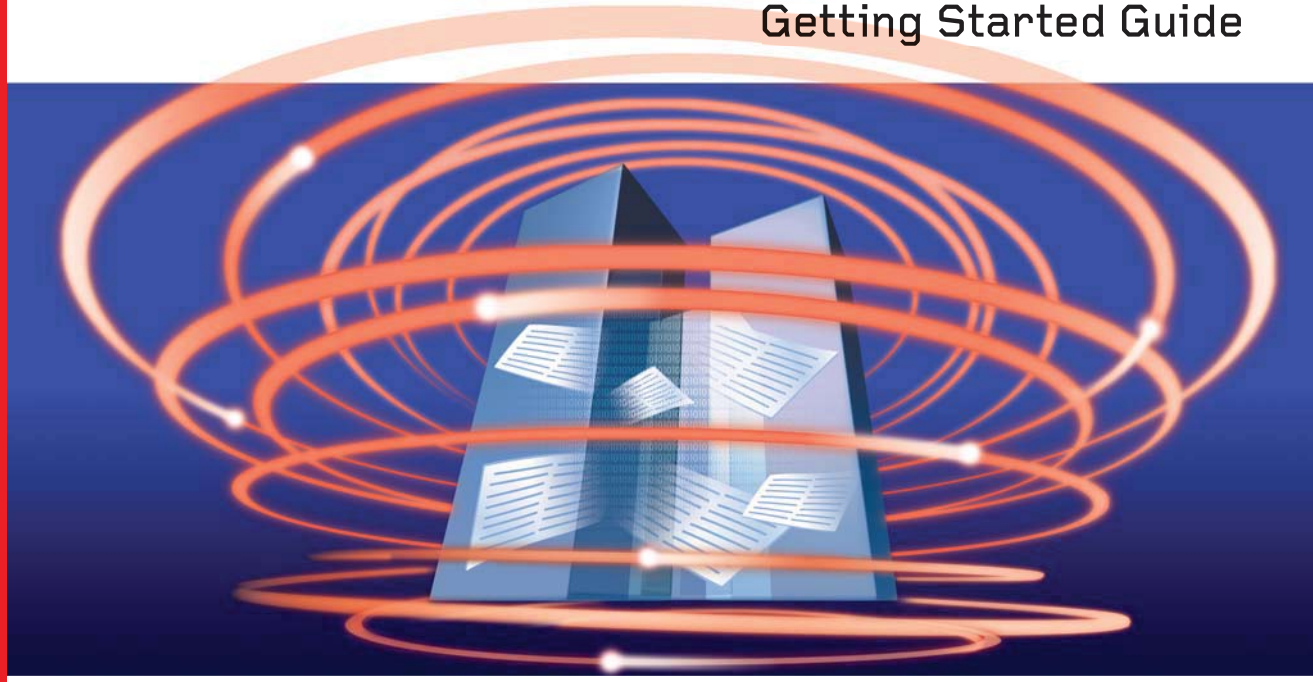
TREND MICRO™
PortalProtect™ 1.7

Getting Started Guide



TREND MICRO™

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.

This product includes software developed by the following third parties:

- OpenSSL Project, copyright (c) 1998-2005. All rights reserved.
- Jean-loup Gailly and Mark Adler, copyright (c) 1995-2004.
  `http://www.gzip.org/zlib/zlib_license.html`
- Apache Software Foundation. Copyright (c) 2004. All rights reserved.
  `http://www.apache.org/licenses/LICENSE-2.0`

Document Part No. PPEM11964/40719

Release Date: May, 2007

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 prior to 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™

Trend Micro PortalProtect™ is a server-based security solution for Microsoft Windows™ SharePoint™ Services, including Microsoft™ SharePoint™ Portal 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 is "checked-in", "checked-out" or published to a SharePoint Portal 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 such tasks as sending notifications, generating reports, and making log queries. Automated notification features such as 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 Portal environments and how PortalProtect protects against these threats.

PortalProtect 1.7 integrates with Trend Micro Control Manager 3.0/3.5 with support for the following services:

- Group policy replication
- Centralized pattern file and scan engine deployment and updating
- Configuration replication
- Outbreak Prevention Service deployment
- Remote agent installation

In this chapter, you will find information about:

What's New in PortalProtect 1.7

- Supports Windows SharePoint Services v3, Office SharePoint 2007
- Supports x86 and x64 OS
- Silent Installation

Note: PortalProtect 1.7 protects Web applications upgraded from SharePoint Server 2003 to SharePoint Server 2007. PortalProtect 1.7 does not protect Web applications that are not upgraded to SharePoint Server 2007.

Benefits and Capabilities

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

- Supports Microsoft SharePoint Portal Server 2007 for secure enterprise information portal environments
- Provides manual and scheduled scans of the SharePoint Portal 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 type" regardless of false extension types
- 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 of a certain type
- 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 Portal Environments

As an organization creates and collects information, people spend increasing amounts of time searching, organizing, and managing that information. SharePoint Portal Server combines the ability to quickly create corporate Web portals with search functions, document management features, and collaboration options. Although SharePoint Portal Server make it possible to easily share information among users regardless of their physical location, it also provides an environment

where viruses and malicious programs such as Trojans and worms can thrive and cause damage.

How PortalProtect Protects SharePoint Portal Servers

PortalProtect guards both SharePoint Portal Server 2007 and SharePoint Services in a number of ways. Scanning and blocking content is the central function. You can configure PortalProtect to take actions whenever it blocks a file or detects a virus. Furthermore, you can have PortalProtect send notifications of these events to administrators or other recipients.

- PortalProtect can block files based on the file extension, specific file name, or true file type. When it detects a file type, it takes an action such as "quarantine" or "delete" as preconfigured by the administrator.
- Scanning employs the latest version of the Trend Micro scan engine to detect viruses and other malicious code. When it detects a virus or malicious code PortalProtect performs a number of actions, such as "delete" or "quarantine", 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 such as component updates and scan actions. You can query these events to create log reports providing 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–PortalProtect performs a scan in real time on the file, whenever a file is "checked in", "checked out", saved or retrieved (when you have enabled SharePoint Services antivirus features). It scans all incoming or outgoing files for viruses or other malicious code. The scan engine has the capacity to maintain multiple threads, thus processing many requests simultaneously.

Manual Scan (Scan Now)–Manual Scan occurs momentarily after you start it and it scans all or some of the files in your Document Library, depending on how you configured it. You can configure the 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 how you have configured it. 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 Portal environments. When you configure and perform a manual scan, it removes the threats to the content stored on the SQL Server content store. When you configure and enable real-time scanning, it protects your SharePoint Portal servers from new threats as they arise. Finally, running regularly scheduled scans maintains a secure SharePoint Portal environment.

PortalProtect Architecture

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

At the center of the PortalProtect security solutions is the Trend Micro patented scan engine. The scan engine integrates with the SharePoint Services Antivirus Manager (AVM). During real-time scanning, the Antivirus Manager calls the Trend Micro scan engine whenever it "checks-in", "checks-out" or publishes content to a SharePoint Portal 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 Portal's SQL database. To prevent redundant scanning, it stores scan results in the SQL store and makes them available to PortalProtect during subsequent scanning.

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

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

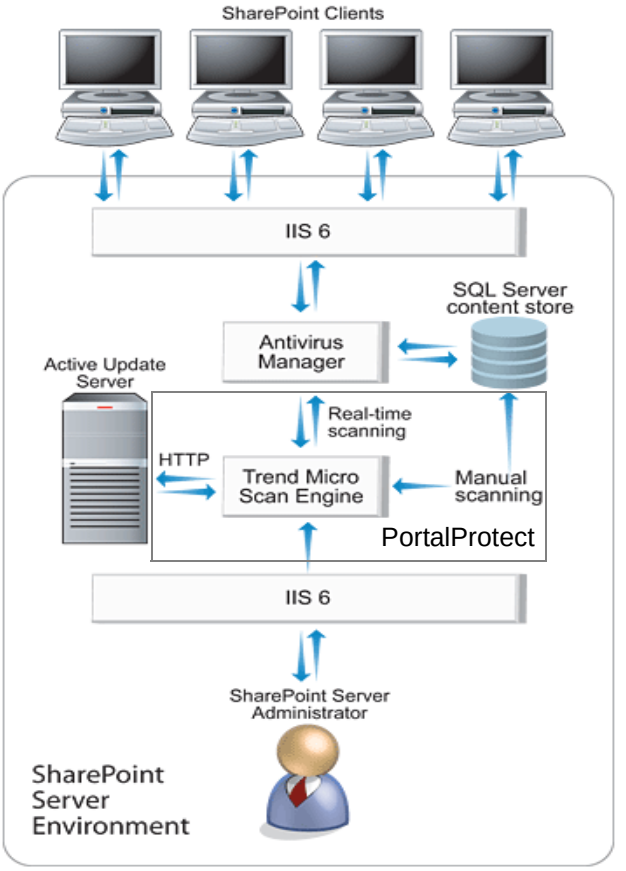


FIGURE 1-1. How PortalProtect interacts with SharePoint Portal Server and SharePoint Services

Controlling Outbreaks

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

- Use PortalProtect notifications to create an early warning for your administrator or IT professionals.

  See *Configuring Outbreak Alert* on page 5-3.

- 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 such as "block" or "quarantine" for PortalProtect to take action on that file type or 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 PortalProtect and remove PortalProtect and lists the minimum system requirements. It also provides information about basic upgrading issues and advice about some 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

You need the following to effectively run PortalProtect 1.7:

- Dual-processor (34-bit or 64-bit) server with a processing speed of 2.5 gigahertz (GHz) (3 GHz or higher recommended)
- 1 GB RAM (2 GB recommended)
- Microsoft Windows Server 2003 Standard Edition or Windows Server 2003 Enterprise Edition
- Microsoft Office SharePoint Server 2007 or Microsoft SharePoint service 3.0
- Microsoft™ Internet Explorer 6.0 (or above) for Web-based management
- Microsoft™ Internet Information Services (IIS) 6.0

You need the following to effectively run the CM agent:

- PortalProtect 1.7
- CM server 3.0 with SP6 or CM server 3.5 with patch 2

Note: The "Display enhanced security configuration dialog" must be enabled on Internet Explorer to access the PortalProtect console. You should add "http://127.0.0.1" to the trusted site else some pages on the PortalProtect console may not be displayed properly.

Note: You need to create at least one Web application on SharePoint to start the PPSrv.exe service.

Note: You need to use the Microsoft JVM to load the CM console (scheduler) properly.

Preparing for Installation

To help you deploy PortalProtect to your network smoothly, consider the following:

- You must install PortalProtect 1.7 on a server on which you have installed Microsoft Office SharePoint Server 2007 or Microsoft SharePoint Services 3.0

and Windows 2003. Microsoft™ Internet Information Services (IIS) is a required component for a successful installation.

- **Registration Key/Activation Code**. During installation, the setup program prompts you to type an Activation Code. You can use the Registration Key that came with PortalProtect to obtain an Activation Code online from the Trend Micro website. The setup program provides a link to the Trend Micro Web site. If you are unable to activate your product during registration, you can do so later. However, until you activate, PortalProtect will only provide a limited service. See *Registering PortalProtect* on page 3-6.
- **Proxy information**. During installation, the setup program prompts you to enter proxy information. If a proxy server handles Internet traffic on your network, you must type the proxy server information and your user name and password to be able to receive virus pattern file and scan engine updates. If you leave the proxy information blank during installation, you can configure it later using the Administration menu. See *Configuring proxy settings* on page 3-6.
- **Console password**. To prevent unauthorized access to the PortalProtect Web console, specify a password that will be required of anyone who tries to open the console. See *Logging On and Off* on page 3-3.

Note: PortalProtect 1.7 does not support upgrade.

Installing PortalProtect

You can install PortalProtect in two ways:

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

Setup.exe Installation

A simple, user-friendly installation Setup program performs both local and remote installation. The Setup program allows you to easily install PortalProtect on one or many servers. This intuitive program lets you rapidly deploy PortalProtect to all the SharePoint Portal servers in your enterprise.

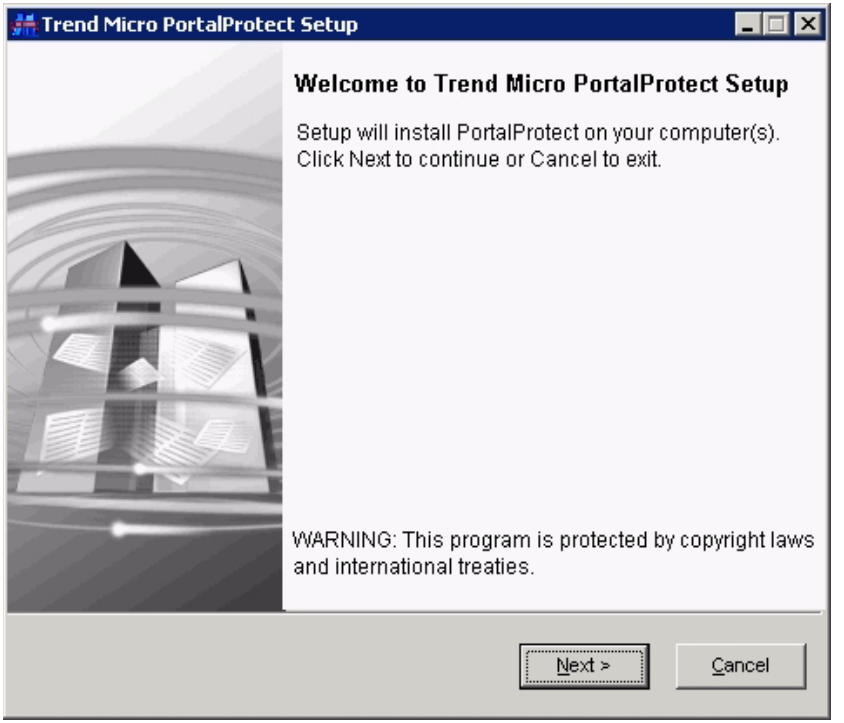
The target servers must be part of your network and you must have access to them with a user account that has administrator privileges.

Note: You must install PortalProtect on a server on which you have installed Microsoft Office SharePoint Server 2007 or Microsoft SharePoint service 3.0 and Windows Server 2003. A successful installation also requires IIS 6.0 and Internet Explorer 6.0.

Note: PortalProtect 1.7 doesn't work with SharePoint Server 2003 and SharePoint Services 2.0. PortalProtect 1.7 is compatible only with SharePoint Server 2007 and SharePoint Services 3.0.

To install PortalProtect on a local server:

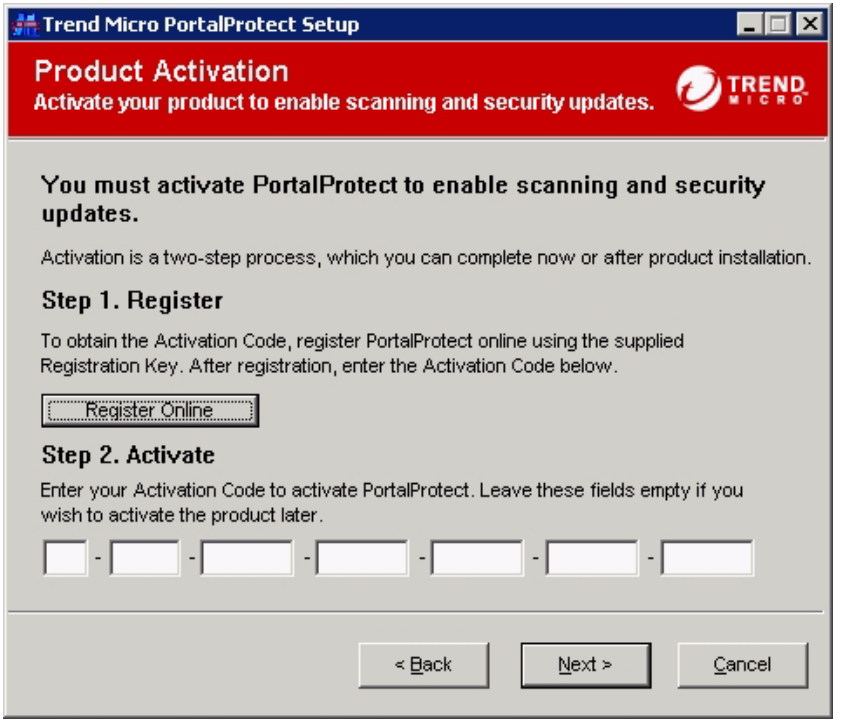
1. Run `setup.exe` from the PortalProtect 1.7 CD to start the installation. The **Welcome to Trend Micro PortalProtect Setup** screen displays.



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

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 **Product Activation** screen displays.



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 in the provided fields and click **Next** to proceed with the installation.

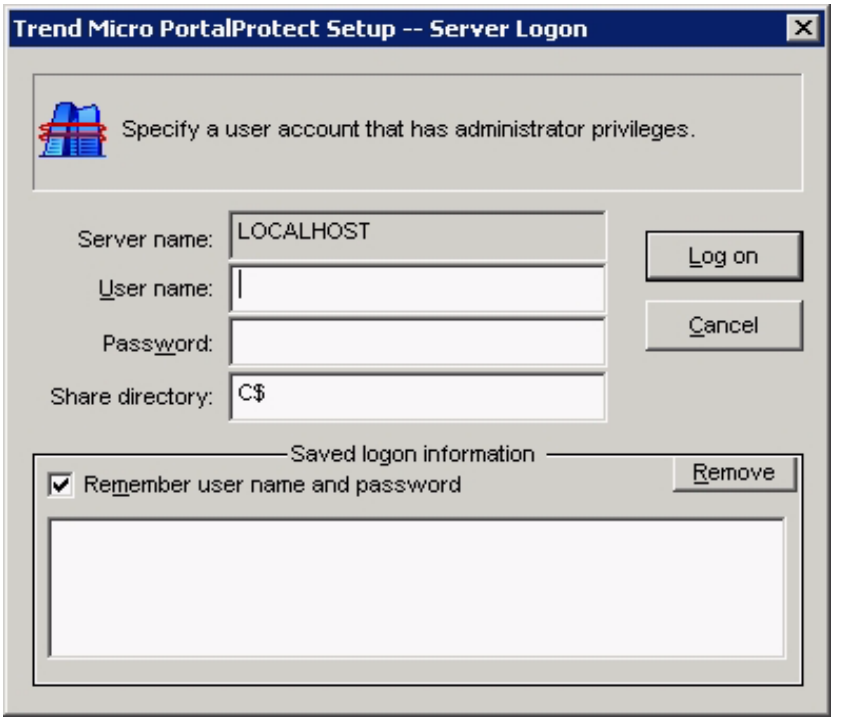
4. The **World Virus Tracking Program** screen appears.

Select **Yes** or **No** and click **Next** to proceed.

5. The **Target Server(s)** screen appears.

Use this screen to choose the target servers to which you want to install PortalProtect. You can type the name of the server or select one or more servers from the list on the left. When you are satisfied with the list of target servers that displays in the **Install on these servers** list, click **Next** to accept the server targets and proceed with the installation.

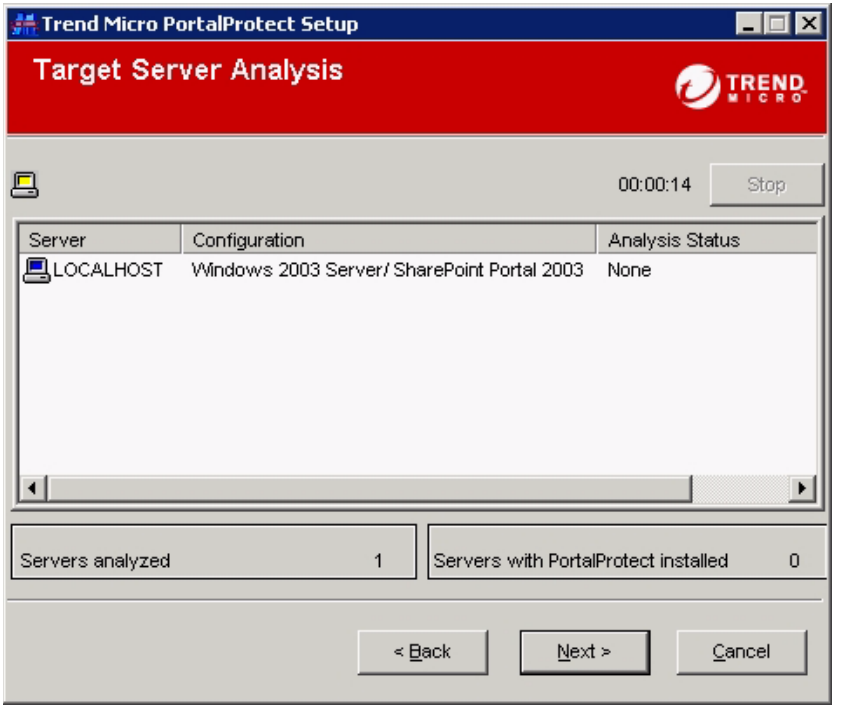
6. The target **Server Logon** screen appears.



The setup program requests that you input a user name and password to connect to a target server. When you have typed the user name and password for this server, the setup program requests you input the user name and password for the next server and so on until you have typed all the user names and passwords for all the servers.

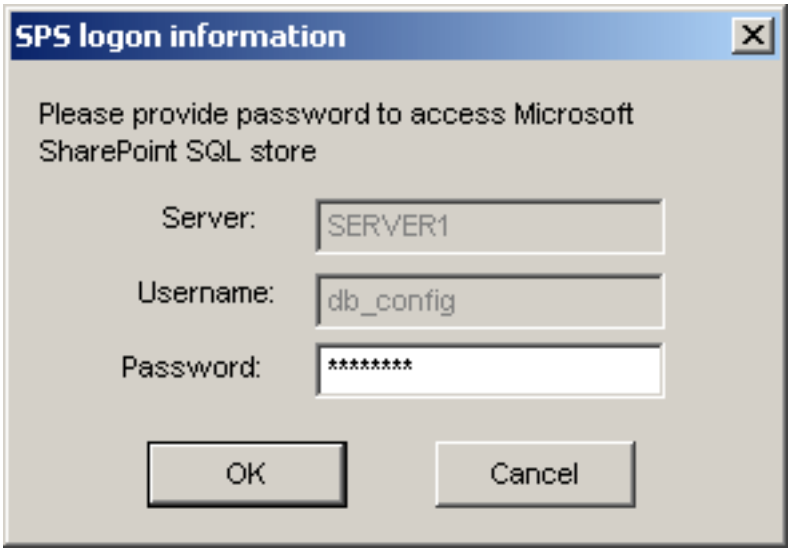
Tip: If you used the same account to log on to multiple servers, make sure the **Remember user name...** check box is selected. This prevents you from having to enter the same logon credentials for each server.

7. The **Target Server Analysis** screen appears and displays all of the target servers and the status of the analysis.



This status report is an in-progress report that shows you each step of the analysis. The setup program disables the navigation buttons while it is analyzing the servers and you must wait until the analysis is complete to continue the installation. When the analysis is complete for all the servers, click **Next** to proceed with the install. If you want to return to the **Target Server(s)** screen to add or remove more servers, click **Back**.

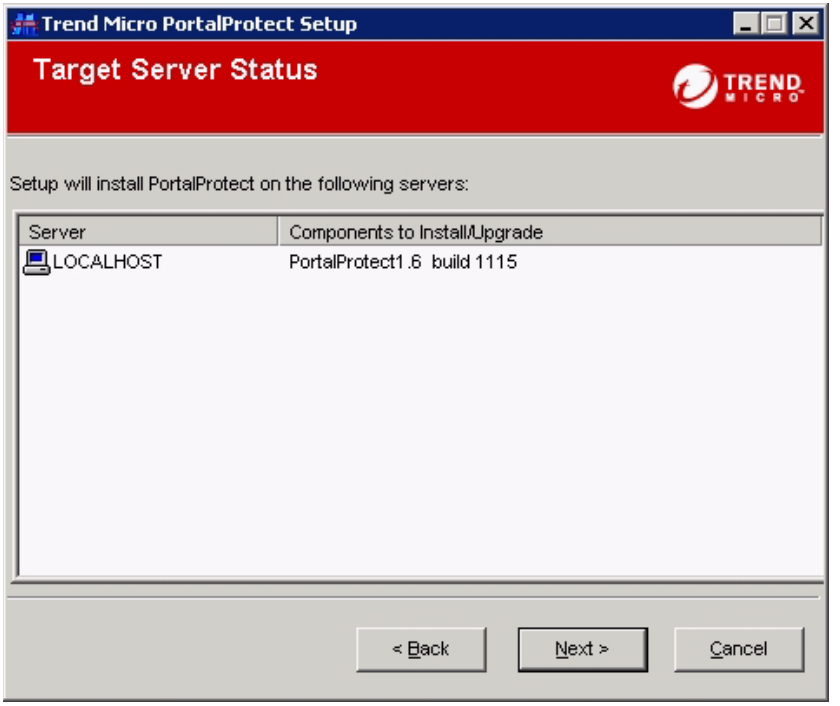
8. The SQL Server logon screen appears.



When a SQL Server has been installed, the setup program requires that you type a password to access SharePoint SQL store. Type the password, and then click **OK**. You must have authorization to access the SharePoint SQL store.

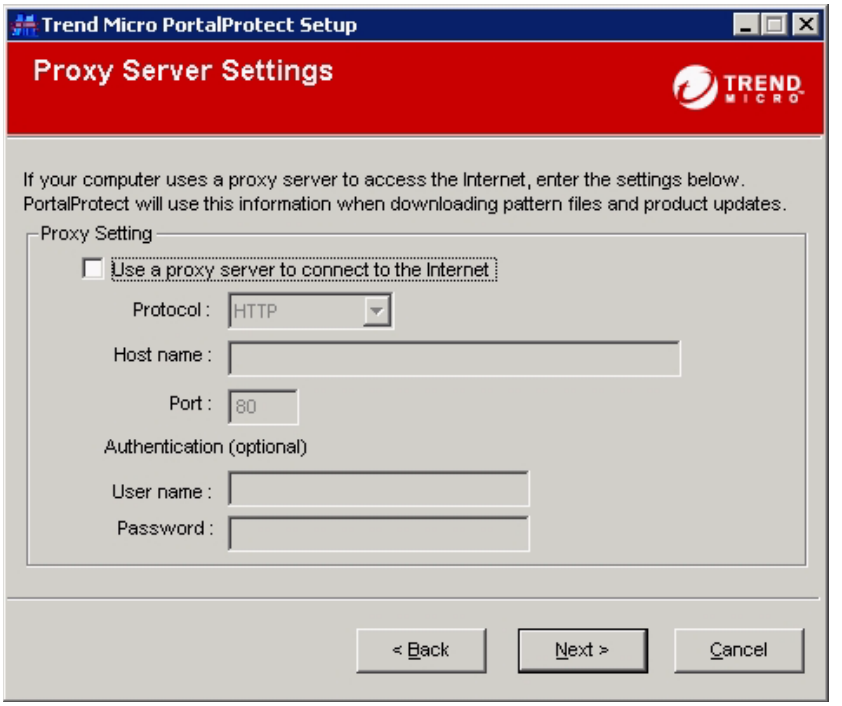
Note: This step is not required when you have installed only the MSDE.

9. When you have typed all of the passwords and the setup program has analyzed every server, the **Target Server Status** screen displays.



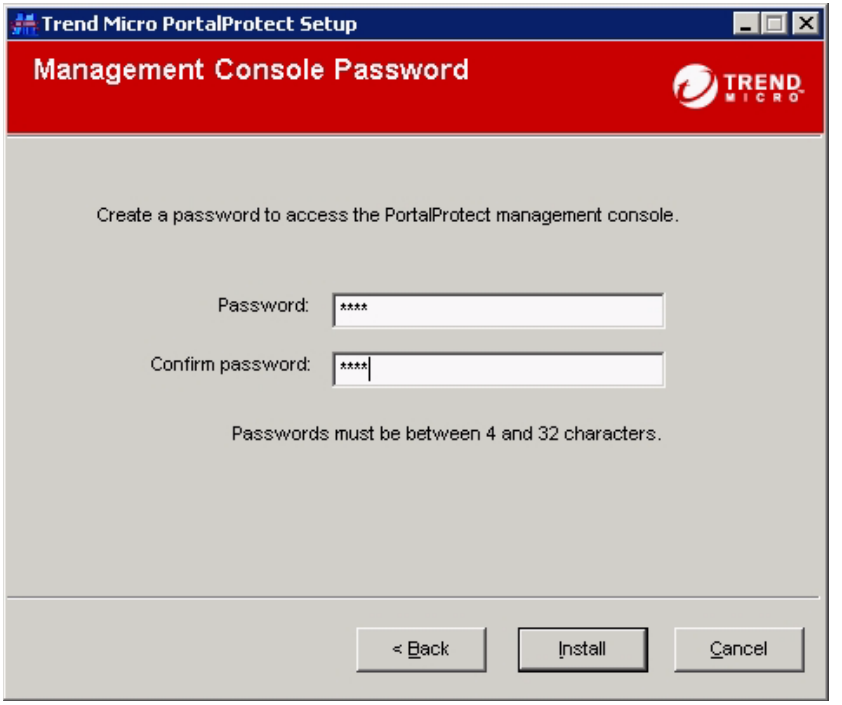
Confirm that the servers are correct, and then click **Next** to proceed.

10. The **Proxy Server Settings** screen appears.



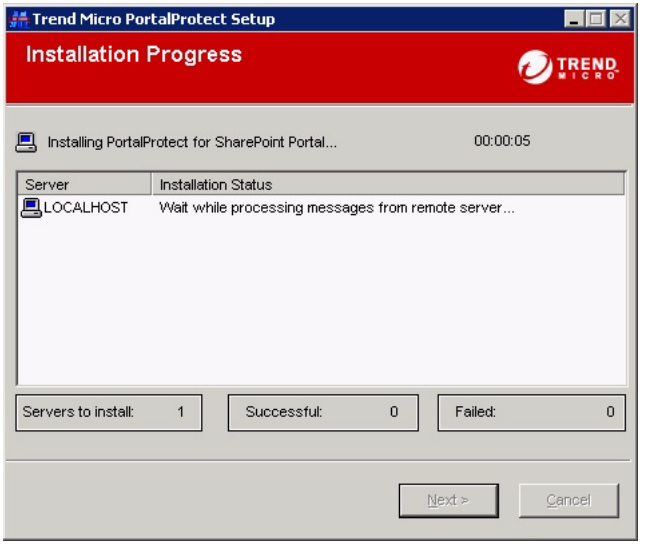
If you use a proxy server, select **Use a proxy server to connect to the Internet**. In the **Protocol**, **Host name**, and **Port** boxes, type the information for your proxy server. If your proxy server requires a password, type your user name and password in the fields provided. See *Configuring proxy settings* on page 3-6 for more information.

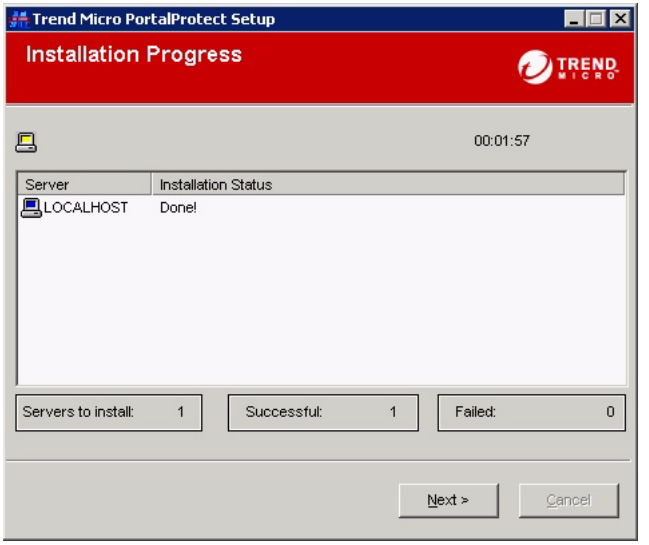
11. The **Management Console Password** screen appears.



Type the password that the administrator will use to access PortalProtect, and then click **Next**.

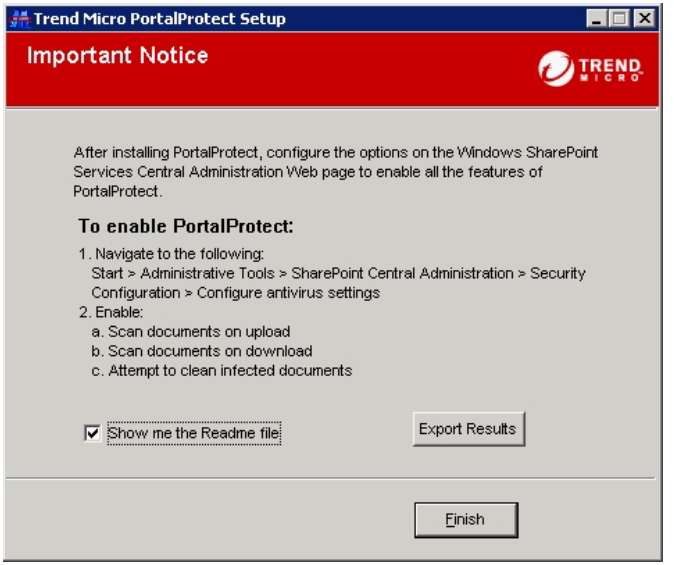
12. The **Installation Progress** screen appears and displays all of the target servers and the status of the installation.





This status report is an in-progress report that shows you each step of the installation. The setup program disables the navigation buttons while the setup program is installing and you must wait. When the installation is complete for all the servers, click **Next** to proceed with the setup.

13. The **Important Notice** screen appears.



Click **Finish** to exit the setup program.

Note: You can export the installation result in a comma-separated format, which most other applications can read.

Note: PortalProtect installs to the default "Program Files" folder of the system as "`%ProgramFiles%\Trend Micro\PortalProtect`".

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 small server farm

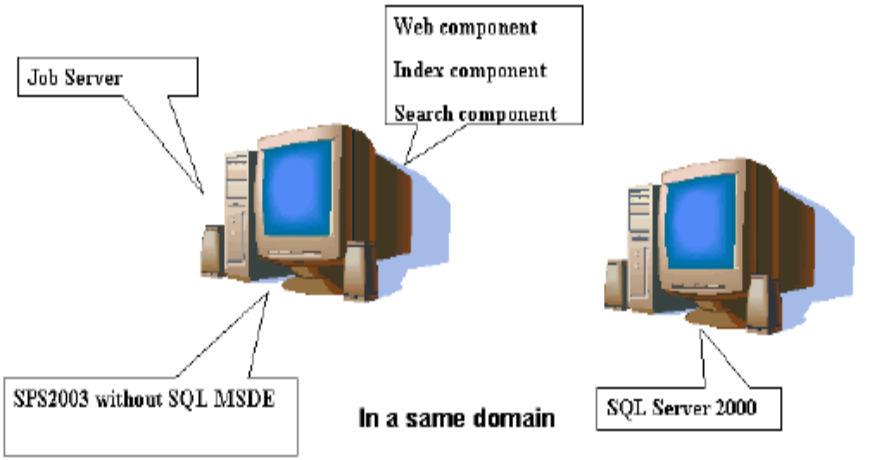


FIGURE 2-1. Small server farm configuration

SharePoint Services medium server farm

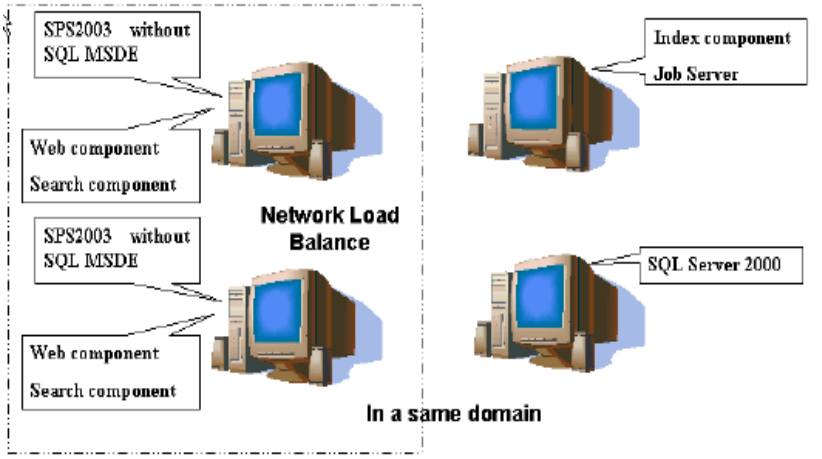


FIGURE 2-2. Medium server farm

SharePoint Services large server farm

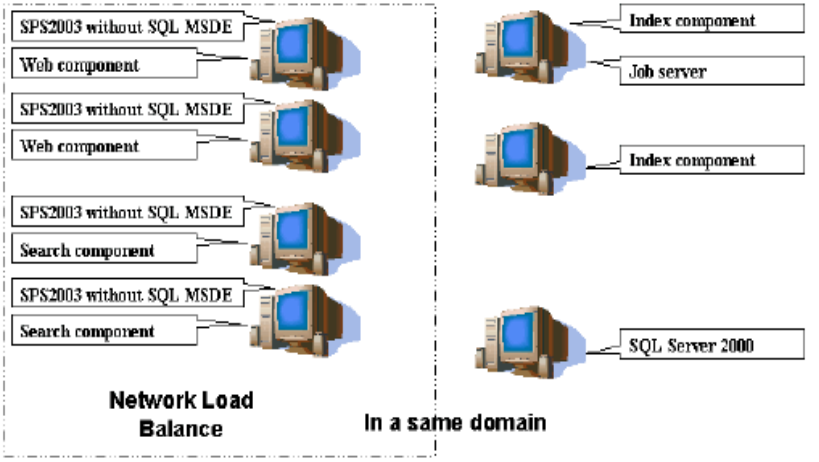


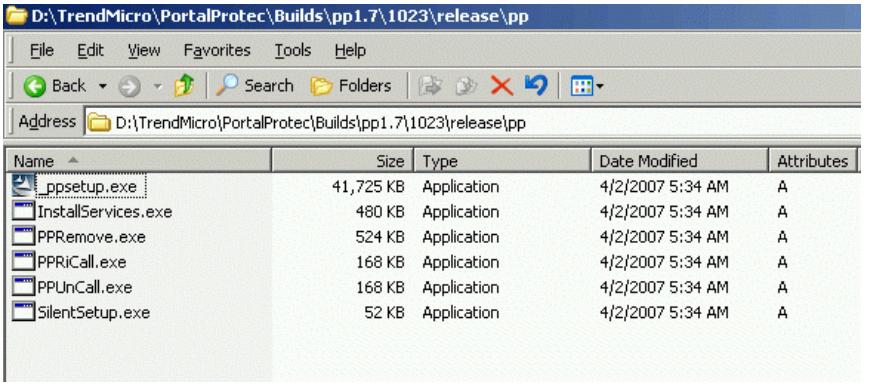
FIGURE 2-3. Large server farm configuration

Silent Installation

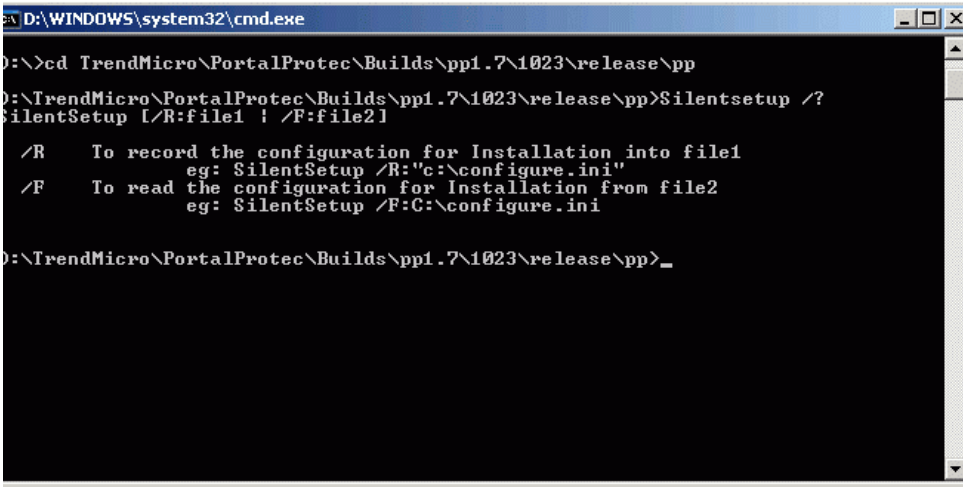
Silent installation pre-populates an INI file with installation parameters and installs PortalProtect without the need for administrator intervention. You need to have a PortalProtect setup package or build to run silent installation.

To install PortalProtect using Silent Install:

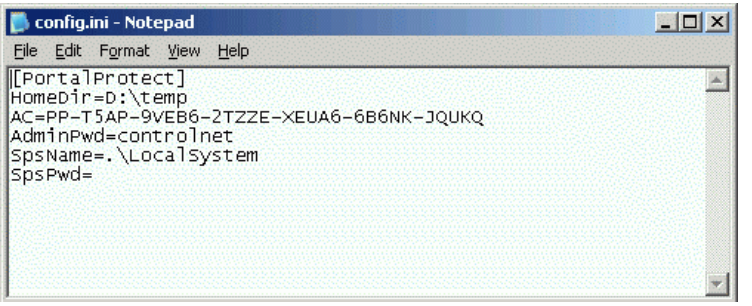
1. Go to **/PP setup package/PP/** where you can see a list of executable files.



2. Copy all the files in the PortalProtect subfolder along with the tool **SilentSetup.exe** 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.
4. Type **SilentSetup.exe /?** to view a list of options that you can use for the Silent Install procedure.



5. Type **SilentSetup /R** to start the Silent Install procedure.
6. The tool generates a configuration file.

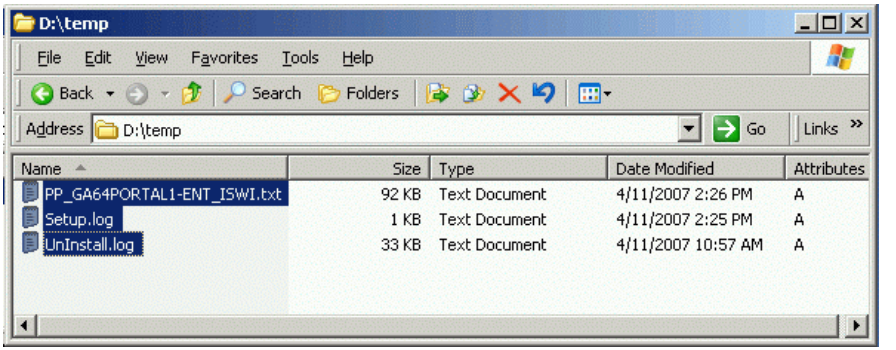


The contents of the configuration file are as follows:

- **HomeDir** - the folder where you want to install the PortalProtect server.
- **AC** - Trial/Full AC to activate PortalProtect during setup.
- **AdminPwd** - password to log on to the PortalProtect Console.
- **SpsName** - name of your SharePoint Server.
- **Sps Pwd** - password of your SharePoint Server.

Note: For **SpsName** and **SpsPwd**, SilentSetup queries the system to get the required information.

7. Run **SilentSetup /F:"c:\config.ini:\"** to enable Silent Install to perform an unattended installation of PortalProtect.
8. After SilentSetup installs PortalProtect on your computer, SilentSetup creates the setup log files in the **HomeDir** folder.



Note: Silent Install allows you to install PortalProtect on any path as per your choice unlike the setup program which installs PortalProtect in the default "Program Files" folder of the system 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 log files of the installation and removal process.

Important Notice:

After installing PortalProtect, you must set some options in the Windows SharePoint Services Central Administration Web page to engage all the features of PortalProtect.

Trend Micro recommends enabling PortalProtect immediately following your installation.

To enable PortalProtect:

1. Open the SharePoint Services Central Administration Web page:

   Start > Administrative Tools > SharePoint Central Administration > Security Configuration > Configure antivirus settings

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

Testing Your Installation

Trend Micro recommends verifying success of 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 other computers on your network that your antivirus installation is currently protecting, attach the `EICAR.com` file to an email message and send it to one of the computers.

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.

To test your installation's HTTP scanning capability:

1. Download the `EICAR.com` test script from either of the following URLs:

   `http://www.TrendMicro.com/vinfo/testfiles/`

   `http://www.eicar.org/anti_virus_test_file.htm`

2. Your antivirus installation should show that the EICAR test virus was detected.

Removing PortalProtect

Removal of PortalProtect both locally and remotely is performed by one simple, 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 to them with a user account that has 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 remove PortalProtect:

Step 1: Begin Removal

1. Insert the PortalProtect program CD into your CD-ROM drive, click **Start** > **Run**. In **Open**, type `D:\uninstall.exe`, and then click **OK** (where `D:\` is the drive letter of your CD-ROM). The Uninstallation program appears.
2. Click **Next**.

Step 2: Select Target Servers

1. From the Domain list in the left pane, double-click a domain name to select the servers you want to remove PortalProtect from. You can either select target

server names individually or select the domain name to remove PortalProtect from all servers in a domain. Instead of a target server name, you can enter the target server IP address.

2. Click **Add**. The selected server(s) appear in the Server name list. To remove server(s) from the Server name list, select them and then click **Remove**.
3. Click **Next** to continue. The Server Logon screen appears.

Step 3: Log on to Servers

1. Do the following:
   - In **User name** and **Password**, type the same user name and password you used when you installed the server that is displayed in **Server name**.
   - Specify the same share name you used during installation (the default is c$).

Tip: If you used the same account to log on to multiple servers, make sure the **Remember user name...** check box is selected. This prevents you from having to enter the same logon credentials for each server.

---

2. Click **Logon** to log on to the server(s). A list of selected servers appears.
3. Click **Next**. A list of components to remove appears.

Step 4: Complete Removal

1. Click **Uninstall** to start removing PortalProtect from the selected servers.
2. Click **Next**. A list of selected servers and successful and unsuccessful uninstallations appears.
3. Click **Finish**.

Chapter 3

Getting Started with PortalProtect

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

In this chapter, you will find information about:

Viewing the PortalProtect Web Management

Console

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

To view the Web Management Console for a local server

1. Click **Start** > **Programs** > **PortalProtect 1.7** > **PortalProtect Console**. The Web Management Console appears.
2. The URL in the Address box should be the following:

```
http://<servername><serverport>/commoncgi/servlet/CCGIServlet?ApHost=PortalProtect&CGIAlias=PortalProtect&Page=file%3Alogin.xhtml
```

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.

To view the Web Management Console for a remote server:

Use Internet Explorer to access `http://<servername>:<port number>`.

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, which 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, which is the menu on the left-hand side of the Management Console. It provides quick access to all PortalProtect settings.
- Main display area- where you can view and set the different options for PortalProtect.
- Tabs are a part of the main display area. Choosing tabs allows you to access a grouping of similar options.
- Help icons. These buttons allow you to access context sensitive help ( ) and provide pop-up information on various features ( ).

Logging On and Off

Log on

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

Log off

You must log off your current session before logging on to a different SharePoint Portal Server. Click **Log Off** from the banner of the Web Management Console to log off.

To change the log in password for the Web console:

1. From the left-hand menu, click **Administration > Password**.
2. Type the old password in the space provided.
3. Type the new password in the **New password** box and type it again to confirm it.
4. Click **Save** to change the password. A message box displays telling you the password changed.

Updating PortalProtect

Antivirus software can only be effective if it is using the latest technology. 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 3-6.
- 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, the Internet, and the intranet UNC path.

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 expires. 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 3-6

After you register, you receive an Activation Code. Use your Activation Code to activate PortalProtect during installation, or at a later time from the Management console.

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 a new 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 website, 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 6-1.

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-hand 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 Internet/intranet 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 **Create a component package ...** 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: During times of virus outbreaks, Trend Micro can update virus pattern files more than once each week. The scan engine updates regularly, but less frequently than once per week. Trend Micro recommends updating daily to help ensure PortalProtect has the current component versions.

To configure scheduled updates:

1. On the left-hand 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 Internet/intranet 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 **Create a component package ...** 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

An update component package consists of the latest pattern file and scan engine on a local PortalProtect Server. If you have many PortalProtect Servers, creating an update component package provides a quick update option. In addition, 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-hand 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.
   - **Other Internet/intranet 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 **Create a component package ...** to create a component package on one server that can be accessed by the other servers on the same local network.

5. Select **Create a component package on this server ...**.
6. Click **Save**.

Note: Once created, other servers can download the package on: `Http://<Server Name>:<Port>/AU.`

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, that 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 3 digits, in the format *xxx*, for example, 786.
2. The new pattern file numbering system, which came into use during 2003, utilizes 6 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 Blocking and Scan Options

This chapter discusses configuring the blocking and scan options for PortalProtect. It describes how to configure PortalProtect to protect your SharePoint environment.

PortalProtect offers three general strategies for protecting Portal Servers:

- Set blocking options to screen out files that meet specified conditions and set options to handle those files.
- Scan content for viruses and other malicious code and have PortalProtect take actions such as "clean", "quarantine", and "block" against content when it detects viruses.
- Use a combination of blocking and scanning. Block or quarantine high-risk files and scan the rest. This saves time and resources and provides reasonable security for the SharePoint Portal servers.

Using advanced options, you can also configure scanning for malicious Macro code, and block and scan compressed files.

In this chapter, you will find information about:

Configuring Blocking Options

You can configure PortalProtect to block files according to file type and file name and then to "quarantine", "block", or "delete" all the files that match your configuration. When you enable file blocking, PortalProtect blocks the files according to your configurations. Blocking can occur during real-time, manual, and scheduled scanning. PortalProtect blocks files that it does not delete or quarantine according to the blocking options that you configure.

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 Portal 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 Portal.

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 Portal servers.

To configure blocking actions:

1. First, choose whether or not to set up a quarantine folder. See *Quarantine Files When They Match Blocking Options* on page 4-3

2. Set an action for PortalProtect to execute on files that match your blocking options. See *Setting Blocking Actions* on page 4-3

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:

- **Quarantine**–Move the file to a restricted access folder, removing it as a security risk to the SharePoint environment. To set the location of the Quarantine folder, click **Specify quarantine folder** at the bottom of this group box, and type the location of the folder (it must be located on a fixed drive).
- **Block**–PortalProtect blocks the file from accessing the SharePoint Portal server and logs an event.
- **Delete**–During manual or scheduled scanning, PortalProtect deletes files that match the blocking options from the SQL content store.

Quarantine Files When They Match Blocking Options

You can configure PortalProtect to move files to a quarantine folder. When PortalProtect moves files to the quarantine folder, it is because it suspects they contain viruses or malicious code or they match 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.

To specify the location of the Quarantine folder:

1. Open the Folder screen:
   - On the left-hand menu, click **Administration** > **Folders**.

     OR
   - Click on a **Specify quarantine folder** link.

2. Under **Quarantine folder path** type the directory path of the Quarantine folder (must be located on a fixed drive). If the directory path does not exist, Portal Protect will create a folder to the specified path.
3. Click **Save**.

Configuring Scan Options

Use the **Scans** menu to setup scans and configure the options for those scans. You can set up real-time scans, manual scans, or scheduled scans. 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 Scans* on page 4-6

About Scanning

Real-time scanning occurs whenever a file is saved to a SharePoint Portal server (check-in) or retrieved from the SharePoint Portal 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.

PortalProtect is capable of processing multiple scan requests. When it receives multiple scan requests, it prioritizes and queues the requests that it cannot run immediately and runs them when resources become available.

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

Note: When real-time scan is disabled and the settings ‘scan documents on download’ and ‘scan documents on upload’ are enabled on SharePoint during upload or download, PortalProtect 1.7 does not scan the files while downloading because SharePoint stamps the files as “scanned” when the files are uploaded. Since files are already found to be scanned, PortalProtect 1.7 does 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.

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: Make sure you never disable the real-time scan. If you must disable the real-time scan, make sure you run the manual scan regularly.

Manual scans

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 real-time or scheduled scan, the manual scan will run at once. You must wait to run your scan when PortalProtect is completing component updates.

Scheduled scans

Scheduled scans automate routine antivirus maintenance procedures as well as improves scan management efficiency and control over security policy. Scheduled scans run according to the interval and time you set. At the configured time, they automatically check for infected files on the SharePoint Portal server(s). When you enable scheduled scans, all the scans you schedule run. You cannot select some scheduled scans to run and other scheduled scans not to run.

Enabling and Disabling Scans

When you enable real-time scanning, it constantly runs in the background of your Portal. Similarly, scheduled scans automatically occur according to the schedule you have configured. You can disable real-time and scheduled scans. Disabling the scan is only temporary and does not disable or change your scan configuration. When you decide to resume real-time scanning, simply enable the scan again.

WARNING! *If you disable real-time scanning, no background scanning or blocking occurs and you are vulnerable to infected files entering the Portal while the scan is disabled.*
If you disable scheduled scanning, no scanning or blocking of your SQL content store occurs and you are vulnerable to infected files being stored on your SharePoint Portal servers while the scan is disabled.

To enable or disable real-time scan:

1. On the left-hand menu, click **Scans >Real-time**.
2. Select **Enable real-time scan** to "turn-on" the scan, or clear the check box to "turn-off" the scan.
3. Click **Save**.

To enable or disable scheduled scans:

1. Click **Scans > Scheduled** from the left-hand menu.
2. Select **Enable scheduled scan** to "turn-on" the scan, or clear the check box to "turn-off" the scan.
3. Click **Save**.

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

Selecting Files to Scan

By default, PortalProtect scans all the files on all your SharePoint Portal servers. This provides the maximum security possible. However, scanning every file requires a lot of time and resources. Therefore, you might want to limit the amount of files PortalProtect includes in its real-time, manual, and scheduled scans.

Configure PortalProtect to limit its scanning to the following files:

- **All file types**–scan 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 4-9.
- **Scan files with the following extension**–PortalProtect suggests a list of extensions. Add more to the list by typing them in the box.

Exclude files from scanning

PortalProtect can exclude files from scanning based on their extension if you consider them to be "safe" file types. By not scanning safe files, PortalProtect reduces the number of files it scans and performance is improved.

PortalProtect will never scan files you exclude from scanning even if you have indicated those file by name or type in the files to include.

Tip: After configuring your scan settings and scanning your SharePoint environment, analyze your results to see if any harmless file types are consistently being scanned. Add these to the exception list to speed up your scanning time.

About IntelliScan

Most antivirus solutions today offer you two options in determining which files to scan for potential threats. PortalProtect either scans all files (the safest approach), or it scans only those files with certain file name extensions (considered the most vulnerable to infection). But recent developments involving files being “disguised” through having their extensions changed has made this 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, especially for SMTP traffic, 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 type

When set to scan true file type 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`," it does not assume the file is a graphic file and skips 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 named 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.

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 or not 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 *Quarantine Files When They Match Blocking Options* on page 4-3

2. Configure the action that PortalProtect executes when it detects viruses or malicious code. You can configure PortalProtect to use ActiveAction™ or configure a customized action. ActiveAction takes the most appropriate action based on the threat type. See *Use ActiveAction* on page 4-11

Back up files before taking action

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

Backed up files should be quickly deleted once you've determined that the original file was not damaged and that it is usable after the PortalProtect has executed an action on it. If the file becomes damaged or unusable, send it to Trend Micro for further analysis. (Even if PortalProtect has completely cleaned and removed the virus itself, some viruses damage the original file code beyond repair.)

To specify the location of the Backup folder:

1. On the left-hand menu, click **Administration** > **Folders**. The Folder screen appears showing information about the Backup folder and Quarantine folder.
2. Under **Backup folder path**, type the directory path of the Backup folder (must be located on a fixed drive).
3. Click **Save**.

Use 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.
- **Microsoft Office macro**–can contain malicious code. Macro viruses are application specific and target Microsoft Office applications.

  See *About macro viruses* on page 4-14
- **Additional Threats**–Pause the cursor on the information button ( ) to see a list of security threats that PortalProtect is able to detect and take action on. The default action for additional threats is "quarantine".

  For more information about these kinds of threats, see the Trend Micro website for security information at `http://www.trendmicro.com/vinfo/`
- **Encrypted/password protected file**–PortalProtect does not scan these type of files. Instead, PortalProtect takes actions 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 "quarantine".

  See *About encrypted and password protected files* on page 4-14
- **Unscannable files**–files that PortalProtect cannot scan, such as those over 4 GB.

  See *About unscannable files* on page 4-15

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 second action specified.

  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 for the second action is "quarantine".

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

Note: You cannot select the "Clean" action for "Additional threats".

- **Strip**–PortalProtect deletes the macro code from the file. If you have configured a backup folder, PortalProtect moves the original file to the backup folder before it strips the macro.

  As an advanced feature, PortalProtect offers the protection of Trend Micro MacroTrap™. To enable it, click the **Advanced** tab and select the **Enable MacroTrap ...**. See *Using MacroTrap to Scan Unknown Macro Viruses* on page 4-18.
- **Delete**–PortalProtect deletes the file and logs an event.
- **Quarantine**–Move the file to a restricted access folder, removing it as a security risk to the SharePoint environment. To set the location of the Quarantine folder, click **Specify quarantine folder** at the bottom of this group box, and then type the location of the folder (must be located on a fixed drive). Click **Save.**
  - During real-time scanning, PortalProtect blocks the file from entering the SharePoint server.
  - During manual or scheduled scanning PortalProtect deletes the file.
- **Rename**–Change the file extension to `vir` to prevent the opening or execution of the infected file.
  - During real-time scanning PortalProtect will allow the renamed file entry to the SharePoint server.
- **Block**–PortalProtect blocks the file from accessing the SharePoint server and logs an event.
- **Pass**–Record virus infection of malicious files in the Virus logs, but take no action.

Note: PortalProtect 1.7 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 if you change the scan action to some other value, the file is not sent to PortalProtect 1.7 for a rescan. 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.

As these file types are often attached to email messages, macro viruses spread readily by means of the Internet in email attachments.

Macro viruses are a common and widespread threat because they ...

- infect files whenever they are opened, closed, or saved
- target applications with a large installation base, such as Microsoft Word and Excel
- spread in email attachments using macro capable applications
- are transmitted across networks and the internet

How does PortalProtect prevent macro viruses from infecting your SharePoint server?

Use PortalProtect to:

- Block file types commonly attacked by macro viruses and "quarantine", "block", or "delete" them.
- Configure MacroTrap to detect unknown macro viruses.
- Configure PortalProtect to scan for macro viruses and take a customized action to prevent infected files from damaging your SharePoint server.

See *Using MacroTrap to Scan Unknown Macro Viruses* on page 4-18

About encrypted and password protected files

PortalProtect does not scan these types of files. Instead, PortalProtect takes actions 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 "quarantine".

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 or password protected files and Unscannable files, it reports to SharePoint Services that the files are infected. In some cases, PortalProtect can make a false positive identification and the files are actually not infected. Trend Micro recommends reviewing your quarantine folder from time to time to prevent the false positive identification of email messages.

About unscannable files

PortalProtect cannot scan some types of files such as those over 4 GB. Instead, PortalProtect takes other actions to prevent these types of files from threatening your SharePoint servers. The action it takes depends on the actions you have configured. The default action is "quarantine".

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. You configure how it scans compressed files using the options from the **Advanced** tab from the **Scans** menu. When PortalProtect detects a virus, it blocks the file or executes a preconfigured action. You enable blocking or set the scanning action from the **Scans** menu.

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 - such as email attachments, FTP, and HTTP. Before any virus detection can occur on a compressed file, however, you must first decompress it.

Recognizing the fundamental importance of decompression in the detection of 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 performs scan actions on the whole compressed file, rather than individual files within the compressed file.

WARNING! *PortalProtect cannot detect viruses located at a compression layer greater than 1 when the compression type is unsupported.*

To scan compressed files:

1. On the left-hand menu, click **Scans**.
2. Open the screen that matches the type of scan for which you want PortalProtect to scan compressed files. PortalProtect can scan compressed files during a real-time, manual, or scheduled scan.
3. From the scan type screen, choose the **Advanced** tab.
4. Select **Scan compressed file if**.
5. Enter the options to control the way PortalProtect scans compressed files.
   - Type a number in the field provided to set a limit for the number of files PortalProtect will scan. When PortalProtect encounters a number of files equal to or greater than this number it will not scan the files, instead, it will execute the action that you specify in the drop-down list next to **When compressed file is beyond limitation, specify action:**.
   - Type a number in the field provided 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, instead, it will execute the action that you specify in the drop-down list next to **When compressed file is beyond limitation, specify action:**.

- Select a number from the list provided 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, instead it will execute the action that you specify in the drop-down list next to **When compressed file is beyond limitation, specify action:**.

6. Click **Save**.

Note: PortalProtect only cleans the viruses found in the PKZIP or LHA compressed files and scans only the first layer in the compressed files.

Using MacroTrap to Scan Unknown Macro Viruses

MacroTrap uses pattern recognition and rule-based technologies to detect known and unknown macro viruses. Enable MacroTrap (Heuristic Scan) to scan files for infected macros.

When MacroTrap detects a macro virus, it executes the action you set for viruses from the **Scans** menu. The default action is "pass".

The scan engine detects macros and viruses according to a list of priorities. MacroTrap has a lower priority than virus detection, but a higher priority than normal Microsoft Office macros.

Example: You configure PortalProtect to clean viruses and strip Office macros. You enable MacroTrap. If PortalProtect receives a file with a macro virus, MacroTrap detects the macro virus and PortalProtect cleans the file. If the file has a macro, but has no virus or malicious macro code, PortalProtect strips the macro.

To set PortalProtect to scan unknown macro viruses:

1. On the left-hand menu, click **Scans**, then click the scan option you want to set (**Manual**, **Real-time**, or **Scheduled**).
2. Click the **Advanced** tab. The Advanced Options screen appears.
3. Under **Scan Unknown Macro Viruses**, select the **Enable MacroTrap...** check box.

4. In the **Scan heuristic level** list, click a Heuristic Scan level.
5. Click **Apply**.

Setting MacroTrap level

Set the Heuristic Scan level depending on the level of security needed.

- Level 2 is the optimal setting for the Heuristic Scan. At Level 2, there is a high rate for detecting unknown macro viruses, fast scanning speed, and only necessary rules are used to check for macro virus strings. In addition, the false alarm rate is very low.
- Level 4 is the fastest and has the highest detection rate, but may cause more false alarms.
- Level 1 is the slowest and has the lowest detection rate with very few false alarms.

Chapter 5

Notifications, Logs, and Reports

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

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

In this chapter, you will find information about:

Configuring Notifications

Notifications may be sent to the administrator(s) or other specified recipients. With PortalProtect, you can configure notifications through email, Simple Network Management Protocol (SNMP) Trap, pager, or the Windows Event Log.

To enable event notifications:

1. On the left-hand menu, click **Notifications** > **Events**. The **Event Notifications** screen opens.
2. Select the check-boxes for the events for which you want PortalProtect to send notifications.
3. Click **Save**. The next time that these events happen, PortalProtect will notify the chosen recipients.

To configure event notifications:

1. On the left-hand menu, click **Notifications** > **Events**. The **Event Notifications** screen opens.
2. Click the events for which you want configure notifications. When you click an event, a new screen opens displaying the notification details for that event.
3. Select the check box(es) for the type of notification you prefer:
   - **Enable Email notification**–Notify the recipients via Email.
   - **Enable SNMP Trap notification**–Notifies an SNMP Trap server. View data with a Management Information Base browser.
   - **Enable Pager notification**–Notifies the specified individual via pager.
   - **Enable Windows Event Log notification**–PortalProtect records the event in the Windows Event log.
4. Customize the message text for Email and SNMP Trap notifications:
   - In **Subject**, type a descriptive subject.
   - In **Message**, type a customized message. Insert the cursor in the text message and select a message type from the drop-down list. The message type is inserted in the text and surrounded by square brackets. All text enclosed within brackets is dynamically generated. For example, [Server name] will display the actual name of the PortalProtect Server.
5. Click **Save**.

Setting Notification Recipients

After you select the types of notifications, select the notification recipients.

To set notification recipients:

1. On the left-hand menu, click **Notifications** > **Recipient**. The **Notification Recipients** screen appears.

   Alternatively, click **Notifications > Events** and then click **Edit Recipients**.
2. Do the following:
   - Type the address of the sender.
   - Type the address information for the recipients.
     - Type the recipient's email address.
     - Type the mail server address. This can be either the domain name or the IP address.
     - Type the port number.
   - To set SNMP Trap, under **SNMP Trap** type the IP address number or name of the SNMP Trap server and the Community Name (public or private). For example:

     ```
     IP address: 123.123.123.123
     Community name: public
     ```
   - To set a pager number, under **Pager**, type the pager number and select the `COM` port used by the modem.
3. Click **Save**.

Configuring Outbreak Alert

To configure an Outbreak Alert:

1. On the left-hand menu, click **Notifications > Events**. The **Event Notifications** screen opens
2. Click **Outbreak Alert**. The **Outbreak Alert** screen appears.
3. Under **Enable Outbreak Alert**, do the following:
   - To set the number of detected viruses and the span of time that triggers the Outbreak Alert, select the **When viruses exceed ...** check box, and then type the number of viruses and set the duration.

- To set the number of detected uncleanable viruses and the span of time that triggers the Outbreak Alert, select the **When uncleanable viruses exceed ...** check box, and then type the number of viruses and set the duration.

4. Select the check box(es) for the type of notification you prefer:
   - **Enable Email notification**–Notify the recipients via Email.
   - **Enable SNMP Trap notification**–Notifies an SNMP Trap server. View data with a Management Information Base browser.
   - **Enable Pager notification**–Notifies the specified individual via pager.
   - **Enable Windows Event Log notification**–PortalProtect records the event in the Windows Event log.
5. Customize the message text for Email and SNMP Trap notifications:
   - In **Subject**, type a descriptive subject.
   - In **Message**, type a customized message. Insert the cursor in the text message and select a message type from the drop-down list. The message type is inserted in the text and surrounded by square brackets. All text enclosed within brackets is dynamically generated. For example, [Server name] will display the actual name of the PortalProtect Server.
6. Click **Save**.

Configuring Virus Detected Notification

Configure the Virus detected notification to notify specified individuals when PortalProtect detects viruses and takes actions on those viruses. Designated individuals can receive Virus detected notifications via email, SNMP, pager, or the Windows Event Log. In addition, you can customize the message of the Virus detection notification.

To configure a Virus Detected notification:

1. On the left-hand menu, click **Notifications** > **Events**. The Event Notifications screen opens.
2. Click **Virus detected**. The Virus Detected Notification screen appears.
3. Select the actions for which you want to send a notification. When PortalProtect detects a virus and takes these actions, it will automatically send the recipients a notification.
4. Select the check box(es) for the type of notification you prefer:

- **Enable Email notification**–Notify the recipients via Email.
- **Enable SNMP Trap notification**–notifies an SNMP Trap server. View data with a Management Information Base browser.
- **Enable Pager notification**–notifies the specified individual via pager.
- **Enable Windows Event Log notification**–PortalProtect records the event in the Windows Event log.

5. Customize the message text for Email and SNMP Trap notifications:
   - In **Subject**, type a descriptive subject.
   - In **Message**, type a customized message. Insert the cursor in the text message and select a message type from the drop-down list. The message type is inserted in the text and surrounded by square brackets. All text enclosed within brackets is dynamically generated. For example, [Server name] will display the actual name of the PortalProtect Server.
6. Click **Save**.

Configure Blocked Files Notification

Configure the File blocked notification to notify specified individuals when PortalProtect blocks files and takes actions on those files. Designated individuals can receive notifications via email, SNMP, pager, or the Windows Event Log. In addition, you can customize the message of the Virus detection notification.

To configure a Blocked Files notification:

1. On the left-hand menu, click Notifications > Events. The Event Notifications screen opens.
2. Click **File blocked**. The File Blocked Notification screen appears.
3. Select the check box(es) for the type of notification you prefer:
   - **Enable Email notification**–Notify the recipients via Email.
   - **Enable SNMP Trap notification**–Notifies an SNMP Trap server. View data with a Management Information Base browser.
   - **Enable Pager notification**–Notifies the specified individual via pager.
   - **Enable Windows Event Log notification**–PortalProtect records the event in the Windows Event log.
4. Customize the message text for email and SNMP Trap notifications:

- In **Subject**, type a descriptive subject.
- In **Message**, type a customized message. Insert the cursor in the text message and select a message type from the drop-down list. The message type is inserted in the text and surrounded by square brackets. All text enclosed within brackets is dynamically generated. For example, [Server name] will display the actual name of the PortalProtect Server.

5. Click **Save**.

Configure System Event Notifications

Configure PortalProtect to send notifications when certain system events occur, including whether the PortalProtect service or the scan process stopped.

See *Configuring Notifications* on page 5-2.

Configure Update Notifications

Configure PortalProtect to send notifications when certain updates occur, including which components are updated.

See *Configuring Notifications* on page 5-2.

Working with Logs

PortalProtect provides comprehensive information about scans, updates, system events, blocked files, quarantined files, and backed up files. It saves this information to a database. You can query the database and get logs to analyze. For example, you can analyze Virus logs to view the most common viruses and scan actions as well as users who are introducing viruses to the network.

Use this information to reduce the vulnerabilities of an environment and review the effectiveness of your security policy and, if necessary, adjust the policy accordingly. You can also export the log information to a database or spreadsheet application for further analysis or to easily share the information.

In addition to displaying the date and the time of each recorded log, the various log types provide log-specific information:

- **Event logs**–contains information about PortalProtect System events, including successful updates, or if the PortalProtect service or scanning stopped.
- **Virus logs**–contains information about detected virus or malicious code incidents, including the type of malicious code, the name of the author, the action taken, and the infected file name and location.
- **Update logs**–contains information about update events, including the update method, source, success or failure, and what components were updated.
- **Quarantine logs**–contains information about files that were quarantined, including the name of the original and the quarantined file.
- **Block Logs**–contains information about files that were specified to be blocked, the action taken on the file, and the name of the original and quarantined file.
- **Backup logs**–contains information about files that were backed up, including the name of the original and the backed up file.

Query Logs

PortalProtect gives you the ability to view many types of logs, which you can export and print. Use the Query function to configure 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 make a log query:

1. From the sidebar, click **Logs > Query**.
2. Select the type of query you want to get from **Logs type** drop-down list.
3. Select the options for the date range for your log query. You can query logs according to preset date ranges including **All dates**, **Today**, **Yesterday**, **Past 7 days**, and **Past 30 days**, or select **Specified** and then specify any date range that you want.
4. You can sort logs by date/time or event type, but only event logs can be sorted by event type.
5. You can also select how you want to sort the query information and how many logs to display per page.
6. When you are finished setting your query options click **Query**. PortalProtect opens a new screen displaying the results.

7. Click **Export** to export the result of your query as a comma-separated value (CSV) file (Unicode standard).
8. Click **Print** to print the result of your query.
9. Click **New Query** to query other types of logs.

View Event Logs

View Event logs to see information about PortalProtect System events, including: whether or not an update succeeded and if the PortalProtect service or scanning stopped.

View Virus Logs

View Virus logs for information about viruses and other malicious code PortalProtect detects.

Virus logs contain the following information:

- Date and time when the virus was detected
- Scan actions that PortalProtect performed
- The names of users who introduced viruses or malicious code to the SharePoint environment
- Names of the malicious code
- Actions taken
- Infected files and their location

View Update Logs

View Update logs to gain information about the update process, including: the method of update, the source of the update, whether the update was successful, and the program components that were updated.

View Quarantine Logs

All files that are quarantined are written as an entry in the Quarantine Logs. The Quarantine Logs contain information including: the name of the user that introduced the virus or malicious code, and both the name of the original and quarantined files.

View Blocked File Logs

View Block logs to see information about blocked files. PortalProtect takes actions such as "quarantine", and "delete" when it finds files that match the blocking options you configured. PortalProtect makes a log of these actions whenever they occur.

View Backup Logs

All files that are backed up are written as an entry in Backup Logs. In addition to the name of the user that introduced the file that was backed up, the Backup Logs also contain both the name of the original file and the backup file.

Export Logs

You can save log entries, and print them or examine them onscreen in detail. PortalProtect saves log entries as a comma-separated value (CSV) file (Unicode standard).

To export a log entry:

1. On the left-hand menu, click **Logs > Query**.
2. Select the type of log you want to export.
3. Click **Query** to generate the log.
4. Click **Export**.

Delete Logs

Delete log entries if the information they provide is no longer useful. If the logs are taking up too much disk space, you can delete log entries for specific dates. PortalProtect lets you delete logs both automatically and manually.

Manually delete logs

You can manually delete logs if they are taking up too much disk space.

To manually delete logs:

1. On the sidebar, click **Logs > Maintenance**.
2. Click the **Manual Deletion** tab.
3. In the **Delete logs before** box, enter the date of the logs you want to delete. All logs before this date will be deleted.
4. Select the check box(es) of the logs you want to delete.
5. Click Delete. A new page appears informing you that you successfully deleted the log.

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. On the sidebar, click **Logs > Maintenance**.
2. Click the **Auto Deletion** tab.
3. Under Logs, select the checkbox(es) of the logs you want to automatically delete, and then do the following:
   a. To delete logs before a number of days, under **Maximum Age (days)**, select the type of log and type the maximum number of days that the log can be stored. Before this date, PortalProtect deletes it.
   b. To delete logs after they have become a certain size, under **Maximum Size (MB)**, select the type of log and type the size that the log can have. After this size is reached, PortalProtect deletes the excess logs to reduce the total to under the maximum.

   Note: The maximum size for any log is 512MB.

4. Click **Save**.

Viewing and Generating Reports

You can set PortalProtect to generate Daily, Weekly, and Monthly reports. These reports are generated from log events. You can view previously generated reports from the Management console.

Reports contain the following information:

- Report Highlights. Highlights include information about how the report was generated. It describes the components used to perform the scanning.
- Scan Summary. The scan summary provides information about the scan itself. It shows the number of files that were scanned and the number of files that PortalProtect blocked and detected viruses for.
- Actions Taken on Infected Files. This describes the actions that PortalProtect executed during the scan, including "clean", "quarantine", "delete", and "pass".
- Top 10 lists about viruses, blocked file types, and the author of infected files.

To generate a report:

1. From the sidebar, click **Reports** and then click either **Daily**, **Weekly** or **Monthly**.
2. Click **Settings**. The **Report Settings** screen opens.
3. Select **Generate report**.
4. Select **Send the report to the following recipients**.
5. Type the email addresses for the recipients, the subject, and the message.

Note: The mail server setting is the same as recorded at **Notifications** > **Recipients**

---

6. Click **Save**.

View Previous Reports

All generated reports are stored and can be easily accessed. Use the information generated by reports to tighten security, create policies, or identify weak points in your defense.

To view a previous report:

1. From the sidebar, click **Reports** and then click either **Daily**, **Weekly** or **Monthly**. The Reports screen opens, displaying all previously generated reports.
2. Click the report for which you want to view details.

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

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 website is subject to change without notice.

The Trend Micro website 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)

ActiveUpdate Questions

How does ActiveUpdate deliver updates?

ActiveUpdate is a common module of Trend Micro. PortalProtect calls the ActiveUpdate API to implement active update. ActiveUpdate is not an ActiveX or Java, it is a DLL (TmUpdate.dll).

What protocol does ActiveUpdate use in PortalProtect 1.7?

PortalProtect can use not only HTTP, but also Sockets as protocol for ActiveUpdate. If a user wants to connect directly to the ActiveUpdate server, he/she can also disable proxy settings (for example, when ActiveUpdate server is local server).

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 I configure PortalProtect to use another Internet/intranet source for updates, how does PortalProtect determine if its components are outdated?

PortalProtect ActiveUpdate only supports VSAPI pattern and engine updates. The ActiveUpdate module determines if components need periodic updates. You can customize the period and it can be as frequent as hourly or daily.

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 set it as the update server 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 **Other Internet/intranet source** and enter this URL: http://<SERVERNAME>:<PORTNUMBER>/au

- SERVERNAME is the server hostname or IP address that contains the component package source.
- PORTNUMBER is the port number of PortalProtect web console.

Scanning Questions

I set PortalProtect to block zip files, and then uploaded a zip file. The file was blocked, but the message showed *"a.zip" contains the following virus: "It has been blocked; final action is:[Quarantined]"*. However, this file has no virus. Why does the message tell me the file has a virus?

Microsoft SharePoint Services provides this format and Trend Micro modifies the content within the double quotation mark. To understand the message more clearly, ignore ***"****contains the following virus****"*** and read only the content inside the double quotation marks.

Once I add a folder into Scan Target, I cannot add its sub-folders. Why?

When a folder is included as a target for a scan, PortalProtect also scans all sub-folders of this folder. Therefore, PortalProtect automatically removes the sub-folder from the list of selected folders.

On my server, quarantine and backup always fails. 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 never set "file blocking", but some files can never be uploaded or downloaded. Why?

Please check SharePoint Services block list settings. Share Point Server blocks files with the suffixes you specified. Please use SharePoint Services Central Management Page to remove the configuration.

To remove the file blocking configuration from SharePoint Services:

1. Go to SharePoint Central Administration page.
2. Click SharePoint Server at left navigation. (If this item is not shown, skip this step)
3. Click "Manage blocked file types" in "Security Configuration"
4. Check the extension name in text-box. If the extension name is included, SharePoint Services will block this file when this file is uploaded or downloaded.

When I upload virus file to SharePoint Services, PortalProtect cannot find virus. Why?

Check the following:

- SharePoint Services anti-virus settings:
  - **a.** Go to SharePoint Central Administration page.
  - **b.** Click SharePoint Server at left navigation. (If this item is not shown, skip this step).
  - **c.** Click “Configure anti-virus settings” in “Security Configuration”.
  - **d.** If “Scan documents on upload” is disabled, SharePoint Services will not pass the file to PortalProtect 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 you disable “Attempt to clean infected documents”, PortalProtect only scans the file, but does not clean the file when it detects the file is infected by virus.
- Check PortalProtect real-time scan status:
  - **a.** Log in PortalProtect web console.
  - **b.** Go to Scans->Real-time.
  - **c.** Select “Enable real-time scan”.

I cannot scan viruses in real-time and block files on my server. Why?

- Ensure real-time scan is enabled.
  - **a.** Open the **Real-time Scan**: Scans > Real-time> Virus Scan
  - **b.** Select **Enable real-time scan**

- Ensure you have selected the following options from SharePoint Services under "Anti Virus Setting":
  - scan `upload doc`
  - scan download doc
  - attempt clean virus

For macro code, what does the strip action do? Does it always strip the macro code from a file, or does it do this only when PortalProtect detects an infected file?

Strip action removes all macro code from Microsoft Office files. There are total 5 threat types:

- Virus
- Microsoft Office Macro
- Additional threats
- Encrypted
- Unscannable

If the Microsoft Office file is infected, it will be regarded it as a "Virus" type, the default action is not “strip”, but “clean”. If the file is not infected and has macro code, it will be regarded as “Macro” type, and the default action is “strip”.

When the macro code is removed from the Microsoft Office file, is the file automatically quarantined even if the macro is stripped and the rest of the file is safe?

No, it is not automatically quarantined. If the **Back up file to a specified folder before taking action** is checked, it will be backed up before it is stripped.

If the user does not enable compressed file scanning, does PortalProtect have a default to scan a certain number of compression layers? (If it does what is the number of layers?)

On the **File Blocking** screen, if **Block compressed files** is checked, compressed files will be blocked. Otherwise, if **Scan compressed files if** in **Advanced** screen is not checked, there is no default scan on compressed files.

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?

For blocking operation, the compressed file will be regarded as a single file by PortalProtect. For Scan/Quarantine/Clean operation, PortalProtect will deal with the files that are in the compressed file one by one. Therefore, it is impossible that any infected file will 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”, not by file extension. That is to say, VSAPI can distinguish it even when you rename a `.zip` file to `.txt`. VSAPI scans `.zip` and `.lzh` files in same way.

You can configure scans to have a first action and second action. Is the second action executed only after the first action fails, or can PortalProtect execute both actions? For example: when the first action is "quarantine", and the second action is "clean". Does this mean that PortalProtect will clean the file in the quarantine folder?

Yes, the second action is executed only when the first action fails. You can select a second action only when the first action is “clean”. Trend Micro considers that only "clean" actions can 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's an unscannable file?

Unscannable files are files that VSAPI cannot scan. For example, files of a size exceeding 4GB.

Can PortalProtect scan encrypted files?

No. Encrypted files are an individual threat type in scan settings. User can customize the action for these kinds of files.

In my Portal Protect server, I can scan viruses, but I 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 get the author and location information of the file in the report or the virus log, why?

This is due to lack of information. Microsoft SharePoint Server doesn't provide the information while triggering real-time scan service of PortalProtect.

Installation Questions

Do I need to install PortalProtect on Index server?

The file stream routes to the SQL server directly and does not pass Search or Index server. If you have already installed PortalProtect on the front end SharePoint 2007 server with SharePoint Service 2.0, you do not need to install PortalProtect on the Index, Search, or Job server.

The index server gets its data via the protocol handler that comes with SharePoint. If the content indices for search are set up properly, the index server can get the data from SQL through the protocol handler, run it through the appropriate filter (depending on the file type) and maintain the index. This enables Search to work properly. The Index Server does not need a front end.

Both Microsoft SharePoint 2007 and Trend PortalProtect 1.7 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.

I installed Portal Protect on different servers, but the port number is different from each other. Why?

Portal Protect creates a website as the web console. The default port of the web console is from 30250 to 30260. If the first port in the series is occupied, Portal Protect detects the next port until if finds one that is available. If all the ports from 30250 to 30260 are occupied, Portal Protect cannot be installed successfully.

How to install PortalProtect in Cluster environment?

PortalProtect 1.7 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.

Why can’t I start PortalProtect sometimes?

PortalProtect needs to connect to SharePoint Services database (SQL Server 2000 or SQL MSDE) during the starting phase. If SharePoint Services database cannot be

started, neither can PortalProtect. Before starting PortalProtect, ensure that the SharePoint Services database has started.

Why can't I log in during installation?

Windows only uses one credential to access other Windows machines. Log off and log on to Windows again, then install PortalProtect again.

Why is there a Save button at the bottom of the Manual Scan screen?

You must save scan settings before doing a manual scan. Otherwise, PortalProtect will pop up a warning box to remind you to save it first.

Can you install PortalProtect to the root directory of a drive for example, C:\?

The default install path is: `c:\Program Files\Trend Micro\PortalProtect`.

Why do some administrators require a password for their proxy server and some not?.

Normally, SOCKS v5 need a password certificate, but SOCKS v4 and HTTP do not.

During installation, after the target server analysis, when the customer chooses Back to add/remove some more servers to the list, and then returns to the Target Server Analysis, does the Setup have to restart with the very first server again, or just check the new servers?

The Setup will check all target servers and make analysis.

How long (approximately) does it take for typical installation?

It will take about 1.6 to 2 minutes to do a typical installation to a server. The total time depends on the number of target servers to which you install. The PortalProtect installer creates up to 32 threads to deal with multiple simultaneous deployments . That is to say, the time spent to install to 32 servers is the same as the time spent to install to one server.

Can you remotely configure PortalProtect on one machine, using the Web Management Console from another machine?

To view the Web Management Console for a remote server:

- Click **Start > Programs > Trend Micro PortalProtect > PortalProtect Web Configuration** (Remote Server). A Web page loads with a list of SharePoint Portal Servers that have installed PortalProtect.

- Click the name of the server you want to access. The Web Management Console appears.
- Open this URL and modify the server name to the remote server:

```
http://<remote server
name>/commoncgi/servlet/CCGIServlet?ApHost=PortalProtect&CGI
Alias=PortalProtect&Page=file%3Alogin.xhtml
```

What is the name of the Virus Scan API used by PortalProtect 1.7?

PortalProtect hooks the Microsoft SharePoint Virus Scan API. VSI 1.1 (SP VS API).

Is VSAPI 7.0 the name of the Trend scan engine? Is this the version used in PP 1.7?

VSAPI is the scan engine name of Trend Micro. PortalProtect uses VSAPI 7.0.

Who has the rights to install PortalProtect? What access privilege does the installer need? What information does s/he need to have (IP addresses, domain names, etc)?

Users in the local administrators group have the rights to install PortalProtect. Usually the domain administrator is a member of local administrators group.

To view the local administrators group:

- Right click “My Computer”
- Select “Manage”> “Local users and groups”> “Groups” > “Administrators”.

Besides the Web Management Console, can the customers view PortalProtect through any other interface - perhaps a Web page within SharePoint?

Trend Micro does not provide an alternative viewer.

Must administrators still log on/off of PortalProtect?

You must log on to PortalProtect before you can configure any settings. You must log off your current session before logging on to a different SharePoint Portal Server. When PortalProtect detects no action for 15 minutes, it automatically logs off. Clicking **Refresh** prevents automatic log off.

General Issues

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

Internet Explorer securitysettings 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://127.0.0.1:30250 or http://hostname:30250)

1. Open Internet Explorer
2. Click **Tools>Internet Options**. Choose the Security tab.
3. Click **Trusted Sites** icon and then click **Sites ...**.
4. In the field for trusted zones, type the IP address: 127.0.0.1 or hostname.
5. Click **Add**.

Do customers still need to configure their AV software to not scan:
`Drive:\Program Files\SharePoint Portal Server`

`Drive:\Program Files\Common Files\Microsoft Shared\Web Storage System`

It is not necessary to exclude the folder for scanning. However, to optimize performance, exclude folders from scanning in other Trend Micro products (for example: OSCE). There are 3 folders should be excluded in other Trend Micro products:

- quarantine folder
- backup folder
- temp folder.

You can change Quarantine and Backup folder:

Backup folder:
`Drive:\Program Files\Trend Micro\PortalProtect\BackupFolder`

Quarantine folder:
`Drive:\Program Files\Trend Micro\PortalProtect\QuarantineDir`

Temp folder:
`C:\Program Files\Trend Micro\PortalProtect\temp`

Can Trend Micro's PortalProtect and ServerProtect be installed on the same server?

PortalProtect 1.7 can be installed with ServerProtect.

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 it reads the extension, how does PortalProtect know when 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

This appendix introduces Trend Micro Control Manager and describes how it can help simplify the administration of Trend Micro antivirus and content security solutions in your organization. It also provides instructions on how to install the agent for PortalProtect and how to access the PortalProtect server from the Control Manager management console.

The topics discussed in this appendix include:

Introducing Control Manager

Trend Micro Control Manager™ is a central management console that manages Trend Micro products and services, third-party antivirus and content security products 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 allows system administrators to monitor and report on activities such as infections, security violations, or virus entry points. System administrators can download and deploy update components throughout the network, helping ensure that protection is consistent and up-to-date. Update components include virus pattern files, scan engines, and anti-spam rules. Control Manager allows both manual and pre-scheduled updates. Control Manager allows the configuration and administration of products as groups or as individuals for added flexibility.

What You Can Do with Control Manager and PortalProtect

Control Manager builds on the centralized management concept Trend Micro pioneered with Trend Virus Control System (Trend VCS). If you are currently running Trend VCS, you can purchase an upgrade to obtain all the new benefits of Control Manager. For more information on upgrading your management server from Trend VCS to Control Manager, see the *Control Manager Getting Started Guide*.

Using Control Manager, you can accomplish the following:

- Configure, monitor, and maintain most Trend Micro software, including PortalProtect, from a single console, regardless of location or platform
- Simplify the implementation of a your organization’s antivirus security policies
- Delegate tasks and determine access control based on a hierarchical structure. You can assign different operators separate access to individual branches of the hierarchy
- Respond to outbreaks quickly using Outbreak Prevention Service

Note: If there is a proxy between TMCM and PortalProtect, deployment from the TMCM will fail.

What is a Control Manager Agent?

A Control Manager agent is an application installed on a computer with a Trend Micro product installation. The agent allows Control Manager to manage the product. It receives commands from the Control Manager server, applies them to the managed product, and collects logs to send to Control Manager.

Requirements for Installing the Agent

The requirements for installing the agent are the same as those for installing the PortalProtect server.

Note: You cannot install the Control Manager agent on Microsoft Windows .NET™ Server.

For information on the minimum system requirements for the PortalProtect server, see *System Requirements* on page 2-2.

Required Information for Agent Installation

You will need the following information before deploying the agent:

- The fully qualified domain name (FQDN) or IP address of the Control Manager server
- Administrator privileges to the server where you want to install the agent
- A Control Manager User ID with Administrator, Power User, or Operator privileges. It is very important to maintain this account. If the Control Manager User ID is deleted, the agent will not be able to re-register with the Control Manager server.
- The location of the public encryption key of the Control Manager server with which you will register the agents

Obtaining the Public Encryption Key

All products that Control Manager manages are required to have a public encryption key to register and establish communications with the Control Manager server. Obtain the public encryption key with the Control Manager management console.

To obtain the public encryption key:

1. On any computer on the network, open a Web browser and type `http://{Control Manager Server Name}/ControlManager`, where `{Control Manager Server Name}` is the computer name or IP address of the Control Manager server.

   The **Welcome** screen of the Control Manager management console appears.

2. Type a user ID and password.
3. Click **Products**.
4. Click **Add/Remove Product Agents**.
5. Right-click the **Public encryption key**, then click **Save As**.
6. Save the public encryption key `E2EPublic.dat` to a location that is accessible to the PortalProtect server where the agent will be installed.

Installing the Control Manager Agent

After obtaining the public encryption key and storing it on the PortalProtect server, install the agent.

The following agent install methods are available:

- **The PortalProtect server master installer** – install the agent at the same time you install the PortalProtect server (see *Installing PortalProtect* on page 2-3)
- **The Control Manager Agent setup program** – use the remote install tool available from the Control Manager management console and on the PortalProtect Standard CD at the following location:

  `output/CMAgent/ControlManagerAgent Setup.exe`

To install the agent:

1. Do one of the following:
   - If installing with the PortalProtect master installer, when the **Select Components** screen appears, select the **Install Control Manager agent** check box. Later, the Control Manager agent installation screen appears.
   - If installing the control manager agent from the included CD, double click the
2. Type an existing ID for the Control Manager server. Trend Micro recommends using the root user ID.
3. Confirm the name of the PortalProtect server in the **Entity Name** field.
4. Click **Next**.
   If the installer does not detect any Control Manager installation (including Control Manager server or Control Manager agent) on the computer, the **Message Routing Path** screen appears.
   If the installer detects a Control Manager installation on the computer, a prompt appears asking you if you want to reconfigure the settings for the upgrade to the current version of Control Manager agent.
   - Click **No** to keep the original settings and complete the upgrade.
   - Click **Yes** to modify the settings. The **Setup Message Routing Path** screen appears.

   Note: When upgrading to the current version of Control Manager agent, you cannot modify the Control Manager account name associated with the agent. The installer preserves the account name used with the previous installation.
5. Specify a path for the incoming messages from the Control Manager server:
   - **Any host** – click to have the agent accept incoming messages from any host on the network.
   - **IP port forwarding** – click if incoming messages from the Control Manager server pass through a firewall or network device that uses port forwarding and type the device IP address, the port number the device listens at, and the port number to which it forwards messages.

- **Proxy server** – click if incoming messages route through a proxy server and click **Proxy Server Configuration** to configure the proxy server settings. The **Proxy Configuration** screen appears.

  i. Type the name of the proxy server, the port number it uses, and the type of protocol it supports (HTTP or SOCKS 4/5).

  ii. If the proxy server requires log on credentials, click the **Authentication required** text box and type the user name and password.

  iii. Click **OK** to return to the **Message Routing Path** screen.

6. Specify the route for outgoing messages:

   - **Route direct to server** – click if outgoing messages, which include commands, directly to the Control Manager server
   - **Proxy server** – click if outgoing messages route through a proxy server and click **Proxy Server Configuration** to configure the proxy server settings. The **Proxy Configuration** screen appears.

     i. Type the name of the proxy server, the port number it uses, and the type of protocol it supports (HTTP or SOCKS 4/5).

     ii. If the proxy server requires log on credentials, click the **Authentication required** text box and type the user name and password.

     iii. Click OK to return to the **Setup Message Routing Path** screen.

7. Click **Next**. The **Register with Control Manager** screen appears.
8. Click **Import** to select the public encryption key `E2EPublic.dat` you obtained from the Control Manager server (see see *Obtaining the Public Encryption Key* on page A-4).
9. Select the public encryption key and click **Open**. The Control Manager information appears under **Server Information**.
10. Click **Next**. When the installation is complete, a notification message appears.
11. Click **OK**.

Verifying a Successful Control Manager Agent

Installation

To verify a successful agent installation, access the Control Manager management console to see that the product has successfully registered with Control Manager and the Product Directory lists it as a managed product.

To verify a successful Control Manager agent installation:

1. Access the Control Manager management console.
2. Click **Products** on the main menu.
3. On the left-hand menu select **Managed Products** from the list, and then click **Go**.

Under the **New entity** folder in the Product Directory, the PortalProtect managed product icon appears.

If you do not see the ScanMail managed product, try the following:

1. Refresh the Product Directory. Click the **Refresh** icon on the upper right corner of the left-hand menu.
2. From the PortalProtect server, ping the Control Manager server to confirm that connection is functioning correctly.
3. Restart the Trend Micro Management Infrastructure service on the PortalProtect server.
4. Reinstall the Control Manager agent for PortalProtect (see *Installing the Control Manager Agent* on page A-4).

Accessing PortalProtect with Control Manager

The Control Manager agent for PortalProtect accepts commands from the Control Manager server and instructs PortalProtect to carry out actions. For example, when you click **Tasks** > **Deploy engines** on the Control Manager console, the agent instructs PortalProtect to deploy the latest scan engine.

To open the Control Manager console:

1. On any computer on the network, open a Web browser and type `http://{Control Manager server name}/ControlManager`, where

`{Control Manager server name}` can be the computer name or IP address of the Control Manager server.

The **Welcome** screen of the Control Manager console appears.

2. Click **Products**.
3. In the **Product Directory**, click the PortalProtect server to manage. The following tabs are displayed:
   - **Product Status** – view PortalProtect server information, such as the server name, the version numbers of components, the operating system used on the server machine, and Control Manager agent details
   - **Configuration** – access the PortalProtect Web console
   - **Tasks** – deploy the scan engine and virus pattern file, and replicate the configuration
   - **Logs** – view Control Manager event and security logs

Removing the Agent

You can easily remove the Trend Micro Control Manager agent for PortalProtect using the **Add/Remove Programs** function of Windows.

To remove the agent:

1. On the server where the agent is installed, click the **Start** menu and click **Settings** > **Control Panel > Add/Remove Programs**. The **Add/Remove Programs** window appears.
2. Click **Trend Micro Control Manager Agent for PortalProtect**, and then click **Change/Remove**. A confirmation screen appears.
3. Click **Yes**. Windows removes the agent from the server. When the agent is completely removed, click **OK**.

Index

T

U

V

W