TREND MICRO™

2.5 PortalProtect™

Installation and Deployment Guide

Highly Effective Protection, Minimal IT Impact

for Microsoft™ SharePoint

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:

http://docs.trendmicro.com/en-us/enterprise/portalprotect-for-sharepoint.aspx

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

Document Part No. PPEM27723/170216

Release Date: March 2017

Protected by U.S. Patent No. 5951698

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 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

Chapter 3: Getting Support and Contacting Trend Micro

Appendix A: PortalProtect Database Permission Requirements

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

PortalProtect documentation consists of the following:

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

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

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

Planning PortalProtect™ Installation and Upgrade

Trend Micro PortalProtect™ is a server-based security solution for Microsoft SharePoint™ Server 2010/2013/2016. Trend Micro designed PortalProtect to provide protection against attacks from viruses and other security threats.

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

The following sections lists the system requirements for PortalProtect.

PortalProtect 2.5 with SharePoint Server 2016

You need the following to effectively run PortalProtect 2.5 with SharePoint Server 2016:

TABLE 1-1. PortalProtect 2.5 with SharePoint Server 2016

HARDWARE/SOFTWARE	REQUIREMENT	RECOMMENDED
Processor	• X64 architecture-based processor that supports Intel Extended Memory 64 Technology (Intel EM64T) • X64 architecture-based computer with AMD 64-bit processor that supports AMD64 platform	
Memory	1-GB RAM (Exclusively for PortalProtect)	2-GB RAM or higher (Exclusively for PortalProtect)
Disk Space	2-GB free disk space	5-GB free disk space
Windows Server	• Windows Server 2016 Standard or Datacenter • Windows Server 2012 R2 Standard or Datacenter • Windows Server 2012 Standard or Datacenter	
SharePoint Service / Server	• Microsoft SharePoint Server 2016	

HARDWARE/SOFTWARE	REQUIREMENT	RECOMMENDED

Web Server	• Microsoft Internet Information Services (IIS) 8.5
	• Microsoft Internet Information Services (IIS) 8.0
	The following IIS features are required for PortalProtect installation:
	• Common HTTP Features
	  • Static Content
	  • Default Document
	  • Directory Browsing
	  • HTTP Errors
	• Application Development
	  • Common Gateway Interface (CGI)
	  • ISAPI Extensions
	  • ISAPI Filters
	• Health and Diagnostic
	  • HTTP Logging
	  • Request Monitor
	• Security
	  • Windows Authentication
	• Performance
	  • Static Content Compression
	• Management Tools
	  • IIS Management Console
	  • IIS 6 Management Compatibility
	  • IIS 6 Metabase Compatibility
	  • IIS 6 WMI Compatibility
	  • IIS 6 Scripting Tools
	  • IIS 6 Management Console
	Note: CGI must be installed manually, while other features are installed together with SharePoint servers.	

Browser	• Microsoft Internet Explorer 7.0 or above • Mozilla Firefox 3.0 or above	

PortalProtect 2.5 with SharePoint Server 2013

You need the following to effectively run PortalProtect 2.5 with SharePoint Server 2013:

TABLE 1-2. PortalProtect 2.5 with SharePoint Server 2013

HARDWARE/SOFTWARE	REQUIREMENT	RECOMMENDED
Processor	• X64 architecture-based processor that supports Intel Extended Memory 64 Technology (Intel EM64T) • X64 architecture-based computer with AMD 64-bit processor that supports AMD64 platform	
Memory	1-GB RAM (Exclusively for PortalProtect)	2-GB RAM or higher (Exclusively for PortalProtect)
Disk Space	2-GB free disk space	5-GB free disk space
Windows Server	• Windows Server 2012 R2 Standard or Datacenter • Windows Server 2012 Standard or Datacenter • Windows Server 2008 R2 Standard with SP1 (64-bit) • Windows Server 2008 R2 Enterprise with SP1 (64-bit)	
SharePoint Service / Server	• Microsoft SharePoint Server 2013 or above	

HARDWARE/SOFTWARE	REQUIREMENT	RECOMMENDED

Web Server	• Microsoft Internet Information Services (IIS) 8.5
	• Microsoft Internet Information Services (IIS) 8.0
	• Microsoft Internet Information Services (IIS) 7.5
	The following IIS features are required for PortalProtect installation:
	• Common HTTP Features
	  • Static Content
	  • Default Document
	  • Directory Browsing
	  • HTTP Errors
	• Application Development
	  • Common Gateway Interface (CGI)
	  • ISAPI Extensions
	  • ISAPI Filters
	• Health and Diagnostic
	  • HTTP Logging
	  • Request Monitor
	• Security
	  • Windows Authentication
	• Performance
	  • Static Content Compression
	• Management Tools
	  • IIS Management Console
	  • IIS 6 Management Compatibility
	  • IIS 6 Metabase Compatibility
	  • IIS 6 WMI Compatibility
	  • IIS 6 Scripting Tools
	  • IIS 6 Management Console
	Note: CGI must be installed manually, while other features are installed together with SharePoint servers.	

Browser	• Microsoft Internet Explorer 7.0 or above • Mozilla Firefox 3.0 or above	

PortalProtect 2.5 with SharePoint Server 2010

You need the following to effectively run PortalProtect 2.5 with SharePoint Server 2010:

TABLE 1-3. PortalProtect 2.5 with SharePoint Server 2010

HARDWARE/SOFTWARE	REQUIREMENT	RECOMMENDED
Processor	• X64 architecture-based processor that supports Intel Extended Memory 64 Technology (Intel EM64T) • X64 architecture-based computer with AMD 64-bit processor that supports AMD64 platform	
Memory	1-GB RAM (Exclusively for PortalProtect)	2-GB RAM or higher (Exclusively for PortalProtect)
Disk Space	2-GB free disk space	5-GB free disk space
Windows Server	• Windows Server 2008 R2 Standard with SP1 (64-bit) • Windows Server 2008 R2 Enterprise with SP1 (64-bit) • Windows Server 2008 with Service Pack 2 (64-bit)	
SharePoint Service / Server	• Microsoft SharePoint Server 2010 or above	

HARDWARE/SOFTWARE	REQUIREMENT	RECOMMENDED

Web Server	• Microsoft Internet Information Services (IIS) 7.5
	• Microsoft Internet Information Services (IIS) 7.0
	The following IIS features are required for PortalProtect installation:
	• Common HTTP Features
	  • Static Content
	  • Default Document
	  • Directory Browsing
	  • HTTP Errors
	• Application Development
	  • Common Gateway Interface (CGI)
	  • ISAPI Extensions
	  • ISAPI Filters
	• Health and Diagnostic
	  • HTTP Logging
	  • Request Monitor
	• Security
	  • Windows Authentication
	• Performance
	  • Static Content Compression
	• Management Tools
	  • IIS Management Console
	  • IIS 6 Management Compatibility
	  • IIS 6 Metabase Compatibility
	  • IIS 6 WMI Compatibility
	  • IIS 6 Scripting Tools
	  • IIS 6 Management Console
	Note: CGI must be installed manually, while other features are installed together with SharePoint servers.	

Browser	• Microsoft Internet Explorer 7.0 or above • Mozilla Firefox 3.0 or above	

PortalProtect supports the following Microsoft SQL Server versions:

- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2008

Note: Trend Micro recommends using the same SQL Server for PortalProtect and SharePoint.

You need the following to effectively run the CM agent:

- CM server 6.0 or above

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.

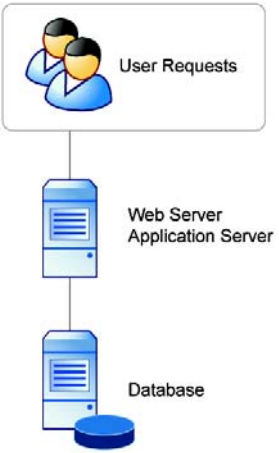

FIGURE 1-1. Small server farm configuration

SharePoint Services Medium Server Farm

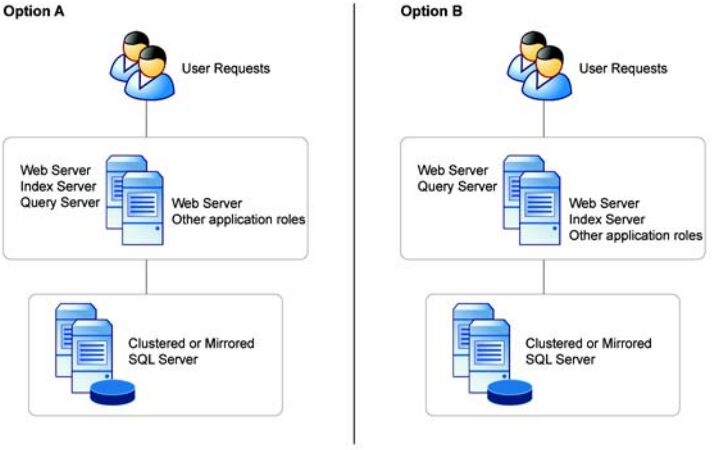

FIGURE 1-2. Medium server farm

SharePoint Services Large Server Farm

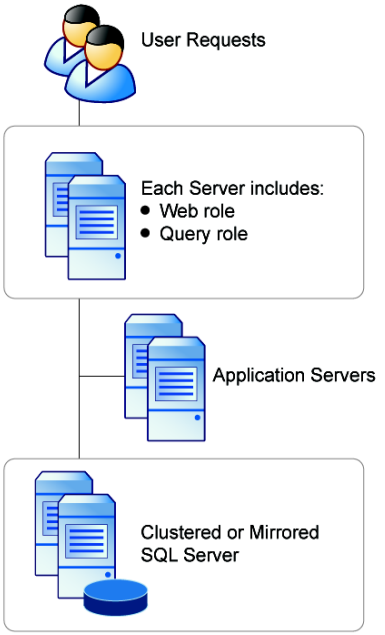

FIGURE 1-3. Large server farm configuration

Preparing for Installation

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

- Install PortalProtect 2.5 to a server with the appropriate server platforms installed; see *System Requirements* starting on page 1-2 for more information. Microsoft Internet Information Services (IIS) is a required for a successful installation.
- A started IIS Web application pool **`DefaultAppPool`** will be used for PortalProtect 2.5 installation. If **`DefaultAppPool`** does not exist, create it using the following basic settings:
  - .NET CLR version: V4.0
  - Managed pipeline mode: Integrated
- **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 Required Accounts**: Specify the permissions for the following accounts required in installation:
  - **Program Setup Account:** The program setup account is used to authorize execution of the installation program. It must have local administrator privileges to where you launch the installation program and local administrator privileges to all the target server(s) where you plan to install PortalProtect 2.5. It must also be the user account that already joins the domain where the server(s) to install PortalProtect 2.5 belong.
  - **PortalProtect Configuration Database Access Account:** Specify required database roles for the account to access PortalProtect configuration databases. See *PortalProtect Database Permission Requirements* on page A-1 for more information.
  - **SharePoint Database Access Account**: Specify required database roles for the account to access SharePoint databases. See *PortalProtect Database Permission Requirements* on page A-1 for more information.

Note: Trend Micro highly recommends that you use the same account to access the PortalProtect and SharePoint databases.

- **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.

Chapter 2

Installing and Removing PortalProtect

This section describes how to install and remove PortalProtect. It also provides information 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 of PortalProtect

Tip: Before installing PortalProtect 2.5, 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** (see *To perform a fresh installation using setup.exe:* on page 2-2
- Using a silent installation program called **SilentSetup.bat** (see *To perform a fresh installation of PortalProtect using SilentSetup.bat:* on page 2-20**)**

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.

To perform a fresh installation using setup.exe:

1. Run ***setup.exe*** from the PortalProtect 2.5 to start the installation.

   The **PortalProtect Installation Welcome** screen appears.

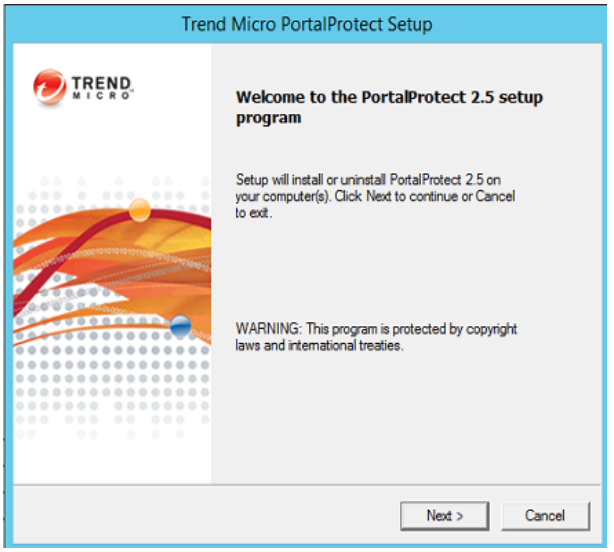

FIGURE 2-1. PortalProtect Installation Welcome screen

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

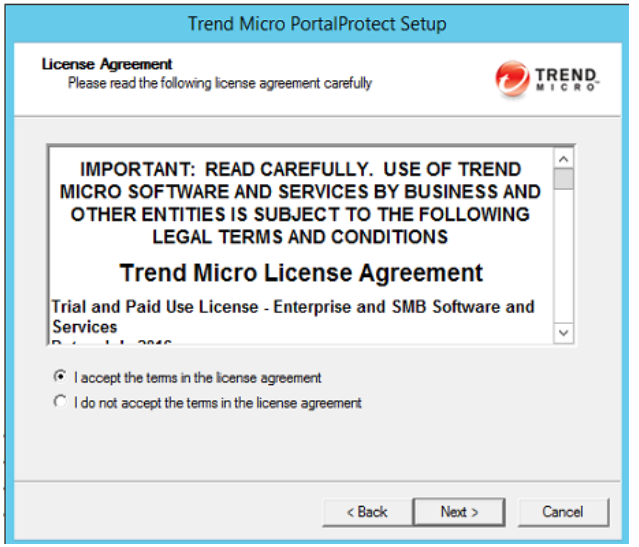

FIGURE 2-2. License Agreement screen

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 **Select an Action** screen (1) appears. Choose one of the following installation 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**.

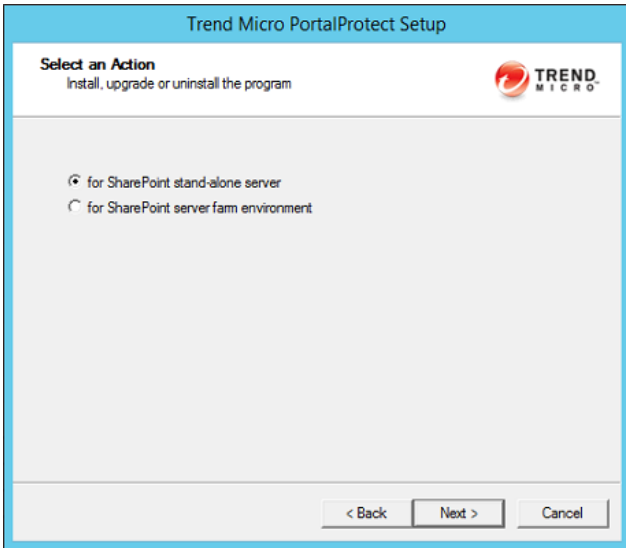

FIGURE 2-3. Select an Action screen (1)

4. The **Select an Action Install, upgrade or uninstall PortalProtect** screen appears.

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

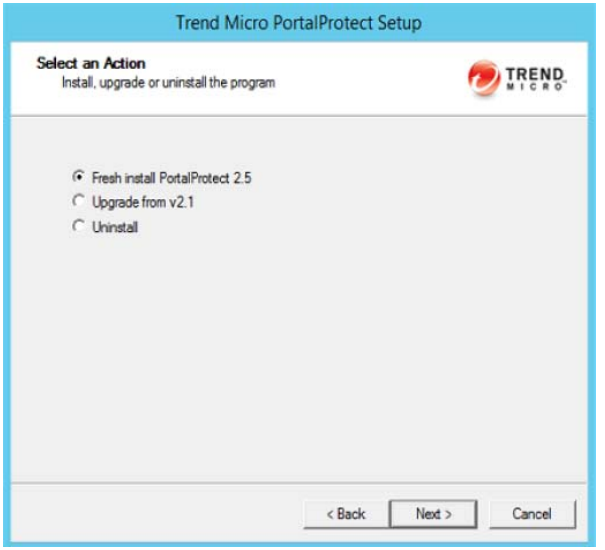

FIGURE 2-4. Select an Action screen (2)

5. The **Product Activation** screen appears.

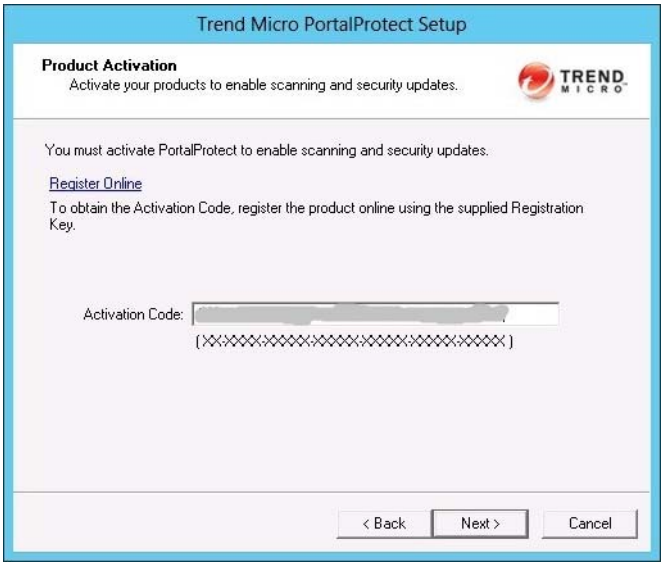

FIGURE 2-5. Product Activation screen

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.

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

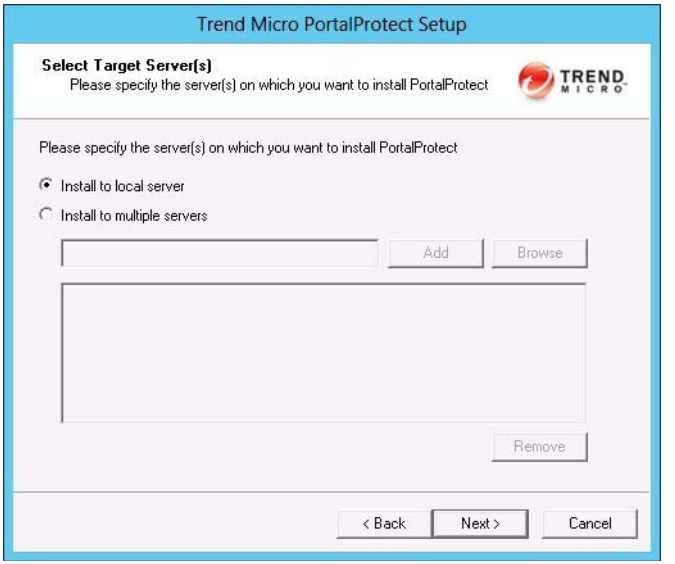

FIGURE 2-6. Select Target Server(s) screen

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 displays.

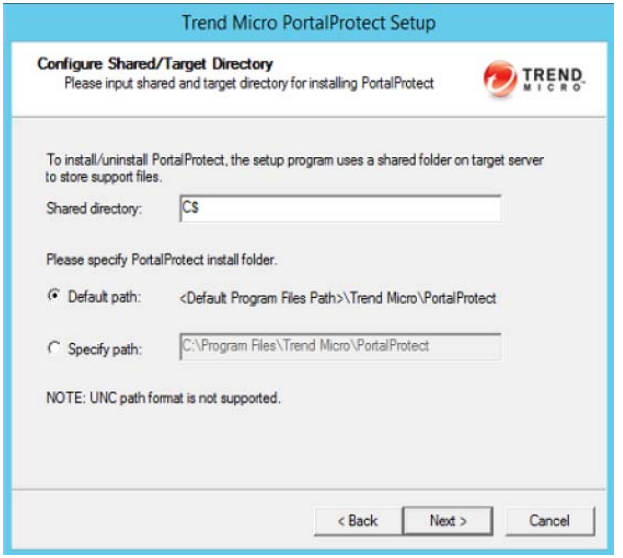

FIGURE 2-7. Configure Shared/Target Directory screen

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.

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

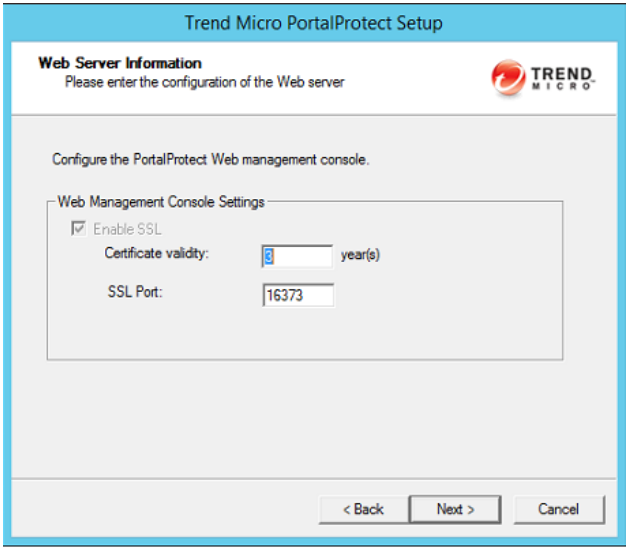

FIGURE 2-8. Web Server Information screen

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

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

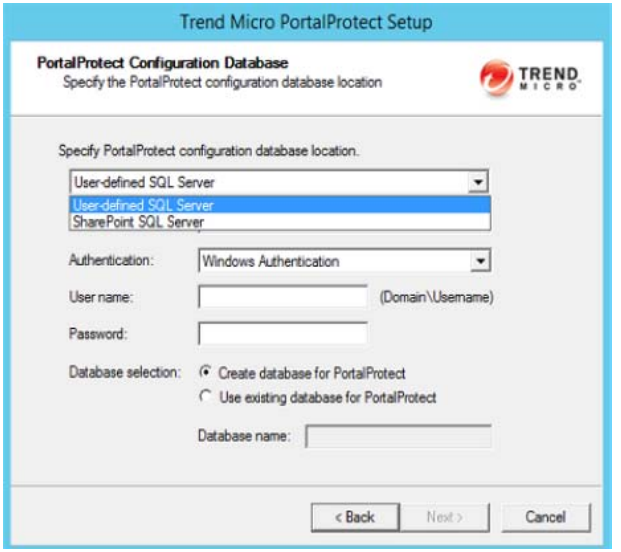

FIGURE 2-9. PortalProtect Configuration Database screen

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 or use an existing 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.

- **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

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

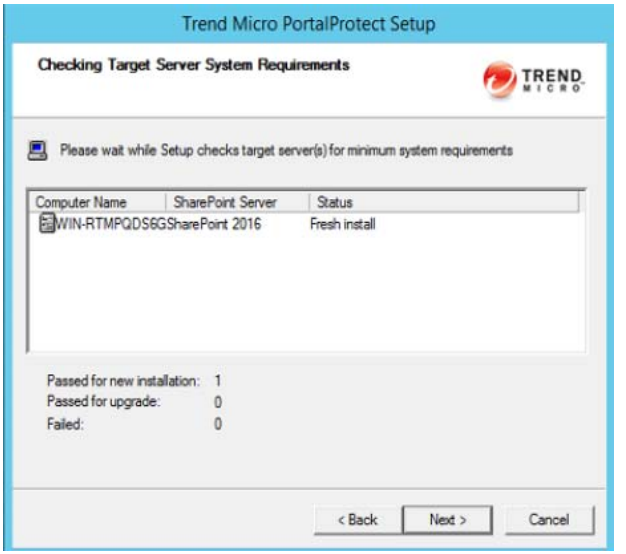

FIGURE 2-10. Checking Target Server System Requirements screen

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.

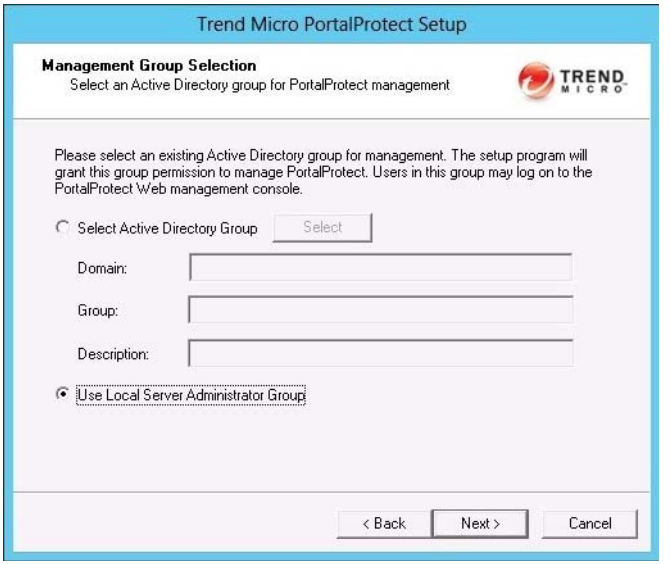

FIGURE 2-11. Management Group Selection screen

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.

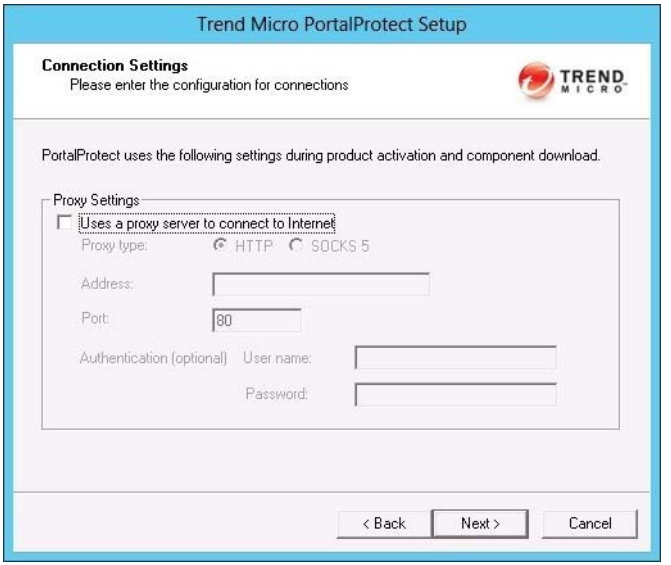

FIGURE 2-12. Connection Settings screen

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 >**.

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

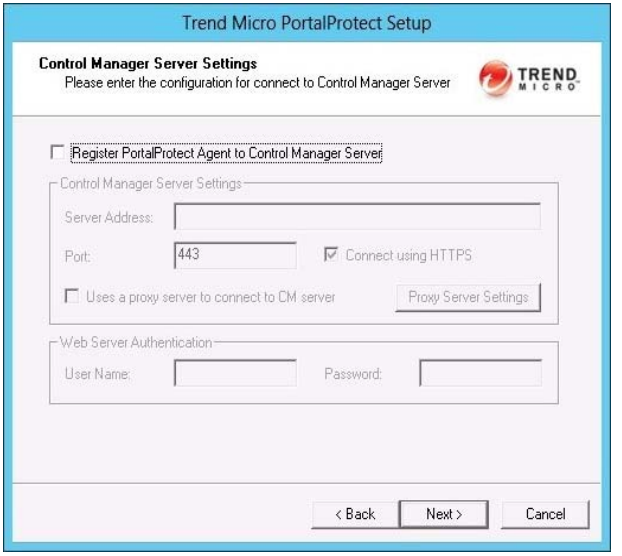

FIGURE 2-13. Control Manager Server Settings screen

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 >**.

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

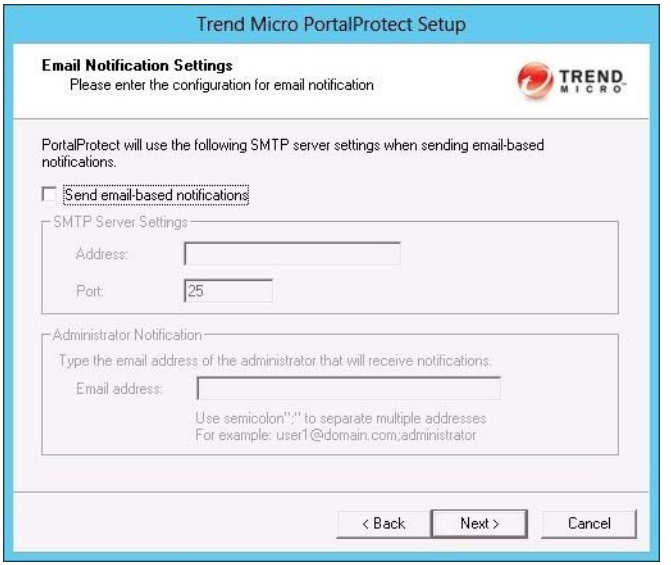

FIGURE 2-14. Email Notification Settings screen

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 >**.

16. The **Review Settings** screen appears.

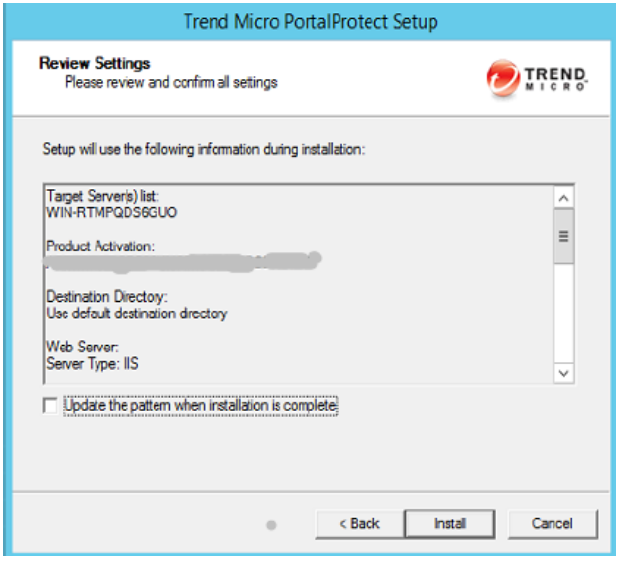

FIGURE 2-15. Review Settings screen

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**.

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

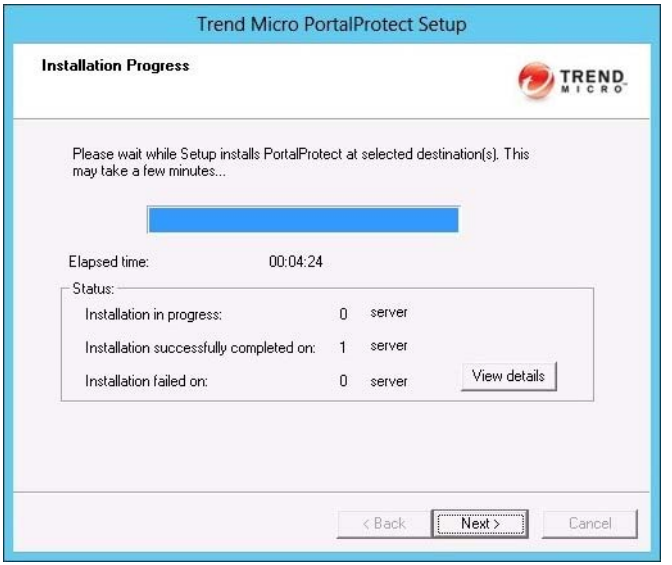

FIGURE 2-16. Installation Progress screen

18. While the installation is active, click **View details** to check the status (see *Figure 2-17* on page 2-19).

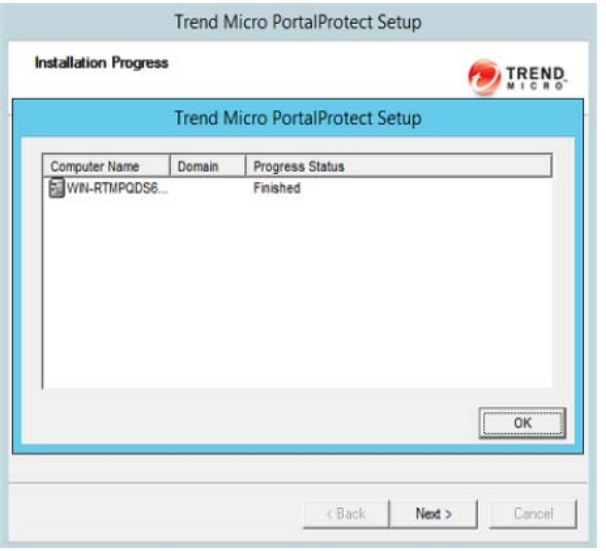

FIGURE 2-17. Installation progress status (Finished)

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

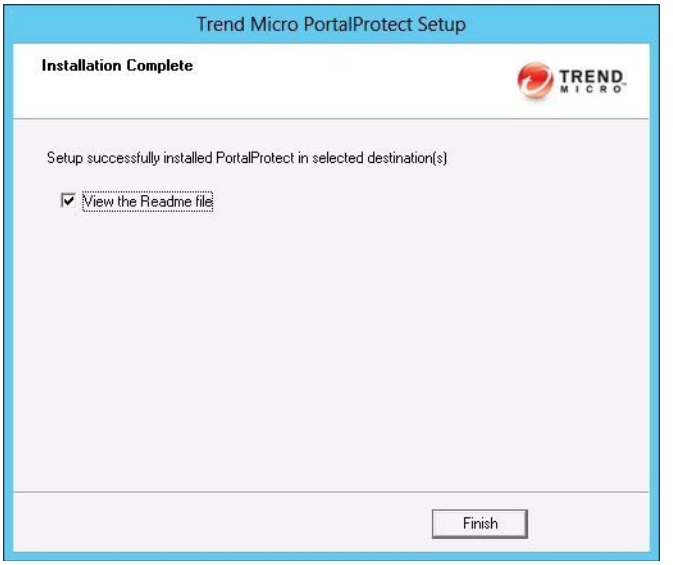

FIGURE 2-18. Installation Complete screen

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

Silent Fresh Installation

Silent Fresh 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 perform a fresh installation of PortalProtect using SilentSetup.bat:

1. Go to **PortalProtect setup package** where you can see a list of executable files.
2. Copy all the files in the PortalProtect setup package along with the tool **SilentSetup.bat** 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 a specified location.

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

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

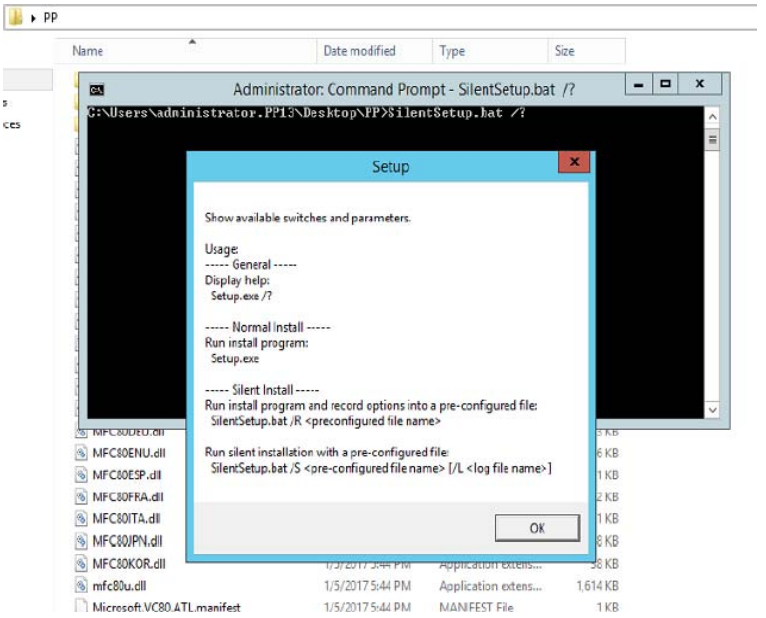

FIGURE 2-19. Silent setup help

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

Note: This step records the configurations that PortalProtect silent installation will use.

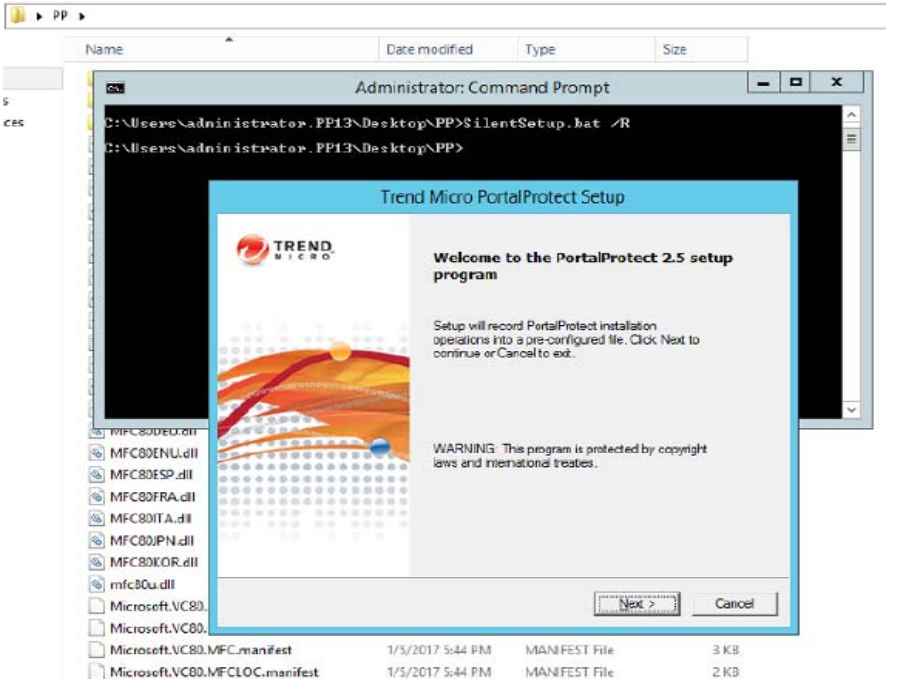

FIGURE 2-20. Silent installation welcome screen

Note: You can define a specific path to store the pre-configured file using: **SilentSetup /R <pre-configuration file>**. If you do not specify the pre-configuration file, 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`.

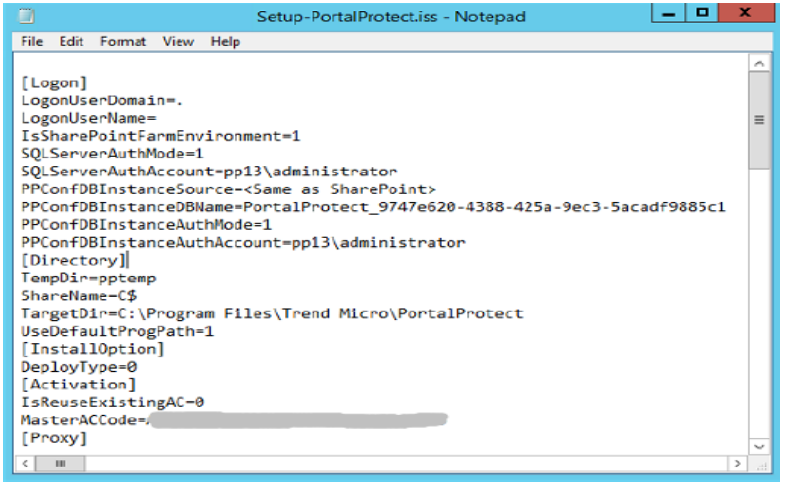

FIGURE 2-21. Setup-PortalProtect.iss file

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

---

7. Run **SilentSetup /S** <preconfiguration file> to enable Silent Install to perform an unattended installation of PortalProtect.

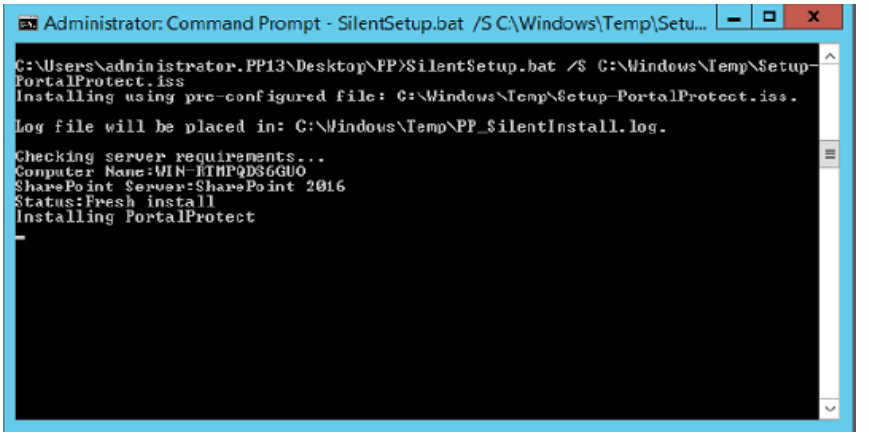

FIGURE 2-22. Installation screen

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

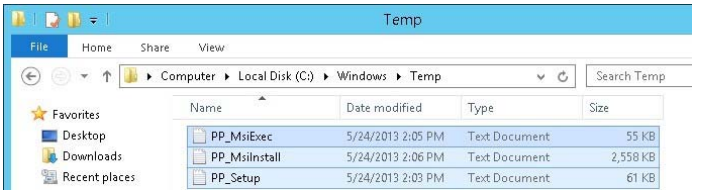

FIGURE 2-23. Setup log files

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\PortalProtect`.

Post Installation

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 Server:

1. From within SharePoint, go to **SharePoint 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**

Note: Make sure the **SharePoint 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**.

Notice:

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.

Upgrading PortalProtect

You can upgrade PortalProtect in two ways:

- Using an installation program called **setup.exe** (*Upgrading Using Setup Program* on page 2-26**)**
- Using a silent installation program called **SilentSetup.bat** (see *To perform a fresh installation of PortalProtect using SilentSetup.bat:* on page 2-20**)**

Upgrading Using Setup Program

To upgrade PortalProtect using setup program:

1. From your upgrade package, run ***`Setup.exe`***.

   The welcome screen appears.

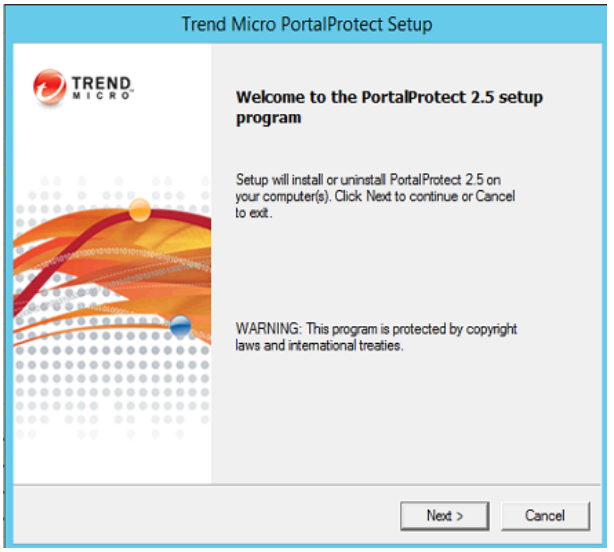

FIGURE 2-24. PortalProtect Upgrade Welcome screen

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

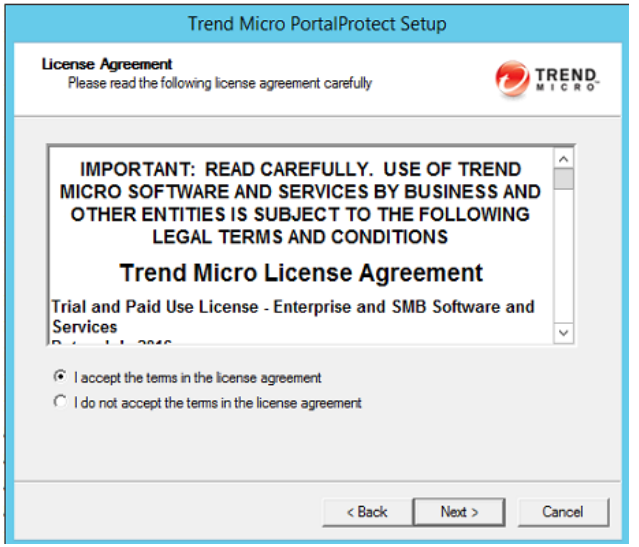

FIGURE 2-25. License Agreement screen

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 **Select an Action** screen (1) appears. Choose one of the following installation 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**.

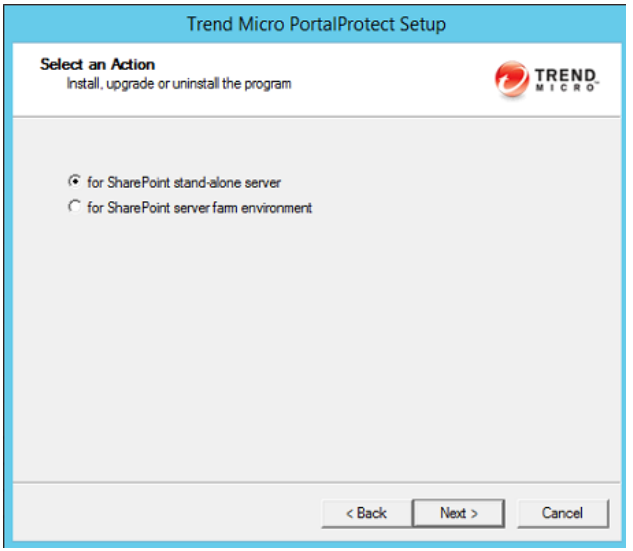

FIGURE 2-26. Select an Action screen (1)

4. Select the appropriate option and click **Next**.

   The **Select an Action Install, upgrade or uninstall PortalProtect** screen appears.

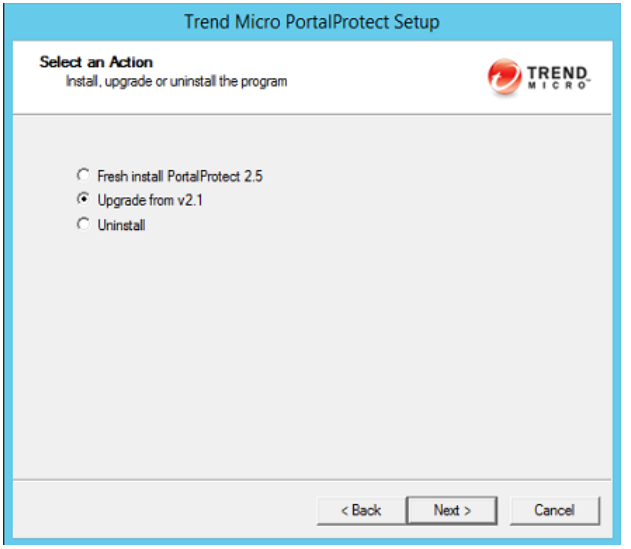

FIGURE 2-27. Select an Action screen (2)

5. Select **Upgrade from v2.1** and click **Next >**.

   The **Product Activation** screen appears.

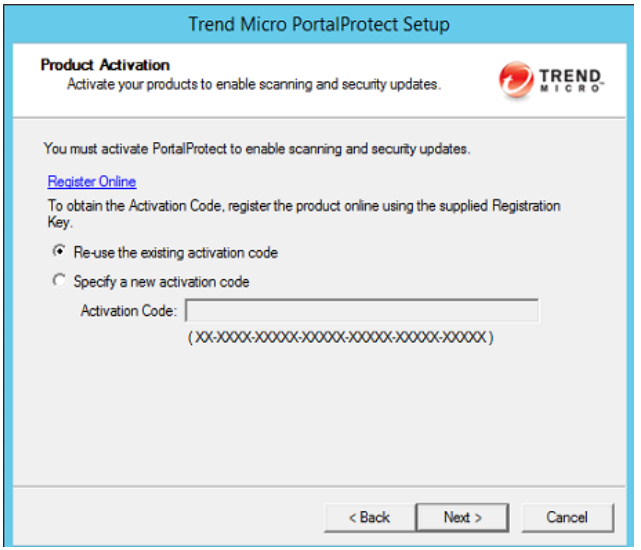

FIGURE 2-28. Product Activation screen

6. Enter the **Activation Code**. You can use your existing activation code or specify a new one. Click **Next >**.

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

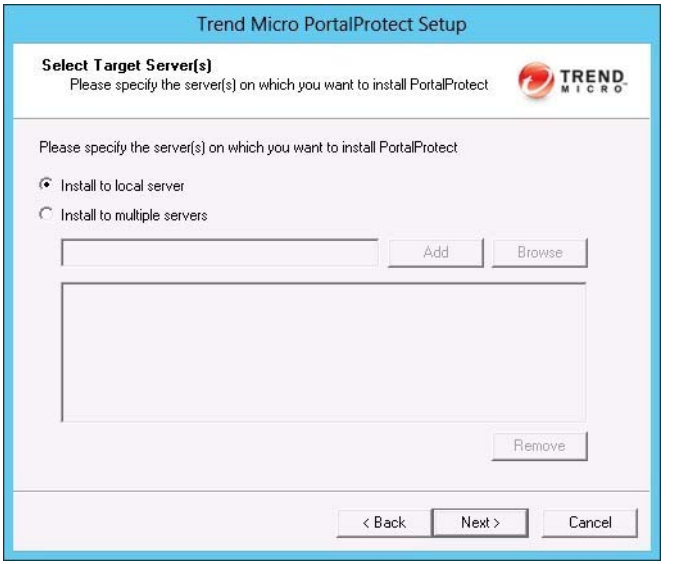

FIGURE 2-29. Select Target Server(s) screen

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 displays.

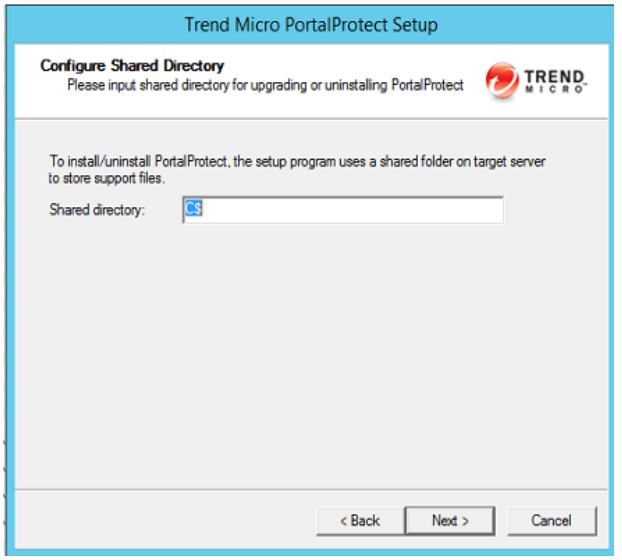

FIGURE 2-30. Configure Shared/Target Directory screen

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.

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

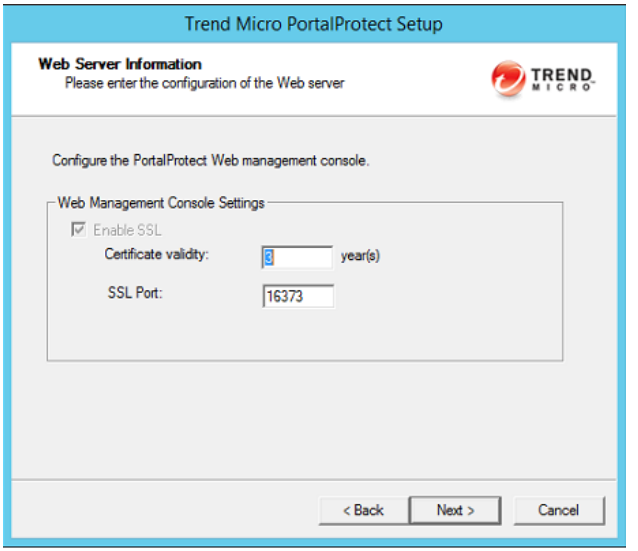

FIGURE 2-31. Web Server Information screen

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

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

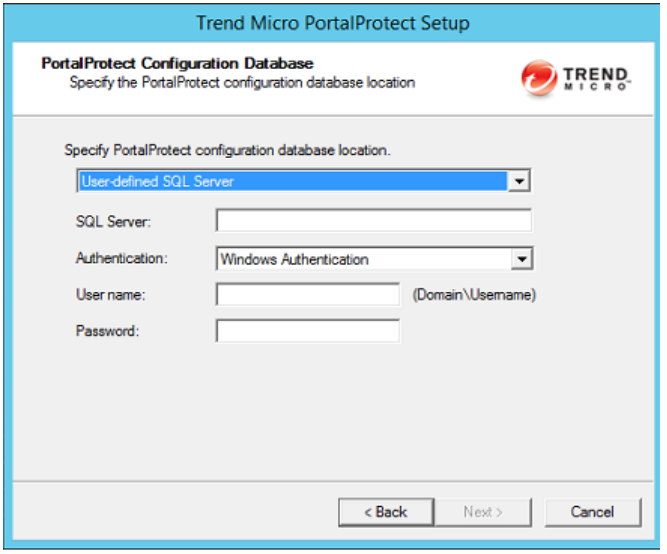

FIGURE 2-32. PortalProtect Configuration Database screen

WARNING! **Make sure to use the same database settings as used for the previous version.**

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 or use an existing 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.

- **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

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

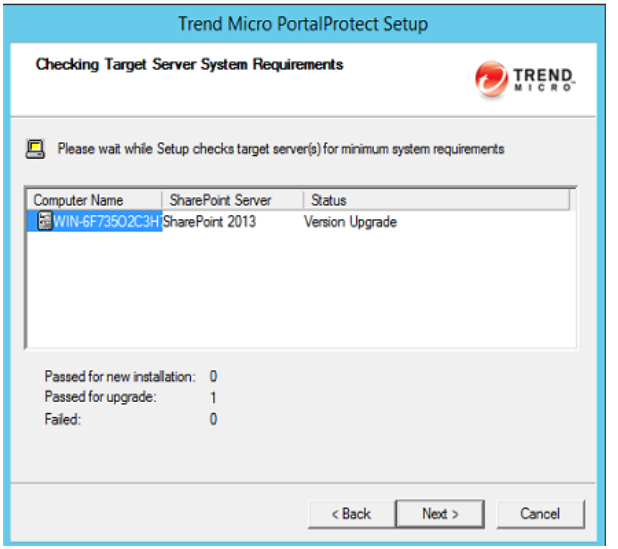

FIGURE 2-33. Checking Target Server System Requirements screen

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

Whether PortalProtect 2.1 is 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 SharePoint DB access account is identical with PortalProtect 2.1
- Whether the PortalProtect DB access account is identical with PortalProtect 2.1

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

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

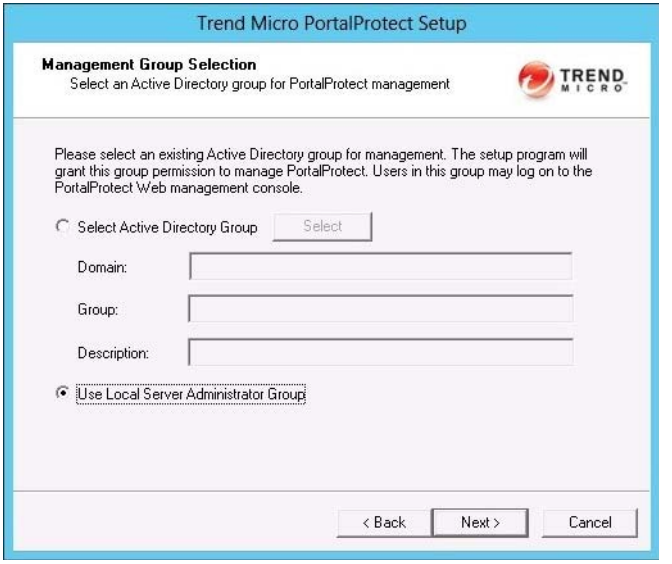

FIGURE 2-34. Management Group Selection screen

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 >**.

    The **Review Settings** screen appears.

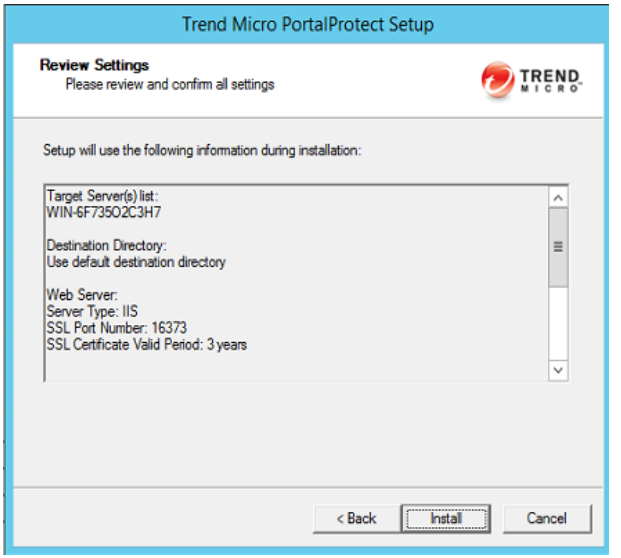

FIGURE 2-35. Review Settings screen

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**.

13. The **Installation Progress** screen displays.

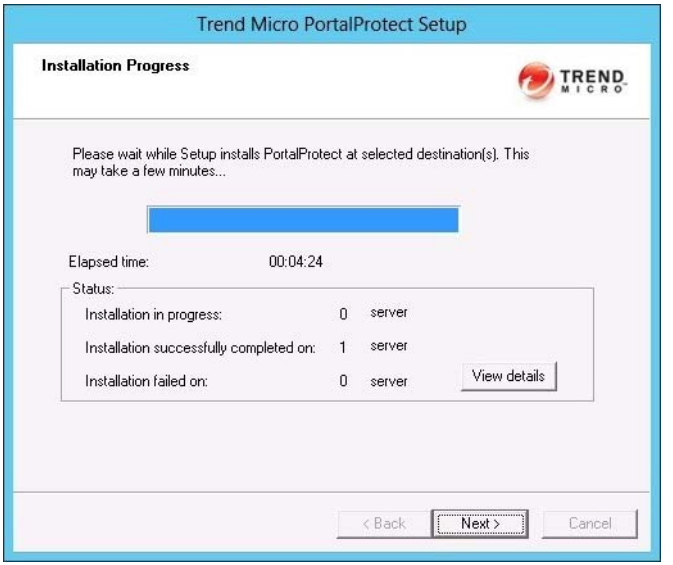

FIGURE 2-36. Installation Progress screen

14. While the installation is active, click **View details** to check the status (see *Figure 2-17* on page 2-19).

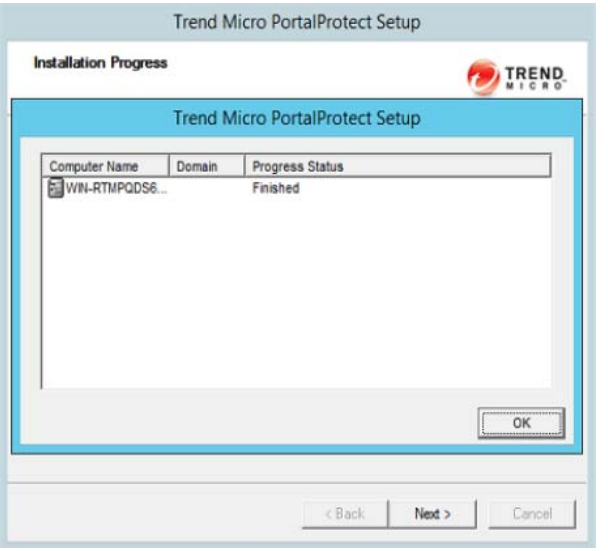

FIGURE 2-37. Installation progress status (Finished)

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

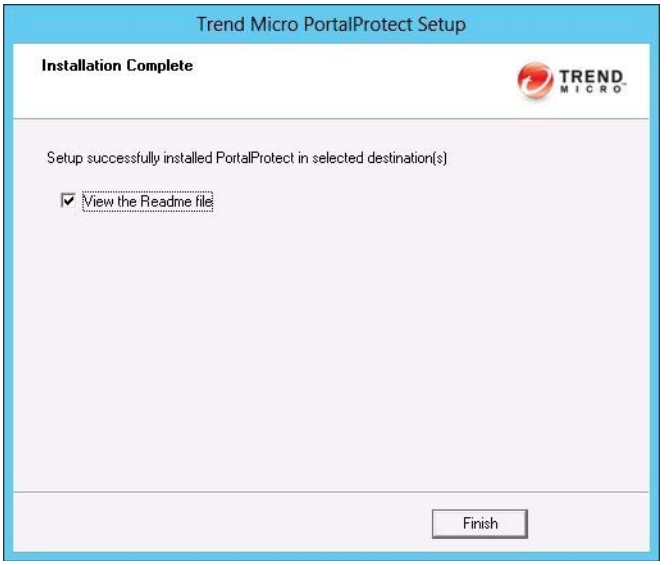

FIGURE 2-38. Installation Complete screen

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

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:

- From the Windows Control Panel—Add/Remove Programs (recommended)
- Using ***`Setup.exe`*** program

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 ***`Setup.exe`*** program.

To uninstall PortalProtect using Setup.exe program:

1. Navigate to ***Setup.exe*** and open it.
2. The Trend Micro PortalProtect setup program screen displays.

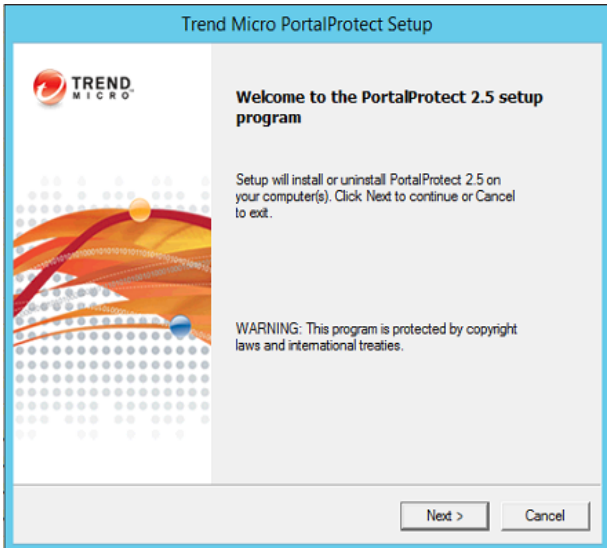

FIGURE 2-39. Trend Micro PortalProtect setup program screen

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

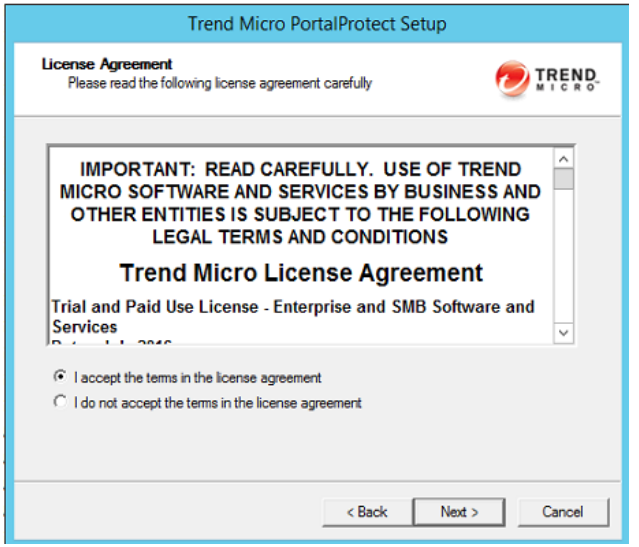

FIGURE 2-40. License Agreement screen

4. Select **I accept the terms in the license agreement** and click **Next >**.
5. The **Select an Action** screen (1) appears. Choose one of the following installation options:
   - **for SharePoint stand-alone server**
   - **for SharePoint server farm environment**

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

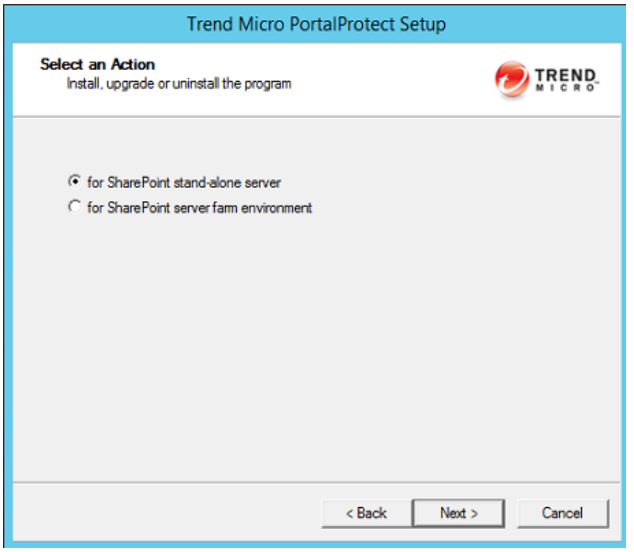

FIGURE 2-41. Select an Action screen (1)

6. Select the appropriate option and click **Next**.

   The **Select an Action - Install, upgrade or uninstall PortalProtect** screen appears.

7. Select **Uninstall** and click **Next**.

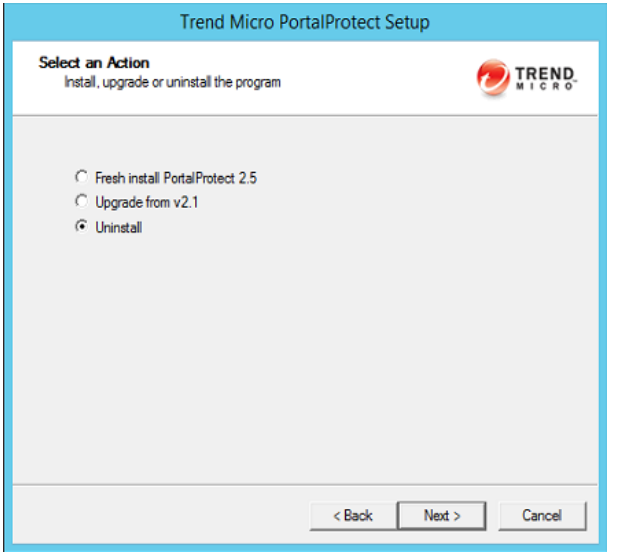

FIGURE 2-42. Select an Action screen (2)

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

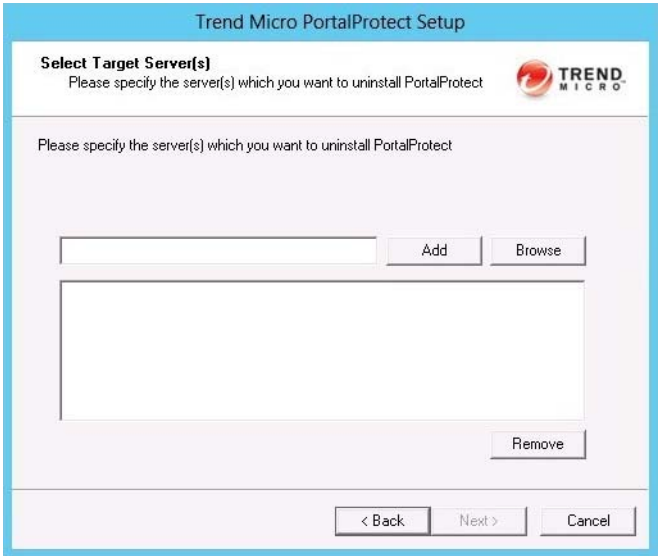

FIGURE 2-43. Select Target Server(s) screen

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

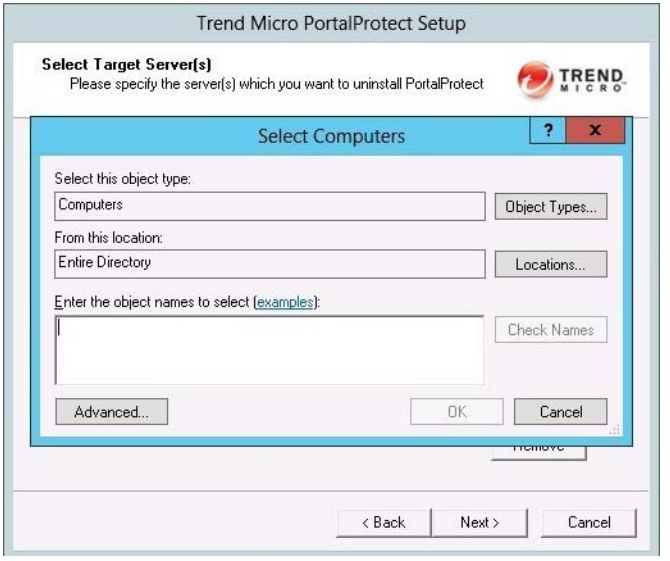

FIGURE 2-44. Select Computers dialog

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

FIGURE 2-45. Logon screen

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

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

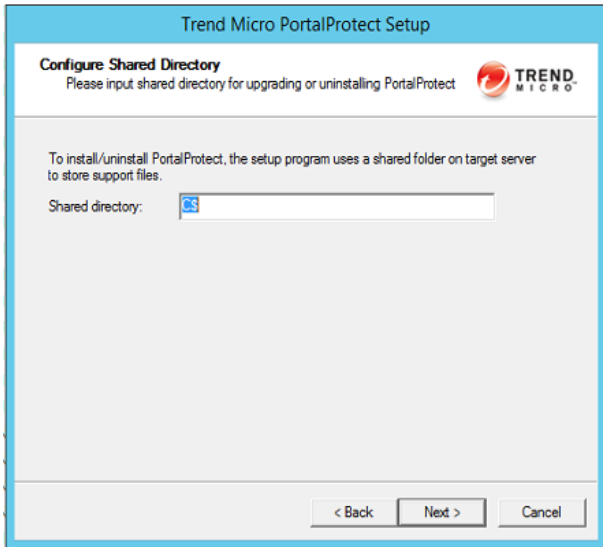

FIGURE 2-46. Configure Shared Directory screen

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

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

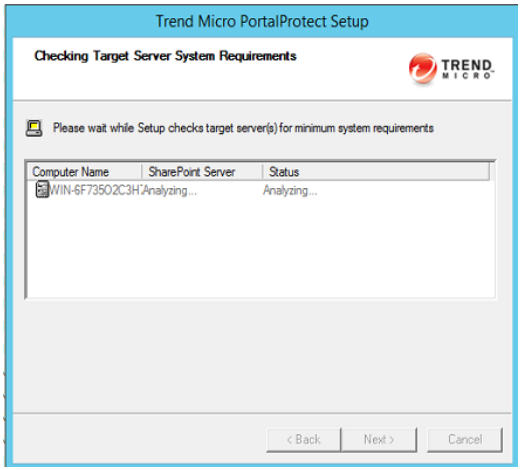

FIGURE 2-47. Checking Target Server System Requirements screen

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

17. The **Uninstall Notice** screen displays.

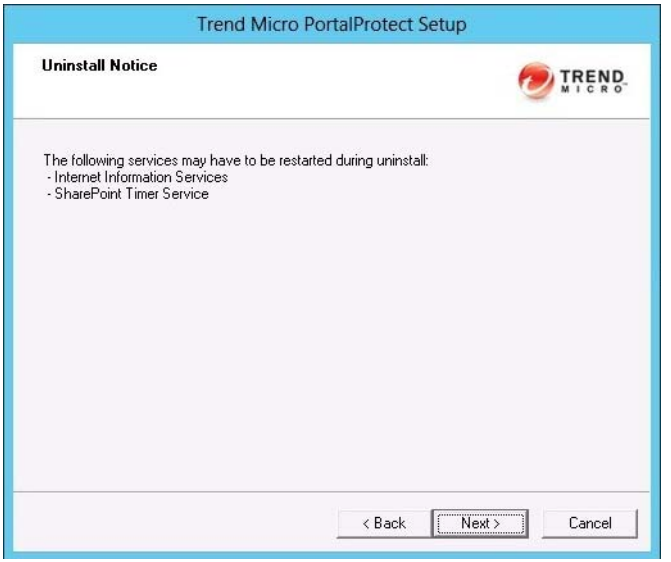

FIGURE 2-48. Uninstall Notice screen

Click **Next >**.

18. The **Review Settings** screen displays.

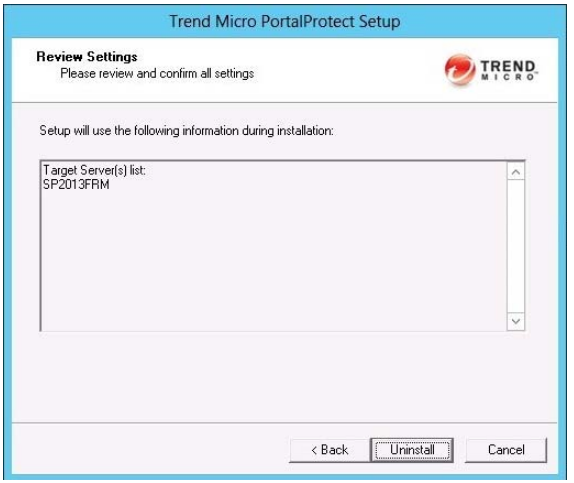

FIGURE 2-49. Review Settings screen

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

19. The **Uninstallation Progress** screen displays.

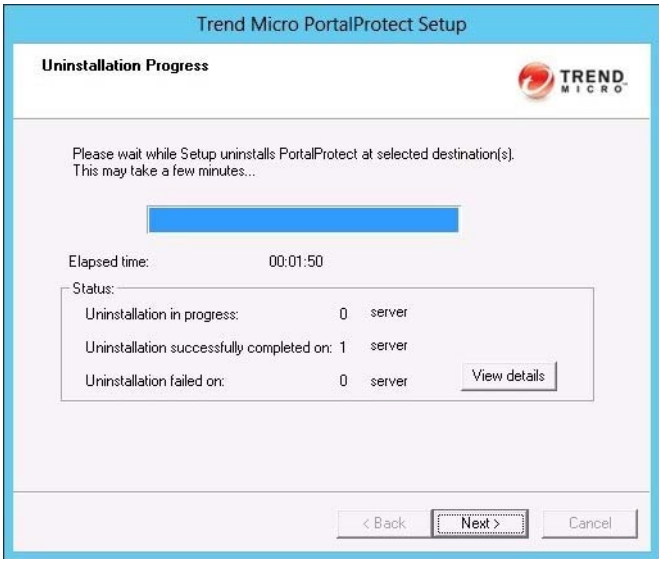

FIGURE 2-50. Uninstallation Progress screen

Click **View Details** to observe the uninstallation progress (see *Figure 2-51* on page 2-55).

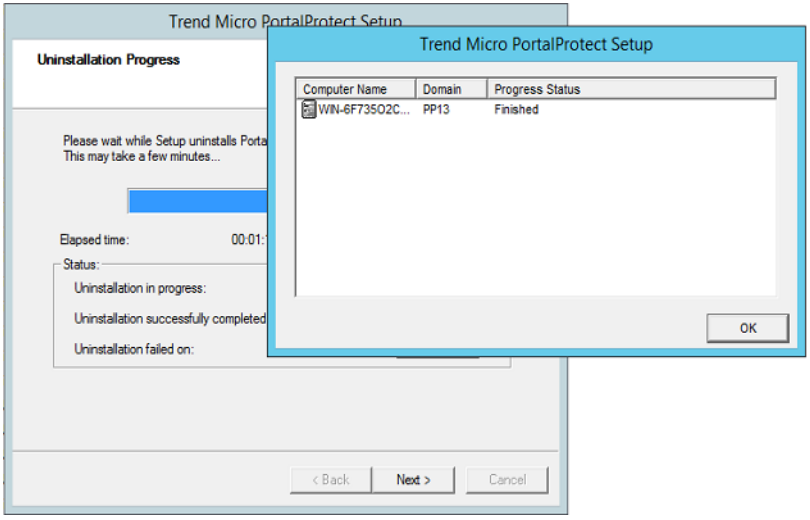

FIGURE 2-51. Uninstallation Progress Status

20. When the **Progress Status** displays **Finished** (*Figure 2-51*), click **OK > Next >**.
21. The **Uninstallation Complete** screen displays.

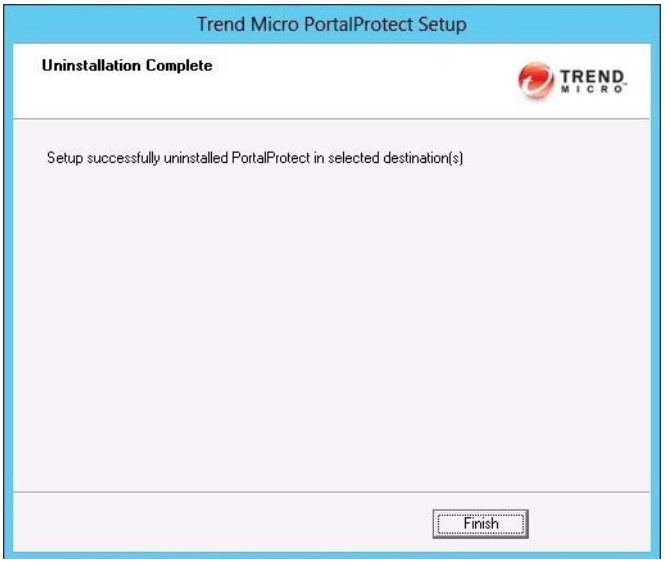

FIGURE 2-52. Uninstallation Complete screen

Chapter 3

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

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

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

- Worldwide support offices:
  http://www.trendmicro.com/us/about-us/contact/index.html
- Trend Micro product documentation:
  http://docs.trendmicro.com

TrendLabs

Trend Micro TrendLabs. is a global network of antivirus research and product support centers providing continuous, 24 x 7 coverage to Trend Micro customers worldwide.

Staffed by a team of more than 250 engineers and skilled support personnel, the TrendLabs dedicated service centers worldwide ensure rapid response to any virus outbreak or urgent customer support issue, anywhere in the world.

The TrendLabs modern headquarters earned ISO 9002 certification for its quality management procedures in 2000. TrendLabs is one of the first antivirus research and support facilities to be so accredited. Trend Micro believes that TrendLabs is the leading service and support team in the antivirus industry.

For more information about TrendLabs, please visit:

http://us.trendmicro.com/us/about/company/trendlabs/

Speeding Up Your Support Call

When you contact Trend Micro, to speed up your problem resolution, ensure that you have the following details available:

- Operating System and Service Pack version
- Network type
- Computer brand, model, and any additional hardware connected to your computer
- Browser version
- Amount of memory and free hard disk space on your computer
- Detailed description of the install environment
- Exact text of any error message given
- Steps to reproduce the problem

Using the Support Portal

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

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

> **Note:** To submit a support case online, visit the following URL:
> http://esupport.trendmicro.com/srf/SRFMain.aspx

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

Security Information Site

Comprehensive security information is available at the Trend Micro website:

http://about-threats.trendmicro.com

In the PortalProtect banner at the top of any PortalProtect screen, click the Help drop down, then Security Info.

Information available:

- List of viruses and malicious mobile code are currently "in the wild," or active
- Computer virus hoaxes
- Internet threat advisories
- Virus weekly report
- Virus Encyclopedia, which includes a comprehensive list of names and symptoms for known viruses and malicious mobile code
- Glossary of terms

Frequently Asked Questions (FAQs)

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 Windows 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\SOFTWARE\TrendMicro\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\SOFTWARE\TrendMicro\PortalProtect\CurrentVersion\PPConfDatabasePassword

   b. Change the password and restart PortalProtect Master Service.

Why I cannot open PortalProtect Management Console from Windows Server 2016 Start menu?

In some cases, Windows Server 2016 does not provide a default Web browse application in Start menu. To add a Web browser, such as Internet Explorer, navigate to **Settings** > **Default apps**, and add a link to your desired Web browser.

Which third-party software will be installed during PortalProtect installation?

PortalProtect will install the following third-party software during installation:

- Microsoft Visual C++ 2005 Redistributable (x64)
- Microsoft Visual C++ 2010 x64 Redistributable
- Microsoft SQL Server 2012 Native Client

Note: A system reboot might be required by Microsoft for the installation of "Microsoft Visual C++ 2010 x64 Redistributable" and "Microsoft SQL Server 2012 Native Client".

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 2.5.

- **PortalProtect**—Trend Micro PortalProtect for Microsoft SharePoint
- **SQL Server**—SQL Server 2008, 2012, 2014 or 2016
- **SharePoint**—Microsoft SharePoint Server 2010, 2013 or 2016

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.

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

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

`HKLM\Software\TrendMicro\PortalProtect\CurrentVersion`

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

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.
- If SQL server authentication is used by both PortalProtect and SharePoint databases, Web content scan and manual scan in PortalProtect will not work due to feature limitations.
- The PortalProtect service startup account must have permanent local administrator privileges. Otherwise, the installation will fail.

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 the SharePoint environment, PortalProtect requires a database for fresh install and uses the same databases for upgrade.

For fresh install. PortalProtect will create the following database:

- PortalProtect_{UUID}

The following is the required database permission for the PortalProtect Configuration Database Access Account:

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

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

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: db_datareader** and **WSS_Content_Application_Pools** roles
- **WSS_Content Database: db_owner** role

Note: If there is more than one WSS_Content database, specify this role to each WSS_Content database.

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.

Index

W

TREND MICRO INCORPORATED

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

www.trendmicro.com

Item Code: PPEM27723/170216