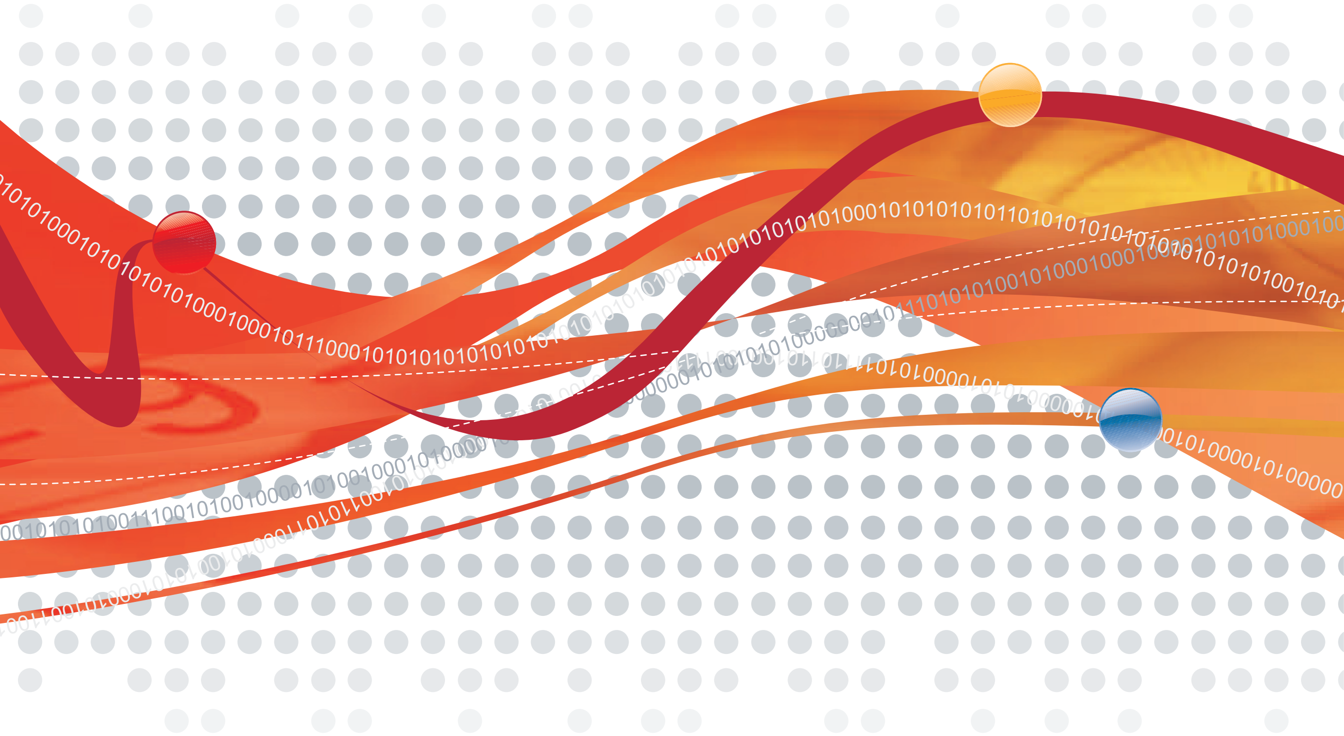
TREND MICRO™

PortalProtect²

Highly Effective Protection, Minimal IT Impact

for Microsoft™ SharePoint

Installation and Deployment Guide



Collaboration Security

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

www.trendmicro.com/download/

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

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

Document Part No. PPEM24426/100310

Release Date: June, 2010

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

The Installation and Deployment Guide for Trend Micro PortalProtect is intended to introduce the main features of the software and provide information to both prepare and install PortalProtect 2.0 in your production environment. You should read this guide completely before installing or using the software.

For technical support, please refer to Contacting Trend Micro in this Installation and Deployment 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

Preface

Chapter 1: Welcome to Trend Micro™ PortalProtect™

Chapter 2: Planning PortalProtect Installation and Upgrade

Chapter 3: Installing, Upgrading, and Removing PortalProtect

Chapter 4: Getting Support and Contacting Trend Micro

Appendix A: PortalProtect Database Permission Requirements

Preface

Preface

Welcome to the Trend Micro™ PortalProtect™ Installation and Upgrade Guide. This guide contains basic information about the tasks you need to perform to deploy PortalProtect to protecting your SharePoint servers. It is intended for novice and advanced users who want to plan, deploy, and test PortalProtect.

This preface discusses the following topics:

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

PortalProtect Documentation

PortalProtect documentation consists of the following:

- **Online Help**—Web-based documentation that is accessible from the product console. The Online Help contains explanations about PortalProtect features.
- **Installation and Deployment Guide (IG)**—PDF documentation that is accessible from the Solutions DVD for PortalProtect. It can also be downloaded from the Trend Micro Web site. This document contains instructions about deploying PortalProtect, a task that includes planning and testing.
- **Administrator's Guide**—Helps you configure all product settings.

- **Readme File**—Contains late-breaking product information that might not be found in the other documentation. Topics include a description of features, installation tips, known issues, and product release history.

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

Audience

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

Document Conventions

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

TABLE I-1. Conventions used in PortalProtect documentation

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and ScanMail tasks
`Monospace`	Examples, sample command lines, program code, and program output
Note:	Configuration notes
Tip:	Recommendations

TABLE I-1. Conventions used in PortalProtect documentation

CONVENTION	DESCRIPTION
WARNING!	Reminders on actions or configurations that should be avoided

Chapter 1

Welcome to Trend Micro™ PortalProtect™

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

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

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

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

PortalProtect 2.0 integrates with Trend Micro Control Manager 5.0 with support for the following services:

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

In this chapter, you will find information about:

What's New in PortalProtect 2.0

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

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

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

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

Web Reputation Filtering (see *Web Reputation Filtering* on page 1-5)

- Web Reputation scans URLs in Web content and applies configurable actions when malicious URLs are detected.

Microsoft Active Directory (AD) Integration

- This enhancement supports File Blocking policies and Content Filtering policies with Active Directory users and groups as an exception list.

SharePoint User(s)/Group(s) Integration

- This enhancement supports File Blocking policies and Content Filtering policies with SharePoint users and groups as an exception list.

Management Enhancements (see *Management Enhancements* on page 1-5)

- Supports Single Sign-On (SSO)
- Provides a Real-Time Monitor
- Server Management
- Quarantine Management

Installation Enhancements

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

SharePoint Versions

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

Windows Versions

- Windows 2003 Series

  Windows Server 2003, Standard Edition x86/x64

  Windows Server 2003, Enterprise Edition x86/x64

  Windows Server 2003 R2, Standard Edition x86/x64

  Windows Server 2003 R2, Enterprise Edition x86/x64
- Windows 2008 series

  Windows Server 2008 Standard Edition x86/x64

  Windows Server 2008 Enterprise Edition x86/x64

  Windows Server 2008 R2 Enterprise Edition x64

Windows Server 2008 R2 Standard Edition x64

Microsoft Windows Server 2008 Datacenter x64

Microsoft Windows Web Server 2008 x64

Microsoft Windows Server 2008 HPC x64

Supports both Local and Remote Installation

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

Installation with Remote SQL

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

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

The following SQL server versions are supported:

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

Content Filtering Scans

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

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

Web Reputation Filtering

Web reputation scans URLs contained in Web content and applies configurable actions when malicious URLs are detected. Additionally, this enhancement enables the user to select both manual and scheduled scans for Web Reputation.

Management Enhancements

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

Single Sign On (SSO)

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

Real-time Monitor

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

Server Management

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

Quarantine Management

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

Benefits and Capabilities

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

Fast and Simple Installation

- Install to a single or multiple SharePoint server(s) using a single installation program.

Powerful and Creative Antivirus Features

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

File Blocking

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

Content Filtering

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

Web Reputation

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

Data Loss Prevention

- Uses specially created templates to prevent Personally Identifiable Information (PII) from being posted to or retrieved from a document library, wiki, blog, discussion forum, and so on.

Quarantine

- Provides central quarantine management for quarantined files in one farm.

Manual and Scheduled Scan

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

Updates

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

Easy Management

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

How Viruses Infect SharePoint Environments

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

How PortalProtect Protects SharePoint Servers

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

- PortalProtect can scan files or Web content and determine whether any of that content violates a policy. When a violation is detected, PortalProtect will take an action like: quarantine or delete, as pre-configured by the administrator.
- PortalProtect can scan URL in Web content to detect malicious URL, it takes an action like: block or pass, as pre-configured by the administrator.
- PortalProtect can block files based on the file extension, file name, or true file type. When it detects a file type, it takes an action like: quarantine or delete, as pre-configured by the administrator.
- Scanning employs the latest version of the Trend Micro scan engine to detect viruses and other malicious code. When PortalProtect detects a virus or malicious code, it performs a number of actions like: quarantine or delete, according to how the administrator has it configured. The scan engine can maintain multiple threads, thus processing many requests simultaneously. It can also prioritize requests.

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

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

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

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

Scheduled Scan–Scans all or some of the files in your Document Library, depending on the configuration. You set the time and frequency of the scan. Scheduled Scan automates routine scans on your SharePoint servers, improves antivirus management efficiency, and gives you more control over your antivirus policy.

Trend Micro recommends you use a combination of scanning tasks to create a secure SharePoint environments. When you configure and perform a manual scan, it removes the threats from the content stored on the SQL Server content store. When you configure and enable real-time scanning, it protects your SharePoint servers from new threats as they arise. Finally, running regularly scheduled scans maintains a secure SharePoint environment.

PortalProtect Architecture

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

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

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

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

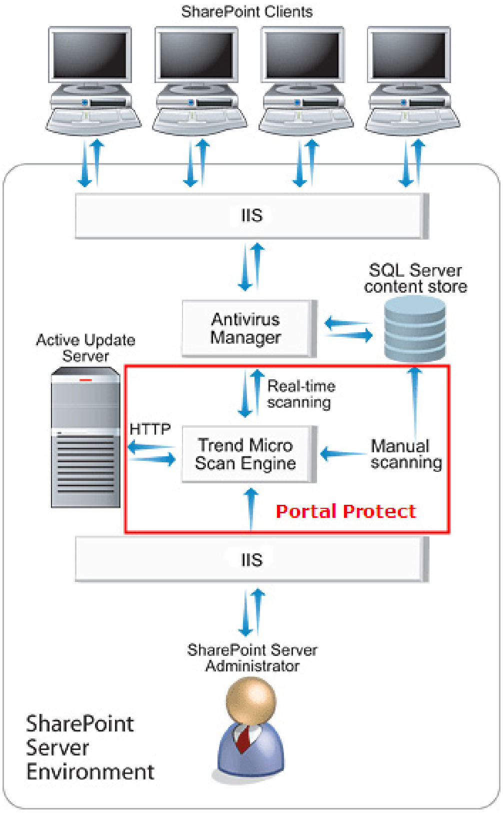


FIGURE 1-1. How PortalProtect interacts with SharePoint Server and SharePoint Services

PortalProtect Technology

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

About the Trend Micro Scan Engine

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

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

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

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

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

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

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

1. Frequent updates to the scan engine's data-file, called the virus pattern file, can be downloaded and read by the engine without the need for any changes to the engine code itself.

2. Technological upgrades in the engine software prompted by a change in the nature of virus threats, such as the rise in mixed-threats like SQL Slammer. In both cases, updates can be automatically scheduled, or the security administrator can handle them manually. International computer security organizations, including the International Computer Security Association (ICSA) annually certify the Trend Micro scan engine.

About Scan Engine Updates

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

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

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

http://www.trendmicro.com

About the Virus Pattern File

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

All Trend Micro antivirus programs using the ActiveUpdate function can detect the availability of a new virus pattern on the Trend Micro server, and/or you can set it to automatically poll the server every week, day, or hour to get the latest file. Trend Micro recommends that you schedule automatic updates at least daily, which is the default setting for PortalProtect. Whether performed in the background or on-demand, the pattern file updates without interrupting users or network traffic.

You can manually download virus pattern files from the following Web site, where you can also find the current version, release date, and a list of all the new viruses definitions included in the file.

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

How Scanning Works

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

Pattern File Numbering

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

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

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

   For the file pattern number 1.786.01:

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

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

About ActiveUpdate

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

Incremental Updates of the Virus Pattern File

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

Using ActiveUpdate with PortalProtect

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

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

About Trend Micro IntelliScan™

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

IntelliScan is a Trend Micro technology that identifies a file's *true file type*, regardless of the file extension name. IntelliScan uses a method that can identify which files to scan and is more efficient than the Scan All files option.

Note: IntelliScan examines the header of every file, but based on certain indicators, selects only files that it determines are susceptible for security risk scanning.

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

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

True File Types

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

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

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

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

About IntelliTrap

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

IntelliTrap uses the following components:

- Virus Scan Engine
- IntelliTrap Pattern
- IntelliTrap Exception Pattern

Trend Micro™ ActiveAction™

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

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

Using ActiveAction provides the following benefits:

- **Time saving and easy to maintain**—ActiveAction uses scan actions recommended by Trend Micro. You do not have to spend time configuring the scan actions.
- **Updateable scan actions**—Virus/malware writers constantly change the way viruses/malware attack computers. Trend Micro updates ActiveAction settings in each new pattern file to protect clients against the latest threats and the latest methods of virus/malware attacks.

Controlling Outbreaks

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

- Use PortalProtect notifications to create an early warning for your administrator or IT professionals.
- Use **Update Now** to immediately download the latest virus pattern file and scan engine. Configure and run a manual scan and set PortalProtect to take action against any viruses. For fast and efficient action, select features such as IntelliScan and ActiveAction and PortalProtect will use Trend Micro recommended blocks and actions against viruses.
- Set the blocking options for manual or real-time scanning to detect a specific file type or name. Set an action like: block or quarantine for PortalProtect to take action on a file type or file name to prevent it from infecting your SharePoint servers.

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

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

- Configure real-time scanning and set PortalProtect to take action against any viruses it detects. For fast and efficient action, select features such as IntelliScan and ActiveAction and PortalProtect will use Trend Micro recommended blocks and actions against viruses.
- Generate reports and make log queries to analyze the results of your counter-actions. Identify the sources and vectors of infection on your SharePoint servers.

Maintenance Agreement

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

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

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

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

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

Renewing Your Maintenance Agreement

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

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

Chapter 2

Planning PortalProtect Installation and Upgrade

This section lists the minimum system requirements and the steps needed to prepare for the PortalProtect installation. It also provides information about basic upgrading issues and suggestions about various PortalProtect features. This chapter includes information about:

- *System Requirements* starting on page 2-2
- *Deployment Strategy* starting on page 2-3
- *Preparing for Installation* starting on page 2-6

System Requirements

You need the following to effectively run PortalProtect 2.0:

Hardware/Software	Requirement	Recommended
Processor	Server with processor speed of 2.5-GHz (32-bit or 64-bit)	Dual processor, 3-GHz or greater (32-bit or 64-bit)
Memory	2-GB RAM	4-GB RAM
Disk Space	2-GB free disk space	5-GB free disk space
Windows Server	• Windows Server 2003, Standard Edition X86/X64 • Windows Server 2003, Enterprise Edition X86/X64 • Windows Server 2003 R2, Standard Edition X86/X64 • Windows Server 2003 R2, Enterprise Edition X86/X64 • Windows Server 2008 Standard Edition X86/X64 • Windows Server 2008 Enterprise Edition X86/X64 • Windows Server 2008 R2 Enterprise Edition X64 • Windows Server 2008 R2 Standard Edition X64 • Microsoft Windows Server 2008 Datacenter X64 • Microsoft Windows Web Server 2008 X64 • Microsoft Windows Server 2008 HPC X64	
SharePoint Service / Server	• Windows SharePoint Service 3.0 X32/X64 • Microsoft Office SharePoint Server 2007 Standard / Enterprise X32/X64 • Windows SharePoint Service 4.0 X64 • Microsoft Office SharePoint Server 2010 Standard / Enterprise X64	
Web Server	• Microsoft Internet Information Services (IIS) 6.0 • Microsoft Internet Information Services (IIS) 7.0	
Browser	• Microsoft Internet Explorer 6.0 or above • Mozilla Firefox 3.0 or above	

You need the following to effectively run the CM agent:

- PortalProtect 2.0 CM server 5.0 with Patch 3 + Hotfix 1760

Deployment Strategy

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

Note: PortalProtect is installed to servers that are running the Web application servers (services), also called the Web front-end servers.

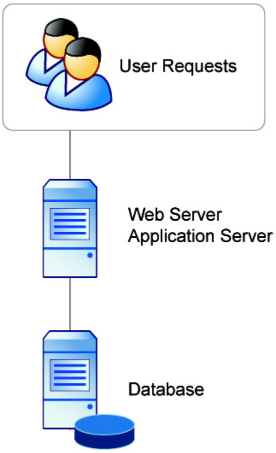


FIGURE 2-1. Small server farm configuration

SharePoint Services Medium Server Farm

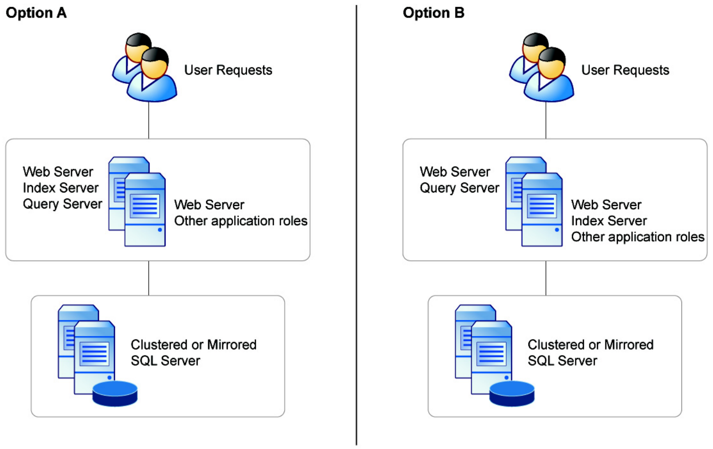


FIGURE 2-2. Medium server farm

SharePoint Services Large Server Farm

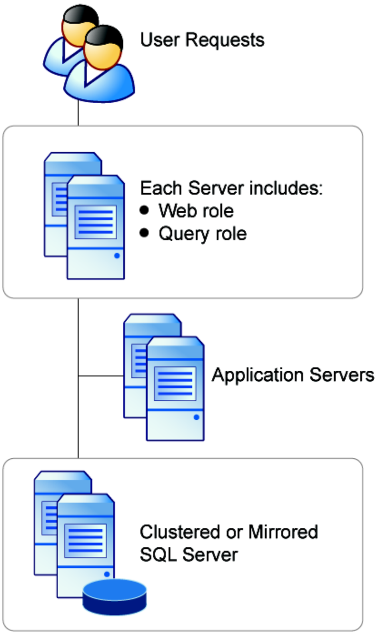


FIGURE 2-3. Large server farm configuration

Preparing for Installation

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

- Install PortalProtect 2.0 to a server with the appropriate server platforms installed; see *System Requirements* starting on page 2-2 for more information. Microsoft Internet Information Services (IIS) is a required for a successful installation.
- **Registration Key/Activation Code**. During installation, the setup program prompts for an Activation Code. Use the Registration Key that came with PortalProtect to obtain an Activation Code online from the Trend Micro Web site. The setup program provides a link to the Trend Micro Web site.
- **Privileges for Installation**. During installation, the account to launch the setup program must have local administrator privileges to where you launch the setup program and this account must have local administrator privilege to all the target servers where you plan to install PortalProtect. If PortalProtect 2.0 is installed in a farm environment, a domain account must be used as the administrator.

Tip: Trend Micro strongly suggests our customers use the local installation method.

- **Privileges for PP Configuration Database:** If your installation requires you to auto-create the PortalProtect configuration database:
  - ◆ Connect to the database with a minimum user privilege of dbcreator.
  - ◆ If the PortalProtect configuration database already exists, only read/write access is required. See *PortalProtect Database Permission Requirements* on page A-1for more information.
- **Proxy information**. During installation, the setup program prompts for proxy information. If a proxy server handles Internet traffic on your network, you must type the proxy server information, user name, and password to receive virus pattern file and scan engine updates. If you do not enter proxy information during installation, you can configure it later from the Administration menu.
- **Management group**. During installation, the setup program prompts for management group selection. Select an existing Active Directory group for management and the setup program will grant this group permission to manage PortalProtect. Users in this group may log on to the PortalProtect Web management console.

Manually Create PortalProtect Configuration Database

Note: This section applies only to users who are unable to grant permission to the database role **dbcreator** for the PortalProtect Configuration Database Access Account.

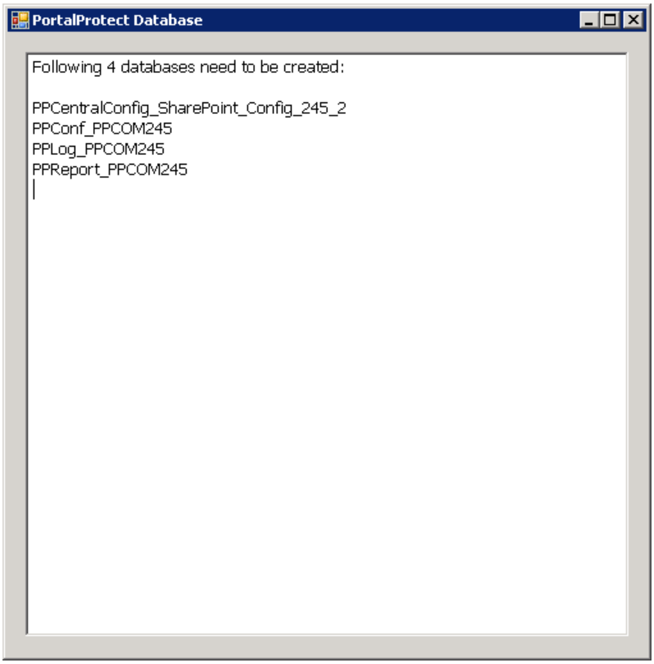
The PortalProtect configuration database account must have a server role **dbcreator** to create the PortalProtect configuration databases. If the configuration database account does not have a **dbcreator** role, PortalProtect provides support to manually create PortalProtect Configuration Databases, and then launches the PortalProtect setup program.

Note: When the setup program finds existing PortalProtect databases, it will not try to create them again.

To manually create PortalProtect Configuration Databases:

1. From a SharePoint server, open the setup package folder: ***tool\PreCreatePortalProtectDatabases\SharePoint2007***.
2. Run the executable file: ***toolListPortalProtectDatabase.exe***. After you run the executable, a screen similar to the one shown in *Figure 2-4* appears.

   Note: For SharePoint 2010 users, the executable path is: ***tool\PreCreatePortalProtectDatabases\SharePoint2010)***



```
Following 4 databases need to be created:

PPCentralConfig_SharePoint_Config_245_2
PPConf_PPCOM245
PPLog_PPCOM245
PPReport_PPCOM245
```

FIGURE 2-4. PortalProtect Database add screen

3. Create the databases as directed by **ToolListPortalProtectDatabase.exe** (*Figure 2-4*).

Note: ToolListPortalProtect.exe enumerates each SharePoint front-end server, and assumes it will be installed as a front-end server.

WARNING! **If SharePoint is installed with a database account that uses Windows Authentication, and PortalProtect SharePoint Database Access Account is configured using SQL Server Authentication, then the PortalProtect Content Filtering feature will not function. To resolve, you must specify the PortalProtect SharePoint Database Access Account to use Windows Authentication when installing PortalProtect.**

Chapter 3

Installing, Upgrading, and Removing PortalProtect

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

Administrators can easily install PortalProtect to a local server or 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:

- *Performing a Fresh Installation* starting on page 3-2
- *Upgrading to PortalProtect 2.0* on page 3-21
- *Migrating to PortalProtect 2.0* starting on page 3-33
- *Post Installation* starting on page 3-47
- *Testing Your Installation* starting on page 3-49
- *Removing PortalProtect* starting on page 3-49

Performing a Fresh Installation

Tip: Before installing PortalProtect 2.0, be sure to review the "Known Issues" contained in the Readme document.

You can install PortalProtect in two ways:

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

Setup.exe Installation

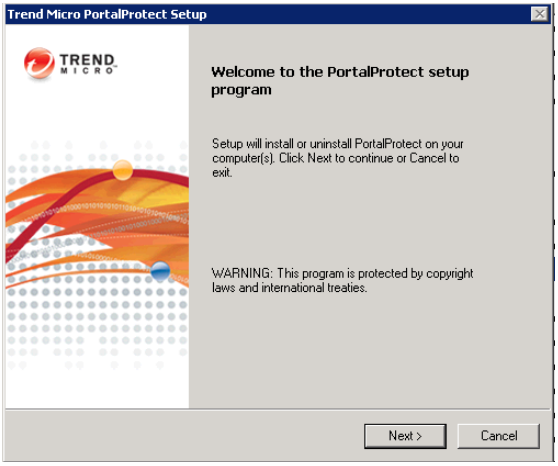
PortalProtect provides a user-friendly installation program, which can be used for both local and remote installation. The setup program enables you to install PortalProtect on one or many servers and rapidly deploy it to all SharePoint servers in your enterprise.

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

Note: You must install PortalProtect on a server that matches the system requirements stipulated in this GSG (see *Performing a Fresh Installation* starting on page 3-2). A successful installation also requires IIS 7.0 and Internet Explorer 6.0.

To perform a fresh installation:

1. Run `setup.exe` from the PortalProtect 2.0 CD to start the installation. The **PortalProtect Installation Welcome** screen appears.



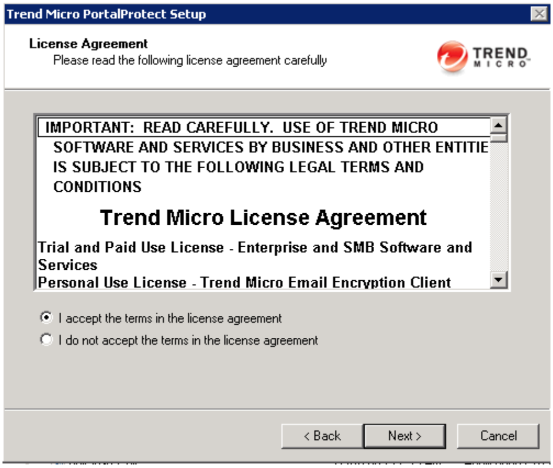
Welcome to the PortalProtect setup program

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

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

FIGURE 3-1. PortalProtect Installation Welcome screen

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



Trend Micro PortalProtect Setup

License Agreement
Please read the following license agreement carefully

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

Trend Micro License Agreement

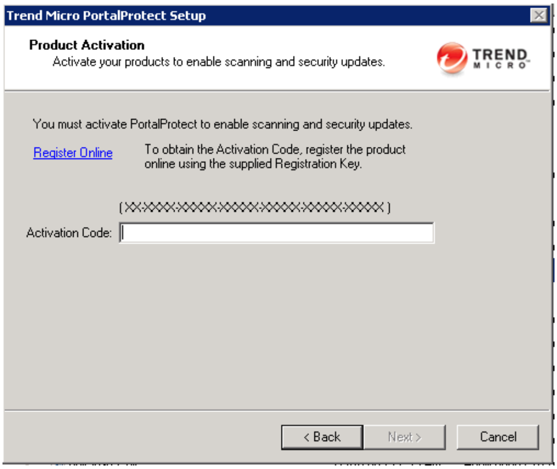
Trial and Paid Use License - Enterprise and SMB Software and Services
Personal Use License - Trend Micro Email Encryption Client

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

FIGURE 3-2. License Agreement screen

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 appears.



Trend Micro PortalProtect Setup

Product Activation

Activate your products to enable scanning and security updates.

You must activate PortalProtect to enable scanning and security updates.

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

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

Activation Code:

FIGURE 3-3. Product Activation screen

Product Activation requires two steps:

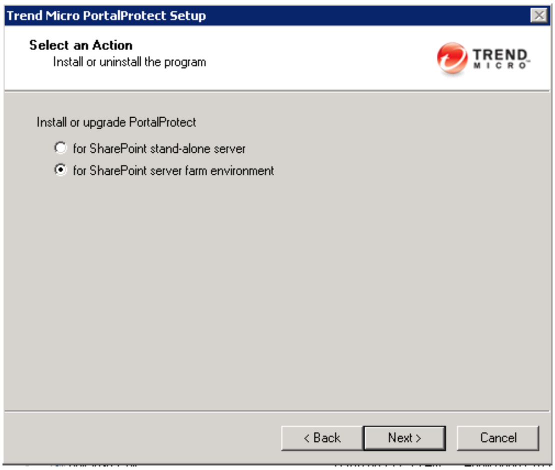
a. You must register PortalProtect online to receive an Activation Code. Click **Register Online**. This opens the Trend Micro online registration Web page in your browser. Follow the prompts to complete the registration. When you have registered, Trend Micro sends you an Activation Code via e-mail.

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

4. The **Select an Action** screen appears. Select from the following options:
   - **for SharePoint stand-alone server**
   - **for SharePoint server farm environment**

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

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



Trend Micro PortalProtect Setup

Select an Action

Install or uninstall the program

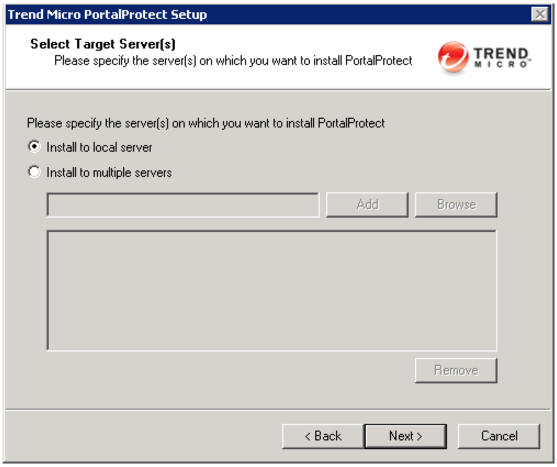
Install or upgrade PortalProtect

○ for SharePoint stand-alone server

● for SharePoint server farm environment

FIGURE 3-4. Select an Action screen

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



Trend Micro PortalProtect Setup

Select Target Server(s)

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

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

● Install to local server

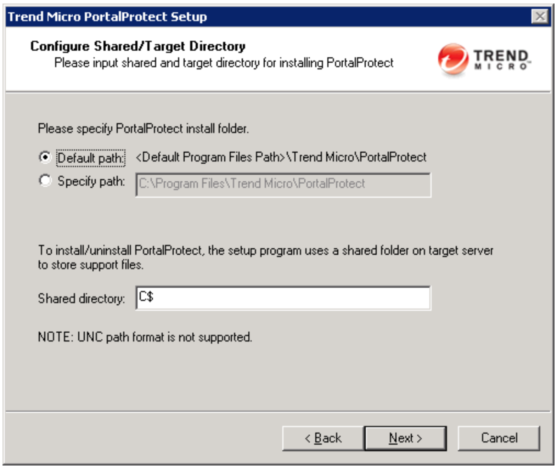
○ Install to multiple servers

FIGURE 3-5. Select Target Server(s) screen

Select from the following options:

- **Install to local server** (recommended)—use to install to a local server. After selecting, click **Next** > to continue the installation.
- **Install to multiple servers** (remote installation)—select and choose the target servers to which you want to install PortalProtect. Type or **Browse** for the **Computer name**, and **Add** one or more servers. When you are satisfied with the list of target servers, click **Next** > to continue the installation. You will be prompted to enter your remote server logon account information.

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



Trend Micro PortalProtect Setup

Configure Shared/Target Directory
Please input shared and target directory for installing PortalProtect

Please specify PortalProtect install folder.

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

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

Shared directory: C$

NOTE: UNC path format is not supported.

FIGURE 3-6. Configure Shared/Target Directory screen

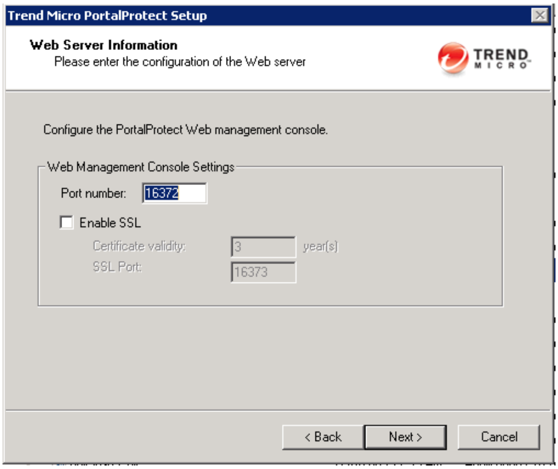
Accept the default path for the shared folder on the target server, or type a new path in the **Specify path** field. Click **Next >**.

WARNING! You must enter English-only characters in the Specify path field otherwise the installation will be unsuccessful.

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

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

7. The **Web Server Information** screen appears.


Trend Micro PortalProtect Setup

Web Server Information

Please enter the configuration of the Web server

Configure the PortalProtect Web management console.

Web Management Console Settings

Port number: 16372

□ Enable SSL

Certificate validity: 3 year(s)

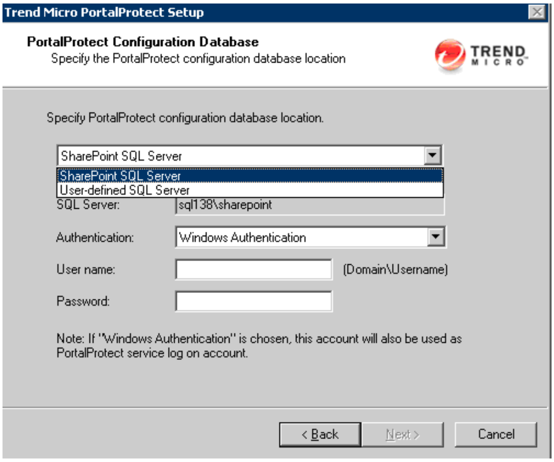
SSL Port: 16373

FIGURE 3-7. Web Server Information screen

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

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

8. The **PortalProtect Configuration Database** screen appears.



Trend Micro PortalProtect Setup

PortalProtect Configuration Database

Specify the PortalProtect configuration database location

Specify PortalProtect configuration database location.

SharePoint SQL Server

SharePoint SQL Server
User-defined SQL Server

SQL Server: sql138\sharepoint

Authentication: Windows Authentication

User name: (Domain\Username)

Password:

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

FIGURE 3-8. PortalProtect Configuration Database screen

Select from the following options:

- **Specify PortalProtect configuration database location**:
  - i. **SharePoint SQL Server**—installs PortalProtect to a SharePoint SQL server
  - ii. **User-defined SQL Server**—installs PortalProtect to a user-defined SQL server

---

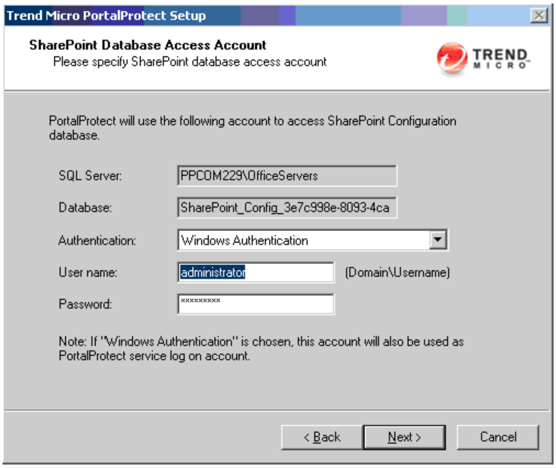
Note: To automatically create the PortalProtect configuration database, you must perform this installation from an account with dbcreator permission privilege. If the dbcreator role is not available, see *PortalProtect Database Permission Requirements* on page A-1 and *Manually Create PortalProtect Configuration Database* on page 2-7.

- **Authentication**—choose from Windows Authentication or SQL Server Authentication

Note: Trend Micro strongly suggests using Windows Authentication.

- **User name**—type as required
- **Password**—type as required

9. Click **Next >**. The **SharePoint Database Access Account** screen appears.



Trend Micro PortalProtect Setup

SharePoint Database Access Account

Please specify SharePoint database access account

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

SQL Server: PPCOM229\OfficeServers

Database: SharePoint_Config_3e7c998e-8093-4ca

Authentication: Windows Authentication

User name: administrator (Domain\Username)

Password: *********

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

FIGURE 3-9. SharePoint Database Access Account screens

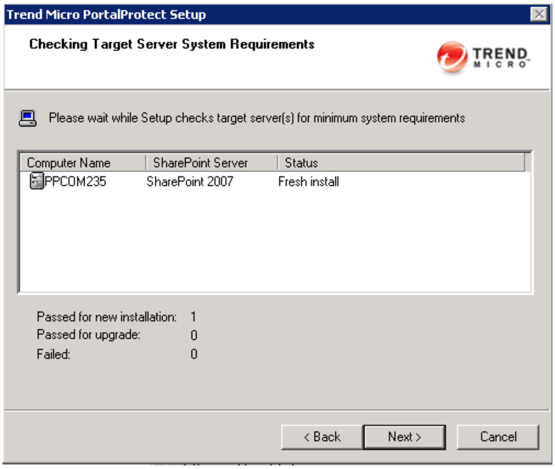
Note: If you choose to install or upgrade to a SharePoint standalone server, the installation/upgrade will skip the **Database Access Account** screen.

Verify and select from the following options:

- **SQL Server**—verify the listing is correct; click < Back to change.
- **Database**—verify the listing is correct; click < Back to change.
- **Authentication**—choose from Windows Authentication or SQL Server Authentication

Note: Trend Micro strongly suggests using Windows Authentication.

10. Click **Next >**. The **Checking Target Server System Requirements** screen appears.



Checking Target Server System Requirements

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

Computer Name	SharePoint Server	Status
PPCOM235	SharePoint 2007	Fresh install

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

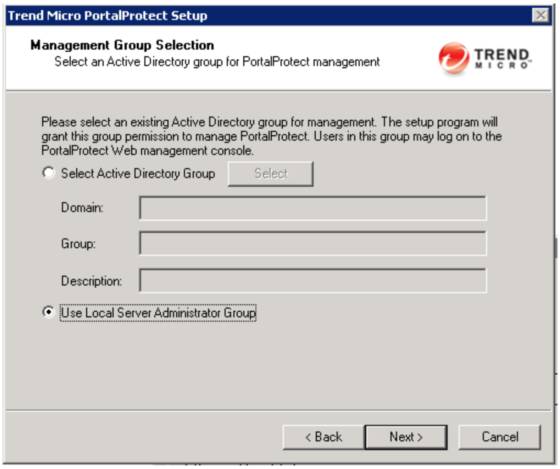
FIGURE 3-10. Checking Target Server System Requirements screen

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

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

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

11. The **Management Group Selection** screen appears.



Trend Micro PortalProtect Setup

Management Group Selection

Select an Active Directory group for PortalProtect management

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

○ Select Active Directory Group [Select]

Domain:

Group:

Description:

● Use Local Server Administrator Group

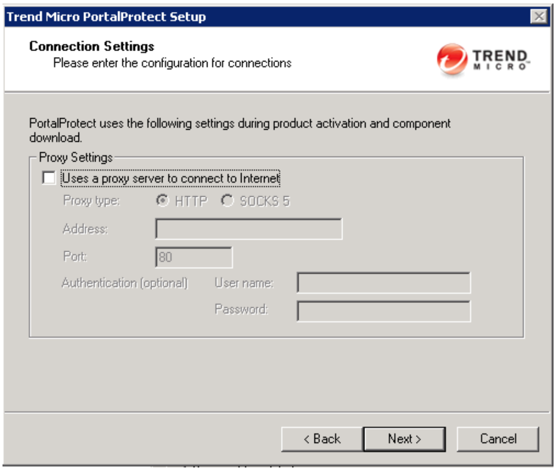
FIGURE 3-11. Management Group Selection screen

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

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

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

12. Click **Next >**.
13. The **Connection Settings** screen appears.



Trend Micro PortalProtect Setup

Connection Settings

Please enter the configuration for connections

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

Proxy Settings

☐ Uses a proxy server to connect to Internet

Proxy type: ● HTTP ○ SOCKS 5

Address:

Port: 80

Authentication (optional) User name:

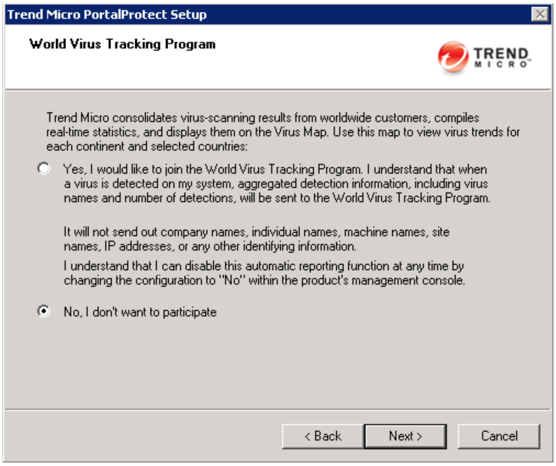
Password:

FIGURE 3-12. Connection Settings screen

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

- **Proxy type**—(HTTP or SOCKS 5)
- **Address**—(IP)
- **Port**—(Port number)
- If your proxy server requires a password, type the **User name** and **Password** in the fields provided.

14. Click **Next >**.
15. The **World Virus Tracking Program** screen appears.



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

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

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

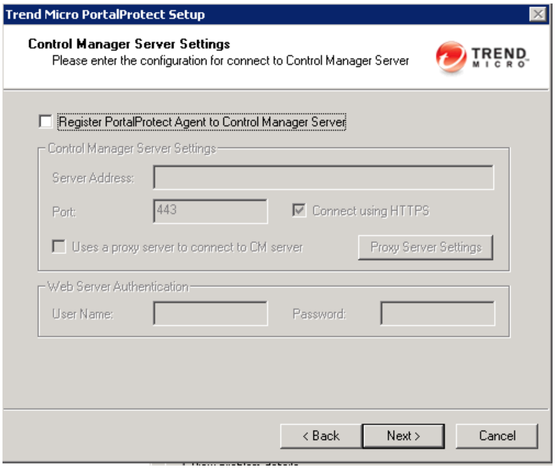
I understand that I can disable this automatic reporting function at any time by changing the configuration to "No" within the product's management console.

● No, I don't want to participate

FIGURE 3-13. World Virus Tracking Program screen

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

16. The **Control Manager Server Settings** screen appears.



Control Manager Server Settings

Please enter the configuration for connect to Control Manager Server

□ Register PortalProtect Agent to Control Manager Server

Control Manager Server Settings

Server Address:

Port: 443

☑ Connect using HTTPS

□ Uses a proxy server to connect to CM server

Web Server Authentication

User Name:

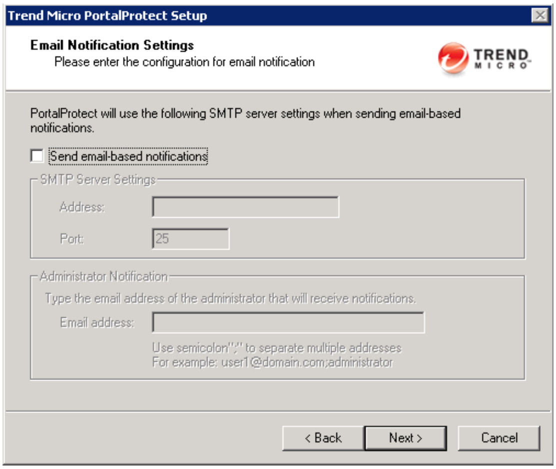
Password:

FIGURE 3-14. Control Manager Server Settings screen

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

- **Server Address**
- **Port**—Port number
- **Connect using HTTPS**—(if desired).
- If a proxy server is used, select **Uses a proxy server to connect to CM server**, and click **Proxy Server Settings** to modify. Refer to the Administrator's Guide for more information.
- If **Web Server Authentication** is required, type the **User Name** and **Password**.
- Click **Next >**.

17. The **Email Notification Settings** screen appears.



Trend Micro PortalProtect Setup

Email Notification Settings

Please enter the configuration for email notification

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

□ Send email-based notifications

SMTP Server Settings

Address:

Port: 25

Administrator Notification

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

Email address:

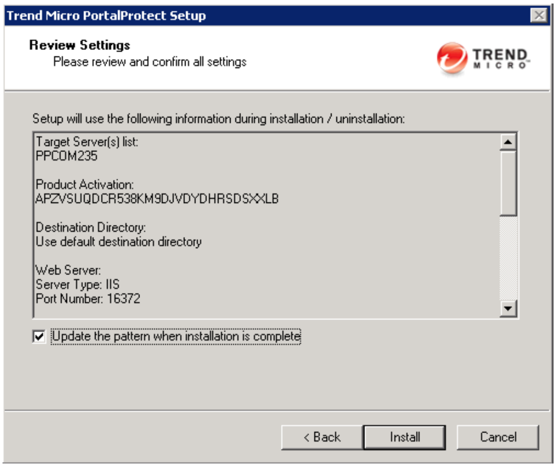
Use semicolon";" to separate multiple addresses
For example: user1@domain.com;administrator

FIGURE 3-15. Email Notification Settings screen

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

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

18. The **Review Settings** screen appears.



Review Settings

Please review and confirm all settings

Setup will use the following information during installation / uninstallation:

Target Server(s) list:
PPCOM235

Product Activation:
APZVSUQDCR538KM9DJVDYDHRSDSXXLB

Destination Directory:
Use default destination directory

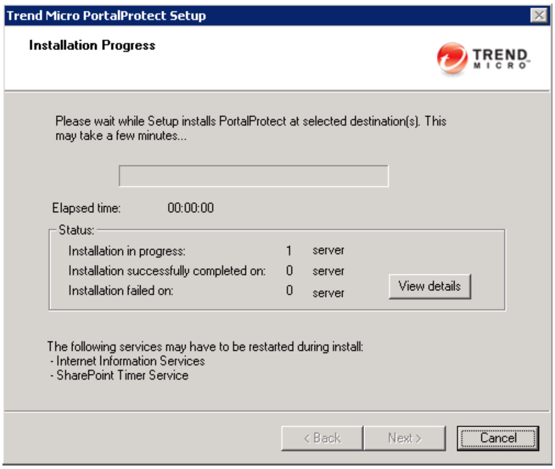
Web Server:
Server Type: IIS
Port Number: 16372

☑ Update the pattern when installation is complete

FIGURE 3-16. Review Settings screen

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

19. The **Installation Progress** screen displays.



Trend Micro PortalProtect Setup

Installation Progress

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

Elapsed time: 00:00:00

Status:

Installation in progress: 1 server

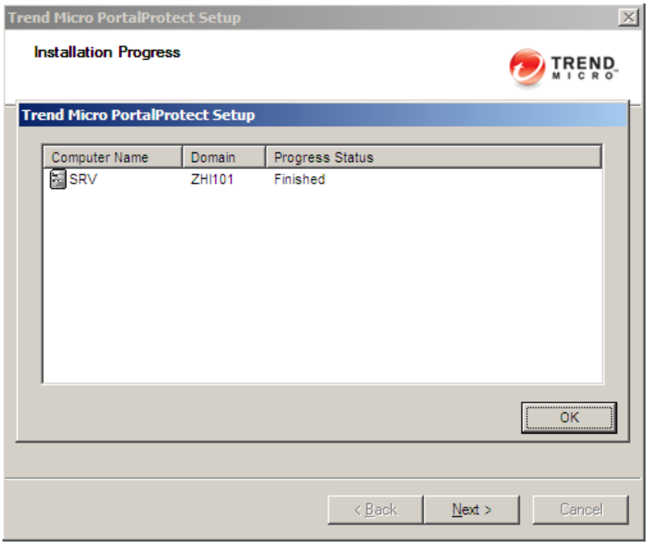
Installation successfully completed on: 0 server

Installation failed on: 0 server

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

FIGURE 3-17. Installation Progress screen

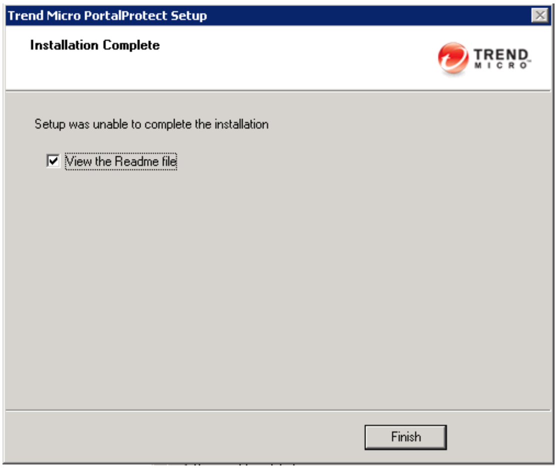
20. While the installation is active, click **View details** to check the status (see Figure 3-18.


Trend Micro PortalProtect Setup
Installation Progress
TREND MICRO
Trend Micro PortalProtect Setup
OK
< Back
Next >
Cancel

Computer Name	Domain	Progress Status
SRV	ZHI101	Finished

FIGURE 3-18. Installation progress status (Finished)

21. After the installation status displays **Finished**, click **Next >**.
22. The **Installation Complete** screen appears.



Trend Micro PortalProtect Setup

Installation Complete

Setup was unable to complete the installation

☑ View the Readme file

FIGURE 3-19. Installation Complete screen

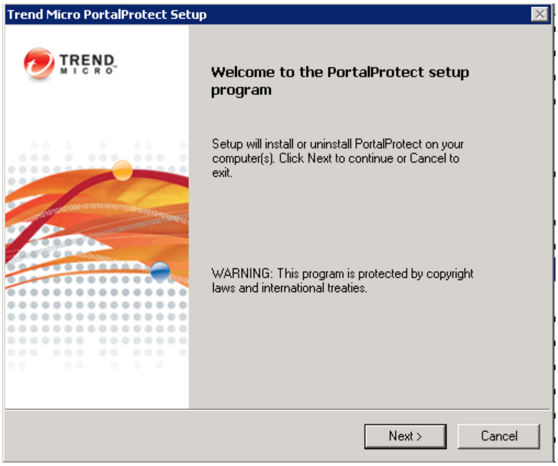
23. Select **View the Readme file**, if you wish to view it, and **Finish** to complete the installation.

Upgrading to PortalProtect 2.0

PortalProtect 2.0 supports upgrading from the previous builds of PortalProtect 2.0. This section describes the steps required to perform this kind of upgrade.

To upgrade PortalProtect 2.0 to a new build:

1. Run **setup.exe** from the PortalProtect 2.0 CD to start the installation. The **PortalProtect Installation Welcome** screen appears.



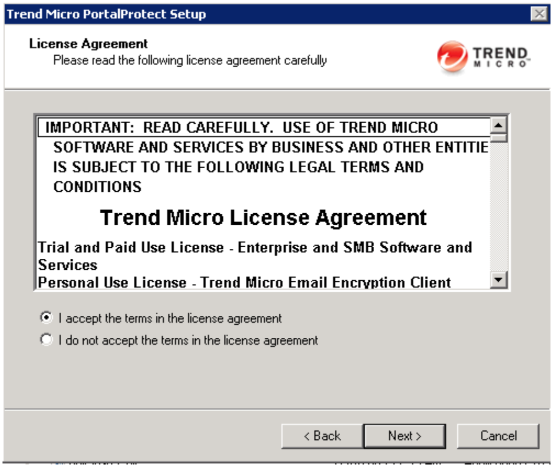
Welcome to the PortalProtect setup program

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

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

FIGURE 3-20. PortalProtect installation welcome screen

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



Trend Micro PortalProtect Setup

License Agreement

Please read the following license agreement carefully

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

Trend Micro License Agreement

Trial and Paid Use License - Enterprise and SMB Software and Services

Personal Use License - Trend Micro Email Encryption Client

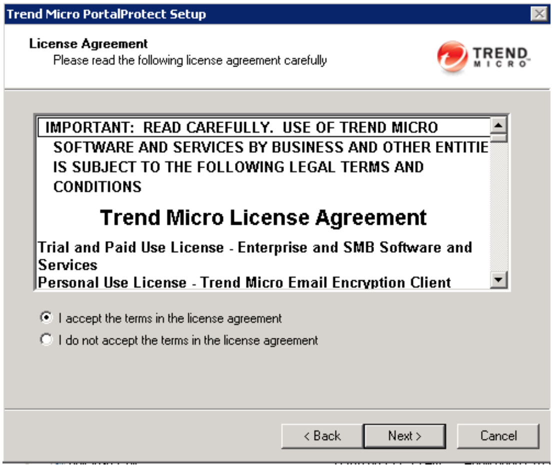
● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

FIGURE 3-21. License Agreement screen

Read the license agreement. If you accept the terms, select **I accept the terms in the license agreement** and click **Next>**. If you do not accept the terms, click **Cancel** to exit the setup program.

3. Click **Next** >. The **License Agreement** screen appears.



Trend Micro PortalProtect Setup

License Agreement

Please read the following license agreement carefully

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

Trend Micro License Agreement

Trial and Paid Use License - Enterprise and SMB Software and Services

Personal Use License - Trend Micro Email Encryption Client

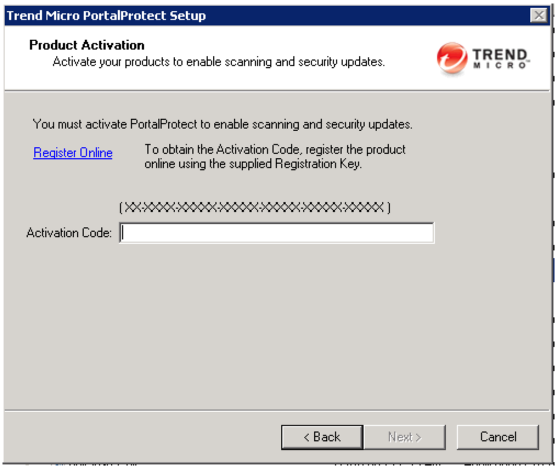
● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

FIGURE 3-22. License Agreement screen

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.

4. The **Product Activation** screen appears.



Trend Micro PortalProtect Setup

Product Activation

Activate your products to enable scanning and security updates.

You must activate PortalProtect to enable scanning and security updates.

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

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

Activation Code:

FIGURE 3-23. Product Activation screen

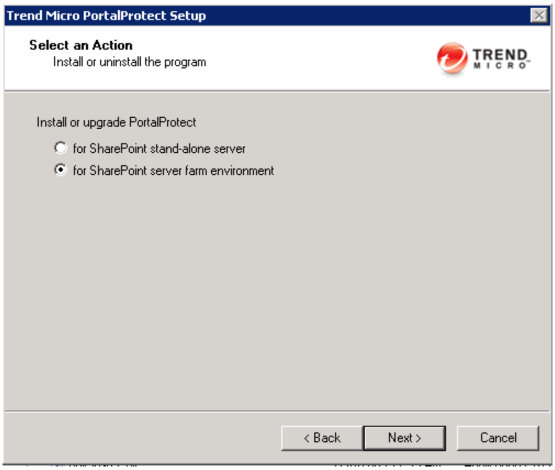
Product Activation requires two steps:

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

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

5. The **Select an Action** screen appears. Select from the following options:
   - **for SharePoint stand-alone server**
   - **for SharePoint server farm environment**

Note: Whether to select install **for SharePoint stand-alone server** or install **for SharePoint server farm environment** depends on your SharePoint deployment mode.



Select an Action

Install or uninstall the program

Install or upgrade PortalProtect

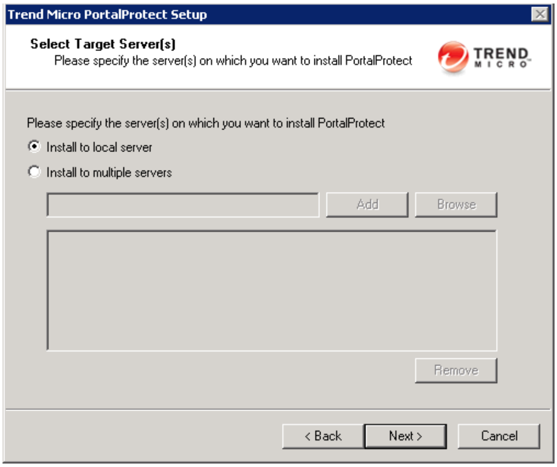
○ for SharePoint stand-alone server

● for SharePoint server farm environment

FIGURE 3-24. Select an Action screen

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

6. The **Select Target Server(s)** screen appears.



Trend Micro PortalProtect Setup

Select Target Server(s)

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

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

● Install to local server

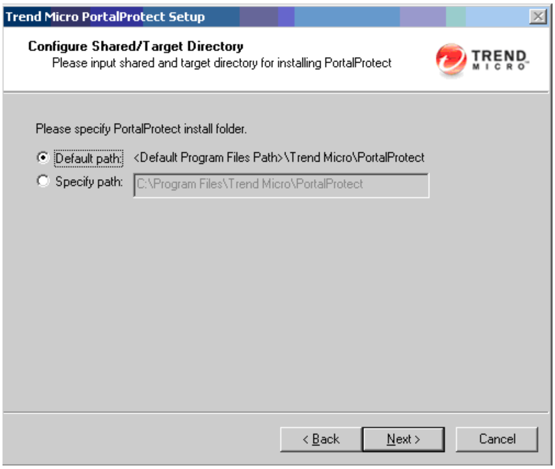
○ Install to multiple servers

FIGURE 3-25. Select Target Server(s) screen

Select from the following options:

- **Install to local server** (recommended)—use to install to a local server. After selecting, click **Next** > to continue the installation.
- **Install to multiple servers** (remote installation)—select and choose the target servers to which you want to install PortalProtect. Type or **Browse** for the **Computer name**, and **Add** one or more servers. When you are satisfied with the list of target servers, click **Next** > to continue the installation. You will be prompted to enter your remote server logon account information.

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



Configure Shared/Target Directory

Please input shared and target directory for installing PortalProtect

Please specify PortalProtect install folder.

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

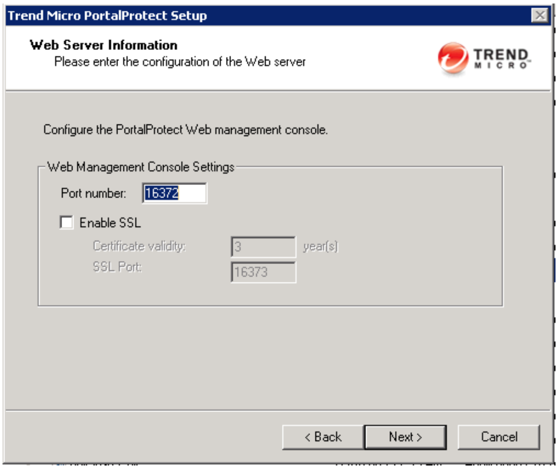
○ Specify path: C:\Program Files\Trend Micro\PortalProtect

FIGURE 3-26. Configure Shared/Target Directory screen

Note: If you specify a different PortalProtect installation path from the previous version, PortalProtect will still install to the path defined in the previous version.

Select the appropriate path and click **Next>**.

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


Trend Micro PortalProtect Setup

Web Server Information

Please enter the configuration of the Web server

Configure the PortalProtect Web management console.

Web Management Console Settings

Port number: 16372

□ Enable SSL

Certificate validity: 3 year(s)

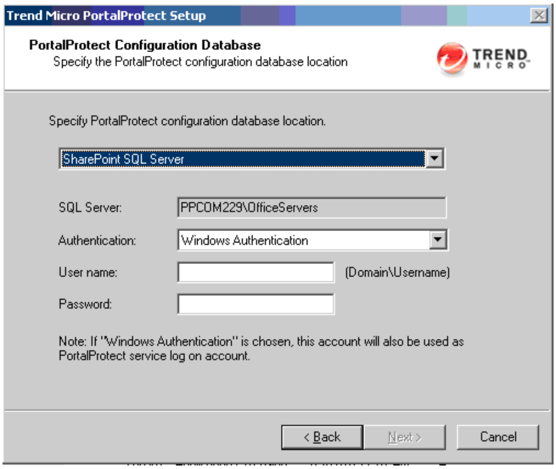
SSL Port: 16373

FIGURE 3-27. Web Server Information screen

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

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

9. The **PortalProtect Configuration Database** screen appears.



PortalProtect Configuration Database
Specify the PortalProtect configuration database location

Specify PortalProtect configuration database location.

SharePoint SQL Server

SQL Server: PPCOM229\OfficeServers

Authentication: Windows Authentication

User name: (Domain\Username)

Password:

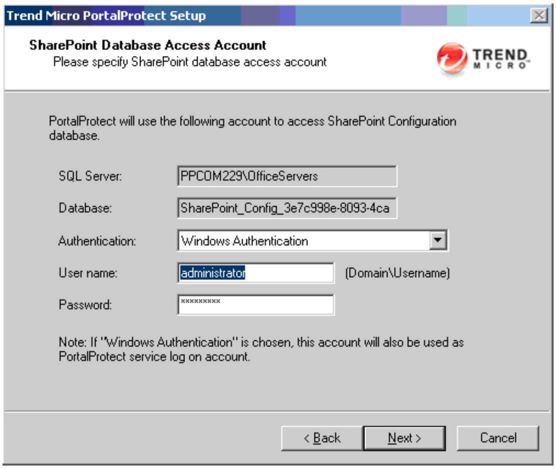
Note: If "Windows Authentication" is chosen, this account will also be used as PortalProtect service log on account.

FIGURE 3-28. PortalProtect Configuration Database screen

Specify the same PortalProtect configuration database information as was used in the previous installation. This includes:

- **SQL Server**
- **Authentication**
- **User name**
- **Password**

10. Click **Next >**. The **SharePoint Database Access Account** screen appears.



SharePoint Database Access Account
Please specify SharePoint database access account

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

SQL Server: PPCOM229\OfficeServers

Database: SharePoint_Config_3e7c998e-8093-4ca

Authentication: Windows Authentication

User name: administrator (Domain\Username)

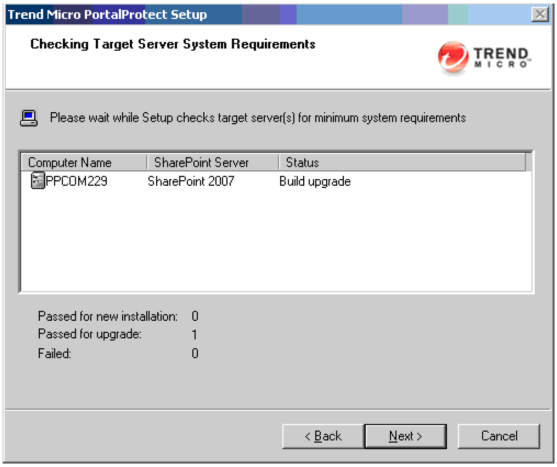
Password: *********

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

FIGURE 3-29. SharePoint Database Access Account screens

Specify the same SharePoint database information as was selected in the previous installation.

11. Click **Next >**. The **Checking Target Server System Requirements** screen appears.



Trend Micro PortalProtect Setup

Checking Target Server System Requirements

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

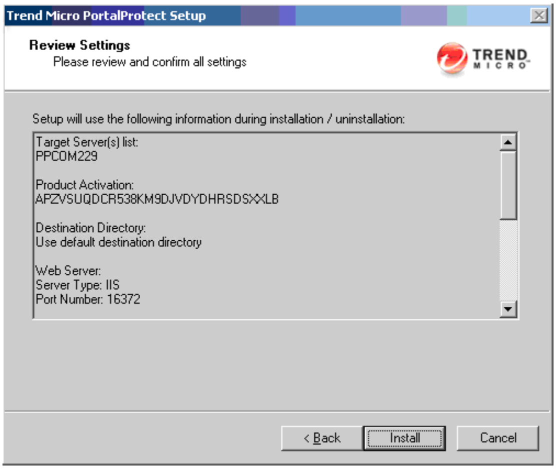
Computer Name	SharePoint Server	Status
PPCOM229	SharePoint 2007	Build upgrade

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

FIGURE 3-30. Checking Target Server System Requirements screen

The installation program then analyzes the systems. Verify the Status reads **Build upgrade**, and click **Next >**.

12. The **Review Settings** screen appears. Click **Install** to start the upgrade.


Trend Micro PortalProtect Setup
Review Settings
Please review and confirm all settings
TREND MICRO

Setup will use the following information during installation / uninstallation:

Target Server(s) list:
PPCOM229

Product Activation:
APZVSUQDCR538KM9DJVDYDHRSDSXXLB

Destination Directory:
Use default destination directory

Web Server:
Server Type: IIS
Port Number: 16372

FIGURE 3-31. Review Settings screen

Migrating to PortalProtect 2.0

PortalProtect 2.0 provides a configuration migration tool to export settings to PortalProtect 2.0. This PortalProtect 2.0 migration tool supports **exporting** settings from the following versions:

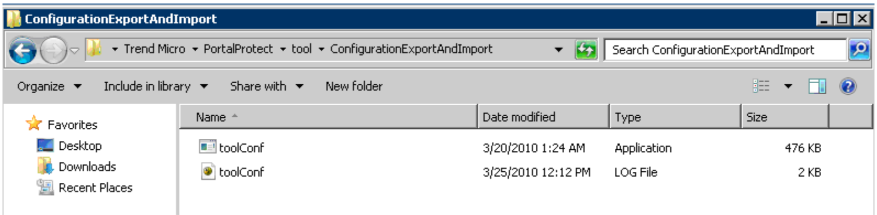
- PortalProtect 1.7
- PortalProtect 1.8
- PortalProtect 2.0

PortalProtect supports **importing** settings to the following versions:

- PortalProtect 2.0

To migrate PortalProtect settings:

1. Go to **\Installation Folder\tool\ ConfigurationExportAndImportTool** and locate the file **toolConf.exe**, which is the migration configuration tool. See *Figure 3-32*.


ConfigurationExportAndImport
Trend Micro ▸ PortalProtect ▸ tool ▸ ConfigurationExportAndImport
Search ConfigurationExportAndImport
Organize ▾
Include in library ▾
Share with ▾
New folder
Favorites
Desktop
Downloads
Recent Places

Name	Date modified	Type	Size
toolConf	3/20/2010 1:24 AM	Application	476 KB
toolConf	3/25/2010 12:12 PM	LOG File	2 KB

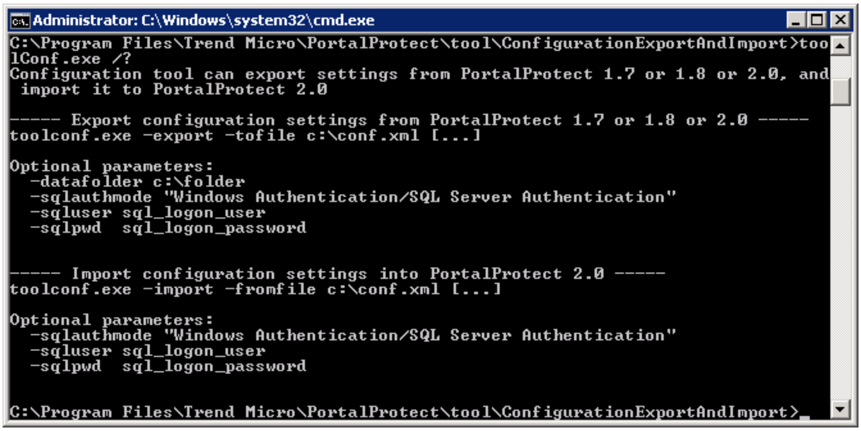
FIGURE 3-32. Configuration Export / Import Tool

Note: From the setup program, the tool location is:
`%SETUPDIR%\tool\ConfigurationExportAndImportTool\toolConf.exe`

From the installed binary, the tool location is:
`%INSTALLDIR%\tool\ConfigurationExportAndImportTool\toolConf.exe`

2. Copy the file **toolConf.exe** to the location where you want to execute the configuration migration tool for PortalProtect.
3. After copying the file, go to the command prompt and change the current directory to the folder location that now contains this tool.

4. Type **toolConf /?** to view a list of options that you can use for the migration tool. See *Figure 3-33*.



```
C:\Program Files\Trend Micro\PortalProtect\tool\ConfigurationExportAndImport>too
lConf.exe /?
Configuration tool can export settings from PortalProtect 1.7 or 1.8 or 2.0, and
 import it to PortalProtect 2.0

----- Export configuration settings from PortalProtect 1.7 or 1.8 or 2.0 -----
toolconf.exe -export -tofile c:\conf.xml [...]

Optional parameters:
  -datafolder c:\folder
  -sqlauthmode "Windows Authentication/SQL Server Authentication"
  -sqluser sql_logon_user
  -sqlpwd  sql_logon_password

----- Import configuration settings into PortalProtect 2.0 -----
toolconf.exe -import -fromfile c:\conf.xml [...]

Optional parameters:
  -sqlauthmode "Windows Authentication/SQL Server Authentication"
  -sqluser sql_logon_user
  -sqlpwd  sql_logon_password


C:\Program Files\Trend Micro\PortalProtect\tool\ConfigurationExportAndImport>_
```

FIGURE 3-33. Configuration Export / Import options

Choose from the following options:

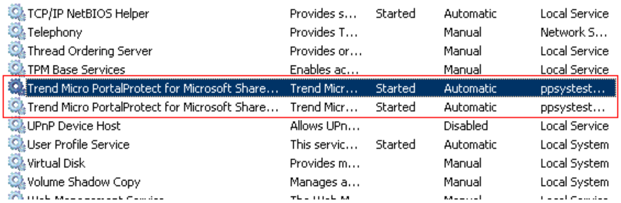
- **-export**—exports the configuration to a file defined using the parameter **-tofile**
- **-import**—imports the configuration from a file defined using the parameter **-fromfile**
- **-tofile**—indicates the location for the exported configuration file
- **-fromfile**—indicates the location for the imported configuration file
- **-datafolder c:\xxx**—this folder contains log and report data.

WARNING! **If the -datafolder option is not provided, PortalProtect will not export log and report data.**

- **-sqlauthmode**, **-sqluser**, and **-sqlpwd**—these parameters are used to connect to the PortalProtect SQL database. If not provided, PortalProtect will use the same account used to run toolConf.exe.

5. Export settings from the previous version of PortalProtect by doing the following:

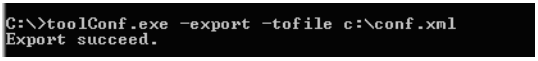
   a. Stop PortalProtect services (see *Figure 3-34*).



TCP/IP NetBIOS Helper	Provides s...	Started	Automatic	Local Service
Telephony	Provides T...		Manual	Network S...
Thread Ordering Server	Provides or...		Manual	Local Service
TPM Base Services	Enables ac...		Manual	Local Service
Trend Micro PortalProtect for Microsoft Share...	Trend Micr...	Started	Automatic	ppsystest...
Trend Micro PortalProtect for Microsoft Share...	Trend Micr...	Started	Automatic	ppsystest...
UPnP Device Host	Allows UPn...		Disabled	Local Service
User Profile Service	This servic...	Started	Automatic	Local System
Virtual Disk	Provides m...		Manual	Local System
Volume Shadow Copy	Manages a...		Manual	Local System

FIGURE 3-34. Stop PortalProtect services

b. Export settings using: toolConf.exe -export -tofile c:\conf.xml (see *Figure 3-35*).



```
C:\>toolConf.exe -export -tofile c:\conf.xml
Export succeed.
```

FIGURE 3-35. Export settings example

6. Uninstall the previous version of PortalProtect:

   a. **To uninstall PortalProtect 2.0**: see *Removing PortalProtect* on page 3-49.

   b. **To uninstall PortalProtect 1.8**: refer to "Uninstalling PortalProtect" in the PP 1.8 Getting Started Guide.

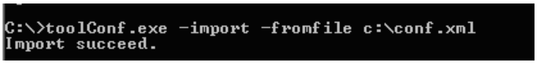
   c. **To uninstall PortalProtect 1.7**: refer to "Removing PortalProtect" in the PP 1.7 Getting Started Guide.

7. Install the new version of PortalProtect: see *Performing a Fresh Installation* on page 3-2.

8. Import settings to the newly installed version of PortalProtect:

   a. Stop PortalProtect Services.

   b. Import Settings using: toolConf.exe -import -fromfile c:\conf.xml (see *Import settings example* on page 3-36).



```
C:\>toolConf.exe -import -fromfile c:\conf.xml
Import succeed.
```

FIGURE 3-36. Import settings example

Post Migration Tasks

After completing the *Migrating to PortalProtect 2.0* tasks, you must start PortalProtect services to verify that the all configurations were imported correctly. Check the configurations for the following:

- Real-time scan
- File blocking
- Content filtering
- Manual scan
- Scheduled scan
- Updates - Download Source
- Alerts
- Reports - Scheduled Reports template
- Reports - Maintenance
- Log - Maintenance
- Administration

Note: Log, Report, and Quarantined data will not be imported.

Migration Changes from PP 1.7 to PP 2.0

This section discusses the configuration changes made during migration from PortalProtect 1.7 to PortalProtect 2.0.

Feature	Configuration Changes after Migration
Real-time Virus Scan	**PP 1.7 Path: Scans > Real-time > Virus Scan** • File type exceptions from PP 1.7 Virus Scan will not be imported • The Quarantine action from PP 1.7 will import as the Block action • Actions on Microsoft Office macros from PP 1.7 will not be imported • Actions on unscannable files from PP 1.7 will not be imported **PP 1.7 Path: Scans > Real-time > Advanced** • If the setting: **"The size of decompressed files is less than"** is set to **KB** in PP 1.7, it will be imported as **MB** • The setting: **"When compressed file is beyond limitation, specify action"** from PP 1.7 will import to: **"Security Rick Scan > Action > Unscannable Files > Files exceeding specified scanning restrictions"**
Real-time File Blocking	• **"Scans > Real-time > File Blocking > Block the selected true file types"** will import to: **"File Blocking > Target > File types"** • **Document > Microsoft Word (.doc;.dot)** will import to: **Microsoft OLE (.doc - Word 6.0-2003; .dot; .vss; .shs)** • **Video > RealAudio (.ra; .ram)** will import to: **Audio > RealAudio (.ra; .ram)** • **Compressed > Macros in MS Office compressed** will import to: **Documents > Macros in MS Office compressed by ActiveMime (.mso)** **"Scans > Real-time > File Blocking > Action on Matches" in PortalProtect 1.7** • The **Quarantine** action will import as the **Block** action

FEATURE	CONFIGURATION CHANGES AFTER MIGRATION
Manual Scan	**Scans > Manual > Select Target(s) to Scan in PP 1.7** - The Scan target option will not be imported **Scans->Manual->Virus Scan" in PortalProtect 1.7** - The configuration changes for this option are the same as those for **Real-time Virus Scan** **Scans > Manual > File blocking in PortalProtect 1.7** - The configuration changes for this option are the same are the same as those for **Real-time File Blocking**
Scheduled Scan	**Scan > Schedule > Schedule task > Schedule in PortalProtect 1.7** - The **"Hourly and Once"** schedule will import as **"Daily and 00:30"** to: **"Scheduled Scan > Schedule"** **Scan > Scheduled > Schedule task > Scan Target in PortalProtect 1.7** - Scan target selection configurations will be imported. **Scan > Scheduled > Schedule task > Virus Scan in PortalProtect 1.7** - Configuration changes are the same as those for **Manual Virus Scan**. **Scan > Scheduled > Schedule task->File Blocking in PortalProtect 1.7** - Configuration changes are the same as those for **Manual File Blocking Scan**

FEATURE	CONFIGURATION CHANGES AFTER MIGRATION
Notifications	**Notifications > Events in PortalProtect 1.7** • The **Virus detected**, **File Blocked**, **Real-time scan stopped**, **Service stopped**, **Engine update successful**, and **Engine update unsuccessful** options will not be imported • The **Manual/Scheduled scan aborted** option will import to: **Alerts > System Events > Manual/Scheduled scan tasks were unsuccessful**. However, the contents of the notification contents will not be imported. • The **Manual/Scheduled scan finished** option will import to: **Alerts > System Events > Manual/Scheduled scan tasks were successful**. However, the contents of the notification will not be imported.
Administration	**Password** and **Folder** will not be imported

Migration Changes from PP 1.8 to PP 2.0

This section discusses the configuration changes made during migration from PortalProtect 1.8 to PortalProtect 2.0.

FEATURE	CONFIGURATION CHANGES AFTER MIGRATION
Real-time Scan	**Virus Scan Configurations in PP 1.8** • The **Quarantine** action will import as the **Block** action **File Blocking Scan Configurations in PP 1.8** • The **Quarantine** action will import as the **Block** action

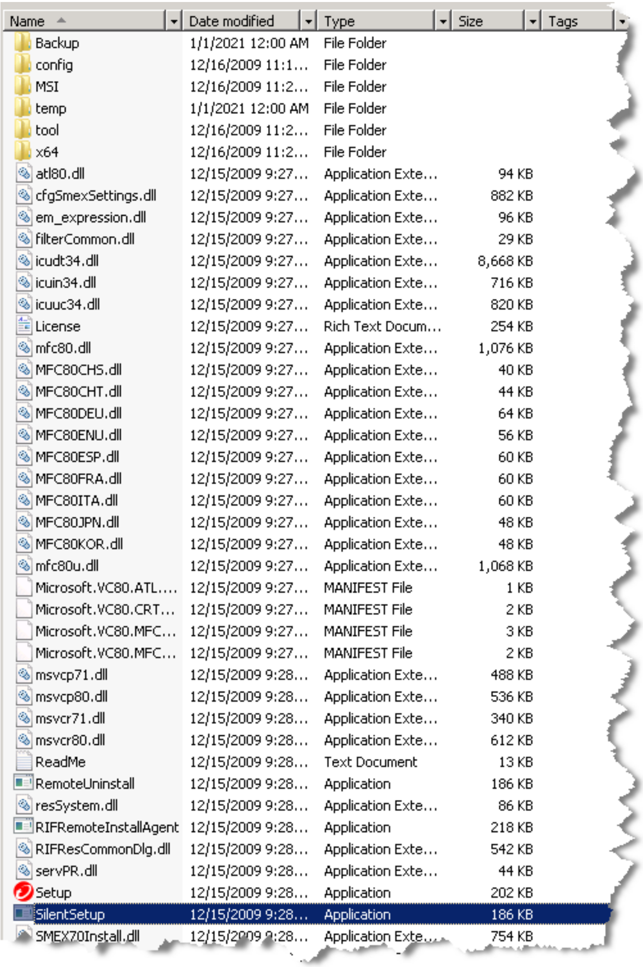
Feature	Configuration Changes after Migration
Other Configurations	**Note:** Some configurations will not import from PP 1.8 to PP 2.0. These include: • Summary Page • Log / Report / Quarantined data • Administration > Control manager settings • Administration > Trend Support/Debugger • Single sign on • Administration > Product license

Silent Installation

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

To install PortalProtect using Silent Install:

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



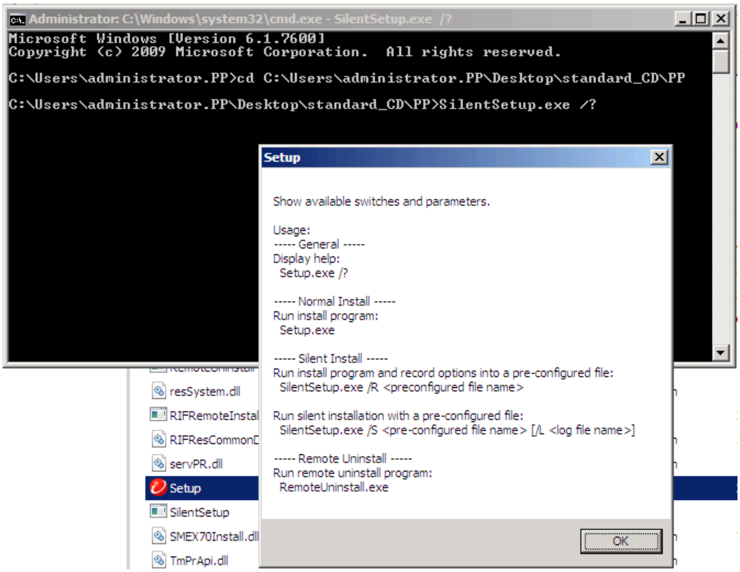
Name	Date modified	Type	Size	Tags
Backup	1/1/2021 12:00 AM	File Folder		
config	12/16/2009 11:1...	File Folder		
MSI	12/16/2009 11:2...	File Folder		
temp	1/1/2021 12:00 AM	File Folder		
tool	12/16/2009 11:2...	File Folder		
x64	12/16/2009 11:2...	File Folder		
atl80.dll	12/15/2009 9:27...	Application Exte...	94 KB	
cfgSmexSettings.dll	12/15/2009 9:27...	Application Exte...	882 KB	
em_expression.dll	12/15/2009 9:27...	Application Exte...	96 KB	
filterCommon.dll	12/15/2009 9:27...	Application Exte...	29 KB	
icudt34.dll	12/15/2009 9:27...	Application Exte...	8,668 KB	
icuin34.dll	12/15/2009 9:27...	Application Exte...	716 KB	
icuuc34.dll	12/15/2009 9:27...	Application Exte...	820 KB	
License	12/15/2009 9:27...	Rich Text Docum...	254 KB	
mfc80.dll	12/15/2009 9:27...	Application Exte...	1,076 KB	
MFC80CHS.dll	12/15/2009 9:27...	Application Exte...	40 KB	
MFC80CHT.dll	12/15/2009 9:27...	Application Exte...	44 KB	
MFC80DEU.dll	12/15/2009 9:27...	Application Exte...	64 KB	
MFC80ENU.dll	12/15/2009 9:27...	Application Exte...	56 KB	
MFC80ESP.dll	12/15/2009 9:27...	Application Exte...	60 KB	
MFC80FRA.dll	12/15/2009 9:27...	Application Exte...	60 KB	
MFC80ITA.dll	12/15/2009 9:27...	Application Exte...	60 KB	
MFC80JPN.dll	12/15/2009 9:27...	Application Exte...	48 KB	
MFC80KOR.dll	12/15/2009 9:27...	Application Exte...	48 KB	
mfc80u.dll	12/15/2009 9:27...	Application Exte...	1,068 KB	
Microsoft.VC80.ATL....	12/15/2009 9:27...	MANIFEST File	1 KB	
Microsoft.VC80.CRT...	12/15/2009 9:27...	MANIFEST File	2 KB	
Microsoft.VC80.MFC...	12/15/2009 9:27...	MANIFEST File	3 KB	
Microsoft.VC80.MFC...	12/15/2009 9:27...	MANIFEST File	2 KB	
msvcp71.dll	12/15/2009 9:28...	Application Exte...	488 KB	
msvcp80.dll	12/15/2009 9:28...	Application Exte...	536 KB	
msvcr71.dll	12/15/2009 9:28...	Application Exte...	340 KB	
msvcr80.dll	12/15/2009 9:28...	Application Exte...	612 KB	
ReadMe	12/15/2009 9:28...	Text Document	13 KB	
RemoteUninstall	12/15/2009 9:28...	Application	186 KB	
resSystem.dll	12/15/2009 9:28...	Application Exte...	86 KB	
RIFRemoteInstallAgent	12/15/2009 9:28...	Application	218 KB	
RIFResCommonDlg.dll	12/15/2009 9:28...	Application Exte...	542 KB	
servPR.dll	12/15/2009 9:28...	Application Exte...	44 KB	
Setup	12/15/2009 9:28...	Application	202 KB	
SilentSetup	12/15/2009 9:28...	Application	186 KB	
SMEX70Install.dll	12/15/2009 9:28...	Application Exte...	754 KB	

FIGURE 3-37. Select and copy files

2. Copy all the files in the PortalProtect sub-folder 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.

WARNING! You must use silentsetup.exe for silent installation. Never use setup.exe.

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



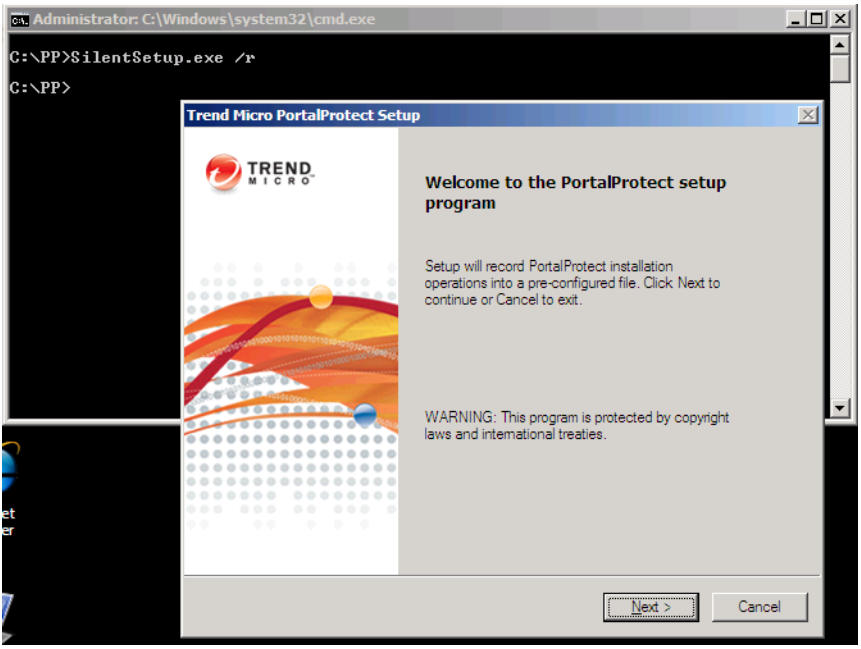
Administrator: C:\Windows\system32\cmd.exe - SilentSetup.exe /?

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\administrator.PP>cd C:\Users\administrator.PP\Desktop\standard_CD\PP

C:\Users\administrator.PP\Desktop\standard_CD\PP>SilentSetup.exe /?
```

```
Show available switches and parameters.

Usage:
----- General -----
Display help:
  Setup.exe /?

----- Normal Install -----
Run install program:
  Setup.exe

----- Silent Install -----
Run install program and record options into a pre-configured file:
  SilentSetup.exe /R <preconfigured file name>

Run silent installation with a pre-configured file:
  SilentSetup.exe /S <pre-configured file name> [/L <log file name>]

----- Remote Uninstall -----
Run remote uninstall program:
  RemoteUninstall.exe
```

FIGURE 3-38. Silent setup help

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


Administrator: C:\Windows\system32\cmd.exe
Trend Micro PortalProtect Setup
TREND MICRO
Next >
Cancel

```
C:\PP>SilentSetup.exe /r

C:\PP>
```

Welcome to the PortalProtect setup program

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

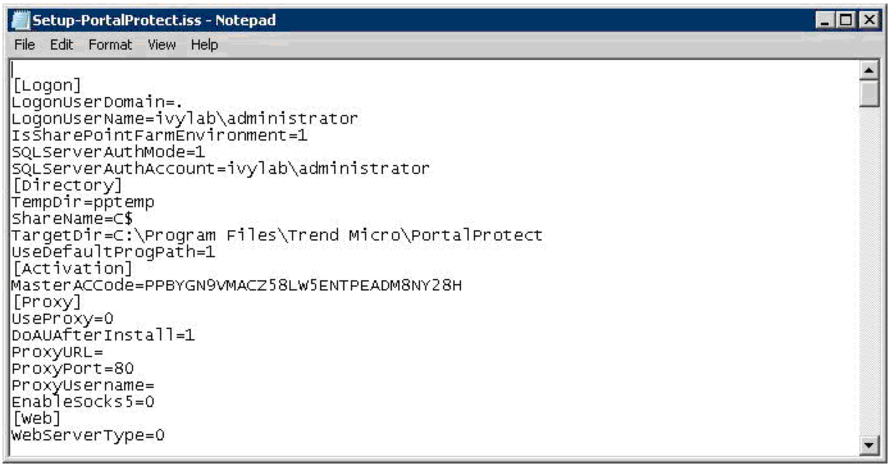
WARNING: This program is protected by copyright laws and international treaties.

FIGURE 3-39. Silent installation welcome screen

For the next steps, refer to *Silent Installation* on page 3-41.

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

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



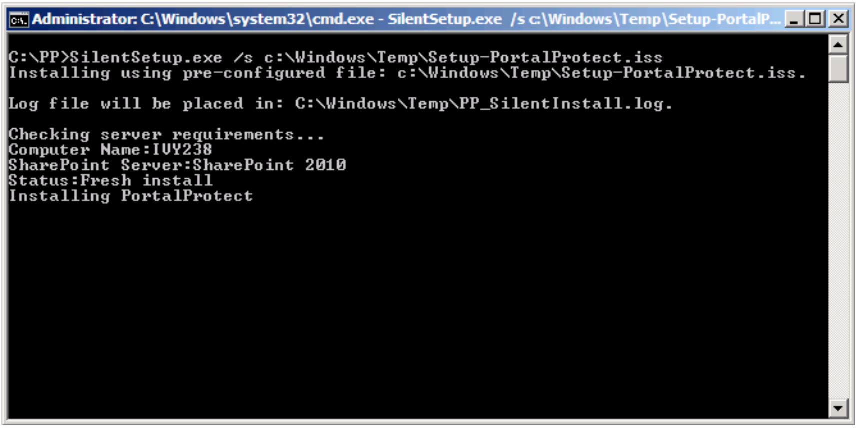
```
[Logon]
LogonUserDomain=.
LogonUserName=ivylab\administrator
IsSharePointFarmEnvironment=1
SQLServerAuthMode=1
SQLServerAuthAccount=ivylab\administrator
[Directory]
TempDir=pptemp
ShareName=C$
TargetDir=C:\Program Files\Trend Micro\PortalProtect
UseDefaultProgPath=1
[Activation]
MasterACCode=PPBYGN9VMACZ58LW5ENTPEADM8NY28H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

FIGURE 3-40. Setup-PortalProtect.iss file

WARNING! **All passwords are encrypted for security. Do NOT modify the ConsoleGroup or ServerManagementGroupSid. If you need to change this password, see** *Change Silent Installation Password* **on page 3-47.**

---

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

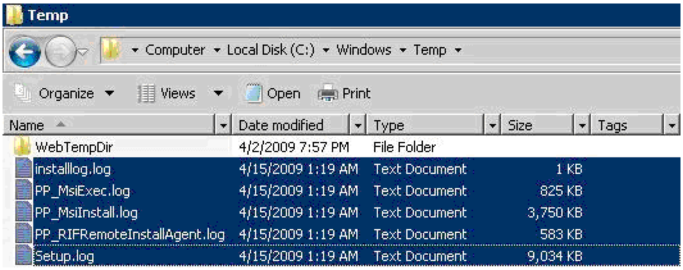


Administrator: C:\Windows\system32\cmd.exe - SilentSetup.exe /s c:\Windows\Temp\Setup-PortalP...

```
C:\PP>SilentSetup.exe /s c:\Windows\Temp\Setup-PortalProtect.iss
Installing using pre-configured file: c:\Windows\Temp\Setup-PortalProtect.iss.

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

Checking server requirements...
Computer Name:IVY238
SharePoint Server:SharePoint 2010
Status:Fresh install
Installing PortalProtect
```

FIGURE 3-41. Installation screen

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



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

FIGURE 3-42. Setup log files

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

Change Silent Installation Password

This section describes the steps required to change the Silent Installation password.

To change the silent installation password:

1. Type the new password directly in the file ***`Setup-PortalProtect.iss`***.
2. PortalProtect 2.0 supports changing the following five passwords in this file:
    - SQLServerAuthPassword = Password
    - PPConfDBInstanceAuthPassword = Password
    - ProxyPassword = Password
    - ConnectCMServerProxyPassword = Password
    - CMServerWebPassword = Password

WARNING! **If you change password in this file, PortalProtect will not encrypt these passwords again.**

Post Installation

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

Important Notice:

After installing PortalProtect, configure the antivirus settings in the SharePoint Central Administration and Web content scan settings from the PortalProtect management console. This will enable PortalProtect to function correctly.

To enable the antivirus settings in SharePoint 2007:

1. From within SharePoint, go to **SharePoint 3.0 Central Administration > Operations > Security Configuration > Antivirus**.
2. Enable the following:
    - **Scan documents on upload**
    - **Scan documents on download**
    - **Attempt to clean infected documents**

To enable the antivirus settings in SharePoint 2010:

1. From within SharePoint, go to **SharePoint 2010 Central Administration > Security > General Security > Manage antivirus settings**.
2. Enable the following:
   - **Scan documents on upload**
   - **Scan documents on download**
   - **Attempt to clean infected documents**

To enable Web content scan settings in PortalProtect:

1. From PortalProtect, go to the **PortalProtect Management Console > Summary > System > Microsoft SharePoint Services**.
2. Enable the following:
   - **Scan Web content**
     If your PortalProtect server has an antivirus product installed, configure it so that it does not scan the following folders:

     Assume > C:\Program Files\Trend Micro\PortalProtect is the installation folder.

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

     Backup folder, whose default location is: C:\Program Files\Trend Micro\PortalProtect\storage\Backup

     Shared Resource Pool folder, whose default location is: C:\Program Files\Trend Micro\PortalProtect\SharedResPool
   - For example: if using Trend Micro ServerProtect, add these folders to the Exclude folder list.

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

Testing Your Installation

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

http://www.eicar.org

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

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

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

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

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

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

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

Removing PortalProtect

There are two methods to remove PortalProtect 2.0:

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

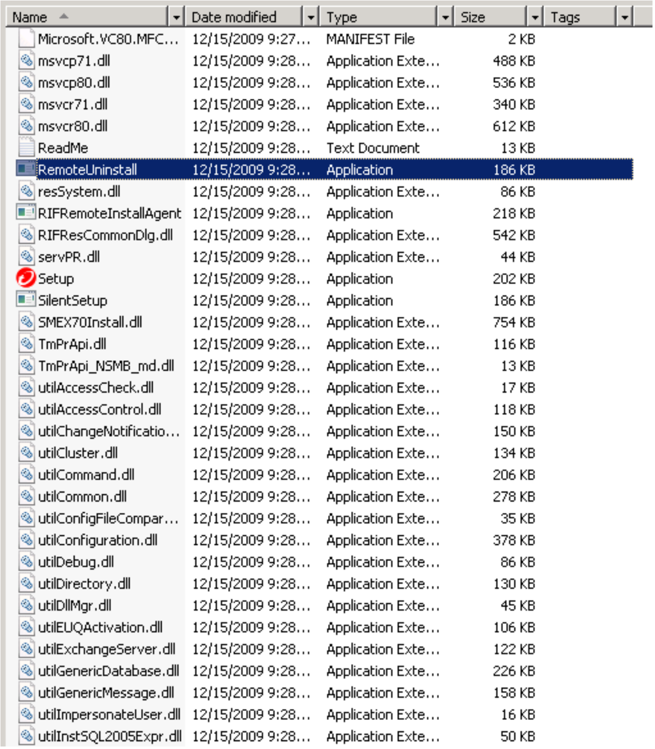
Removing PortalProtect both locally and remotely is performed with a user-friendly uninstallation program. This program allows you to easily remove PortalProtect from one or many servers.

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

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

To uninstall PortalProtect remotely:

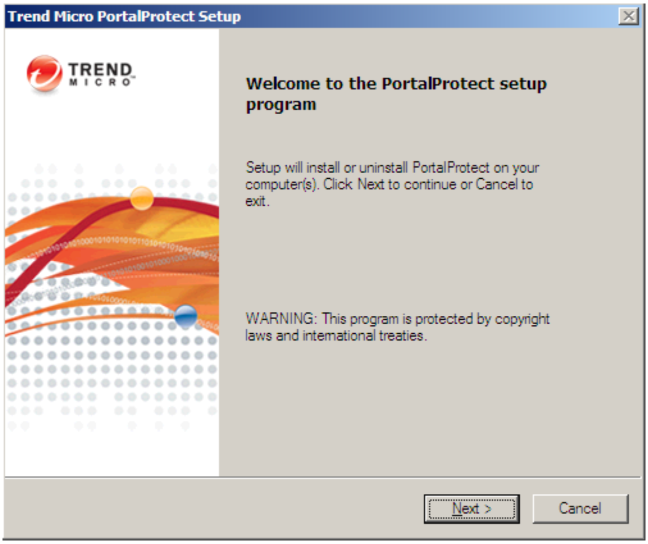
1. Insert the PortalProtect program CD into your CD-ROM drive, and navigate to RemoteUninstall.exe and open it.



Name	Date modified	Type	Size	Tags
Microsoft.VC80.MFC...	12/15/2009 9:27...	MANIFEST File	2 KB	
msvcp71.dll	12/15/2009 9:28...	Application Exte...	488 KB	
msvcp80.dll	12/15/2009 9:28...	Application Exte...	536 KB	
msvcr71.dll	12/15/2009 9:28...	Application Exte...	340 KB	
msvcr80.dll	12/15/2009 9:28...	Application Exte...	612 KB	
ReadMe	12/15/2009 9:28...	Text Document	13 KB	
RemoteUninstall	12/15/2009 9:28...	Application	186 KB	
resSystem.dll	12/15/2009 9:28...	Application Exte...	86 KB	
RIFRemoteInstallAgent	12/15/2009 9:28...	Application	218 KB	
RIFResCommonDlg.dll	12/15/2009 9:28...	Application Exte...	542 KB	
servPR.dll	12/15/2009 9:28...	Application Exte...	44 KB	
Setup	12/15/2009 9:28...	Application	202 KB	
SilentSetup	12/15/2009 9:28...	Application	186 KB	
SMEX70Install.dll	12/15/2009 9:28...	Application Exte...	754 KB	
TmPrApi.dll	12/15/2009 9:28...	Application Exte...	116 KB	
TmPrApi_NSMB_md.dll	12/15/2009 9:28...	Application Exte...	13 KB	
utilAccessCheck.dll	12/15/2009 9:28...	Application Exte...	17 KB	
utilAccessControl.dll	12/15/2009 9:28...	Application Exte...	118 KB	
utilChangeNotificatio...	12/15/2009 9:28...	Application Exte...	150 KB	
utilCluster.dll	12/15/2009 9:28...	Application Exte...	134 KB	
utilCommand.dll	12/15/2009 9:28...	Application Exte...	206 KB	
utilCommon.dll	12/15/2009 9:28...	Application Exte...	278 KB	
utilConfigFileCompar...	12/15/2009 9:28...	Application Exte...	35 KB	
utilConfiguration.dll	12/15/2009 9:28...	Application Exte...	378 KB	
utilDebug.dll	12/15/2009 9:28...	Application Exte...	86 KB	
utilDirectory.dll	12/15/2009 9:28...	Application Exte...	130 KB	
utilDllMgr.dll	12/15/2009 9:28...	Application Exte...	45 KB	
utilEUQActivation.dll	12/15/2009 9:28...	Application Exte...	106 KB	
utilExchangeServer.dll	12/15/2009 9:28...	Application Exte...	122 KB	
utilGenericDatabase.dll	12/15/2009 9:28...	Application Exte...	226 KB	
utilGenericMessage.dll	12/15/2009 9:28...	Application Exte...	158 KB	
utilImpersonateUser.dll	12/15/2009 9:28...	Application Exte...	16 KB	
utilInstSQL2005Expr.dll	12/15/2009 9:28...	Application Exte...	50 KB	

FIGURE 3-43. Select and run RemoteUninstall.exe

2. The Trend Micro PortalProtect setup program screen displays.



Trend Micro PortalProtect Setup

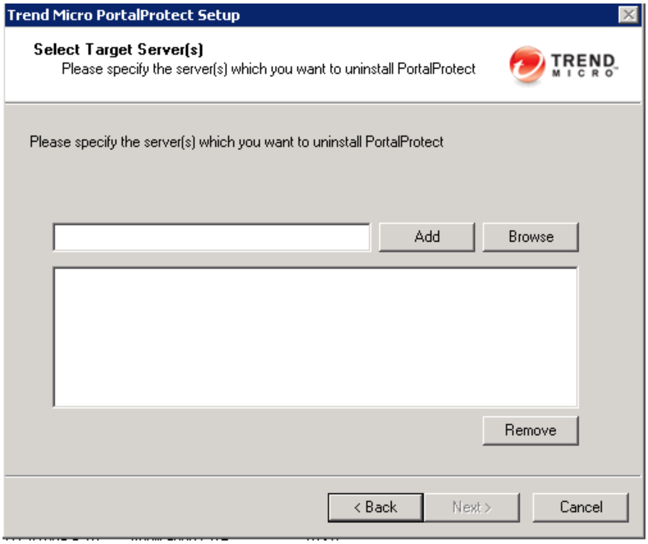
Welcome to the PortalProtect setup program

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

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

FIGURE 3-44. Trend Micro PortalProtect setup program screen

3. Click **Next**. The **Select Target Servers** screen displays.



Trend Micro PortalProtect Setup

Select Target Server(s)

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

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

FIGURE 3-45. Select Target Server(s) screen

4. **Add** / **Browse** for the **Computer name(s)** where you want to uninstall PortalProtect; then, select the added server(s) and click **Next >**.
5. The **Select Computers** dialog appears.

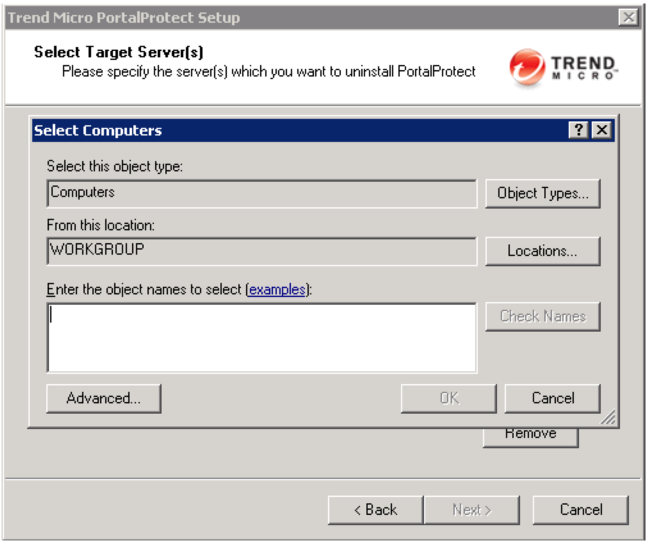
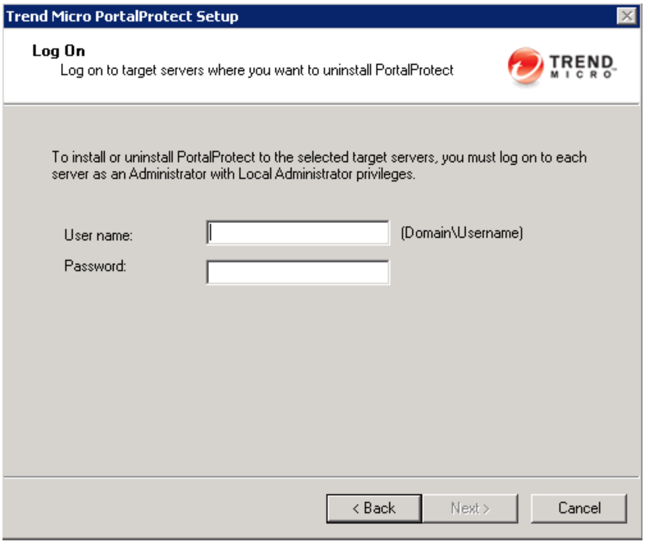


FIGURE 3-46. Select Computers dialog

6. Select the computers from which you want to uninstall PortalProtect and click **OK**.
7. The **Select Target Servers** screen appears.
8. **Add / Browse** to select additional servers as required and click **Next>**.
9. The **Logon** screen displays.



Trend Micro PortalProtect Setup

Log On

Log on to target servers where you want to uninstall PortalProtect

To install or uninstall PortalProtect to the selected target servers, you must log on to each server as an Administrator with Local Administrator privileges.

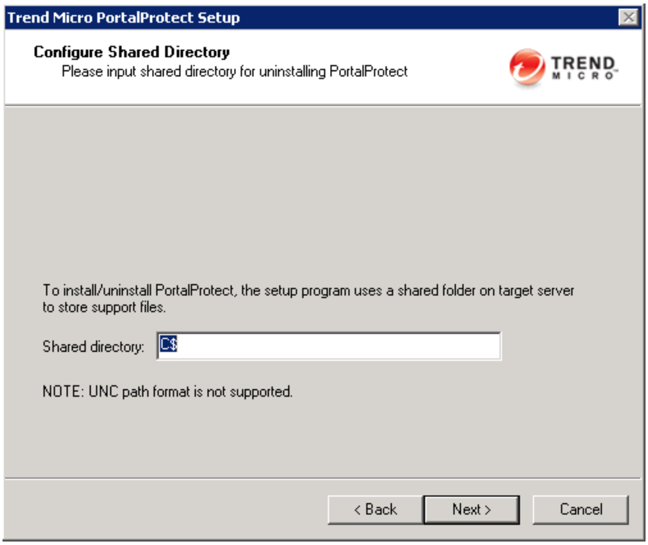
User name: (Domain\Username)

Password:

FIGURE 3-47. Logon screen

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

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



Trend Micro PortalProtect Setup

Configure Shared Directory

Please input shared directory for uninstalling PortalProtect

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

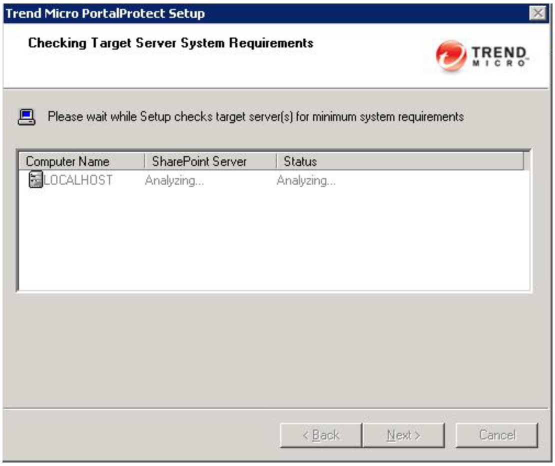
Shared directory: C$

NOTE: UNC path format is not supported.

FIGURE 3-48. Configure Shared Directory screen

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

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



Trend Micro PortalProtect Setup

Checking Target Server System Requirements

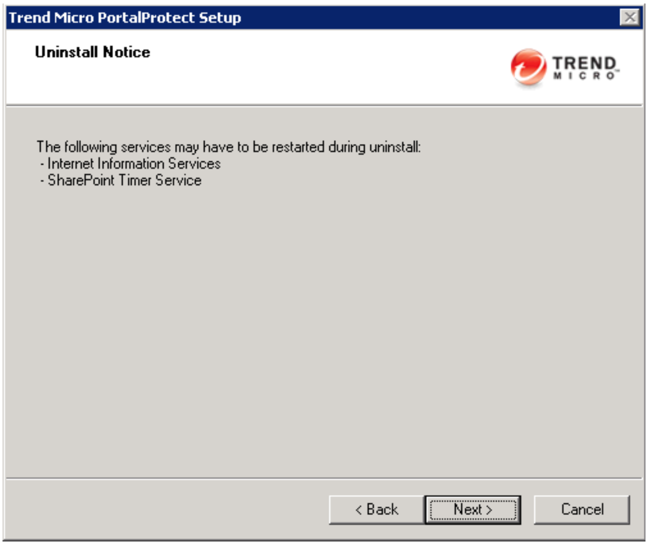
Please wait while Setup checks target server(s) for minimum system requirements

Computer Name	SharePoint Server	Status
LOCALHOST	Analyzing...	Analyzing...

FIGURE 3-49. Checking Target Server System Requirements screen

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

12. The **Uninstall Notice** screen displays.

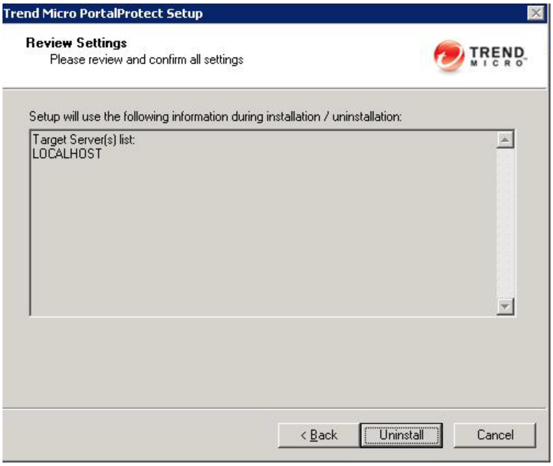


The following services may have to be restarted during uninstall:
- Internet Information Services
- SharePoint Timer Service

FIGURE 3-50. Uninstall Notice screen

Click **Next >**.

13. The **Review Settings** screen displays.


Trend Micro PortalProtect Setup
Review Settings
Please review and confirm all settings
TREND MICRO
< Back
Uninstall
Cancel

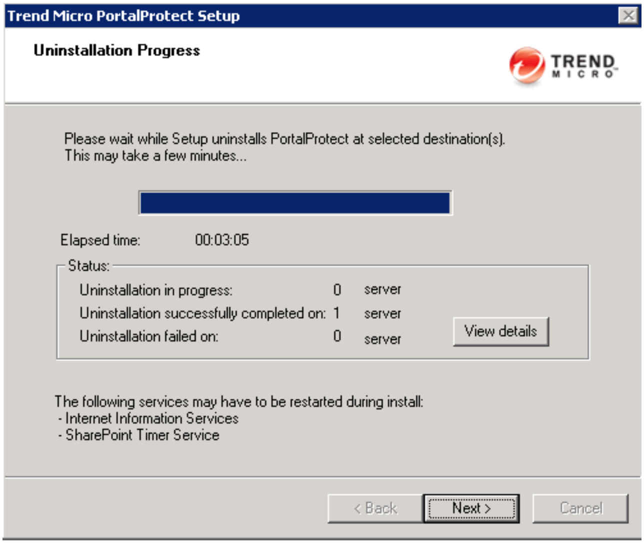
Setup will use the following information during installation / uninstallation:

Target Server(s) list:
LOCALHOST

FIGURE 3-51. Review Settings screen

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

14. The **Uninstallation Progress** screen displays.



Trend Micro PortalProtect Setup

Uninstallation Progress

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

Elapsed time: 00:03:05

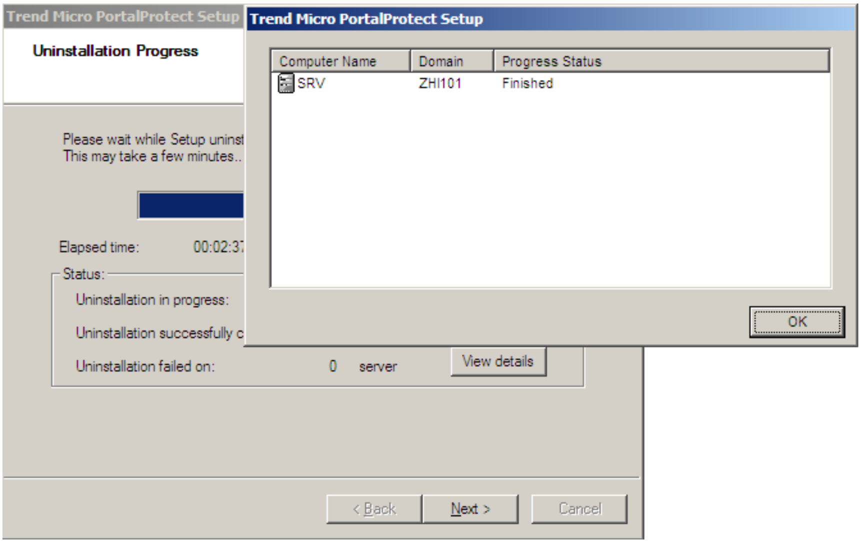
Status:

Uninstallation in progress: 0 server
Uninstallation successfully completed on: 1 server
Uninstallation failed on: 0 server

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

FIGURE 3-52. Uninstallation Progress screen

Click **View Details** to observe the uninstallation progress (see *Figure 3-53* on page 3-61).


Trend Micro PortalProtect Setup

Uninstallation Progress

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

Elapsed time: 00:02:37

Status:

Uninstallation in progress:

Uninstallation successfully c

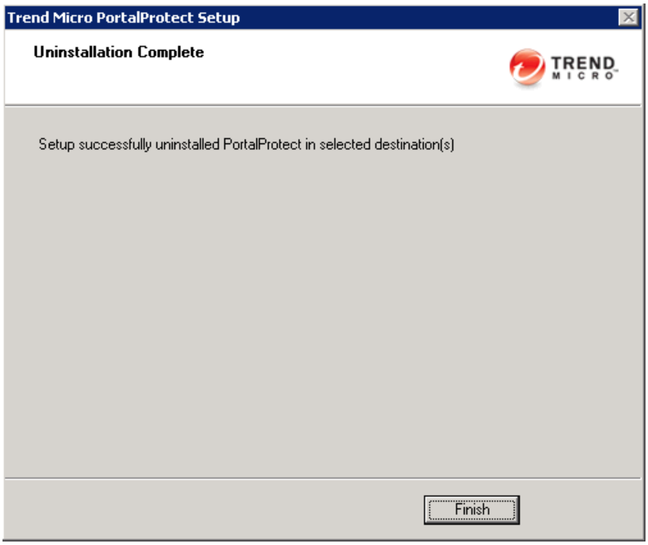
Uninstallation failed on: 0 server

Trend Micro PortalProtect Setup

Computer Name	Domain	Progress Status
SRV	ZHI101	Finished

FIGURE 3-53. Uninstallation Progress Status

15. When the **Progress Status** displays **Finished** (*Figure 3-53*), click **OK > Next >**.
16. The **Uninstallation Complete** screen displays.



Trend Micro PortalProtect Setup

Uninstallation Complete

Setup successfully uninstalled PortalProtect in selected destination(s)

FIGURE 3-54. Uninstallation Complete screen

Chapter 4

Getting Support and Contacting Trend Micro

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

In this chapter, you will find information about:

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

Contacting Trend Micro

Trend Micro Incorporated has its world headquarters at:

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

In the United States, Trend Micro is located at:

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

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

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

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

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

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

Contacting Technical Support

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

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

To contact Trend Micro technical support:

1. Visit the following URL:

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

You can find Trend Micro contacts in the following regions:

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

Before Contacting Technical Support

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

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

  The documentation set for this product includes the following:

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

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

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

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

TrendLabs

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

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

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

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

Frequently Asked Questions (FAQ)

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

Installation

Where should I install PortalProtect to protect my SharePoint environments?

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

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

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

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

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

How to install PortalProtect in Cluster environment?

PortalProtect 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.

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

Check as following:

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

b. Make sure the PortalProtect application pool, virtual site, and virtual directories exist.

c. Make sure the IIS site is running.

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

e. Make sure the PortalProtect master service is running.

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

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

1. If SharePoint used Windows authentication to connect to the database and PortalProtect used Windows authentication to connect to the database...

To change SharePoint database password or PortalProtect database password:

a. Select **Administrative Tools > Service**.

b. Locate Trend Micro PortalProtect for Microsoft SharePoint Master Service.

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

2. If SharePoint used Windows authentication to connect to the database and PortalProtect used SQL authentication to connect to the database...

To change SharePoint DB password:

a. Select **Administrative Tools > Service**.

b. Locate Trend Micro PortalProtect for Microsoft SharePoint Master Service.

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

To change PortalProtect DB password:

a. Open the Registry and locate:

“HKLM\...\PortalProtect\CurrentVersion\PPConfDatabasePassword”

b. Change the password and restart PortalProtect Master Service.

Note: You can type the password in the PPConfDatabasePassword field. The password will be encrypted when the PortalProtect Master Service restarts.

3. If SharePoint used SQL authentication to connect to the database and PortalProtect used SQL authentication to connect to the database...

   To change SharePoint DB password:

   a. Open the Registry and locate:

      HKLM\...\PortalProtect\CurrentVersion\SharePointDBAccessPassword

   b. Change the password and restart the PortalProtect Master Service.

   Note: You can type the password in the SharePointDBAccessPassword field. The password will be encrypted when the PortalProtect Master Service restarts.

   To change PortalProtect DB password:

   a. Select **Administrative Tools > Service**.

   b. Locate Trend Micro PortalProtect for Microsoft SharePoint Master Service.

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

4. If SharePoint used SQL authentication to connect to the database and PortalProtect used SQL authentication to connect to the database...

   To change SharePoint DB password:

   a. Open the Registry and locate:

      HKLM\...\PortalProtect\CurrentVersion\SharePointDBAccessPassword

   b. Change the password and restart the PortalProtect Master Service.

   Note: You can type the password in the SharePointDBAccessPassword field. The password will be encrypted when the PortalProtect Master Service restarts.

   To change PortalProtect DB password:

   a. Open the Registry and locate:

      HKLM\...\PortalProtect\CurrentVersion\PPConfDatabasePassword

   b. Change the password and restart PortalProtect Master Service.

Appendix A

PortalProtect Database Permission Requirements

This appendix provides more information about the technical details required for PortalProtect database permissions.

This chapter discusses the following topics:

Applications

This section describes the applications used for PortalProtect 2.0.

- **PortalProtect**—Trend Micro PortalProtect for Microsoft SharePoint
- **SQL Server**—SQL Server 2005 or 2008
- **SharePoint**—Windows SharePoint Services 3.0, Windows SharePoint Services 4.0, Microsoft Office SharePoint Server 2007, Microsoft Office SharePoint Server 2010

Background

PortalProtect must have access to the following SQL Server database sources:

- PortalProtect Configuration Database
- SharePoint Databases

To access these databases, PortalProtect requires the following database access accounts:

- PortalProtect Configuration Database Access Account
- SharePoint Database Access Account

Note: These database access accounts must support either Windows Authentication or SQL Server Authentication.

If an access account is configured with SQL Server Authentication, the access account password will be saved and encrypted in the registry.

If an access account is configured with Windows Authentication, it will be used as the PortalProtect service log on account.

If both access accounts use Windows Authentication, they must be the same account, and will be used as the PortalProtect service log on account. *Table A-1* shows the PortalProtect service log on account.

Note: Trend Micro highly recommends you use Windows Authentication. Windows Authentication provides a more stable environment and does not require you to save your password in any form.

TABLE A-1. PortalProtect service log on account

PortalProtect Configuration Database Access Account	SharePoint Database Access Account	PortalProtect Service Startup Account
Windows Authentication	Windows Authentication	Both access accounts must be the same. PortalProtect will use these for the service startup account
Windows Authentication	SQL Server Authentication	PortalProtect Configuration Database Access Account
SQL Server Authentication	Windows Authentication	SharePoint Database Access Accounts
SQL Server Authentication	SQL Server Authentication	Local System

Note: If the access account is configured with SQL Server Authentication, the password will be saved under the following registry key:

```
HKLM\Software\TrendMicro\PortalProtect\Current
Version
```

This registry key also contains SharePoint behavior; the password is encrypted.

Requirements for PortalProtect Configuration Database Access Account

Besides authentication, these access accounts also require database permissions. The following sections will introduce the minimal permissions required for each database access account.

PortalProtect saves data—like configuration settings, logs, reports, quarantined data—to the PortalProtect Configuration Database. For one SharePoint environment, PortalProtect requires 3X+1 databases, where X is the number of PortalProtect servers.

Each PortalProtect server requires the following three (3) databases:

- PPConf_{ServerName}
- PPLog_{ServerName}
- PPReport_{ServerName}

Note: {ServerName} is the actual server name.

Theses three databases contain independent settings and data for each PortalProtect server. Additionally, the following is a database for all PortalProtect servers:

- PPCentralConfig_{SharePoint_Config_DB_Name}

Note: Different SharePoint farms may have the same Configure DB Name. Therefore, installing PortalProtect to different SharePoint farms using one DB instance with the same Configure DB Name is not recommended.

PPCentralConfig database contains global settings and data that are shared across all PortalProtect servers. The following are the required database permissions for PortalProtect Configuration Database Access Accounts:

- The access account must have server role **dbcreator**

Server role **dbcreator** is only needed when you install PortalProtect. You can remove this permission after the installation is complete.

dbcreator is a server role with increased privileges. In some cases, PortalProtect administrators may not be able to accommodate for it. If so, the PortalProtect administrator can follow the steps contained in *Manually Create PortalProtect Configuration Database* on page 2-7 to install PortalProtect without **dbcreator** permission.

Note: Trend Micro highly recommends that you specify the same database account as the one used to deploy SharePoint.

Requirements for SharePoint Database Access Account

This section applies only to SharePoint farm environments. SharePoint standalone environment keep data on the local SQL Server, and do not need to specify an access account.

PortalProtect will fetch or modify data in the SharePoint database. You need specify a database access account with relevant permissions. The following is a list of the required database permissions:

- **SharePoint Config Database:** access account must have at least database role **db_datareader**
- **SharePoint Content Database:** access account must have a database role of **db_owner**

PortalProtect needs to execute SharePoint internal stored procedures. The stored procedures execution permission are only granted to the **db_owner**. For this reason PortalProtect needs a database role **db_owner**. PortalProtect will not modify the SharePoint database schema.

Note: Trend Micro highly recommends that you specify the same database account as the one used to deploy SharePoint.

Index