

# 2.6 PortalProtect™ Installation and Deployment Guide

for Microsoft™ SharePoint



Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

http://docs.trendmicro.com/en-us/enterprise/endpoint-encryption.aspx

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

Copyright © 2023. Trend Micro Incorporated. All rights reserved.

Document Part No.: PPEM28660/190425

Release Date: March 2022

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

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

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

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

Evaluate this documentation on the following site:

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

**Privacy and Personal Data Collection Disclosure** 

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

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

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

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

https://www.trendmicro.com/privacy



# **Table of Contents**

#### Preface

Preface	iv
PortalProtect Documentation	iv
Audience	v
Document Conventions	v

#### Chapter 1: Planning PortalProtect Installation and Upgrade

System Requirements	1-2
PortalProtect 2.6 with SharePoint Server Subscription	
Edition	1-2
PortalProtect 2.6 with SharePoint Server 2019	1-4
PortalProtect 2.6 with SharePoint Server 2016	1-6
PortalProtect 2.6 with SharePoint Server 2013	1-8
Deployment Strategy	1-10
Deployment Strategy SharePoint Services Small Server Farm	1-10 1-10
Deployment Strategy SharePoint Services Small Server Farm SharePoint Services Medium Server Farm	1-10 1-10 1-12
Deployment Strategy SharePoint Services Small Server Farm SharePoint Services Medium Server Farm SharePoint Services Large Server Farm	1-10 1-10 1-12 1-13

#### **Chapter 2: Installing and Removing PortalProtect**

Performing a Fresh Installation of PortalProtect	. 2-2
Setup.exe Installation Silent Fresh Installation	. 2-2 2-22
Post Installation	2-28
Upgrading PortalProtect	2-29
Upgrading Using Setup Program	2-29
Testing Your Installation	2-46
Removing PortalProtect	2-47

#### **Chapter 3: Technical Support**

Troubleshooting Resources	3-2
Using the Support Portal Threat Encyclopedia	3-2 3-2
Contacting Trend Micro	3-3
Speeding Up the Support Call	3-3
Sending Suspicious Content to Trend Micro	3-4
Email Reputation Services File Reputation Services Web Reputation Services	3-4 3-4 3-5
Other Resources	3-5
Download Center Documentation Feedback	. 3-5 . 3-5

#### Chapter 4: Frequently Asked Questions (FAQs)

nstallation 4-2
-----------------

#### **Appendix A: PortalProtect Database Permission Requirements**

Applications	A-2
Background	A-2
Requirements for PortalProtect Configuration Database	
Access Account	A-4
Requirements for SharePoint Database Access Account	A-4

#### Index

ii

Index IN	V	-	1
----------	---	---	---



iii



#### Preface

Welcome to the Trend Micro<sup>™</sup> PortalProtect<sup>™</sup> Installation and Deployment Guide. This guide contains basic information about the tasks you need to perform to deploy PortalProtect to protect your SharePoint servers according to your specific needs. It is intended for novice and advanced users who want to plan, deploy and test PortalProtect.

This preface discusses the following topics:

- PortalProtect Documentation on page iv
- Audience on page v
- Document Conventions on page v

# **PortalProtect Documentation**

PortalProtect documentation consists of the following:

- **Online Help**: Web-based documentation that is accessible from the product console. The Online Help contains explanations about PortalProtect features.
- **Installation and Deployment Guide**: PDF documentation that can be downloaded from the Trend Micro Web site. This document contains instructions about deploying PortalProtect, a task that includes planning and testing.
- Administrator's Guide: Helps you configure all product settings.
- **Readme File**: Contains late-breaking product information that might not be found in the other documentation. Topics include a description of features, installation tips, known issues, and product release history.

#### 🕴 Note

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

# Audience

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

## **Document Conventions**

The documentation uses the following conventions.

TABLE 1.	Document	Conventions
----------	----------	-------------

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

CONVENTION	DESCRIPTION
WARNING!	Critical actions and configuration options





# **Chapter 1**

# Planning PortalProtect Installation and Upgrade

Trend Micro PortalProtect<sup>™</sup> is a server-based security solution for Microsoft SharePoint<sup>™</sup> Server 2013/2016/2019/Subscription Edition. 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 on page 1-2
- Deployment Strategy on page 1-10
- Preparing for Installation on page 1-14

# **System Requirements**

The following sections list the system requirements for PortalProtect.

#### PortalProtect 2.6 with SharePoint Server Subscription Edition

You need the following to effectively run PortalProtect 2.6 with SharePoint Server Subscription Edition:

HARDWARE/SOFTWARE	REQUIREMENT	RECOMMENDED
Processor	<ul> <li>X64 architecture-based processor that supports Intel Extended Memory 64 Technology (Intel EM64T)</li> <li>X64 architecture-based computer with AMD 64-bit processor that supports AMD64 platform</li> </ul>	
Memory	1-GB RAM	2-GB RAM or higher
	(Exclusively for PortalProtect)	(Exclusively for PortalProtect)
Disk Space	2-GB free disk space	5-GB free disk space
Windows Server	<ul> <li>Windows Server 2019 Standard or Datacenter</li> <li>Windows Server 2022 Standard or Datacenter</li> <li>PortalProtect supports the following Windows Server installation options: <ul> <li>Server with Desktop Experience</li> <li>Server Core</li> </ul> </li> </ul>	
SharePoint Service/Server	Microsoft SharePoint Server Subscription Edition	

TABLE 1-1. PortalProtect 2.6 with SharePoint Server Subscription Edition

1-2

HARDWARE/SOFTWARE	REQUIREMENT	RECOMMENDED
Web Server	Microsoft Internet Informa	tion Services (IIS) 10.0
	The following IIS features are re installation:	quired for PortalProtect
	Common HTTP Features	
	Static Content	
	<ul> <li>Default Document</li> </ul>	
	<ul> <li>Directory Browsing</li> </ul>	
	HTTP Errors	
	<ul> <li>Application Development</li> </ul>	
	<ul> <li>Common Gateway Int</li> </ul>	erface (CGI)
	ISAPI Extensions	
	<ul> <li>ISAPI Filters</li> </ul>	
	<ul> <li>Health and Diagnostic</li> </ul>	
	HTTP Logging	
	<ul> <li>Request Monitor</li> </ul>	
	Security	
	<ul> <li>Windows Authenticat</li> </ul>	ion
	Performance	
	Static Content Compr	ession
	CGI must be installed m are installed together v	nanually, while other features vith SharePoint servers.
Browser	Microsoft Internet Explorer	7.0 or above
	• Mozilla Firefox 3.0 or above	2
	Google Chrome	
	<ul> <li>Microsoft Edge</li> </ul>	

1-4

HARDWARE/SOFTWARE	REQUIREMENT	RECOMMENDED
.NET Framework	3.5	

#### PortalProtect 2.6 with SharePoint Server 2019

You need the following to effectively run PortalProtect 2.6 with SharePoint Server 2019:

HARDWARE/SOFTWARE	REQUIREMENT	RECOMMENDED
Processor	<ul> <li>X64 architecture-based processor that supports Intel Extended Memory 64 Technology (Intel EM64T)</li> <li>X64 architecture-based computer with AMD 64-bit processor that supports AMD64 platform</li> </ul>	
Memory	1-GB RAM	2-GB RAM or higher
	(Exclusively for PortalProtect)	(Exclusively for PortalProtect)
Disk Space	2-GB free disk space	5-GB free disk space
Windows Server	<ul> <li>Windows Server 2016 Standard or Datacenter (Desktop Experience)</li> </ul>	
	<ul> <li>Windows Server 2019 Stan Experience)</li> </ul>	dard or Datacenter (Desktop
	<ul> <li>Windows Server 2022 Stan Experience)</li> </ul>	dard or Datacenter (Desktop
SharePoint Service/Server	Microsoft SharePoint Serv	er 2019

TABLE 1-2. PortalProtect 2.6 with SharePoint Server 2019

HARDWARE/SOFTWARE	REQUIREMENT	RECOMMENDED
Web Server	Microsoft Internet Informa	tion Services (IIS) 10.0
	The following IIS features are re installation:	quired for PortalProtect
	Common HTTP Features	
	Static Content	
	Default Document	
	<ul> <li>Directory Browsing</li> </ul>	
	HTTP Errors	
	Application Development	
	Common Gateway Int	erface (CGI)
	ISAPI Extensions	
	ISAPI Filters	
	<ul> <li>Health and Diagnostic</li> </ul>	
	HTTP Logging	
	Request Monitor	uest Monitor
	Security	
	<ul> <li>Windows Authenticat</li> </ul>	ion
	Performance	
	Static Content Compr	ession
	CGI must be installed m are installed together w	nanually, while other features vith SharePoint servers.
Browser	Microsoft Internet Explorer	7.0 or above
	• Mozilla Firefox 3.0 or above	2
	Google Chrome	
	Microsoft Edge	

1-6

HARDWARE/SOFTWARE	REQUIREMENT	RECOMMENDED
.NET Framework	3.5	

#### PortalProtect 2.6 with SharePoint Server 2016

You need the following to effectively run PortalProtect 2.6 with SharePoint Server 2016:

HARDWARE/SOFTWARE	REQUIREMENT	RECOMMENDED
Processor	<ul> <li>X64 architecture-based processor that supports Intel Extended Memory 64 Technology (Intel EM64T)</li> </ul>	
	<ul> <li>X64 architecture-based computer with AMD 64-bit processor that supports AMD64 platform</li> </ul>	
Memory	1-GB RAM	2-GB RAM or higher
	(Exclusively for PortalProtect)	(Exclusively for PortalProtect)
Disk Space	2-GB free disk space	5-GB free disk space
Windows Server	• Windows Server 2012 R2 S	tandard or Datacenter
	Windows Server 2016 Standard or Datacenter	
	Windows Server 2019 Stan	dard or Datacenter
SharePoint Service/Server	Microsoft SharePoint Server 2016	

#### TABLE 1-3. PortalProtect 2.6 with SharePoint Server 2016

HARDWARE/SOFTWARE	REQUIREMENT RECOMMENDED	
Web Server	Microsoft Internet Informa	tion Services (IIS) 10.0
	Microsoft Internet Informa	tion Services (IIS) 8.5
	Microsoft Internet Informa	tion Services (IIS) 8.0
	The following IIS features are reinstallation:	quired for PortalProtect
	Common HTTP Features	
	Static Content	
	<ul> <li>Default Document</li> </ul>	
	Directory Browsing     HTTP Errors	
Application     Comm	<ul> <li>Application Development</li> </ul>	
	Common Gateway Int	erface (CGI)
	ISAPI Extensions	
	<ul> <li>ISAPI Filters</li> </ul>	
	<ul> <li>Health and Diagnostic</li> </ul>	
	HTTP Logging	
	Request Monitor	
	Security	
	<ul> <li>Windows Authenticat</li> </ul>	ion
	Performance	
	Static Content Compr	ession
	CGI must be installed n are installed together v	nanually, while other features vith SharePoint servers.



HARDWARE/SOFTWARE	REQUIREMENT	RECOMMENDED
Browser	Microsoft Internet Explorer 7.0 or above	
	Mozilla Firefox 3.0 or above	
	Google Chrome	
	<ul> <li>Microsoft Edge</li> </ul>	
.NET Framework	3.5	

#### PortalProtect 2.6 with SharePoint Server 2013

You need the following to effectively run PortalProtect 2.6 with SharePoint Server 2013:

HARDWARE/SOFTWARE	REQUIREMENT	RECOMMENDED
Processor	<ul> <li>X64 architecture-based processor that supports Intel Extended Memory 64 Technology (Intel EM64T)</li> </ul>	
	<ul> <li>X64 architecture-based computer with AMD 64-bit processor that supports AMD64 platform</li> </ul>	
Memory	1-GB RAM	2-GB RAM or higher
	(Exclusively for PortalProtect)	(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 S	tandard with SP1 (64-bit)
	• Windows Server 2008 R2 E	nterprise with SP1 (64-bit)
SharePoint Service/Server	Microsoft SharePoint Serve	er 2013 or above

 TABLE 1-4. PortalProtect 2.6 with SharePoint Server 2013

1-8

HARDWARE/SOFTWARE	REQUIREMENT RECOMMENDED	
Web Server	Microsoft Internet Informa	tion Services (IIS) 8.5
	Microsoft Internet Informa	tion Services (IIS) 8.0
	Microsoft Internet Informa	tion Services (IIS) 7.5
	The following IIS features are re installation:	equired for PortalProtect
	Common HTTP Features	
	Static Content	
	<ul> <li>Default Document</li> </ul>	
	Directory Browsing     HTTP Errors	
	Application Development	
	Common Gateway Int	erface (CGI)
	ISAPI Extensions	
	ISAPI Filters	
	<ul> <li>Health and Diagnostic</li> </ul>	
	<ul> <li>HTTP Logging</li> </ul>	
	<ul> <li>Request Monitor</li> </ul>	
	Security	
	<ul> <li>Windows Authenticat</li> </ul>	ion
	Performance	
	Static Content Compr	ession
	CGI must be installed n are installed together v	nanually, while other features vith SharePoint servers.

1-9

HARDWARE/SOFTWARE	REQUIREMENT	RECOMMENDED
Browser	Microsoft Internet Explorer 7.0 or above	
	Mozilla Firefox 3.0 or above	
	Google Chrome	
	<ul> <li>Microsoft Edge</li> </ul>	
.NET Framework	3.5	

## **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



1-10

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

1-12

1-13

#### **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 2.6 to a server with the appropriate server platforms installed; see *System Requirements 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 2.6 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 2.6. It must also be the user account that already joins the domain where the server(s) to install PortalProtect 2.6 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.



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 on page 2-2
- Post Installation on page 2-28
- Upgrading PortalProtect on page 2-29
- Testing Your Installation on page 2-46
- Removing PortalProtect on page 2-47

# **Performing a Fresh Installation of PortalProtect**

#### ) Тір

Before installing PortalProtect 2.6, 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 *Setup.exe Installation on page 2-2*)
- Using a silent installation program called SilentSetup.bat (see *Silent Fresh Installation on page 2-22*)

#### **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.

#### Procedure

2-2

1. Run setup.exe from the PortalProtect 2.6 to start the installation.



#### The PortalProtect Installation Welcome screen appears.

FIGURE 2-1. Installation Welcome screen

2. Click Next >.

#### The License Agreement screen appears.

	ORTANT: READ	CAREFULLY. U	SE OF TREND BUSINESS AND	^
OTHE	R ENTITIES IS S LEGAL TERM	UBJECT TO TH	E FOLLOWING	
	Trend Micro	License Agr	eement	
Trial and Services	Paid Use License	- Enterprise and S	MB Software and	~
I accept	the terms in the license a	greement		
C I do not	accept the terms in the lie	cense agreement		

FIGURE 2-2. License Agreement screen

2-4

**3.** 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.

Trend Micro Por	talProtect Set	up
Select an Action Install, upgrade or uninstall the program		
● for SharePoint stand-alone server		
○ for SharePoint server farm environment		
	< Back	Next > Cance

#### The **Select an Action** screen (1) appears.



- **4.** Choose one of the following installation options:
  - for SharePoint stand-alone server
  - for SharePoint server farm environment
- 5. After selecting the appropriate options, click Next >.



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**.

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

Trend Micro Por	talProtect Setup
Select an Action Install, upgrade or uninstall the program	
<ul> <li>Fresh install PortalProtect 2.6</li> <li>Upgrade from PortalProtect 2.5 SP1</li> <li>Uninstall</li> </ul>	
	< Back Next > Cancel

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

2-6

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

The Product Activation screen appears.

Trend Micro PortalProtect Setup		
Product Activation Activate your prod	ucts to enable scanning and security updates.	
You must activate Por	alProtect to enable scanning and security updates.	E.
Register Online		
To obtain the Activati Key.	on Code, register the product online using the supp	lied Registration
Activation Code		1
	(>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	××)
	< Back Next	t> Cancel

FIGURE 2-5. Product Activation screen

- 7. 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.

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

Select Target Server(s) Please specify the server(s) on which you want to install PortalProtect		
Please specifu the server(s) on which	you want to install PortalProtect	
Install to local server		
C Install to multiple servers		
	Add Browse	
	Remove	

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

- 8. 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.

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

To install/uninstall P to store support files	PortalProtect, the setup program uses a shared folder on target server
Shared directory:	Cs
Please specify Porta	alProtect install folder.
verauli patri.	<default files="" path="" program="">\Trend Micro\PortalProtect</default>
C Specify path:	C:\Program Files\Trend Micro\PortalProtect

FIGURE 2-7. Configure Shared/Target Directory screen

**9.** 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.



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

The **Web Server Information** screen appears.

Web Server Information Please enter the configuration	of the Web server	
Configure the PortalProtect Wel	o management console.	
_ Web Management Console Se	ttings	
🔽 Enable SSL		
Certificate validity:	g year(s)	
SSL Port:	16373	

FIGURE 2-8. Web Server Information screen

**10.** Type the SSL port number for the Web Management Console in the **SSL Port** field. Click **Next** >.
#### The **PortalProtect Configuration Database** screen appears.

pecify PortalProtect configuration data	abase location.
User-defined SQL Server	<u>-</u>
SharePoint SQL Server	
Authentication: Windows Aut	hentication 💌
User name:	(Domain\Usemame)
Password:	
Database selection: ( Create dat	abase for PortalProtect
C Use existin	ig database for PortalProtect
Database and	ve:

#### FIGURE 2-9. PortalProtect Configuration Database screen

- **11.** Select from the following options:
  - Specify PortalProtect configuration database location:
    - **SharePoint SQL Server**—installs PortalProtect to a SharePoint SQL server
    - User-defined SQL Server—installs PortalProtect to a userdefined SQL server



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



Trend Micro strongly suggests using Windows Authentication.

- User name-type as required
- Password-type as required
- 12. Click Next >.

2-12

### The Checking Target Server System Requirements screen appears.

	Trend Micro P	ortalProtect Setu	р
Checking Target S	Server System Requ	irements	
Please wait while	Setup checks target se	rver(s) for minimum syste	m requirements
Computer Name	SharePoint Server	Status	
WIN-RTMPQDS6	GSharePoint 2016	Fresh install	
Passed for new insta	slation: 1		
Passed for upgrade:	0		
	0		
Failed:	°,		

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

The Management Group Selection screen appears.

Select an Active D	Selection rectory group f	or PortalP	rotect manage	ment		
Please select an exist grant this group permi PortalProtect Web ma	ng Active Dire ssion to manag nagement con	ctory grou le PortalPr isole. Seler	p for managen otect. Users in t	nent. The setu I this group ma	p program will ay log on to the	1)
Domain:						
Group:						
Description:						
Use Local Server	Administrator G	iroup				

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.

**14.** 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 preexisting group; the **Domain**, **Group**, and **Description** fields then populate accordingly.

15. Click Next >.

#### The **Connection Settings** screen appears.

Please enter the	configuration for connections	
PortalProtect uses the	following settings during product activat	ion and component download.
Proxy Settings		
Proxy type:	rver to connect to Internet	
Address:		
Port:	80	
Authentication (	optional) User name:	
	Password:	7
		530

**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.

16. Click Next >.

The Control Manager Server Settings screen appears.

Register Port	alProtect Agent to I	Control Manager Server		
– Control Manage	er Server Settings-			
Server Addres	s;			
Port	443	Conne	et using HTTPS	
🗖 Uses a pro	xy server to conne	ct to CM server	Proxy Server	Settings
-Web Server Au	ithentication	0.		
User Name:		Password:		

FIGURE 2-13. Control Manager Server Settings screen

- 17. 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**.
- 18. Click Next >.

The Email Notification Settings screen appears.

Please enter the o	configuration	for email no	tification		
PortalProtect will use t	he following !	SMTP serve	er settings when s	sending email-b	ased
Send email-based	notifications				
- SMTP Server Setting	38				
Address:					
Port:	25				
- Administrator Notifica	ation				
Type the email add	ess of the ac	dministrator t	hat will receive n	otifications.	
Email address:					
	Use semi For exam	colon'','' to s ple: user1@	eparate multiple: domain.com;adm	addresses iinistrator	

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.
- 19. Click Next >.

The **Review Settings** screen appears.

Please review and confirm all se	ettings	
Setup will use the following informati	ion during installation:	
Target Server(s) list: WIN-RTMPQDS6GUO		^
Product Activation:		=
Destination Directory: Use default destination directory		
Web Server: Server Type: IIS		~
Update the pattern when installa	ation is complete	
Web Server: Server Type: IIS Update the pattern when installa	alion is complete	

#### FIGURE 2-15. Review Settings screen

**20.** 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**.

The Installation Progress screen displays.

Please wait while Setup installs PortalPro may take a few minutes	otect al	selected des	tination(s). This
Elapsed time: 00:04:2	4		
┌─ Status: ────			
Installation in progress:	0	server	
Installation successfully completed on:	1	server	
Installation failed on:	0	server	View details

FIGURE 2-16. Installation Progress screen

21. While the installation is active, click **View details** to check the status.

	Trend N	licro PortalProtect Setup	
Computer Name	Domain	Progress Status Finished	

### FIGURE 2-17. Installation progress status (Finished)

22. After the installation status displays Finished, click Next >.

The Installation Complete screen appears.

Trend Micro PortalProtec	ct Setup
Installation Complete	
Setup successfully installed PortalProtect in selected destin	nation(s)
	Finish

#### **FIGURE 2-18. Installation Complete screen**

**23.** 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.

#### Procedure

- **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.

2-24



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. 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.

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



**FIGURE 2-22. Installation screen** 

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

	📕 💽 🗓 🗧 📔 Temp						
File H	lome	Share	/iew				
€ .	1	▶ Compu	ter 🕨 Local Disk (C:)	▶ Windows ▶ Temp	~ C	Search Temp	
🚖 Favorit	es	N	ame	Date modified	Туре	Size	
💻 Deski	top		PP_MsiExec	5/24/2013 2:05 PM	Text Document	55 KB	
👢 Dowr	nloads		PP_Msilnstall	5/24/2013 2:06 PM	Text Document	2,558 KB	
🔛 Rece	nt places		PP_Setup	5/24/2013 2:03 PM	Text Document	61 KB	

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.

2-27

# **Post Installation**

#### Important

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.

#### Procedure

- 1. Enable the antivirus settings in SharePoint Server.
  - a. From within SharePoint, go to SharePoint Central Administration > Security > General Security > Manage antivirus settings.
  - **b.** Enable the following:
    - Scan documents on upload
    - Scan documents on download
    - · Attempt to clean infected documents
- 2. Enable Web content scan settings in PortalProtect.
  - a. From PortalProtect, go to the **PortalProtect Management Console** > **Summary > System > Microsoft SharePoint Services**.
  - **b.** 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**.

If your PortalProtect server has an antivirus product installed, configure it so that it does not scan the following folders:

- Assumed installation folder: C:\Program Files\Trend Micro \PortalProtect
- 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 PortalProtect, add these folders to the Exclude folder list.

## **Upgrading PortalProtect**

You can upgrade PortalProtect in two ways:

- Using an installation program called setup.exe (see *Upgrading Using Setup Program on page 2-29*)
- Using a silent installation program called SilentSetup.bat (see *Silent Fresh Installation on page 2-22*)

### **Upgrading Using Setup Program**

#### Procedure

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.

Trend Micro I	PortalProtect Set	q
License Agreement Please read the following license agree	ment carefully	
IMPORTANT: READ CAR MICRO SOFTWARE AND SE OTHER ENTITIES IS SUB LEGAL TERMS A	REFULLY. USE ( ERVICES BY BU JECT TO THE F AND CONDITION	OF TREND SINESS AND OLLOWING IS
Trend Micro Lic	ense Agree	ment
Trial and Paid Use License - En Services	terprise and SMB	Software and
	2	
<ul> <li>I accept the terms in the license agree</li> <li>I do not accept the terms in the license</li> </ul>	ment e agreement	
	Rack	Next > Cancel

FIGURE 2-25. License Agreement screen

**3.** 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.

### The **Select an Action** screen (1) appears.

Trend Micro Por	talProtect Set	tup	
Select an Action Install, upgrade or uninstall the program		0	TREND
for SharePoint stand-alone server			
C for SharePoint server farm environment			
	< Back	Next >	Cancel

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

- **4.** Choose one of the following installation options:
  - for SharePoint stand-alone server
  - for SharePoint server farm environment
- 5. After selecting the appropriate options, click Next >.



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**.

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

Trend Micro Por	talProtect Setup
Select an Action Install, upgrade or uninstall the program	
<ul> <li>Fresh install PortalProtect 2.6</li> <li>Upgrade from PortalProtect 2.5 SP1</li> <li>Uninstall</li> </ul>	
	< Back Next > Cancel

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

6. Select Upgrade from PortalProtect 2.5 SP1 and click Next >.

The **Product Activation** screen appears.

	Trend Micro PortalProtect Setup	
Product Activation Activate your produ	cts to enable scanning and security updates.	
You must activate Porta	alProtect to enable scanning and security updates.	
To obtain the Activatio Key.	n Code, register the product online using the suppli	ed Registration
Re-use the existing	activation code	
C Specify a new act	vation code	
Activation Code:		
	()XX-XXXX-XXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXX	(X)
	< Back Next	> Cancel

FIGURE 2-28. Product Activation screen

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

The <b>Se</b> l	lect Target	Server(s)	screen	appears.
-----------------	-------------	-----------	--------	----------

Tren	d Micro PortalProtect Setup
Select Target Server(s) Please specify the server(s)	on which you want to install PortalProtect 🛛 🥏 TREND
Please specify the server(s) on w	which you want to install PortalProtect
Install to local server	
C Install to multiple servers	
	Add Browse
,	
1	
	Remove
	< Back Next > Cancel

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

- 8. 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.

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

To install/uninstall F to store support files	PortalProtect, the setup program uses a shared folder on target server 3.
Shared directory:	Cs
Planas anasily Past	alProtect install folder.
riease specily rolla	
Default path:	<default files="" path="" program="">\Trend Micro\PortalProtect</default>
Default path:     Specify path:	<default files="" path="" program="">\Trend Micro\PortalProtect C:\Program Files\Trend Micro\PortalProtect</default>

FIGURE 2-30. Configure Shared/Target Directory screen

**9.** 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.

The Web Server Information screen appears.

Configure the PortalProtect Wel	o management console.	
- Web Management Console Se	ttings	
🔽 Enable SSL		
Certificate validity:	g year(s)	
SSL Port:	16373	

FIGURE 2-31. Web Server Information screen

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

### The PortalProtect Configuration Database screen appears.

User-defined SQL	configuration database location.	
SQL Server:		
Authentication:	Windows Authentication	-
User name:		(Domain\Usemame)
Password:		

FIGURE 2-32. PortalProtect Configuration Database screen

### 👔 Note

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

- **11.** Select from the following options:
  - Specify PortalProtect configuration database location:

- · SharePoint SQL Server-installs PortalProtect to a SharePoint SQL server
- User-defined SQL Server-installs PortalProtect to a userdefined SQL server

A	Note
A	

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
- 12. Click Next >.

#### The Checking Target Server System Requirements screen appears.

Checking Tarnet	Trend Micro P	ortalProtect Setup	
choosing raigo			
] Please wait while	e Setup checks target se	rver(s) for minimum system rea	quirements
Computer Name	SharePoint Server	Status	
WIN-6F73502C3	3H SharePoint 2013	Version Upgrade	
Passed for new in	etallation 0		
Passed for new ins Passed for upgrad	stallation: 0 e: 1		
Passed for new ins Passed for upgrad Failed:	stallation: 0 e: 1 0		

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:

PortalProtect is installed:

- Whether PortalProtect 2.5 SP1 is installed
- Whether the target server is running the correct version of Windows

2-40

- 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 2.5 SP1
- Whether the PortalProtect DB access account is identical with PortalProtect 2.5 SP1
- 13. Verify the Status reads Fresh Install, and click Next >.

The Management Group Selection screen appears.

Management Group Sele Select an Active Directo	ction ry group for Porta	IProtect managem	ent 🤇	TREND
Please select an existing A	ctive Directory gr	oup for manageme	nt. The setup pro	ogram will
PortalProtect Web manage	ment console.	in fotect. Osers in t	ns group may log	fon to the
C Select Active Directory	Group Se	lect		
Domain:		- N.S.O.		
Group:				
Description:				
Use Local Server Admir	nistrator Group			
<b>.</b>				

FIGURE 2-34. Management Group Selection screen



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.

**14.** 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 preexisting group; the **Domain**, **Group**, and **Description** fields then populate accordingly.

15. Click Next >.

2-42

84 B	
Review Settings Please review and confirm all settings	
Setup will use the following information during installation:	
Target Server(s) list: WIN-6F735O2C3H7	^
Destination Directory: Use default destination directory	=
Web Server: Server Type: IIS SSL Port Number: 16373 SSL Certificate Valid Period: 3 years	

FIGURE 2-35. Review Settings screen

**16.** 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**.

The Installation Progress screen displays.

Please wait while Setup installs PortalPr may take a few minutes	otect at	selected des	tination(s). This
Elapsed time: 00:04:2	24		
┌─ Status:			
Installation in progress:	0	server	
Installation successfully completed on	: 1	server	
Installation failed on:	0	server	View details

FIGURE 2-36. Installation Progress screen

17. While the installation is active, click **View details** to check the status.

	Trend N	ficro PortalProtect Setu	р
Computer Name	Domain	Progress Status Finished	
			[

FIGURE 2-37. Installation progress status (Finished)

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

The Installation Complete screen appears.

Trend Micro PortalPro	Trend Micro PortalProtect Setup				
Installation Complete					
Setup successfully installed PortalProtect in selected d	lestination(s)				
	Finish				

**FIGURE 2-38. Installation Complete screen** 

**19.** 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:

2-46
#### 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.

#### Procedure

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

X50!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.



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 userfriendly 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.

#### Procedure

1. Navigate to Setup.exe and open it.



The Trend Micro PortalProtect setup program screen displays.

FIGURE 2-39. Trend Micro PortalProtect setup program screen

2. Click Next >.

#### The License Agreement screen appears.

Trend Micro PortalProtect Setup	
License Agreement Please read the following license agreement carefully	REN
IMPORTANT: READ CAREFULLY. USE OF TREND MICRO SOFTWARE AND SERVICES BY BUSINESS AND OTHER ENTITIES IS SUBJECT TO THE FOLLOWING LEGAL TERMS AND CONDITIONS	^
Trend Micro License Agreement	
Trial and Paid Use License - Enterprise and SMB Software and	
Services	~
I accent the terms in the license acreement	
C I do not accept the terms in the license agreement	
C I do not accept the terms in the license agreement	
Rack Nexts	Cancel
COOK NOAL /	Carroot

FIGURE 2-40. License Agreement screen

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

Trend Micro Por	talProtect Set	up
Select an Action Install, upgrade or uninstall the program		
for SharePoint stand-alone server		
C for SharePoint server farm environment		
	< Back	Next > Cance

#### The **Select an Action** screen (1) appears.



- **4.** Choose one of the following installation options:
  - for SharePoint stand-alone server
  - for SharePoint server farm environment
- 5. After selecting the appropriate options, click Next >.

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

Trend Micro Por	rtalProtect Setup	
Select an Action Install, upgrade or uninstall the program		
<ul> <li>Fresh install PortalProtect 2.6</li> <li>Upgrade from PortalProtect 2.5 SP1</li> <li>Uninstall</li> </ul>		
	< Back Next > Cancel	

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

6. Select Uninstall and click Next.

2-52

The Select Target Server(s)	screen	displays.
-----------------------------	--------	-----------

Trend Mic	ro PortalProte	ect Setup	
Select Target Server(s) Please specify the server(s) which y	you want to uninst	all PortalProtect	
Please specify the server(s) which you w	ant to uninstall Po	rtalProtect	
		Add	Browse
1			Remove
	< Ba	ck Nex	t> Cancel

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

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

#### The Select Computers dialog appears.

	Select Computers	?
Select this object type:		
Computers		Object Types.
From this location:		
Entire Directory		Locations
Enter the object names to :	select ( <u>examples)</u> :	
		Check Names
A duran a d		1K Cancel

FIGURE 2-44. Select Computers dialog

8. Select the computers from which you want to uninstall PortalProtect and click **OK**.

The Select Target Servers screen appears.

9. Add / Browse to select additional servers as required and click Next>.

#### The **Logon** screen displays.

	Trend Micro Po	ortalProtect Setup	
Log On Log on to target s	ervers where you want	o uninstall PortalProtect	
To install or uninsta server as an Admin	l PortalProtect to the se strator with Local Admir	lected target servers, you mu istrator privileges.	ust log on to each
User name:		(Domain\Use	rname)
Password:			
		Z Back Mout	Cancel
		C Back HIGA	

FIGURE 2-45. Logon screen

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

The Configure Shared Directory screen displays.

	Trend Micro P	ortalProtect Se	etup	
Configure Shared Please input shar	Directory ed directory for upgradir	ng or uninstalling Po	rtalProtect	TREND
To install/uninstall Po to store support files.	ortalProtect, the setup p	rogram uses a share	ed folder on targe	et server
Shared directory:	<u>CS</u>			1
		< Back	Next >	Cancel
		Duch	There ?	

FIGURE 2-46. Configure Shared Directory screen

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

|--|

	Trend Micro P	ortalProtect Setup	
Checking Target	Server System Requ	irements	
🗐 Please wait whi	e Setup checks target se	rver(s) for minimum system	n requirements
Computer Name	SharePoint Server	Status	
WIN-6F73502C	3H"Analyzing	Analyzing	
		< Back	Next > Cancel

FIGURE 2-47. Checking Target Server System Requirements screen

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

#### The Uninstall Notice screen displays.



FIGURE 2-48. Uninstall Notice screen

**13.** Click **Next >**.

The <b>Review Settings</b> screen displays	The	Review	Settings	screen	displays
--	-----	--------	----------	--------	----------

IProtect Setup	
allation:	
	~
	v
	IProtect Setup

FIGURE 2-49. Review Settings screen

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

#### The Uninstallation Progress screen displays.

tall	Protect Se	tup
Ininstallation Progress		
otect	: at selected c	lestination(s).
0	server	
1	server	
0	server	View details
1		
	0 1 0	talProtect Se

FIGURE 2-50. Uninstallation Progress screen

15. Click View Details to observe the uninstallation progress.

Uninstallation Progress		Trend M	licro PortalProtect Setu	р
	Computer Name	Domain	Progress Status	
Please wait while Setup uninstalls Porta This may take a few minutes	₩N-6F73502C	PP13	Finished	
Elapsed time: 00:01: Status: Uninstallation in progress:				
Uninstallation successfully completed Uninstallation failed on:				ОК

FIGURE 2-51. Uninstallation Progress Status

16. When the **Progress Status** displays **Finished**, click **OK > Next >**.

#### The Uninstallation Complete screen displays.

Trend Micro PortalProte	ect Setup
Uninstallation Complete	
Setup successfully uninstalled PortalProtect in selected de	estination(s)
	[]

FIGURE 2-52. Uninstallation Complete screen





# **Chapter 3**

# **Technical Support**

Learn about the following topics:

- Troubleshooting Resources on page 3-2
- Contacting Trend Micro on page 3-3
- Sending Suspicious Content to Trend Micro on page 3-4
- Other Resources on page 3-5

## **Troubleshooting Resources**

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

#### **Using the Support Portal**

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

#### Procedure

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

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

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

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

#### **Threat Encyclopedia**

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities. Go to <u>http://about-threats.trendmicro.com/us/threatencyclopedia#malware</u> to learn more about:

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

## **Contacting Trend Micro**

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

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

• Worldwide support offices:

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

• Trend Micro product documentation:

https://docs.trendmicro.com

#### **Speeding Up the Support Call**

To improve problem resolution, have the following information available:

• Steps to reproduce the problem

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

### **Sending Suspicious Content to Trend Micro**

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

#### **Email Reputation Services**

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

https://ers.trendmicro.com/

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

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

#### **File Reputation Services**

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

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

Record the case number for tracking purposes.

#### **Web Reputation Services**

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

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

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

### **Other Resources**

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

#### **Download Center**

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

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

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

#### **Documentation Feedback**

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

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



# **Chapter 4**

# **Frequently Asked Questions (FAQs)**

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

This chapter discusses the following topic:

• Installation on page 4-2

## 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:

- 1. Open Control Panel > Administrative Tools > Internet Information Services (IIS) Manager.
- 2. Make sure the PortalProtect application pool, virtual site, and virtual directories exist.

- 3. Make sure the IIS site is running.
- 4. Make sure the IIS site properties are properly configured, and can be accessed by your browser.
- 5. Make sure the PortalProtect master service is running.
- 6. 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. Choose **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. Choose **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.



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. Choose 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:

4-4

a. Open the Registry and locate:

 $\label{eq:hklm} HKLM\SOFTWARE\TrendMicro\PortalProtect\CurrentVersion \SharePointDBAccessPassword$ 

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

Note		
Vou		

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:

 $\label{eq:hklm} HKLM \software \red micro \Portal Protect \Current Version \PPC on f Database Password$ 

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++ 2015 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".





A-1

# **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 on page A-2
- Background on page A-2

# Applications

This section describes the applications used for PortalProtect 2.6.

- PortalProtect-Trend Micro PortalProtect for Microsoft SharePoint
- SQL Server-SQL Server 2008, 2012, 2014, 2016, or 2019
- **SharePoint**—Microsoft SharePoint Server 2013, 2016, 2019, or Subscription Edition

## 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. The following table shows the 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

TABLE	A-1. Por	talProtec	t service	log on	account

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

D

documentation feedback, 3-5

S

support resolve issues faster, 3-3





#### 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@tredmicro.com



Item Code: PPEM28660/190425