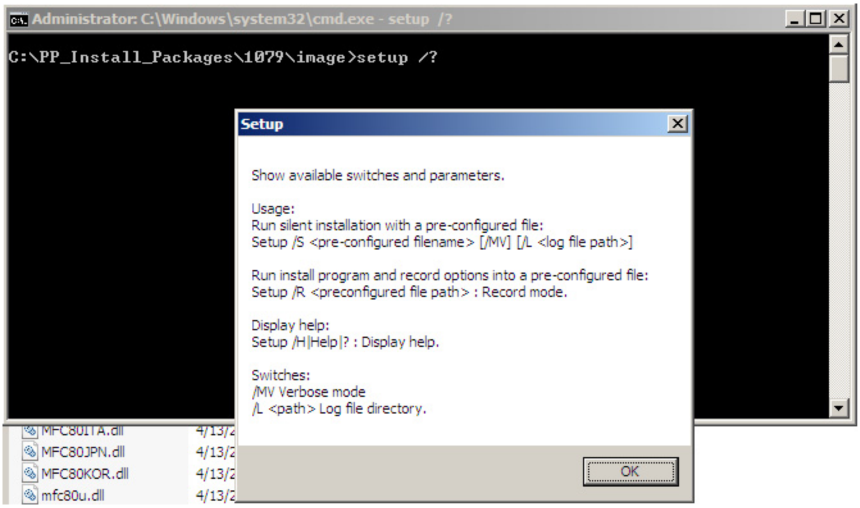


Name	Date modified	Type	Size	Tags
config	4/13/2009 4:45 PM	File Folder		
MSI	4/13/2009 4:45 PM	File Folder		
SQL2005Express	4/13/2009 4:45 PM	File Folder		
tool	4/13/2009 4:45 PM	File Folder		
x64	4/13/2009 4:45 PM	File Folder		
atl80.dll	4/13/2009 4:45 PM	Application Exte...	94 KB	
cfgSmexSettings.dll	4/13/2009 4:45 PM	Application Exte...	782 KB	
em_expression.dll	4/13/2009 4:45 PM	Application Exte...	96 KB	
filterCommon.dll	4/13/2009 4:45 PM	Application Exte...	29 KB	
icudt34.dll	4/13/2009 4:45 PM	Application Exte...	8,668 KB	
icuin34.dll	4/13/2009 4:45 PM	Application Exte...	716 KB	
icuuc34.dll	4/13/2009 4:45 PM	Application Exte...	820 KB	
instISDeferredCusto...	4/13/2009 4:45 PM	Application Exte...	196 KB	
License.rtf	4/13/2009 4:45 PM	Rich Text Docum...	49 KB	
mfc80.dll	4/13/2009 4:45 PM	Application Exte...	1,076 KB	
MFC80CHS.dll	4/13/2009 4:45 PM	Application Exte...	40 KB	
MFC80CHT.dll	4/13/2009 4:45 PM	Application Exte...	44 KB	
MFC80DEU.dll	4/13/2009 4:45 PM	Application Exte...	64 KB	
MFC80ENU.dll	4/13/2009 4:45 PM	Application Exte...	56 KB	
MFC80ESP.dll	4/13/2009 4:45 PM	Application Exte...	60 KB	
MFC80FRA.dll	4/13/2009 4:45 PM	Application Exte...	60 KB	
MFC80ITA.dll	4/13/2009 4:45 PM	Application Exte...	60 KB	
MFC80JPN.dll	4/13/2009 4:45 PM	Application Exte...	48 KB	
MFC80KOR.dll	4/13/2009 4:45 PM	Application Exte...	48 KB	
mfc80u.dll	4/13/2009 4:45 PM	Application Exte...	1,068 KB	
Microsoft.VC80.ATL....	4/13/2009 4:45 PM	MANIFEST File	1 KB	
Microsoft.VC80.CRT...	4/13/2009 4:45 PM	MANIFEST File	2 KB	
Microsoft.VC80.MFC...	4/13/2009 4:45 PM	MANIFEST File	3 KB	
Microsoft.VC80.MFC...	4/13/2009 4:45 PM	MANIFEST File	2 KB	
msvcp71.dll	4/13/2009 4:45 PM	Application Exte...	488 KB	
msvcp80.dll	4/13/2009 4:45 PM	Application Exte...	536 KB	
msvcr71.dll	4/13/2009 4:45 PM	Application Exte...	340 KB	
msvcr80.dll	4/13/2009 4:45 PM	Application Exte...	612 KB	

2. Copy all the files in the PortalProtect sub-folder along with the tool **Setup.com** to the location where you want to execute the Silent Install for PortalProtect.
3. After copying the files, go to the command prompt and change the current directory to refer to the PortalProtect folder.

WARNING! You must use setup.com for silent installation, never use setup.exe.

4. Type **Setup /?** to view a list of options that you can use for the Silent Install procedure.



```
C:\PP_Install_Packages\1079\image>setup /?
```

Show available switches and parameters.

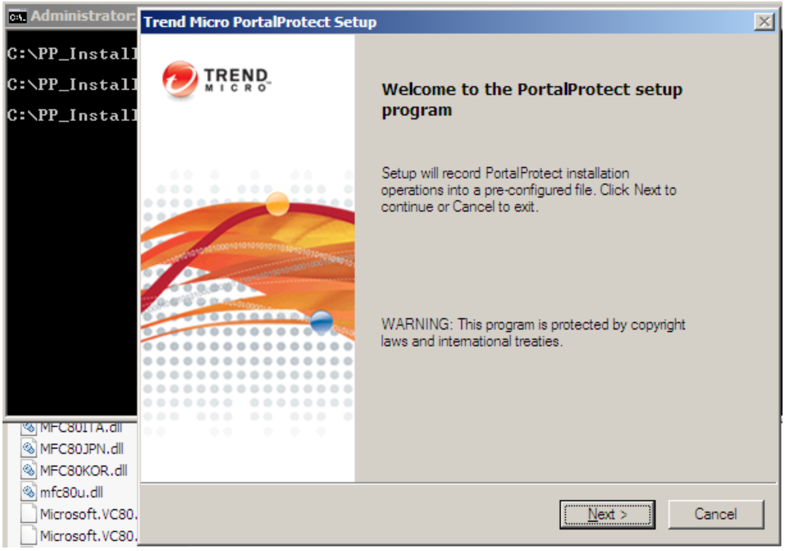
Usage:
Run silent installation with a pre-configured file:
Setup /S <pre-configured filename> [/MV] [/L <log file path>]

Run install program and record options into a pre-configured file:
Setup /R <preconfigured file path> : Record mode.

Display help:
Setup /H|Help|? : Display help.

Switches:
/MV Verbose mode
/L <path> Log file directory.

5. Type **Setup /R** to start the Silent Install procedure, which displays the **Trend Micro Portal Protect Setup** screen.



```
C:\PP_Install
C:\PP_Install
C:\PP_Install
```

Welcome to the PortalProtect setup program

Setup will record PortalProtect installation operations into a pre-configured file. Click Next to continue or Cancel to exit.

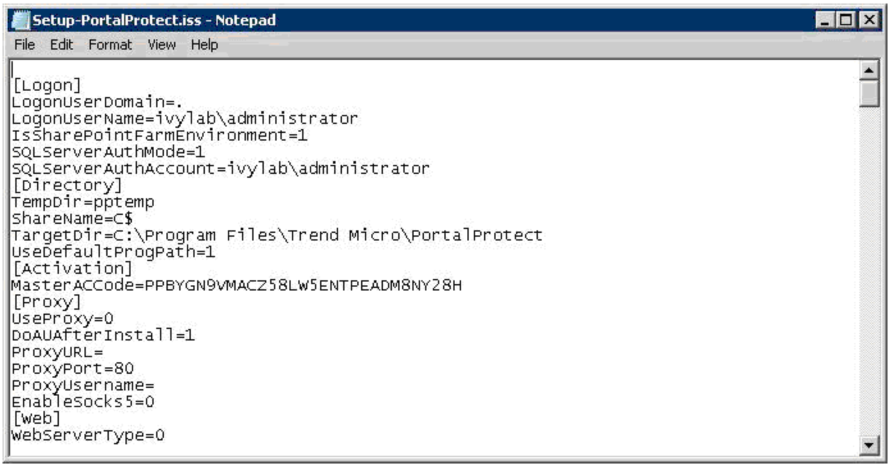
WARNING: This program is protected by copyright laws and international treaties.

For the next steps, refer to *Installation Scenarios Using Server Farms* on page 2-4.

Note: You can define a specific path to store the pre-configured file using: **Setup /R <pre-configured file path>**. If you do not specify the pre-configuration file path, the pre-configuration file will set to: `%Windir%\temp` as ***`Setup-PortalProtect.iss`***.

---

6. The tool generates the pre-configured file: ***`Setup-PortalProtect.iss`***. The default file path is located in the folder: `%windir%\temp`.



```
[Logon]
LogonUserDomain=.
LogonUserName=ivylab\administrator
IsSharePointFarmEnvironment=1
SQLServerAuthMode=1
SQLServerAuthAccount=ivylab\administrator
[Directory]
TempDir=pptemp
ShareName=C$
TargetDir=C:\Program Files\Trend Micro\PortalProtect
UseDefaultProgPath=1
[Activation]
MasterACCode=PPBYGN9VMACZ58LW5ENTPEADM8NY28H
[Proxy]
UseProxy=0
DoAUAfterInstall=1
ProxyURL=
ProxyPort=80
ProxyUsername=
EnableSocks5=0
[Web]
WebServerType=0
```

The contents of the pre-configured file are as follows:

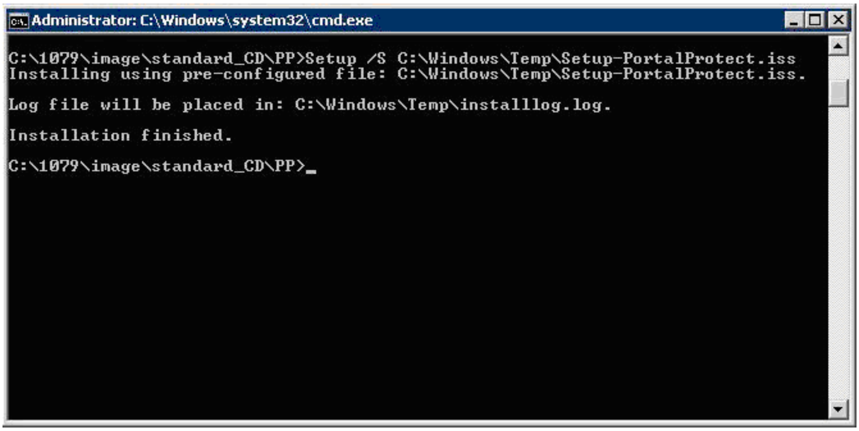
- **LogonUserDomain**—target server domain
- **LogonUserName**—account to logon the target server
- **IsSharePointFarmEnvironment—1:** SharePoint server farm environment; **0:** SharePoint stand-alone server
- **SQLServerAuthMode—1:** Windows Authentication; **0:** SQL Server Authentication
- **SQLServerAuthAccount**—account used to access the SharePoint configuration database
- **TempDir**—directory used to store installation files, which will be deleted after installation
- **ShareName**—name of the shared folder
- **TargetDir**—directory to store support files
- **UseDefaultProgPath—1:** target directory is the default path; **0:** target directory is the specified path
- **MasterACCode**—activation code used to activate your products to enable scanning and security updates

- **UseProxy—1:** enable; **0:** disable
- **DoAUAfterInstall—1:** enable; **0:** disable
- **ProxyURL**—proxy server address
- **ProxyPort**—port number for the proxy server
- **ProxyUsername**—authentication username for the proxy server
- **EnableSocks5—1:** enable**; 0:** disable
- **WebServerType—1:** Apache; **0:** IIS
- **IISSiteType—1:** New Web Site; **0:** Default Web site
- **WebPort**—Web server port number
- **EnableSSL—1:** enable; **0:** disable
- **SSLPort**—SSL port number
- **SSLValidPeriodCertificate**—certificate validity of the SSL
- **WTCEnable—1:** enable; **0:** disable
- **ActivateServerManagement—1:** select active directory group; **0:** skip
- **RegisterCMAgent—1:** enable; **0:** disable
- **CMServerAddress**—CM server address
- **CMServerPortNumber**—CM server port number
- **ConnectCMServerUsingHTTPS—1:** enable; **0:** disable
- **ConnectCMServerUsingProxy—1:** enable; **0:** disable
- **ConnectCMServerProxyAddress**—CM server proxy address
- **ConnectCMServerUseSOCKS5—1:** enable; **0:** disable
- **ConnectCMServerProxyUserName**—authentication username of the proxy server for CM server
- **CMServerWebUserName**—authentication username of the Web server for CM server
- **ConnectCMServerProxyPortNumber**—port number of the proxy server for CM server
- **SQLServerAuthPassword**—password to access the SharePoint configuration database
- **LogonPassword**—password to log on the target server
- **ProxyPassword**—proxy server authentication password

- **ConnectCMServerProxyPassword**—authentication password of the proxy server for CM server
- **CMServerWebPassword**—authentication password of the Web server for CM server
- **ConsoleGroup**—when a domain is selected, the group name displays; otherwise **PortalProtect Admin Group** will display
- **ServerManagementGroupSid**—SID to identify the group
- **UseSMTPNotification—1:** enable; **0:** disable
- **SMTPServerAddress**—SMTP server address
- **SMTPServerPort**—SMTP server port number
- **SMTPAdminEMailAddress**—email address for Administrator Notification

WARNING! **All passwords are encrypted for security. Do NOT modify the ConsoleGroup or ServerManagementGroupSid.**

7. Run **Setup /S C:\Windows\Temp\Setup-PortalProtect.iss** to enable Silent Install to perform an unattended installation of PortalProtect.



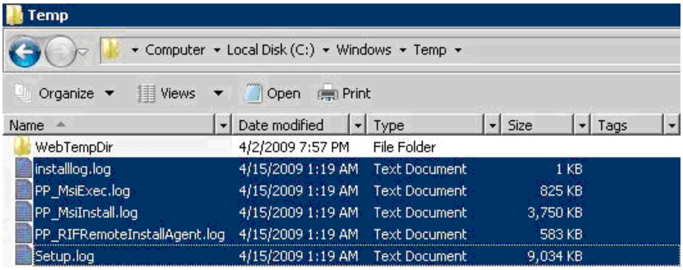
```
C:\1079\image\standard_CD\PP>Setup /S C:\Windows\Temp\Setup-PortalProtect.iss
Installing using pre-configured file: C:\Windows\Temp\Setup-PortalProtect.iss.

Log file will be placed in: C:\Windows\Temp\installlog.log.

Installation finished.

C:\1079\image\standard_CD\PP>_
```

8. After **Setup** installs PortalProtect on your computer, it creates the setup log files in the `%windir%\temp` folder.



Name	Date modified	Type	Size	Tags
WebTempDir	4/2/2009 7:57 PM	File Folder		
installlog.log	4/15/2009 1:19 AM	Text Document	1 KB	
PP_MsiExec.log	4/15/2009 1:19 AM	Text Document	825 KB	
PP_MsiInstall.log	4/15/2009 1:19 AM	Text Document	3,750 KB	
PP_RIFRemoteInstallAgent.log	4/15/2009 1:19 AM	Text Document	583 KB	
Setup.log	4/15/2009 1:19 AM	Text Document	9,034 KB	

Note: Silent Install allows you to install PortalProtect on any path you choose unlike the setup program, which installs PortalProtect in the default system **Program Files** folder as `%ProgramFiles%\Trend Micro\Portal Protect`.

Post Installation

The Setup program will create a folder called `C:\temp` (assuming you installed PortalProtect to the C-drive). This folder contains temporary files of the installation and removal process.

Important Notice:

After installing PortalProtect, you must configure options in the Windows SharePoint Services Central Administration Web page to enable PortalProtect features. Trend Micro recommends enabling PortalProtect immediately after completing the installation.

To enable PortalProtect:

1. Open the SharePoint Services Central Administration Web page:

   Start > Programs > Administrative Tools > SharePoint Central Administration > Operations > Security Configuration > Antivirus

2. Select the following:
   - Scan documents on upload
   - Scan documents on download
   - Attempt to clean infected documents

Note: Make sure the **Windows SharePoint Services Administration** service is running, which regularly checks for PortalProtect status updates for virus scanning and virus signature. You may check the service status from, **Start > Programs > Administrative Tools > Services**.

Testing Your Installation

Trend Micro recommends verifying the installation by using the EICAR test script. EICAR, the European Institute for Computer Antivirus Research, developed the test script as a safe way to confirm that antivirus software is properly installed and configured. Visit the EICAR Web site for more information:

http://www.eicar.org

The EICAR test script is an inert text file with a ***.com*** extension. It is not a virus and does not contain any fragments of viral code, but most antivirus software will react to it as if it were a virus. Use it to trigger a virus incident and confirm that email notifications, HTTP scanning, and virus logs work properly.

WARNING! Never use real viruses to test your antivirus installation.

To test the ability of your installation to detect an infected file:

1. Open an ASCII text file and copy the following 68-character string to it:

   X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

2. Save the file as `EICAR.com` to a `temp` directory. If there is an antivirus installation on your machine, it should immediately detect the file.
3. To test the SharePoint deployment for a network PortalProtect is currently protecting, upload the EICAR.com file to a SharePoint site.

Note: Trend Micro also recommends testing a zipped version of the EICAR file. Using compression software, zip the test script and perform the steps above.

Uninstalling PortalProtect

There are two methods for uninstalling PortalProtect 1.8:

- From the Windows Control Panel (Add/Remove Programs)
- Trend Micro Uninstallation application (recommended)

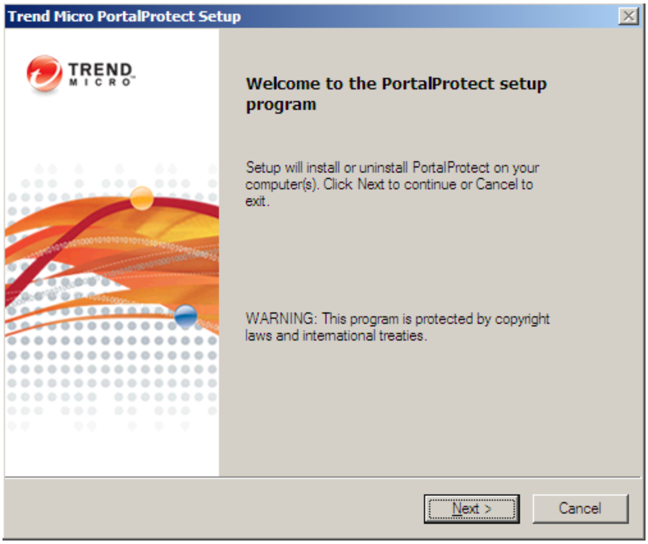
Uninstalling PortalProtect both locally and remotely is performed with a user-friendly uninstallation program. This program allows you to easily remove PortalProtect from one or many servers.

The servers must be part of your network and you must have access with administrator privileges.

Note: For a local server, you can also use the program removal function located in the Windows Control Panel. However, to remotely remove PortalProtect from a server you need to use the PortalProtect uninstallation program.

To uninstall PortalProtect:

1. Insert the PortalProtect program CD into your CD-ROM drive, and navigate to Setup.exe and execute it.
2. The Trend Micro PortalProtect Setup screen displays.



Trend Micro PortalProtect Setup

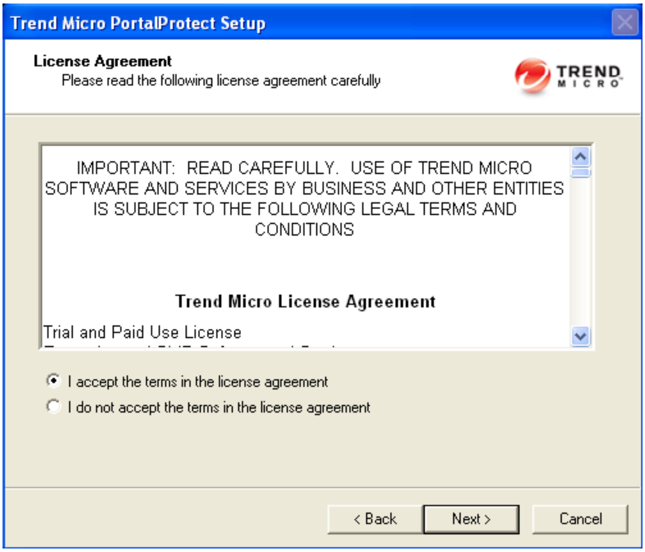
Welcome to the PortalProtect setup program

Setup will install or uninstall PortalProtect on your computer(s). Click Next to continue or Cancel to exit.

WARNING: This program is protected by copyright laws and international treaties.

3. Click **Next**.

4. The **License Agreement** screen displays.



Trend Micro PortalProtect Setup

License Agreement

Please read the following license agreement carefully

IMPORTANT: READ CAREFULLY. USE OF TREND MICRO SOFTWARE AND SERVICES BY BUSINESS AND OTHER ENTITIES IS SUBJECT TO THE FOLLOWING LEGAL TERMS AND CONDITIONS

Trend Micro License Agreement

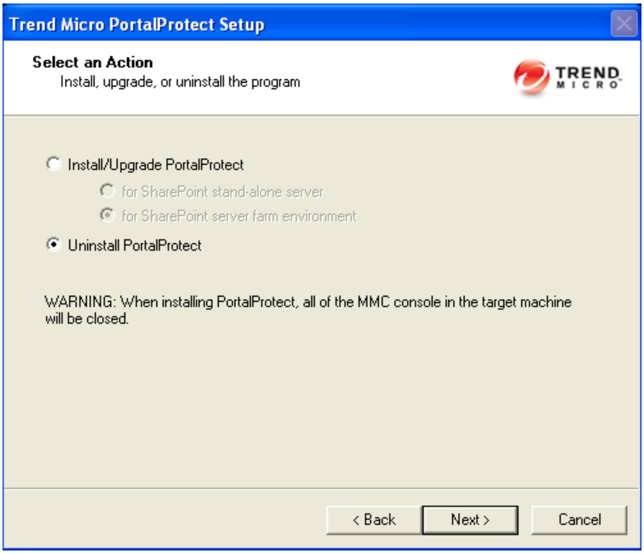
Trial and Paid Use License

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

Select **I accept the terms in the license agreement** and click **Next >**.

5. The **Select an Action** screen displays.



Select an Action

Install, upgrade, or uninstall the program

○ Install/Upgrade PortalProtect

○ for SharePoint stand-alone server

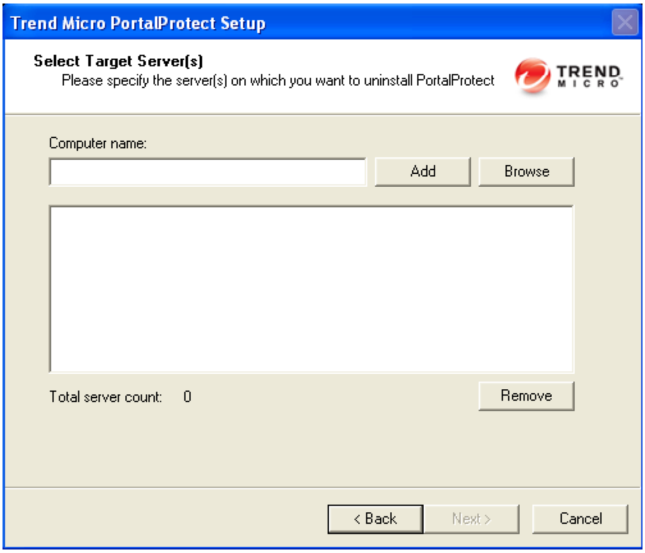
● for SharePoint server farm environment

● Uninstall PortalProtect

WARNING: When installing PortalProtect, all of the MMC console in the target machine will be closed.

Select **Uninstall PortalProtect**.

6. The **Select Target Servers** screen displays.



Trend Micro PortalProtect Setup

Select Target Server(s)

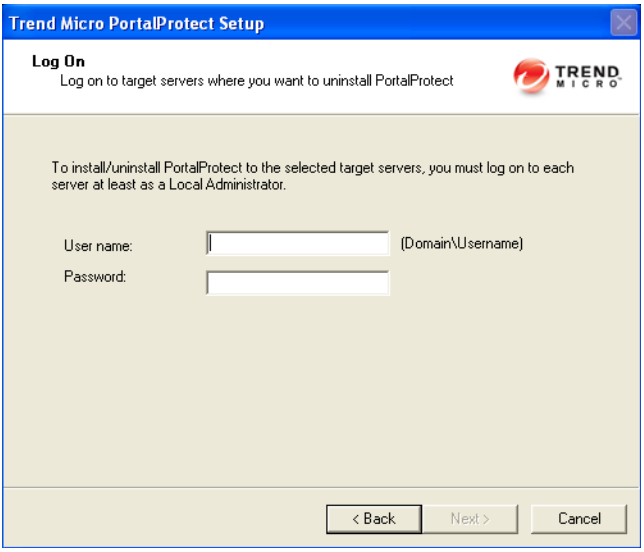
Please specify the server(s) on which you want to uninstall PortalProtect

Computer name:

Total server count: 0

7. **Add** / **Browse** for the **Computer name(s)** where you want to uninstall PortalProtect; then, select the added server(s) and click **Next >**.

8. The **Logon** screen displays.



Trend Micro PortalProtect Setup

Log On

Log on to target servers where you want to uninstall PortalProtect

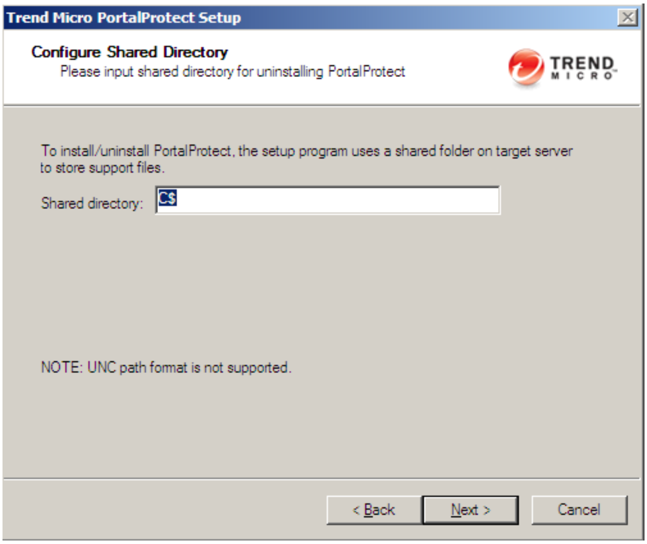
To install/uninstall PortalProtect to the selected target servers, you must log on to each server at least as a Local Administrator.

User name: (Domain\Username)

Password:

Type the server **User name** [Domain\Username] and **Password** and click **Next >**.

9. The **Configure Shared Directory** screen displays.



Trend Micro PortalProtect Setup

Configure Shared Directory

Please input shared directory for uninstalling PortalProtect

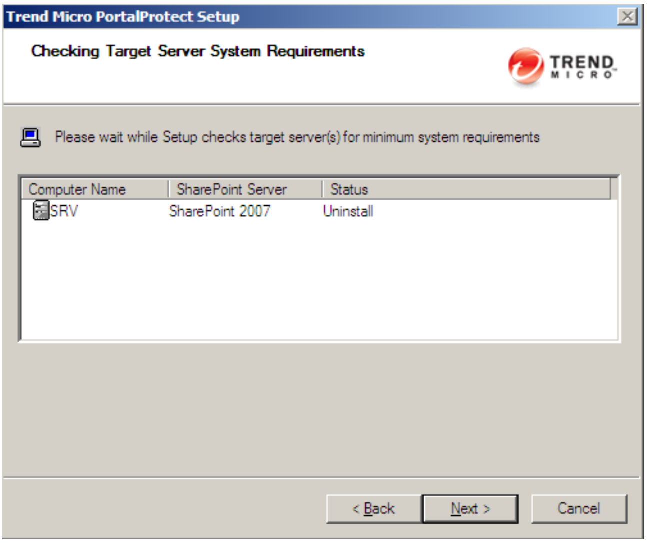
To install/uninstall PortalProtect, the setup program uses a shared folder on target server to store support files.

Shared directory: C$

NOTE: UNC path format is not supported.

Verify the **Shared directory** and click **Next >**.

10. The **Checking Target Server System Requirements** screen displays.



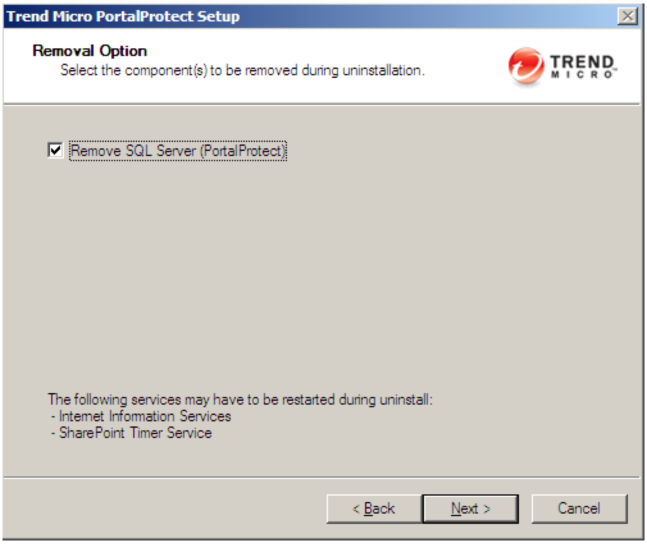
Trend Micro PortalProtect Setup
Checking Target Server System Requirements
TREND MICRO
< Back
Next >
Cancel

Please wait while Setup checks target server(s) for minimum system requirements

Computer Name	SharePoint Server	Status
SRV	SharePoint 2007	Uninstall

Verify the **Computer Name** and **SharePoint Server**. Also, ensure the **Status** reads **Uninstall** and click **Next >**.

11. The **Removal Option** screen displays.



Trend Micro PortalProtect Setup

Removal Option

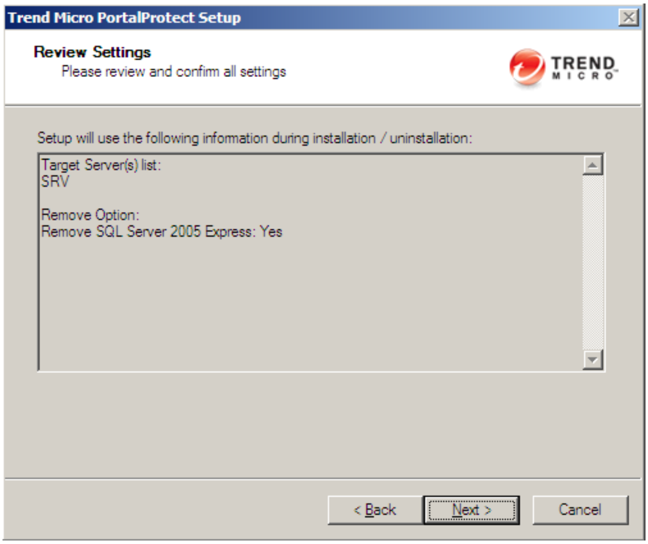
Select the component(s) to be removed during uninstallation.

☑ Remove SQL Server (PortalProtect)

The following services may have to be restarted during uninstall:
- Internet Information Services
- SharePoint Timer Service

Select **Remove SQL Server (PortalProtect)** and click **Next >**.

12. The **Review Settings** screen displays.



Review Settings

Please review and confirm all settings

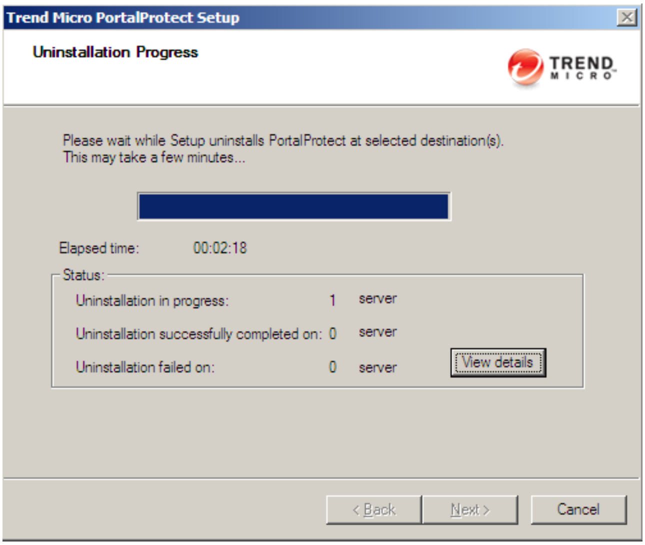
Setup will use the following information during installation / uninstallation:

```
Target Server(s) list:
SRV

Remove Option:
Remove SQL Server 2005 Express: Yes
```

Review the settings displayed on screen. Go **Back** to make changes if needed. Click **Next >** when you are satisfied with the settings.

13. The **Uninstallation Progress** screen displays.



Please wait while Setup uninstalls PortalProtect at selected destination(s).
This may take a few minutes...

Elapsed time: 00:02:18

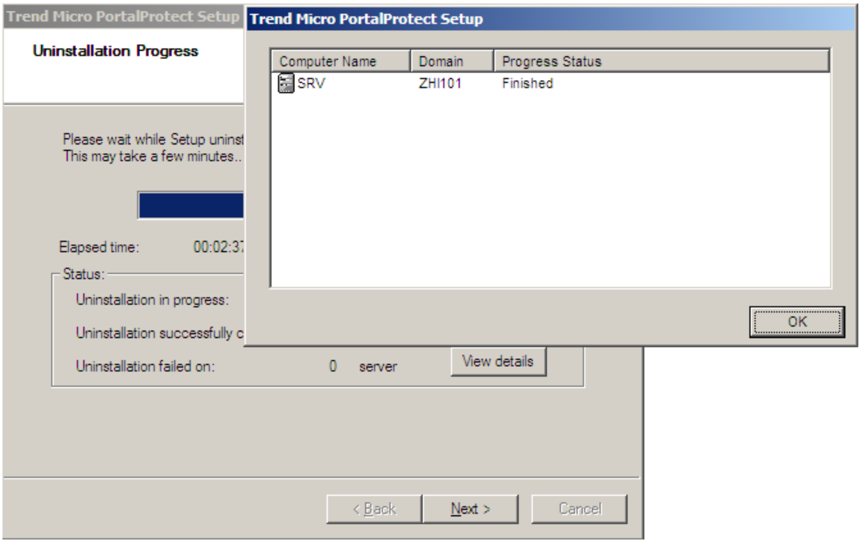
Status:

Uninstallation in progress: 1 server

Uninstallation successfully completed on: 0 server

Uninstallation failed on: 0 server

Click **View Details** to observe the uninstallation progress (see *Figure 2-6* on page 2-46).



Trend Micro PortalProtect Setup

Uninstallation Progress

Please wait while Setup uninst
This may take a few minutes..

Elapsed time: 00:02:37

Status:

Uninstallation in progress:

Uninstallation successfully c

Uninstallation failed on: 0 server

Trend Micro PortalProtect Setup

Computer Name	Domain	Progress Status
SRV	ZHI101	Finished

FIGURE 2-6. Uninstallation Progress Status

14. When the **Progress Status** displays **Finished** (*Figure 2-6*), click **OK > Next >**.
15. The **Uninstallation Complete** screen displays.

Chapter 3

Getting Started with PortalProtect

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

In this chapter, you will find information about:

- *Viewing the PortalProtect Web Management Console* starting on page 3-1
- *Updating PortalProtect* starting on page 3-3
- *Activating PortalProtect* starting on page 3-4
- *Updating Your Components* starting on page 3-7
- *About the Trend Micro Scan Engine* starting on page 3-10
- *About the Virus Pattern File* starting on page 3-12

Viewing the PortalProtect Web Management Console

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

To view the Web Management Console for a local server

1. Click **Start > Programs > Trend Micro PortalProtect for Microsoft SharePoint > PortalProtect Management Console**. The Web Management Console appears.
2. The URL in the Address box should be the following: `http://127.0.0.1[port number]/PortalProtect/Login.htm`

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

To view the Web Management Console for a remote server:

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

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

The Web Management Console Consists of the Following Main Elements:

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

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.

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 3-5.
- If a proxy server handles Internet traffic on your network, you must type the proxy server information. See *Configuring Proxy Settings* on page 3-6.
- Configure your update method and source. Methods include **Manual Update** and **Scheduled Update**. Sources include the ActiveUpdate server, other update source, and the intranet UNC path.

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

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.

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.

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 3-5

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**.

Registering PortalProtect

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

To register your product, do one of the following:

- During installation, you will be prompted to use your Registration Key to register online. Follow the link to the Trend Micro Web site, register your product, and then return to the installation program to complete your installation.
- Contact Trend Micro directly. Provide a Trend Micro representative with your Registration Key and he or she will give you an Activation Code. When you purchase PortalProtect, your vendor provides you with a Registration Key. Trend Micro maintains a list of contacts at:

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

  See *Contacting Trend Micro* on page 6-2.

Configuring Proxy Settings

Most enterprises use proxy servers for added security and more efficient bandwidth utilization. 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 feature use Proxy servers:

- ActiveUpdate
- Product Registration
- World Virus Tracking

To set the Internet proxy:

1. Open the PortalProtect Web console.
2. On the sidebar, click **Administration** > **Proxy**. The **Proxy Settings** screen appears.
3. Select the **Use a proxy server**.
4. Select the proxy type.
5. Type the server name or IP address of the proxy server and its port number.
6. If your proxy server requires a password, type your user name and password in the fields provided.
7. Click **Save** to save your settings.

Updating Your Components

Antivirus software can only be effective if it is using the latest technology. Since viruses and other malicious code are constantly being discovered and evolving, it is crucial that you regularly update your scan engine and pattern files for maximum protection. Before you can update PortalProtect, you must activate your software.

You can update your components manually or according to a schedule. To update PortalProtect, you must choose the components you want to update: virus pattern file and scan engine. In addition, you must specify the download source of the latest components.

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.

To manually install your components:

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. Select the download source.

- **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.
- **Other Update Source**–Download your components from an Internet source that receives updated components.
- **Intranet location containing a copy of the current file**–Type the Universal Naming Convention (UNC) path of another server on your network.

4. 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.
5. Click **Save**.
6. Click **Update Now**. A confirmation dialog box appears.
7. Click **OK**. PortalProtect begins updating. If you want to stop the update process, click Stop Updating, and then click **OK**.

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.

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

To configure scheduled updates:

1. On the left menu, click **Updates** > **Scheduled**. The Scheduled Update screen appears.
2. Check **Enable scheduled update**.
3. Select the check box(es) of the component(s) you want to update.
4. Select the options for the frequency of the update. Remember to set a time when the download occurs for each option.
5. Select the download source.

- **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.
- **Other Update Source**–Download your components from an Internet source that receives updated components.
- **Intranet location containing a copy of the current file**–Type the Universal Naming Convention (UNC) path of another server on your network.

6. Select **Allow other servers to download updates from this server...** to create a component package on one server that can be accessed and downloaded by the other servers on the same local network.
7. Click **Save**.

Creating an Update Component Package

If you have many PortalProtect Servers on your Intranet, using an update component package can provide you a quick update option. An update component package consists of the latest pattern file and scan engine on a local PortalProtect Server. Additionally, using a component package, conserves network bandwidth as it becomes unnecessary for all the PortalProtect Servers to access the Internet to update.

To create an update component package:

1. On the left menu, click **Updates**, then click one of the following:
   - **Manual**. The Manual Update screen appears.
   - **Scheduled**. The Scheduled Update screen appears.
2. Make sure the check box(es) of the component(s) you want to include in the update component package are selected.
3. Under Component **Download Source**, select one of the following:
   - **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.
   - **Other Update Source**–Download your components from an Internet source that receives updated components.

4. Select **Allow other servers to download updates from this server ...** to create a component package on one server, which is able to be accessed by the other servers on the same local network.
5. Click **Save**.

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

About the Trend Micro Scan Engine

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

- in the wild or actively circulating
- in the zoo or controlled viruses that are not in circulation

In addition to having a long history in the industry, the Trend Micro scan engine has also proven in test after test to be one of the fastest—whether checking a single file, scanning 100,000 files on a desktop machine, or scanning email traffic at the Internet gateway. Rather than scan every byte of every file, the engine and pattern file work together to identify not only telltale characteristics of the virus code, but the precise location within a file where the virus would hide. When it detects a virus, the virus can be removed and the integrity of the file restored.

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

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

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

1. Frequent updates to the scan engine's data-file, called the virus pattern file, can be downloaded and read by the engine without the need for any changes to the engine code itself.
2. Technological upgrades in the engine software prompted by a change in the nature of virus threats, such as the rise in mixed-threats like SQL Slammer.

In both cases, updates can be automatically scheduled, or the security administrator can handle them manually.

International computer security organizations, including the International Computer Security Association (ICSA) annually certify the Trend Micro scan engine.

About Scan Engine Updates

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

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

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

`http://www.trendmicro.com`

About the Virus Pattern File

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

All Trend Micro antivirus programs using the ActiveUpdate function can detect the availability of a new virus pattern on the Trend Micro server, and/or you can set it to automatically poll the server every week, day, or hour to get the latest file. Trend Micro recommends that you schedule automatic updates at least weekly, which is the default setting for all shipped products. 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 it Works

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

Pattern File Numbering

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

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

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

For the file pattern number 1.786.01:

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

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

About ActiveUpdate

ActiveUpdate is a function common to many Trend Micro products. It connects to the Trend Micro Internet update server to enable downloads of virus pattern files, scan engines, anti-spam rules, and program files.

ActiveUpdate does not interrupt network services, or require you to reboot your computers. Updates are available on a regularly scheduled interval, or on-demand.

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.

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.

Chapter 4

Configuring Scanning and File Blocking Options

This chapter discusses configuring scanning and file blocking options for PortalProtect. PortalProtect provides the following scanning and blocking functions for your SharePoint environment: Real-time scan, Manual scan, and Scheduled scan.

Each of these scanning options provides its own set of file blocking and virus scan filters. Using advanced options, you can configure PortalProtect to scan for malicious Macro code, and to block and scan compressed files.

In this chapter, you will find information about:

- *Configuring Scan Options* on page 4-2
- *Real-time Scans* on page 4-4
- *Manual Scan* on page 4-5
- *Scheduled Scan* on page 4-6
- *About IntelliScan* on page 4-11
- *Using ActiveAction* on page 4-12
- *Setting Blocking Actions* starting on page 4-9
- *Using ActiveAction* starting on page 4-12

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 Virus Scans* on page 4-4

About Scanning

Real-time scanning occurs whenever a file is saved to a SharePoint server (check-in) or retrieved from the SharePoint server (check-out). Manual scanning scans the SQL content store and occurs immediately after you 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.

Note: See the Online Help for specific information about how to use the PortalProtect Management console to configure and perform scans.

Backup Files Before Taking Action

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

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

See the following for information about how to set backup folder locations:

- *Specify Backup Folder for Real-time Virus Scan* on page 4-5
- *Specify Backup Folder for Manual Scan* on page 4-6
- *Specify Backup Folder for Scheduled Scan* on page 4-7

Selecting Files to Scan

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 IntelliScan* on page 4-11.
- **Scan 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.

Setting Scan Actions

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.

To configure your scan actions:

1. Choose whether to set up a backup folder.

   When you setup a backup folder, PortalProtect sends a copy of the file to the backup folder before it performs the configured actions. See *Specify Backup Folder for Manual Scan* on page 4-6.

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 *Using ActiveAction* on page 4-12

Real-time Scans

Real-time scans protect 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.

Note: Trend Micro recommends that you NOT disable real-time scan functionality. However, if you must disable the real-time scan functionality, be sure to run regular manual scans.

Enabling and Disabling Real-time Virus Scans

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

WARNING! **If you disable real-time scanning, background scanning and file blocking will not occur, making 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.

To enable or disable a real-time virus scan:

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

Specify Backup Folder for Real-time Virus Scan

The following explains the steps required to specify a backup folder for real-time virus scan:

To specify a backup folder location for real-time virus scan:

1. On the left menu, click **Virus Scan**. The **Virus Scan** screen then displays.
2. Click the **Action** tab, and then click **Backup and Quarantine Setting** at the bottom of the screen.
3. In the **Backup directory** field, type the full path in which to save backup files. If the directory path does not exist, Portal Protect will create a folder for the specified path.
4. Click **Save** to accept and save the current setting.

Manual Scan

You can run a manual scan at any time. They scan the SQL database according to your configurations and then stop. If you try to run a manual scan when PortalProtect is running a scheduled scan, the manual scan takes priority.

Specify Backup Folder for Manual Scan

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

To specify a backup folder location for manual scan:

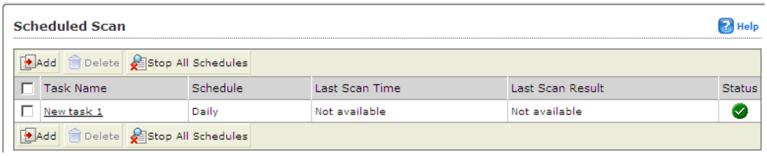
1. On the left menu, click **Manual Scan**. The **Manual Scan** screen then appears.
2. Under **Select the scan type**, click the **Virus scan** link. The **Manual Scan > Virus Scan** screen then appears.
3. Click the **Action** tab, and then click **Backup and Quarantine Setting** at the bottom of the screen.
4. In the **Backup directory** field, type the full path in which to save backup files. If the directory path does not exist, Portal Protect will create a folder for the specified path.
5. Click **Save** to accept and save the current setting.

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.

To enable or disable a scheduled scan:

1. On the left menu, click **Scheduled Scan,** to display the **Scheduled Scan** screen.
2. In the **Status** column, click the green checkmark to **disable** the scan; a red "X" then displays. (See *Figure 4-7* and *Figure 4-8*).

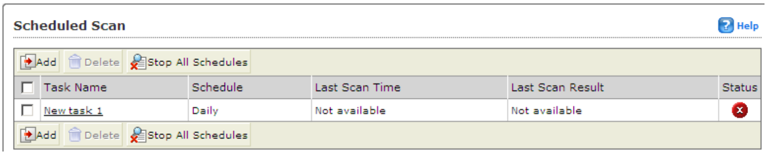


Scheduled Scan

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

FIGURE 4-7. 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 4-8. Scheduled scan disabled

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

Specify Backup Folder for Scheduled Scan

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

To specify a backup folder location for scheduled scan:

1. On the left menu, click **Scheduled Scan**. The **Scheduled Scan** screen then appears.
2. **Add** a new scheduled scan, or click an existing scheduled scan in the **Task Name** column.
3. Under **Select scan type**, click the **Virus scan** link. The **Scheduled Scan > Virus Scan** screen then appears.
4. Click the **Action** tab, and then click **Backup and Quarantine Setting** at the bottom of the screen.
5. In the **Backup directory** field, type the full path in which to save backup files. If the directory path does not exist, Portal Protect will create a folder for the specified path.
6. Click **Save** to accept and save the current setting.

Configuring 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 your choose.

Note: File blocking options vary according to the type of scan performed. Check the actions available for each scan type, whether Virus Scan, Manual Scan, 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. You can temporarily quarantine all high-risk file types or those with a specific name associated with a known virus. Later, when you have more time, you can scan the quarantine folder and take action on infected files.

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.

To configure blocking actions:

1. First, choose whether or not to set up a quarantine folder. See *Quarantine Files that Match Blocking Options* on page 4-10
2. Set an action for PortalProtect to execute on files that match your blocking options. See *Setting Blocking Actions* on page 4-9

Setting Blocking Actions

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. Each time that PortalProtect executes a Quarantine action, it logs an event. You can view these from the **Logs** menu.

Possible Actions

TABLE 4-1. Blocking actions for different scans

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

- **Quarantine**–Move the file to a customized folder, removing it as a security risk from the SharePoint environment. To set the location of the Quarantine folder, click **Quarantine Settings** on the Action tab at the bottom of this group box, and type the location of the folder.
- **Pass**–No action taken. File is passed.
- **Block**–PortalProtect blocks the file from accessing the SharePoint server and logs an event.
- **Delete**–During manual or scheduled scanning, PortalProtect deletes files that match the blocking options from the SharePoint environment.

Quarantine Files that Match Blocking Options

You can configure PortalProtect to move files to a quarantine folder. PortalProtect moves files to the quarantine folder, after the scan determines the file contains a virus or malicious code, or matches the blocking options. Files placed in the quarantine folder will not infect other files. You can examine the content of the quarantine when you have time and take appropriate action. For example, you could send the files to Trend Micro for analysis, delete the files or attempt to clean them.

PortalProtect provides for creating separate folders in which to save quarantined files. You can specify a path and folder for blocked quarantined files for:

- File Blocking (real-time file blocking)
- Manual Scan
- Scheduled Scan

Specify Quarantine Folder for Manual Scan File Blocking

The following describes the steps required to specify a quarantine folder for manual scan file blocking:

To specify the quarantine folder for manual scan file blocking:

1. On the left menu, click **Manual Scan.**
2. Under **Select the scan type**, click the **File blocking** link.
3. Select the **Action** tab.
4. Click **Quarantine Settings** to open the **Quarantine directory** field.
5. In the **Quarantine directory** field, type the full path in which to save quarantined files. If the directory path does not exist, Portal Protect will create a folder to the specified path.
6. Click **Save** to accept and save the current settings, or click **Reset** to change all **Manual Scan** settings to the default value.

Specify Quarantine Folder for Scheduled Scan File Blocking

The following describes the steps required to specify a quarantine folder for scheduled scan file blocking:

To specify the quarantine folder for scheduled scan file blocking:

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 **File blocking** link.
4. Select the **Action** tab.
5. Click **Quarantine Settings** to open the **Quarantine directory** field.
6. In the **Quarantine directory** field, type the full path in which to save quarantined files. If the directory path does not exist, Portal Protect will create a folder to the specified path.
7. Click **Save** to accept and save the current settings, or click **Reset** to change all **Scheduled Scan** settings to the default value.

About IntelliScan

Most antivirus solutions today offer you two options in determining which files to scan for potential threats. PortalProtect will either scan all files (the safest approach), or only true file types and those files with certain file extensions. However, a trend of disguising files by changing the extension makes the latter option less effective.

IntelliScan™ is a Trend Micro technology that identifies a file's "true file type," regardless of the file name extension. IntelliScan uses a method of identifying which files to scan that is more efficient than the standard 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 virus scanning.

Because IntelliScan scans only files that are vulnerable to infection, using IntelliScan brings you 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.

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 result will not assume the file is a graphic file and cease scanning. Instead, 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 be of potential danger. These technologies can mean a reduction in the overall number of files that the scan engine must examine (perhaps as much as a two-thirds reduction), but it comes at the cost of potentially higher 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.

Using ActiveAction

ActiveAction performs primary and secondary scan actions recommended by Trend Micro. If it is unsuccessful in the primary action, it performs the secondary action. There are scan actions pre-configured for viruses, Trojans, and joke programs.

PortalProtect Customized Actions

You can configure PortalProtect to execute actions when it detects a file that presents a security threat to the SharePoint environment. You can customize these actions according to the type of threat presented by viruses or other malicious code.

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 4-15
- **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/`
- **Unscannable, Encrypted or Password protected files**–this functionality is located under **Advanced Options > Unscannable 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 4-15 and *About Unscannable Files* on page 4-16.

Possible Actions

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

Scan actions for viruses include the following:

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

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

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

- **Delete**–Deletes the file and logs an event.
- **Quarantine**–Moves the file to a customized folder, thereby removing it as a security risk to the SharePoint environment. See *Quarantine Files that Match Blocking Options* on page 4-10**.**
- **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 1.8 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 1.8 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 4-2. Scan actions for encrypted and password protected files

During this scan	PortalProtect executes this action
Real-time	Quarantine, 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 Services that the files are infected. In some cases, PortalProtect may identify a file as being infected, when it actually is not. Trend Micro recommends that you review your quarantine folder from time to time for files that may have been identified with a false positive.

About Unscannable Files

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

TABLE 4-3. Scan actions for unscannable files

During this scan	PortalProtect executes this action
Real-time	Quarantine, 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.

Scan Compressed Files for Real-time Virus Scan

The following explains the steps required to scan compressed files for real-time virus scan:

To scan compressed files for real-time virus scan:

1. On the left menu, click **Virus Scan** and select the **Target** tab.
2. From the **Target** tab, under **Advanced Options**, expand the **Scan Restrictions Criteria**.
3. 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.

4. Click **Save**.

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

Scan Compressed Files for Manual Scan

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

To scan compressed files for manual scan:

1. On the left menu, click **Manual Scan**.
2. Under **Select the scan type**, click the **Virus scan** link.
3. Select the **Target** tab. Under **Advanced Options**, expand the **Scan Restrictions Criteria**.
4. 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.

5. Click **Save**.

Scan Compressed Files for Scheduled Scan

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

To scan compressed files for scheduled scan:

1. On the left menu, click **Scheduled Scan**.
2. Click **Add**, to create a new scheduled scan, or click the **Task Name** to edit an existing one.
3. Under **Select scan type**, click the **Virus scan** link.
4. Select the **Target** tab. Under **Advanced Options**, expand the **Scan Restrictions Criteria**.
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**.

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

Configure Macro Scanning Options for Real-time Virus Scan

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

To configure macro scanning options for real-time virus scan:

1. On the left menu, click **Virus 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**.

Configure Macro Scanning Options for Manual Scan

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

To configure macro scanning options for manual scan:

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

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

Configure Macro Scanning Options for Scheduled Scan

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

To configure macro scanning options for scheduled scan:

1. On the left menu, click **Scheduled Scan.**
2. Click **Add**, to create a new scheduled scan, or click the **Task Name** to edit an existing one.
3. Under **Select scan type**, click the **Virus 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**.

Chapter 5

Notifications, Alerts, Logs, and Reports

This chapter discusses PortalProtect Notifications, Alerts, Logs, and Reports. Configure the type of notification and the method to send the notification. Configure system events to provide an alert in the event of an outbreak. View logs to understand what PortalProtect events occur. Logs are an important source of information that you can use for troubleshooting. Use daily, weekly, or monthly reports to share information about the security of your SharePoint environment.

Make notifications part of your proactive security strategy to predict attacks and assess risks. Make logs part of your reactive security strategy to assess and try to determine the causes of the damage. Use both notification and logs to identify vulnerabilities in your SharePoint environment and send reports to share information to other security team members.

In this chapter, you will find information about:

- *Configuring Notifications* starting on page 5-2
- *Alerts* starting on page 5-8
- *Working with Logs* starting on page 5-12
- *Viewing and Generating Reports* starting on page 5-16

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:

- *Virus Scan Notifications* on page 5-3
- *File Blocking Notifications* on page 5-4
- *Manual Scan Notifications* on page 5-5
- *Scheduled Scan Notifications* on page 5-6

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 Virus Scan, File Blocking, Manual Scan, and Scheduled Scan.

To configure global notification settings:

1. From the left menu, click **Administration > Notification Settings**.
2. Under **Administrator Notification**, type the email address for the administrator(s) you wish to receive all notifications. Separate multiple addresses using a semicolon. Click **Apply All**, to update the new settings.
3. Under **Sender Settings**, type the email address of the sender who sends alerts and notifications (for example: PortalProtect_Administrator@do.not.reply).
4. Under **Email Account Settings**, type the SMTP server settings that PortalProtect will use to send email-based notifications for the following:
    - **Display name**: unique identifier, for example: PortalProtect Notification
    - **SMTP Server**
    - **Port**

5. Under **SNMP**, type the following:
   - **IP address**
   - **Community**
6. Click **Save**.

Event Notifications

Portal protect provides various options for sending unique event notifications for: Realtime Scan, Manual Scan and Scheduled Scan for Virus Scan and File Blocking.

Virus Scan Notifications

The following explains the steps required to configure virus scan notifications:

To configure virus scan notifications:

1. On the left menu, click **Virus Scan**. The **Virus Scan** screen appears.
2. Click the **Notification** tab, and select **Notify administrator** to enable virus scan notifications.
3. 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: Virus Scan Notification).
   - **Message**—you can create a unique message using variables like: [Server Name], [Virus Name], [Date], [Time], [File Name], [File Location], and [Action].

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

4. 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.

5. Under **Advanced Notification** (SNMP), select **SNMP** to enable this option.
6. Click Show details to expand the options, and configure according to the following:
   - **IP Address**
   - **Community**
   - **Message**—create a message as stated in Step 3 of this procedure.
7. Select **Write to Windows event log** to write each notification to the Windows event log.
8. Click **Save**.

File Blocking Notifications

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

To configure file blocking notifications:

1. On the left menu, click **File Blocking**. The **File Blocking** screen appears.
2. Click the **Notification** tab, and select **Notify administrator** to enable file blocking notifications.
3. 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], [Date], [Time], [File Name], [File Location], and [Action].

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

4. 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.
5. Under **Advanced Notification** (SNMP), select **SNMP** to enable this option.
6. Click Show details to expand the options, and configure according to the following:
   - **IP Address**
   - **Community**
   - **Message**—create a message as stated in Step 3 of this procedure.
7. Select **Write to Windows event log** to write each notification to the Windows event log.
8. Click **Save**.

Manual Scan Notifications

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

To configure manual scan notifications:

1. On the left menu, click **Manual Scan**. The **Manual Scan** screen appears.
2. Under, **Select the scan type**, click the **Virus scan** or **File Blocking** link.
3. Click the **Notification** tab, and select **Notify administrator** to enable manual virus 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: Virus Scan Notification).

- **Message**—you can create a unique message using variables like: [Server Name], [Virus Name], [Date], [Time], [File Name], [File Location], and [Action].

> **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**.

Scheduled Scan Notifications

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

To configure scheduled scan notifications:

1. On the left menu, click **Scheduled Scan**. The **Scheduled Scan** screen appears.
2. Click **Add**, to add a new task, or click and existing task from the **Task Name** column. The Scheduled **Scan > Add** or, **Edit Scan Task** screen appears.

3. Under, **Select the scan type**, click the **Virus scan** or **File Blocking** link.
4. Click the **Notification** tab, and select **Notify administrator** to enable manual virus scan 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: Virus Scan Notification).
   - **Message**—you can create a unique message using variables like: [Server Name], [Virus Name], [Date], [Time], [File Name], [File Location], and [Action].

   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**—create a message as stated in Step 5 of this procedure.

9. Select **Write to Windows event log** to write each notification to the Windows event log.
10. Click **Save**.

Alerts

The Alerts function provides notifications for System Events and Outbreaks. This section describes how to enable and configure these options.

System Events

System events enables to send notifications regarding the status of various features in PortalProtect (see *Figure 5-9*). These notifications include the following:

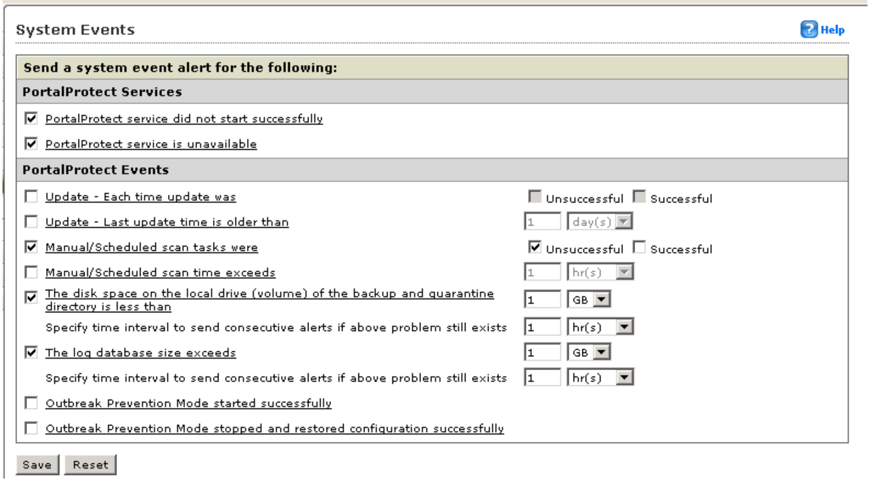
PortalProtect Services

- PortalProtect service did not start successfully
- PortalProtect service is unavailable

PortalProtect Events

- Update—each time update was successful or unsuccessful
- Update—whether last update is older than [x]
- Manual/Scheduled scan tasks were successful or unsuccessful
- Manual/Scheduled scan time exceeds [x]
- Disk space on the local drive for the backup and quarantine directory is less than [x-GB/MB]
- Log database size exceeds [x-GB/MB]
- Outbreak Prevention mode started successfully
- Outbreak Prevention Mode Stopped and restored configuration successfully

Additionally, you can configure a frequency for sending consecutive alerts when a problem continues to exist.



System Events

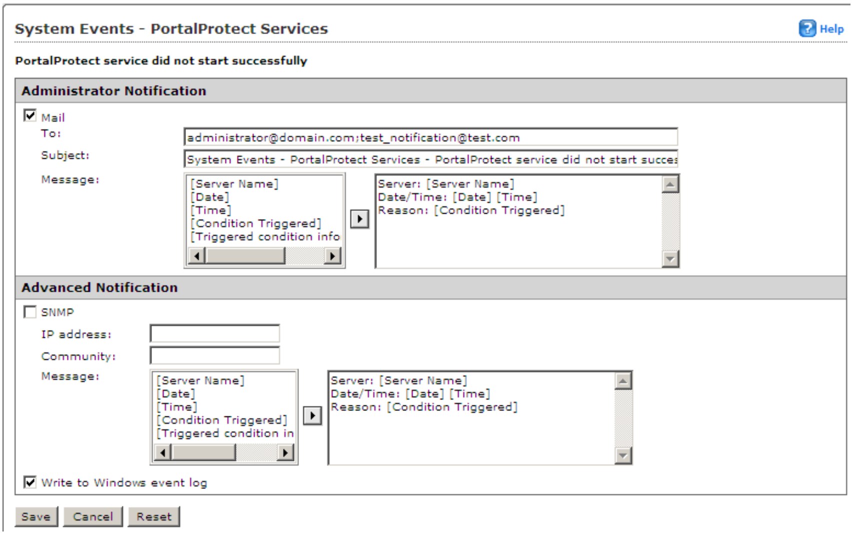
Send a system event alert for the following:	
PortalProtect Services	
☑ PortalProtect service did not start successfully	
☑ PortalProtect service is unavailable	
PortalProtect Events	
□ Update - Each time update was	□ Unsuccessful □ Successful
□ Update - Last update time is older than	1 day(s)
☑ Manual/Scheduled scan tasks were	☑ Unsuccessful □ Successful
□ Manual/Scheduled scan time exceeds	1 hr(s)
☑ The disk space on the local drive (volume) of the backup and quarantine 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)
□ Outbreak Prevention Mode started successfully	
□ Outbreak Prevention Mode stopped and restored configuration successfully	

FIGURE 5-9. **System Events configuration screen**

To configure system events for PortalProtect services:

1. Click **Alerts > System Events**. The **System Events** screen appears.
2. Under **PortalProtect Services**, select from the following options:
   - **PortalProtect service did not start successfully**
   - **PortalProtect service is unavailable**
3. After selecting an option, click the link to display the Administrator Notification screen, similar to that shown in *Figure 5-10*.
4. Create a custom message and email list as explained in *Virus Scan Notifications* on page 5-3.

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 5-10. System Events, administrator notification screen

To configure system events for PortalProtect events:

1. Click **Alerts > System Events**. The **System Events** screen appears.
2. Under **PortalProtect Events**, select from the following options:
   - **Update - each time update was [successful] or [unsuccessful]**—select the option according to whether send a notification if the update was successful or not.
   - **Update - whether last update is older than [x]**—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 [successful] or [unsuccessful]**—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]**—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.

- **Disk space on the local drive for the backup and quarantine directory is less than [x-GB/MB]**—type a value in the field and choose **GB** (gigabyte) or **MB** (megabyte). 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-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.

3. After selecting an option and setting the parameters to trigger the notification, click the link to display the Administrator Notification screen, similar to that shown in *Figure 5-10*.
4. Create a custom message and email list as explained in *Virus Scan Notifications* on page 5-3.

Click **Save.**

Outbreak Alert

Outbreak Alert enables you to configure settings to alert administrators when:

- Viruses detected reach a selected number within a selected time span
- Uncleanable viruses reach a selected number within a selected time span
- Blocked files reach a selected number within a selected time span

To configure an Outbreak Alert:

1. On the left menu, click **Alerts > Outbreak Alert**. The **Outbreak Alert** screen appears.
2. In the Number field, type a number that equals the number of Detected Viruses, Uncleanable Viruses, and Blocked Files that will trigger the alert. Then, type a value in the Time field, and choose whether that value should be expressed in Hours or Minutes.

Note: An Outbreak Alert will be triggered when the Number is reached within the specified time span. For example: for viruses detected, a value of 25 in the **Number** field with a **Time** of 24-hours, will trigger an Outbreak Alert if 25 or more viruses are detected within a 24-hour period.

Configure the following options:

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

Note: Select the checkbox to enable an alert, and clear the checkbox to disable it.

3. Click **Save**.

Working with Logs

PortalProtect provides comprehensive information about virus scan, file blocking, updates, scan events, backup files, unscannable files, and quarantined files. It saves this information to a database. You can query the database and obtain logs for analysis. For example, you can analyze Virus 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:

- **Virus scan logs**–contains information about detected virus or malicious code incidents, including: scan time, file location, author, virus name, file name, and action taken.

- **File blocking logs**–contains information about scan time, file location, author, policy/rule name, filename, and action.
- **Update logs**–contains information about update events, including: the update method, success or failure, and what components were updated.
- **Scan events logs**–contains information about PortalProtect System events, including Manual scans or Scheduled scans that have finished or are in progress.
- **Backup logs**–contains information about files that were backed up, including: scan time, author, virus name, filename, and backup path.
- **Unscannable files logs**–shows files that PortalProtect was unable to scan. Information includes: scan time, file location, author, reason, filename, and action.
- **Quarantine logs**–contains information about files that were quarantined, including: scan time, author, filter, reason, filename and quarantine path.

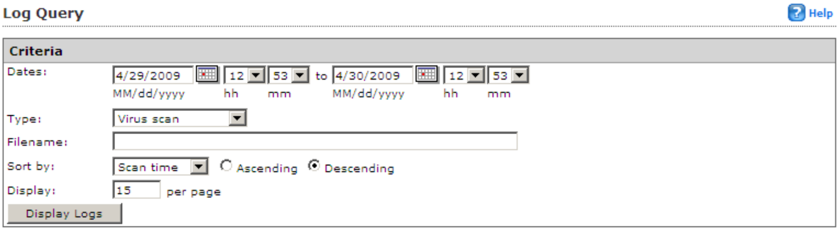
Query Logs

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, files placed in quarantine, blocked files, and files placed in the backup folder. You can export or print the log information you obtain from a query.

To perform a log query:

1. From the left menu, click **Logs > Query**. The **Log Query** screen appears.
2. Select the log type from the **Type** drop-down.
3. To query using a date range:
   - Select a query date range from the **Dates** field. The date range includes a **from:** [MM/dd/yyyy] time of day [hh] and [mm] and **to:** [MM/dd/yyyy] time of day [hh] and [mm].
4. To query using a filename:
   - Type a full or partial filename in the **Filename** field.
5. Select whether to sort logs by: Scan time, Virus name, Filename, or Action; then, select Ascending or Descending.
6. In the Display field, type the number of log entries to display per page; the default is 15.

7. Click **Display Logs** to display the query results.
8. Click **Export** to export the result of your query as a comma-separated value (CSV) file (Unicode standard).
9. Click **Print** to print the result of your query.



Log Query

Help

Criteria

Dates: 4/29/2009 (MM/dd/yyyy) 12 (hh) 53 (mm) to 4/30/2009 (MM/dd/yyyy) 12 (hh) 53 (mm)

Type: Virus scan

Filename:

Sort by: Scan time ○ Ascending ● Descending

Display: 15 per page

FIGURE 5-11. Log Query screen

Log Maintenance

The Log Maintenance screens enable you to set both manual and automatic options for deleting log histories. This functionality can be useful for saving disk space when it becomes an issue or if the information they provide is no longer useful. PortalProtect lets you delete logs both automatically and manually.

Manually Delete Logs

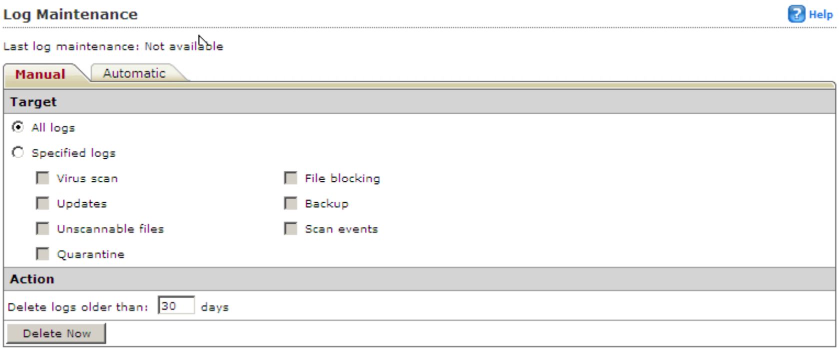
This procedure describes the steps required to manually delete logs for PortalProtect.

To manually delete logs:

1. From the left menu, click **Logs > Maintenance**, and select the **Manual** tab on the **Log Maintenance** screen (*Figure 5-12*).
2. Under the **Target** group, select whether to delete **All logs**, or select **Specified logs** from the following:
   - Virus scan
   - Updates
   - Unscannable files
   - Quarantine
   - File blocking

- Backup
- Scan events

3. Under the **Action** group, type a value in days, in the **Delete logs older than** field. All files will be deleted that are older than the number of days you enter.
4. Click, **Delete Now**.



Log Maintenance

Last log maintenance: Not available

Target

● All logs

○ Specified logs

□ Virus scan □ File blocking

□ Updates □ Backup

□ Unscannable files □ Scan events

□ Quarantine

Action

Delete logs older than: 30 days

FIGURE 5-12. Log Maintenance manual tab

Automatically Delete Logs

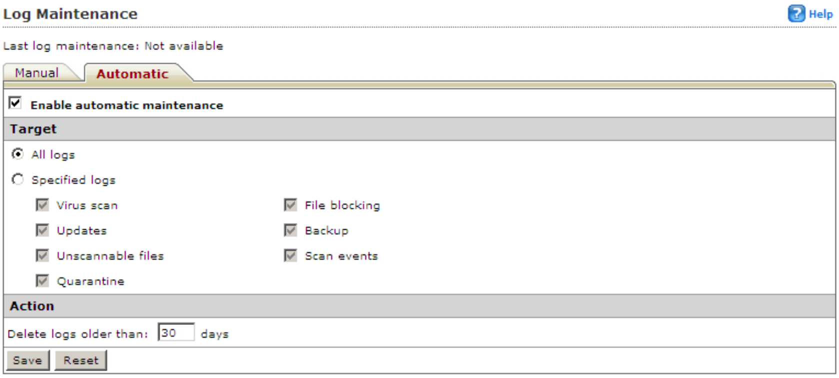
You can configure PortalProtect to automatically delete logs. You can set the number of days and/or the size of the logs that must be exceeded before PortalProtect automatically deletes them. If you only want to set one condition, do not specify a value for the other box.

To automatically delete logs:

1. From the left menu, click **Logs > Maintenance**, and select the **Automatic** tab on the **Log Maintenance** screen (*Figure 5-13*).
2. Select **Enable automatic maintenance**.
3. Under the **Target** group, select whether to delete **All logs**, or select **Specified logs** from the following:
   - Virus scan
   - Updates
   - Unscannable files

- Quarantine
- File blocking
- Backup
- Scan events

4. Under the **Action** group, type a value in days, in the **Delete logs older than** field. All files will be deleted that are older than the number of days you enter.
5. Click **Save.**



Log Maintenance

Last log maintenance: Not available

☑ Enable automatic maintenance

Target

● All logs

○ Specified logs

☑ Virus scan ☑ File blocking

☑ Updates ☑ Backup

☑ Unscannable files ☑ Scan events

☑ Quarantine

Action

Delete logs older than: 30 days

FIGURE 5-13. Log Maintenance automatic tab

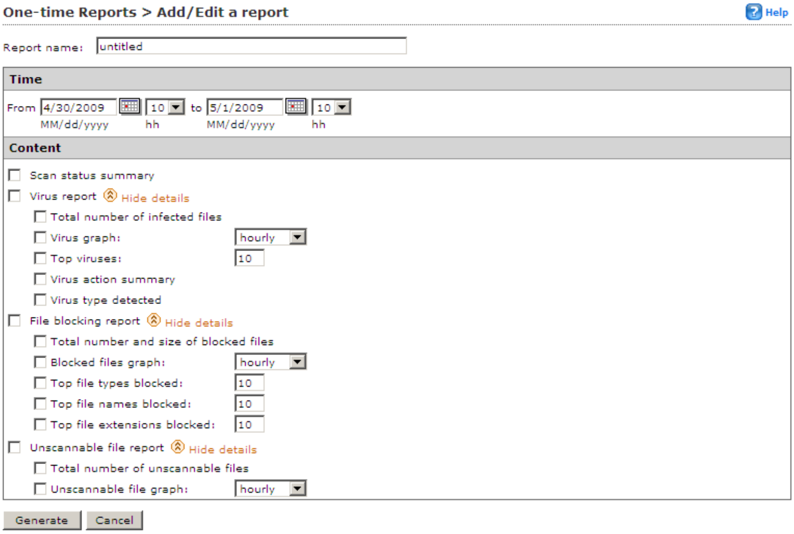
Viewing and Generating Reports

PortalProtect enables you to generate **One-time** or **Scheduled** reports. These reports are created using data from log events. You can view previously generated reports from the Management console.

To generate a one-time report:

1. From the left menu, click **Reports > One-time Reports**. The **One-time Reports** screen appears.
2. From the **One-time Reports screen**, click **Generate report**. The **One-time Reports > Add/Edit a report** screen appears (*Figure 5-14*).
3. In the **Time** group, 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
   - **Virus report**–select to enable and choose from the following:
     - **Total number of infected files**
     - **Virus graph**–from the drop down, choose whether the graph will display, hourly, daily, weekly or monthly data
     - **Top viruses**–type the number of top viruses to display in the report
     - **Virus action summary**–select to display a summary of the action taken on all viruses contained in the report
     - **Virus type detected**–select to display the type of virus detected by PortalProtect
   - **File blocking report**–select to enable and choose from the following:
     - **Total number and size of blocked files**
     - **Blocked files graph**–from the drop down, choose whether the graph will display, hourly, daily, weekly or monthly data
     - **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
   - **Unscannable file report**–select to enable and choose from the following:
     - **Total number of unscannable files**
     - **Unscannable file graph**–from the drop down, choose whether the graph will display, hourly, daily, weekly or monthly data
6. Click **Generate**.



One-time Reports > Add/Edit a report

Report name: untitled

Time

From 4/30/2009 (MM/dd/yyyy) 10 (hh) to 5/1/2009 (MM/dd/yyyy) 10 (hh)

Content

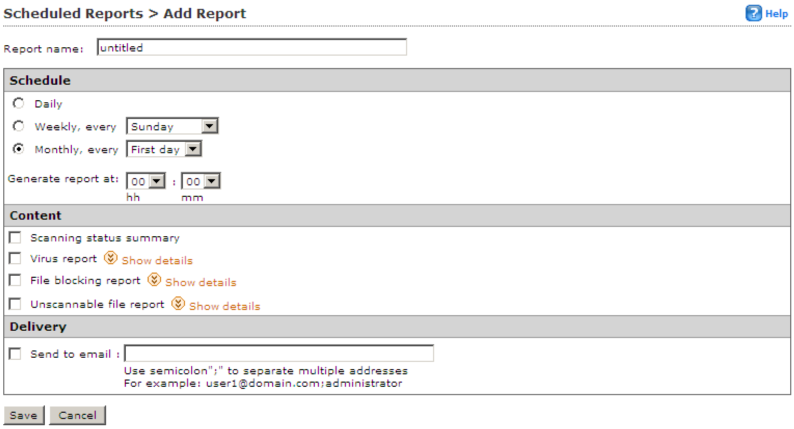
- □ Scan status summary
- □ Virus report — Hide details
  - □ Total number of infected files
  - □ Virus graph: hourly
  - □ Top viruses: 10
  - □ Virus action summary
  - □ Virus type detected
- □ File blocking report — Hide details
  - □ Total number and size of blocked files
  - □ Blocked files graph: hourly
  - □ Top file types blocked: 10
  - □ Top file names blocked: 10
  - □ Top file extensions blocked: 10
- □ Unscannable file report — Hide details
  - □ Total number of unscannable files
  - □ Unscannable file graph: hourly

FIGURE 5-14. Create one-time report screen

To create a scheduled report:

1. From the left menu, click **Reports > Scheduled Reports**. The **Scheduled Reports** screen appears.
2. From the **Scheduled Reports screen**, click **Add**. The **Scheduled Reports > Add Report** screen appears (*Figure 5-15*).
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:
   - **Scan status summary**–displays a summary of the scan status
   - **Virus report**–select to enable and choose from the following:
     - **Total number of infected files**
     - **Virus graph**–from the drop down, choose whether the graph will display, hourly, daily, weekly or monthly data
     - **Top viruses**–type the number of top viruses to display in the report
     - **Virus action summary**–select to display a summary of the action taken on all viruses contained in the report
     - **Virus type detected**–select to display the type of virus detected by PortalProtect
   - **File blocking report**–select to enable and choose from the following:
     - **Total number and size of blocked files**
     - **Blocked files graph**–from the drop down, choose whether the graph will display, hourly, daily, weekly or monthly data
     - **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
   - **Unscannable file report**–select to enable and choose from the following:
     - **Total number of unscannable files**
     - **Unscannable file graph**–from the drop down, choose whether the graph will display, hourly, daily, weekly or monthly data
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 : 00
hh mm

Content

□ Scanning status summary

□ Virus report Show details

□ File blocking report Show details

□ Unscannable file report Show details

Delivery

□ Send to email :

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

FIGURE 5-15. **Create scheduled report screen**

Chapter 6

Getting Support and Contacting Trend Micro

This chapter discusses how to perform miscellaneous administrator tasks as well as how to get technical support.

In this chapter, you will find information about:

- *Contacting Trend Micro* starting on page 6-2
- *Contacting Technical Support* starting on page 6-2
- *TrendLabs* starting on page 6-4
- *Frequently Asked Questions (FAQ)* starting on page 6-5

Contacting Trend Micro

Trend Micro Incorporated has its world headquarters at:

Shinjuku MAYNDS Tower
2-1-1 Yoyogi, Shibuya-ku, Tokyo 151-0053 Japan.

In the United States, Trend Micro is located at:

10101 N. De Anza Blvd.
Cupertino, CA 95014-9985
Tel: +1-408-257-1500
Fax: +1-408-257-2003

Trend Micro has sales and corporate offices located in many cities around the globe. For global contact information, visit the Trend Micro Worldwide site:

`http://www.trendmicro.com/en/about/contact/overview.htm`

Note: The information on this Web site is subject to change without notice.

The Trend Micro Web site has a wealth of sales and corporate information available.

- Corporate information includes our company profile, international business office contacts, and partnering and alliance information.
- Sales information includes product evaluation information and trial downloads, reseller contacts, and virus research information.

Contacting Technical Support

There is an abundance of security information and support available through the Web site. You can find the following:

- Downloadable product upgrades, component updates and hot fix patches
- Security advisories on the latest virus outbreaks
- Downloadable trial versions of Trend Micro products
- Expert advise on specific viruses in the wild and computer security in general
- An encyclopedia of computer security information, white papers, and virus statistics
- Free downloadable software for virus scanning, Web feeds, and security testing

To contact Trend Micro technical support:

1. Visit the following URL:

   `http://kb.trendmicro.com/solutions/`
2. Click the link for the region you want to contact and follow the instructions for contacting support in that region.

You can find Trend Micro contacts in the following regions:

- Asia/Pacific
- Australia and New Zealand
- Latin America
- United States and Canada.

Before Contacting Technical Support

While our basic technical support staff is always pleased to handle your inquiries, there are some things you can do to quickly find the answer you are seeking.

- Check the documentation: the manual and Online Help provide comprehensive information about PortalProtect. Search both documents to see if they contain your solution.

  The documentation set for this product includes the following:

  - Getting Started Guide—This Guide helps you get “up and running” by introducing PortalProtect, assisting with installation planning, implementation, and configuration, and describing the main product functions. It also includes instructions on testing your installation using a harmless test virus. The latest version of the Guide is available in electronic form at:

    http://www.trendmicro.com/download/
  - Online Help—The purpose of Online Help is to provide “how tos” for the main product tasks, usage advice, and field-specific information such as valid parameter ranges and optimal values. Online Help is accessible from the PortalProtect management console.
  - Readme file—The Readme file contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, installation tips, known issues, and release history.
  - Visit Knowledge Base at http://solutionbank.antivirus.com/solutions

This site contains the most up-to-date information about all Trend Micro products. Other inquiries that were already answered are also posted and a dynamic list of the most frequently asked questions is also displayed.

- To speed up your problem resolution, when you contact our staff please provide as much of the following information as you can:
  - Product serial number
  - PortalProtect program, scan engine, pattern file, version number
  - OS name and version
  - Internet connection type
  - Exact text of any error message given
  - Steps to reproduce the problem

TrendLabs

TrendLabs is Trend Micro's global infrastructure of antivirus research and product support centers that provide up-to-the minute security information to Trend Micro customers.

The "virus doctors" at TrendLabs monitor potential security risks around the world, to ensure that Trend Micro products remain secure against emerging threats. The daily culmination of these efforts is shared with customers through frequent virus pattern file updates and scan engine refinements.

TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services. Dedicated service centers and rapid-response teams are located across the world to mitigate virus outbreaks and provide urgent support.

TrendLabs was one of the first antivirus research and support facilities to earn ISO 9002 certification for its quality management procedures. Trend Micro believes TrendLabs is the leading service and support team in the antivirus industry.

Frequently Asked Questions (FAQ)

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

Installation

Where should I install PortalProtect to protect my SharePoint environments?

For SharePoint stand-alone deployment mode: PortalProtect is installed on the stand-alone server itself because the stand-alone server runs the Web application server (service).

For SharePoint farm deployment mode: PortalProtect is installed to servers that are running the Web application servers (services), in other words, the Web front-end servers.

What is the difference between *install to farm* and *install to stand-alone*?

This depends on your SharePoint deployment mode. If SharePoint will be deployed with farm mode, you need to select **install to farm** to install PortalProtect. If SharePoint will be deployed with stand-alone mode (basic deployment), you need to select **install to stand-alone** to install PortalProtect.

When install to stand-alone server is selected, PortalProtect will be installed to the stand-alone SharePoint server without requiring the user to input a SharePoint DB access account because the SharePoint DB is located on the stand-alone server.

How do I handle a password change or expiration of a DB access account?

For PortalProtect deployed with DB access Windows authentication:

a. Open service control.

b. Locate PortalProtect master service.

c. Change the password for the service logon account and restart the service.

For PortalProtect deployed with DB access SQL authentication:

a. Open the Registry and locate:
HKLM\...\PortalProtect\CurrentVersion\SharePointDBAccessPassword

b. Change the password and restart PortalProtect Master service.

How to install PortalProtect in Cluster environment?

PortalProtect 1.8 does not fully support the cluster environment. When installing to a cluster server, you can only install to one server IP in the cluster at a time.

Sometimes, PortalProtect doesn't start. Why?

Check the following:

- The SharePoint database access account should have at least local administrator privilege.
- SQL PortalProtect instance exists and is running
- SQL PortalProtect instance service startup account should be: **LocalSystem**
- The `%PPRoot%\Data` folder should contain three (3) ***.mdf*** files and three (3) ***.ldf*** files. Do NOT delete these files, and make sure they have been loaded by the SQL Server.
- The registry key: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PortalProtect\CurrentVersion should exist. The value **HomeDir** should point to `%PPRoot%`.
- The virtual IIS PortalProtect Web site should exist.

I can't logon the PortalProtect Management Console after installation. Why?

Check as following:

a. Open **Control Panel > Administrative Tools > Internet Information Services (IIS) Manager**

b. Make sure the PortalProtect virtual site and virtual directories exist.

c. Make sure the IIS site is running.

d. Make sure the IIS site properties are properly configured, and can be accessed by your browser.

e. Make sure the PortalProtect master service is running.

f. Make sure the logon account is a local administrator or is a member of the Management Group; this is the PortalProtect Management Group selected during installation.

g. Make sure JRE (Java Sun edition) is installed and enabled.

Scanning

PortalProtect shows file “x.xxx” contains the following virus: “It has been blocked; final action is:[Quarantined]." However, this file does not contain a virus. Why does the message tell me the file contains a virus?

Microsoft SharePoint Services provides this format and Trend Micro modifies the content within the quotation marks. Therefore, when the file is blocked by PortalProtect file blocking 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.

Quarantine and backup are not working on my server. Why?

Check the security attributes of Quarantine Folder and Backup Folder. Ensure that Portal Protect service’s owner can access and write the folders.

I have not enabled “file blocking," but some files are never uploaded or downloaded. Why?

Check SharePoint Services block list settings. SharePoint Server blocks files with the suffixes you specified. Use the SharePoint Services Central Management Page to modify the configuration.

To remove the file blocking configuration from SharePoint Services:

1. Select the **Operations** tab.
2. Select **Blocked file types** from Security Configuration.
3. Check the extension names listed in the dialog box. Any extension name that is included will be blocked by SharePoint Services when it is uploaded or downloaded.

When I upload file containing a virus to SharePoint Services, PortalProtect does not detect it. Why?

Check the following:

- Check the SharePoint Services antivirus settings:
  a. Go to the SharePoint Central Administration page.
  b. Select the **Operations** tab.
  c. Select **Configure antivirus settings** in Security Configuration.
  d. If **Scan documents on upload** is disabled, PortalProtect will not perform a scan when the file is uploaded.

e. If **Scan documents on download** is disabled, SharePoint Services will not pass the file to PortalProtect when the file is downloaded.

f. If **Attempt to clean infected documents** is disabled, PortalProtect will only scan the file, and will not clean the file if it is infected by a virus.

Then, check the PortalProtect real-time virus scan options:

a. Log on the PortalProtect Web console and select **Virus Scan** from the left menu.

b. Select **Enable real-time virus scan**.

What will PortalProtect do if I set PortalProtect to block *.doc* files in file blocking and then, upload a *.doc* file that contains virus?

Files that satisfy both file blocking and virus scan, PortalProtect will execute file blocking actions before a virus scan. For real-time scan, since the file blocking action includes **block** and **quarantine**, the file will not trigger a virus scan. For manual scan and scheduled scan, the action includes **delete**, **quarantine**, and **pass**. If the manual scan file blocking action is **pass**, the file will trigger a virus scan and be scanned by PortalProtect again.

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? For example: the primary action is *quarantine*, and the secondary action is *clean*. Will PortalProtect clean files in the quarantine folder?

Yes. The secondary action is executed only when the primary action fails. You can select a secondary action only when the primary action is **clean**. Trend Micro considers that only a **clean** action will be unsuccessful.

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 Portal Protect 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. See *Renewing Your Maintenance Agreement* on page 3-4.

An infected file was found during real-time scanning, but I cannot find the author and location information in the report or the virus log. Why?

The Microsoft SharePoint Server does not provide that information after a real-time scan service is triggered for PortalProtect.

Both Microsoft SharePoint 2007 and Trend PortalProtect 1.8 have a file blocking / filtering features. Which one should I configure?

If you configure SharePoint 2007 file blocking/filtering, then PortalProtect records no block log. Trend Micro recommends enabling the PortalProtect blocking.

Active Update

Why was the update unsuccessful from the Automatic Update server?

If your system requires a proxy to connect to Internet, check to ensure the settings are correct.

Does ActiveUpdate deliver the virus pattern file and the scan engine in the same way?

Yes. In fact, PortalProtect does not care about how ActiveUpdate downloads these files. PortalProtect sends the current engine/pattern version to ActiveUpdate module, ActiveUpdate checks if there is any more recent version available. It then downloads the files (in zip format), and unzips them automatically after a successful download. Finally, PortalProtect loads the new engine/pattern to use.

When PortalProtect uses an intranet source to receive updates, how is the central location updated?

ActiveUpdate supports downloading the latest components from an intranet machine. Put the update packages on that machine and enable the folder to be shared for other intranet machines to download.

How does the component package get updated?

After a successful download, ActiveUpdate extracts the packages and notifies PortalProtect to load new modules.

How do I update the engine or pattern using another PortalProtect server's component package source?

Choose **Updates > Download Source** and select **Other Update Source,** then type the following URL:

http://<SERVERNAME>:<PORTNUMBER>/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 different between the alert "PortalProtect service did not start successfully" and "PortalProtect service is unavailable?"

- **PortalProtect service did not start successfully:** occurs after an unsuccessful attempt to start the Trend Micro PortalProtect for Microsoft SharePoint Master Service.
- **PortalProtect service is unavailable:** occurs if the PortalProtect main service is already started and stops suddenly.

Why can I receive SNMP alerts but no email alerts?

PortalProtect 1.8 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 cannot access the Web console. My browser displays a 404 error. What can I do to fix this problem?

Internet Explorer security settings on Windows 2003 does not include localhost or hostname as a trusted site when security level is set to **high**. Please add 127.0.0.1 or hostname to the list to solve this problem (http://127.0.0.1:16372).

1. Open Internet Explorer
2. Click **Tools > Internet Options** and select the Security tab.
3. Click **Trusted Sites** > **Sites.**

4. In the field for trusted zones, type the IP address: 127.0.0.1 or hostname.
5. Click **Add**.

I can access the PortalProtect Web console from the local server, but I cannot access it from a remote machine. Why?

Check the following:

- Whether there are network firewalls that block access to the PortalProtect Web Console through the HTTP (default is 16372) or HTTPS (default is 16373) port you specified during installation.
- Whether the Windows firewall on the PortalProtect server blocks the HTTP (default is 16372) or HTTPS (default is 16373) port you specified during installation.

Internet Explorer shuts down with a *Data Execution Prevention alert* when accessing the PortalProtect management console. What can I do to fix this problem?

- Select **Tools > Internet Options > Advanced tab**. Scroll to Security, and clear the checkbox **Enable memory protection to help mitigate online attacks**.

Which folders should I exclude for other Trend Micro Products?

The following four (4) folders should be excluded for other Trend Micro products:

- Quarantine folder
- Backup folder
- Temp folder
- Sharedrespool folder

You can change the location of the Quarantine and Backup folders. The following indicates the default locations:

- Default Backup folder:

  ```
  Drive:\Program Files\Trend
  Micro\PortalProtect\storage\backup
  ```

- Default Quarantine folder:

  ```
  Drive:\Program Files\Trend
  Micro\PortalProtect\storage\quarantine
  ```

- Temp folder:

```
Drive:\Program Files\Trend
Micro\PortalProtect\Temp
```

- Sharedrespool folder:

```
Drive:\Program Files\Trend
Micro\PortalProtect\SharedResPool
```

I cannot open the PortalProtect management console with Firefox. Why?

This is a known bug in JRE, which will not automatically register to a 64-bit Windows OS. This causes **JVM not found** when an attempt is made to open the PortalProtect management console. Additionally, JRE 6 next-generation Java plug-in has compatibility issues with Firefox, which causes the Java plug-in to crash when loaded by Firefox.

a. Install JRE 6 u12 or above.

b. For 64-bit Windows, add `"%JAVAHOME%\jre\bin"` as a path variable for system environment variables.

c. From the Java Control Panel, select the **Advanced** tab, and clear the **Enable the next-generation Java Plug-in** checkbox.

How does PortalProtect read a file to know if it has an extension?

When a user uploads a file to SharePoint Server 2007, SharePoint Server 2007 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.

Appendix A

Using Control Manager with PortalProtect

Trend Micro Control Manager™ is a centralized system that unites Trend Micro antivirus products and services into a cohesive virus security and content management solution.

This chapter discusses the following topics:

Introducing Control Manager

Trend Micro Control Manager is a central management console that manages Trend Micro and third-party antivirus and content security products and services at the gateway, mail server, file server, and corporate desktop levels. The Control Manager Web-based management console provides a single monitoring point for antivirus and content security products and services throughout the network.

Control Manager is available in Standard and Enterprise editions to better satisfy the needs of different enterprises.

- The Standard edition provides powerful management and configuration features that allow you to manage your corporate antivirus and content security.
- The Enterprise edition is for large enterprises and xSPs. This edition adds a variety of advanced features to the Standard edition—such as cascading console support and reporting functions.

Key Features

Key features of Control Manager include:

- Centralized management, which allows administrators to configure, monitor, and maintain Trend Micro software installed on the network from a single console—regardless of location or platform
- Flexible and scalable configuration, which simplifies the administration of a corporate virus and content security policy.
- A hierarchical structure for job delegation so administrators can determine access control—different users can be assigned separate access to individual branches of the hierarchy.
- Outbreak Prevention Services that provides proactive attack protection service and blocks malicious code by file name or specific file details while new pattern files are being developed that can detect and clean the new threat.
- Vulnerability Assessment, a service that assesses network security risk and scans for system vulnerabilities that are associated with known virus and malware attacks and recommends actions to take to eliminate the vulnerabilities.

- Agent-free Damage Cleanup Services (DCS), a comprehensive cleaning service that offers infection assessment and system repair for malicious remnants, such as Worms and Trojans. The service provides system administrators an easy approach for system cleaning without the use of any software locally installed on the client machines.

Using Control Manager with PortalProtect

Control Manager is a useful tool for organizations with multiple PortalProtect servers or for organizations using other Trend Micro products in addition to PortalProtect. The main advantages of using Control Manager with PortalProtect are:

- Centralized virus logging
- Powerful reporting and analysis options
- Faster response to virus outbreak prevention using Outbreak Prevention Services
- Centralized license management console
- Centralized distribution of components

Introducing the Control Manager Management Communication Protocol

The communication between PortalProtect and the Control Manager uses a new protocol called the Trend Micro Control Manager Management Communication Protocol (MCP). PortalProtect no longer supports the Trend Micro Management Infrastructure (TMI) protocol used by previous versions of PortalProtect and the Control Manager.

The Control Manager Agent can be registered after installing PortalProtect. PortalProtect supports single sign-on from the Control Manager. Access the PortalProtect product console directly from the Control Manager product console without typing a separate user name and password for the PortalProtect product console.

Introducing Outbreak Prevention Services

The Outbreak Prevention phase is the critical period when managed products have identified a virus outbreak and a pattern file is not yet available. During this crucial time, system administrators must endure a chaotic, time-consuming process of communication—often to global and decentralized groups within their organizations.

Outbreak Prevention Services delivers notification of new threats and continuous and comprehensive updates on system status as an attack progresses. The timely delivery of detailed virus data coupled with predefined, threat-specific action and scanning policies delivered immediately after a new threat identification allows enterprises to quickly contain viruses and prevent them from spreading.

Additionally, by centrally deploying and managing policy recommendations, Outbreak Prevention Services helps eliminate the potential for miscommunication, applies policies, and deploys information regarding attacks as they are occurring.

By providing automatic or manual download and deployment of policies via Trend Micro Control Manager, Outbreak Prevention Services import knowledge to critical access points on the network directly from experts at TrendLabs, Trend Micro's global security research and support network.

This subscription-based service requires minimal up-front investment and provides enterprise-wide coordination and outbreak management via Trend Micro products, which reside across critical points on the network including the Internet gateway, mail server, file server, caching server, client, remote and broadband user, and third-party enterprise firewalls.

Using Control Manager to Administer PortalProtect

Access the Control Manager management console to configure the PortalProtect managed product from any computer on the network.

Accessing the Control Manager Management Console

There are two ways to access the management console:

- Locally on the Control Manager server
- Remotely using any compatible browser

To access the management console locally from the Control Manager server:

1. Click **Start** > **Programs** > **Trend Micro Control Manager** > **Trend Micro Control Manager**.
2. Provide the **Username** and **Password** in the fields provided.
3. Click **Enter**.

To access the console remotely:

1. Type the following at your browser's address field to open the sign in page:

   ```
   For TMCM 3.5-https://{host name}/ControlManager
   ```

   ```
   For TMCM 5.0-https://{host name}/webapp/login.aspx
   ```

   where `{host name}` is the Control Manager server's fully qualified domain name (FQDN), IP address, or server name.
2. Type the **Username** and **Password** in the fields provided.
3. Click **Enter**.

Managing PortalProtect from the Control Manager Management Console

The Control Manager management console is a Web-based console that lets you use a compatible Web browser to administer the Control Manager network from any machine. For the list of compatible browsers, refer to the Control Manager Getting Started Guide or Online Help.

The Control Manager agent for PortalProtect accepts commands from the Control Manager server and instructs PortalProtect to perform them. For example, when you select **Tasks** > **Deploy scan engine** on the Control Manager management console, the Control Manager agent instructs PortalProtect to deploy the latest scan engine.

To manage PortalProtect from the management console:

1. Access the Control Manager management console.
2. From the main menu, click **Products**.
3. Under Product Directory, expand the PortalProtect folder to perform the following:

To check PortalProtect status:

1. From the working area, click **Status**, to update the currently displayed status.

   The Product Status screen displays the **Product Information**, **Component Status**, **Operating System Information**, **Agent Environment Information**, and **Product License Information**.

Viewing an Active Outbreak Prevention Policy

To view an active Outbreak Prevention Policy:

- Through the Control Manager management console > **Services** page
  - **a.** Access the Control Manager management console.
  - **b.** Click **Services** on the main menu.
  - **c.** From the left menu under Services, click **Outbreak Prevention**.

  This page automatically refreshes to ensure that the top threat and status information is current.

Appendix B

How to Configure PortalProtect to Use an External SQL Server Database

Terminologies

- PortalProtect (Trend Micro PortalProtect for Microsoft SharePoint)
- SQL Server instance (a SQL Server 2005 or 2008 instance)
- PortalProtect Server (The Server that installed PortalProtect)
- Database Server (The Server that installed SQL Server instance, and PortalProtect will use as external SQL server database)

Prerequisites

- An installed and configured SQL Server 2005 (or SQL Server 2008) instance.
- Enable the remote access for this SQL Server instance.
- Enable the SQL authentication on that SQL server instance and having a valid SQL authentication account.

Procedure

1. Stop the following services:
   - TrendMicro PortalProtect for Microsoft SharePoint Master Service
   - Trend Micro PortalProtect for Microsoft SharePoint System Watcher
2. Detach the PortalProtect databases by executing the following statements:
   - sqlcmd -S .\PortalProtect -E -Q "sp_detach_db [PPConf_SERVERNAME]"
   - sqlcmd -S .\PortalProtect -E -Q "sp_detach_db [PPLog_SERVERNAME]"
   - sqlcmd -S .\PortalProtect -E -Q "sp_detach_db [PPReport_SERVERNAME]"

   Note: Replace SERVERNAME with your local host name where PortalProtect is installed.

3. Stop the SQL Server (PortalProtect) service.
4. Backup following folders:
   - %PP_INSTALL_PATH%\config
   - % PP_INSTALL_PATH%\data

   Note: Replace %PP_INSTALL_PATH% to the actual PortalProtect install path.

5. Modify the PortalProtect database profiles.

   Open the following files with Notepad or another text editor:
   - %PP_INSTALL_PATH%\config\dbconf_Conf.xml
   - %PP_INSTALL_PATH%\config\dbconf_Log.xml
   - %PP_INSTALL_PATH%\config\dbconf_Report.xml

   Locate the following strings and replace with your remote SQL servers settings.

   Find this string:
   - <connect_string for="operate">Provider=SQLOLEDB.1;Integrated Security=SSPI;Connect Timeout=180;Persist Security Info=False;Initial Catalog=&DATABASE_NAME;;Data Source=&DATABASE_HOST;;Initial File Name=&DATABASE_FILE;</connect_string>

...and replace with:

<connect_string for="operate">Provider=SQLOLEDB.1;Connect Timeout=180;Initial Catalog=&DATABASE_NAME;;Data Source=&DATABASE_HOST;;Persist Security Info=True;User ID=ppuser;Password=pppassword;</connect_string>

Find this string:

<connect_string for="install">Provider=SQLOLEDB.1;Integrated Security=SSPI;Connect Timeout=180;Persist Security Info=False;Initial Catalog=master;Data Source=&DATABASE_HOST;</connect_string>

...and replace with:

<connect_string for="install">Provider=SQLOLEDB.1;Connect Timeout=180;Initial Catalog=master;Data Source=&DATABASE_HOST;;Persist Security Info=True;User ID=ppuser;Password=pppassword;</connect_string>

Open the following files with Notepad or another text editor:

- %PP_INSTALL_PATH%\config\dbDatabaseCreation.js

  Locate the following strings and replace with your remote SQL servers settings.

  Find this string:

  conn.Open("Provider=SQLOLEDB.1;Integrated Security=SSPI;Persist Security Info=False;Initial Catalog=master;Data Source=" + this.Host);

  ...and replace with:

  conn.Open("Provider=SQLOLEDB.1;Connect Timeout=180;Initial Catalog=master;User ID=ppuser;Password=pppassword;Data Source=" + this.Host);

Note: Replace “ppuser” with your SQL authentication account and “pppassword” with the password for that account.

The stored password is clear text and there is possibility of password disclosure. Carefully configure your account and avoid using “sa”

This account requires a System Administrators role during installation.

- Open %PP_INSTALL_PATH%\config\dbcfg_DatabaseInstance.txt and replace the remote SQL server instance with the following:

  server_name\instance_name

  or...

  server_name

  For example:

  SVR-SQL2005\SQLEXPRESS

  or...

  SVR-SQL2005
- Open % PP_INSTALL_PATH%\config\dbcfg_InstallPath.txt and replace with the desired path to install the databases on that remote server. Please make sure the folder was manually created on that remote SQL server.

  For example:

  C:\PP_DATA

6. Install databases to a remote server instance.

Run the following command from the command line and change the current installation path with the default path (C:\Program Files\Trend Micro\PortalProtect\):

```
C:

cd "c:\program files\Trend Micro\ PortalProtect\config"

CScript //E:JavaScript //NoLogo dbDatabaseCreation.js dbconf_Conf.xml create

CScript //E:JavaScript //NoLogo dbDatabaseCreation.js dbconf_Log.xml create

CScript //E:JavaScript //NoLogo dbDatabaseCreation.js dbconf_Report.xml create
```

Note: For SQL EXPRESS Server...

Ensure the SQL Server Browser service is started with the startup type set to automatic.

Ensure the SQL Server Remote Connection is enabled.

For more information, refer to to this topic in the knowledge base:

http://support.microsoft.com/kb/914277

7. Start the following services:
   - Trend Micro PortalProtect for Microsoft SharePoint Master Service
   - Trend Micro PortalProtect for Microsoft SharePoint System Watcher
8. To test the result, log on the PortalProtect Web console and click the virus scan page. A succesful result diplays the page without errors.

Optional Procedure

1. Remove the dependency between PortalProtect Master service and SQL Server (PortalProtect) service.

   Run the following command from the command line:
   - SC config PortalProtect_Master depend= /
2. Uninstall SQL Server 2005 Express (PortalProtect) instance.

Index