TREND MICRO™

2.5 PortalProtect™

Service Pack 1

Installation and Upgrade Guide

Highly Effective Protection, Minimal IT Impact

for Microsoft™ SharePoint

Collaboration Security

Document Part No.: PPEM28280/180607

Release Date: June 2018

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 docs@trendmicro.com.

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 Policy:

https://www.trendmicro.com/en_us/about/legal/privacy-policy-product.html

Table of Contents

Preface

Welcome to the Trend Micro™ PortalProtect™ Installation and Upgrade Guide. This book contains basic information about the tasks you need to perform to deploy PortalProtect to protect your SharePoint servers. It is intended for novice and advanced users of PortalProtect who want to manage 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 Upgrade Guide**: PDF documentation that discusses requirements and procedures for installing and upgrading the product.
- **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 (http://www.trendmicro.com/download) 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, Installation and Upgrade 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, **File** > **Save** means, click **File** and then click **Save** on the interface
 **Note**	Configuration notes
 **Tip**	Recommendations or suggestions
 **Important**	Information regarding required or default configuration settings and product limitations
 **WARNING!**	Critical actions and configuration options

Chapter 1

Welcome to Trend Micro™ PortalProtect™

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.

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

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

What's New in PortalProtect 2.5 SP1

This version of PortalProtect provides the following new features:

- **Microsoft Visual C++ Redistributable Update**

  PortalProtect 2.5 SP1 uses Microsoft Visual C++ 2015 Redistributable instead of Microsoft Visual C++ 2005 Redistributable.

- **Data Loss Prevention (DLP) Compliance Templates that Support GDPR**

  PortalProtect 2.5 SP1 provides enhanced DLP compliance templates that support GDPR.

Chapter 2

Installing and Removing PortalProtect 2.5 SP1

Install and remove PortalProtect 2.5 SP1 locally or remotely to or from one or more servers using one easy-to-use setup program.

Topics in this chapter:

Upgrade Requirements

The following lists the upgrade requirements for Trend Micro PortalProtect 2.5 SP1:

- Trend Micro PortalProtect 2.5
- Integrated Trend Micro product support as listed in the following table:

TREND MICRO PRODUCT	SUPPORTED VERSIONS
Control Manager™	• 6.0 Service Pack 3 or above • 7.0
Smart Protection Server	• 3.0 or above • OfficeScan Server Integrated Smart Protection Server

Preparing for Installation

Specify the following permissions for the accounts required in installation to ensure a smooth deployment of PortalProtect 2.5 SP1 to your network:

ACCOUNT	PRIVILEGE

Program Setup Account	• Local administrator:
	  ◦ Local administrator privileges to where you launch the installation program
	  ◦ Local administrator privileges to all the target server(s) where you plan to install PortalProtect 2.5 SP1
	• Domain user: User account that already joins the domain where the server(s) to install PortalProtect 2.5 SP1 belong

ACCOUNT	PRIVILEGE
SharePoint Database Access Account	• 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 Configuration Database Access Account	• PortalProtect_{UUID} database (Fresh install of 2.5): **db_owner** role • PPCentralConfig_<SharePoint_Config DB_Name>, PPConf_<ServerName>, PPLog_<ServerName>, and PPReport_<ServerName> databases (Upgraded to 2.5 from a previous version): **db_owner** role

Installing the Service Pack

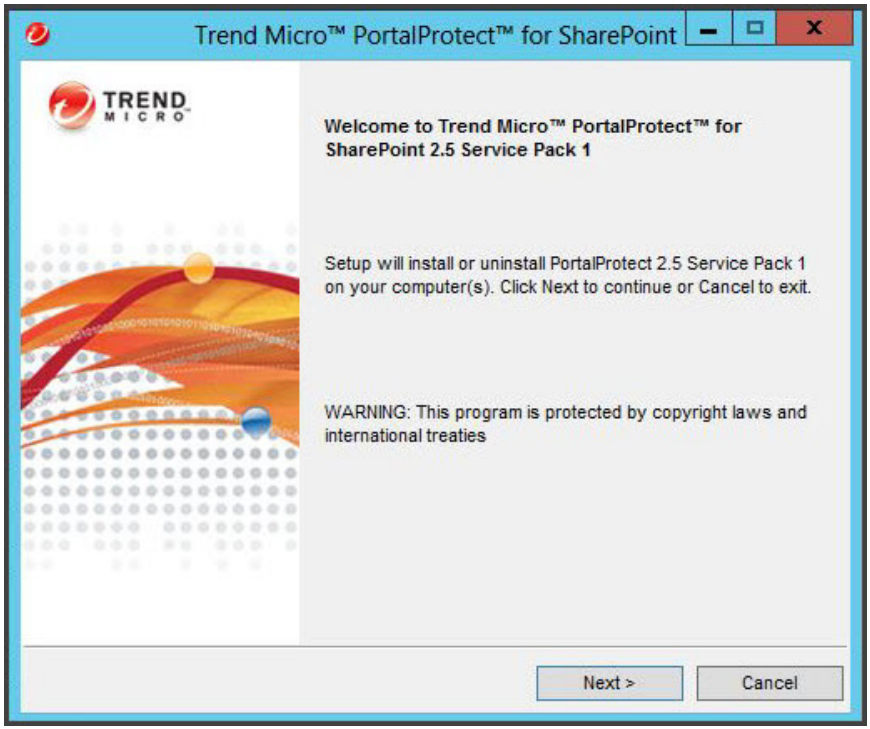
Note

Installation of this service pack does not cause a disruption in file transfer traffic during deployment.

Procedure

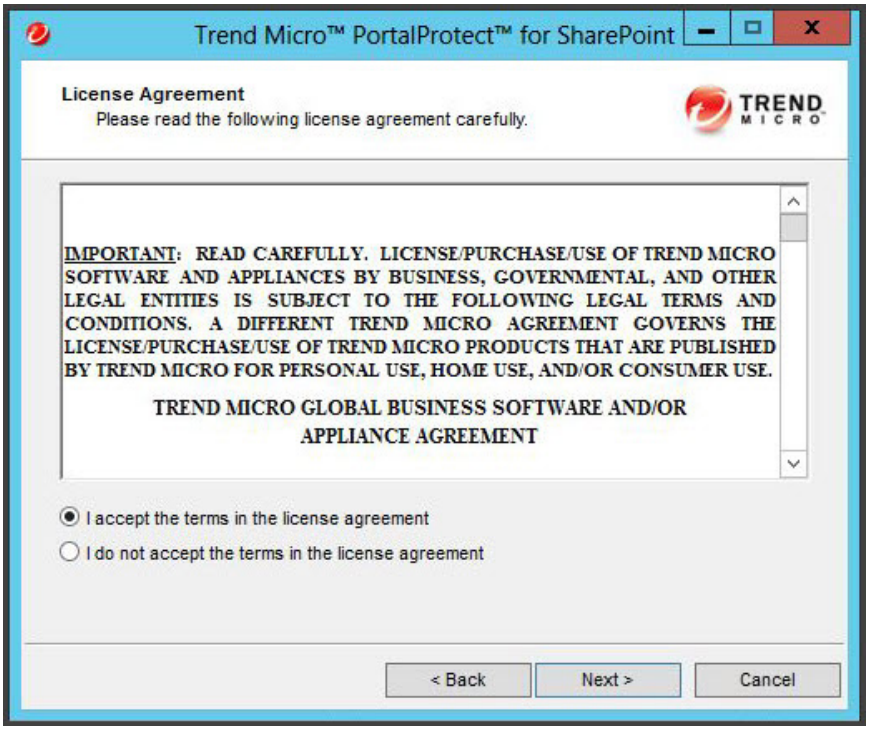
1. Click the installation program **Setup.exe** to start the installation wizard.

The **Welcome** screen appears.



2. Click **Next** to begin the installation.

The **License Agreement** screen appears.

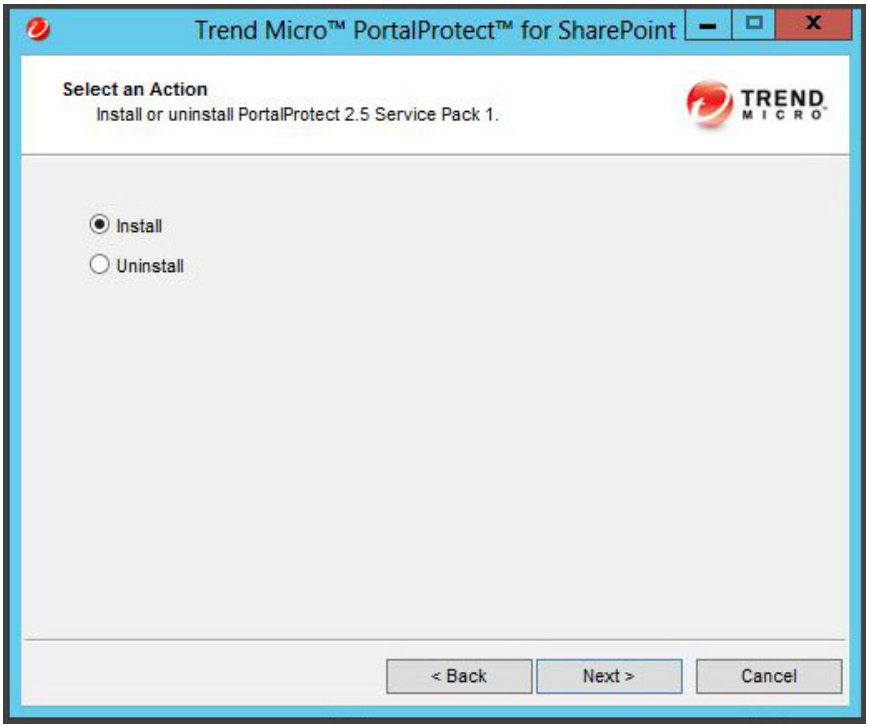


3. Click **I accept the terms in the license agreement** and click **Next**.

Note

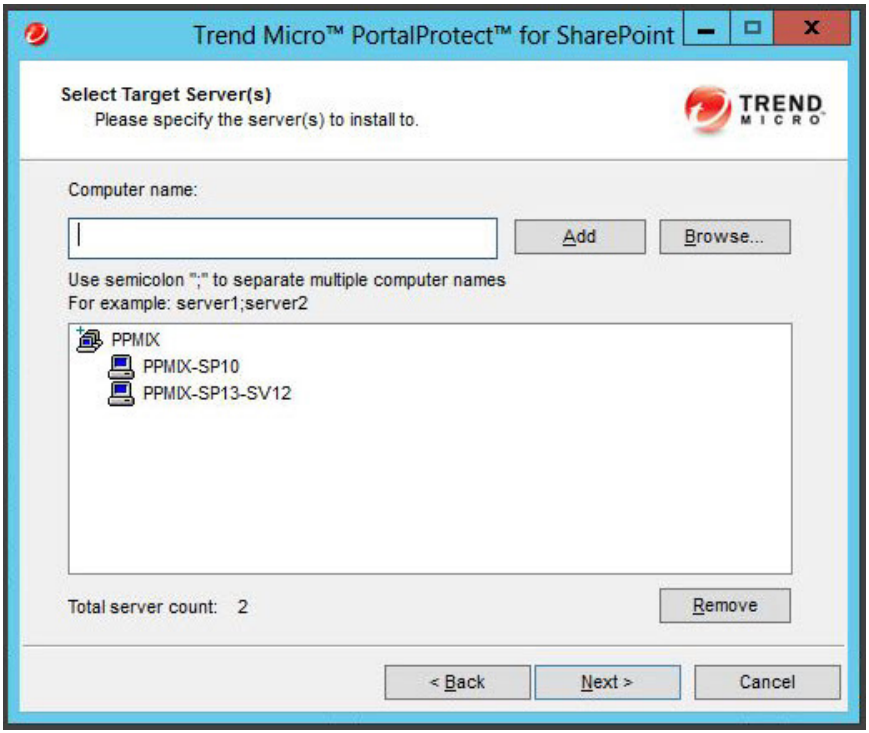
If you do not accept the terms, click **I do not accept the terms in the license agreement**. This terminates the installation without modifying your operating system.

The **Select an Action** screen appears.



4. Select **Install** and click **Next**.

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



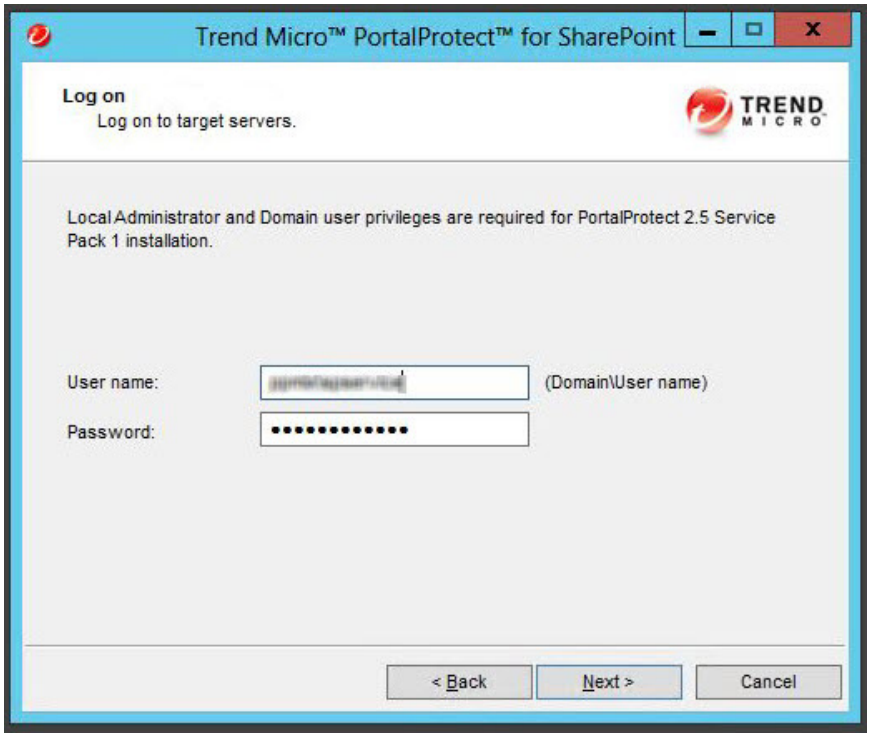
5. Select the servers to which you plan to install PortalProtect.

   a. Perform one of the following:

      - Type the computer name of the server in the **Computer name** text box and click **Add** to add it to the list of servers.
      - Click **Browse** to search for the servers that are available on your network, and then double-click the domain or servers you plan to add to the list.
      - Click **Remove** to remove a server from the list.

b. Click **Next**.

The **Log on** screen appears.

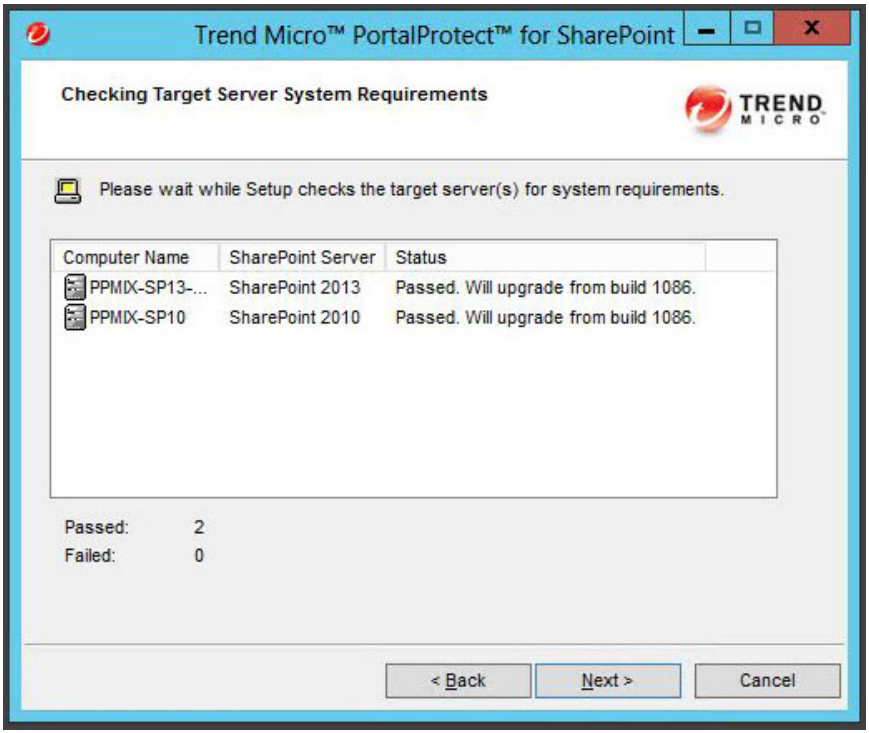


6. Type the PortalProtect program setup account credential to log on to the target server(s), and then click **Next**.

Note

The installation program can install PortalProtect to a number of single servers or to all the servers in a domain. Use an account with the appropriate privileges to access every target server.

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



7. If the **Status** of each target server is **Passed**, click **Next**.

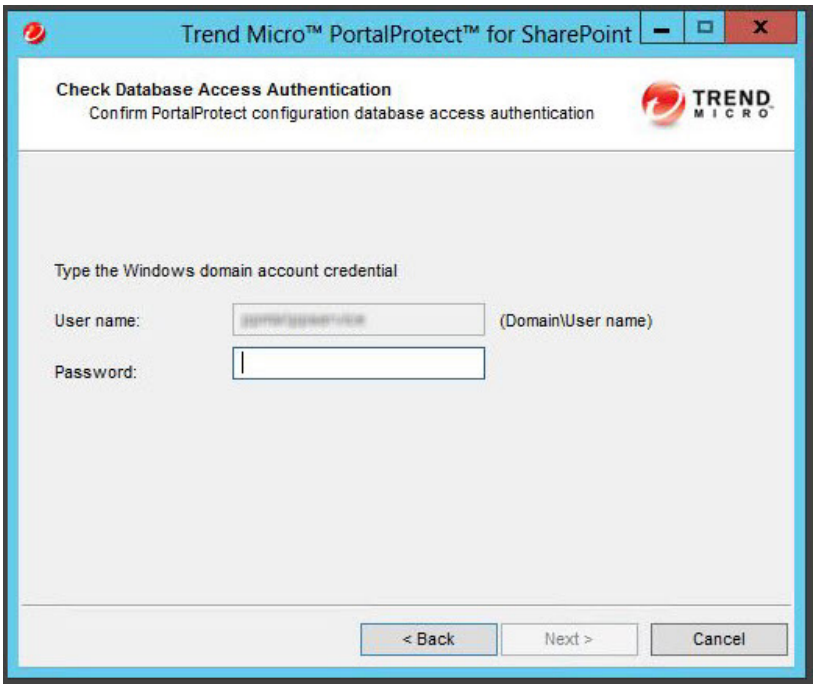
   The installation program then checks the means of authentication in use to access PortalProtect configuration database and SharePoint databases.

   If every target server uses SQL Server Authentication to access the PortalProtect configuration database and Windows Authentication to access SharePoint databases, the installation continues from step 9. Skip step 8 and go to step 9 to continue.

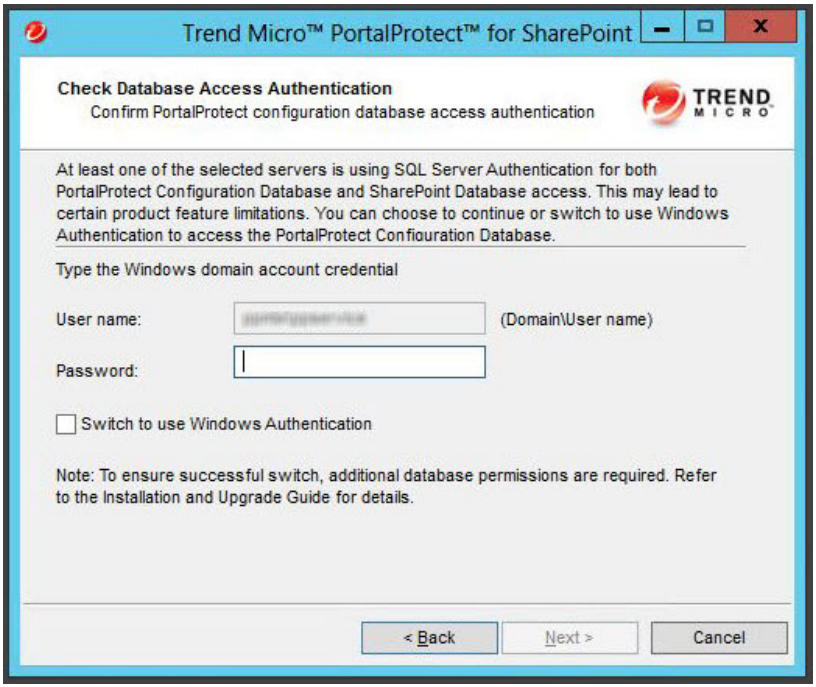
   Otherwise, the **Check Database Access Authentication** screen appears, which varies by the authentication check result.

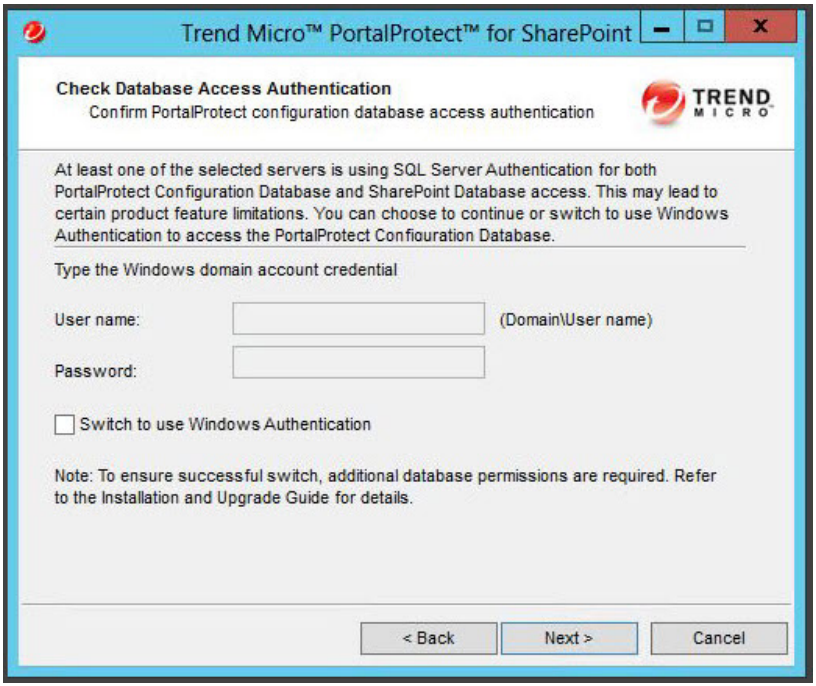
8. Perform one of the following:

   - If the following screen appears, type the password of the account and click **Next**.



- If either of the following screens appears, it means that the current authentication configuration will make Web content scan, manual scan, and scheduled scan in PortalProtect fail to work properly.





Click **Next** if you want to keep the current configuration and continue the installation. If **User name** is already filled in, type the password of the account first.

Important

Trend Micro recommends switching to use Windows Authentication to access PortalProtect configuration database.

To switch to use Windows Authentication, perform the following:

a. Select **Switch to use Windows Authentication**.

b. Type the credential of the Windows domain account, which is also the PortalProtect configuration database access account.

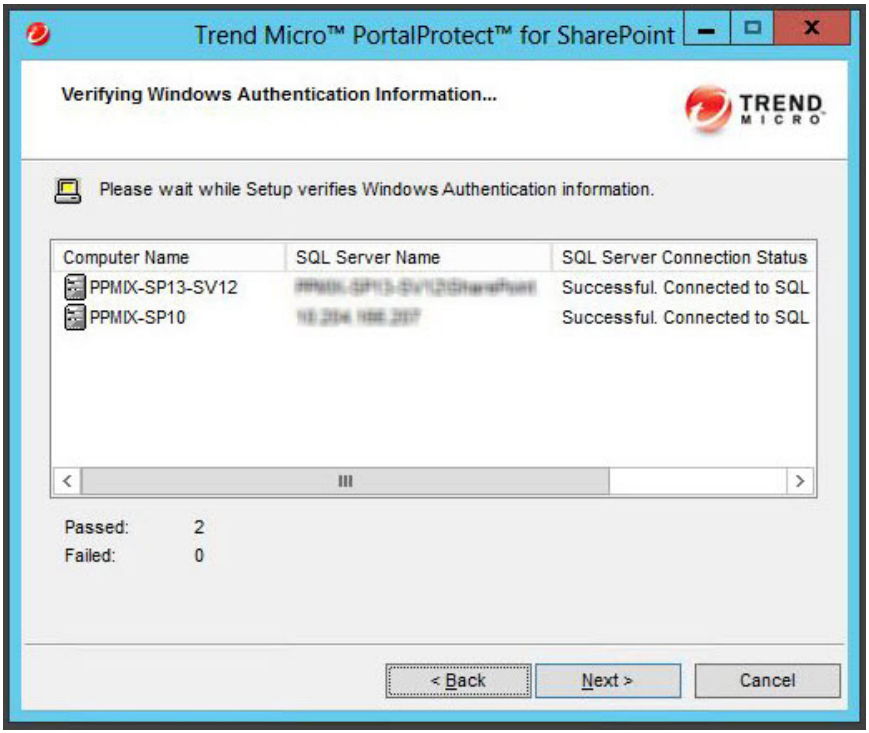
Important

Make sure that this account is also the local administrator of all the target server(s).

c. Check if this domain account has required database permissions. If not, grant the permissions to this domain account. For details, see *Preparing for Installation on page 2-2*.

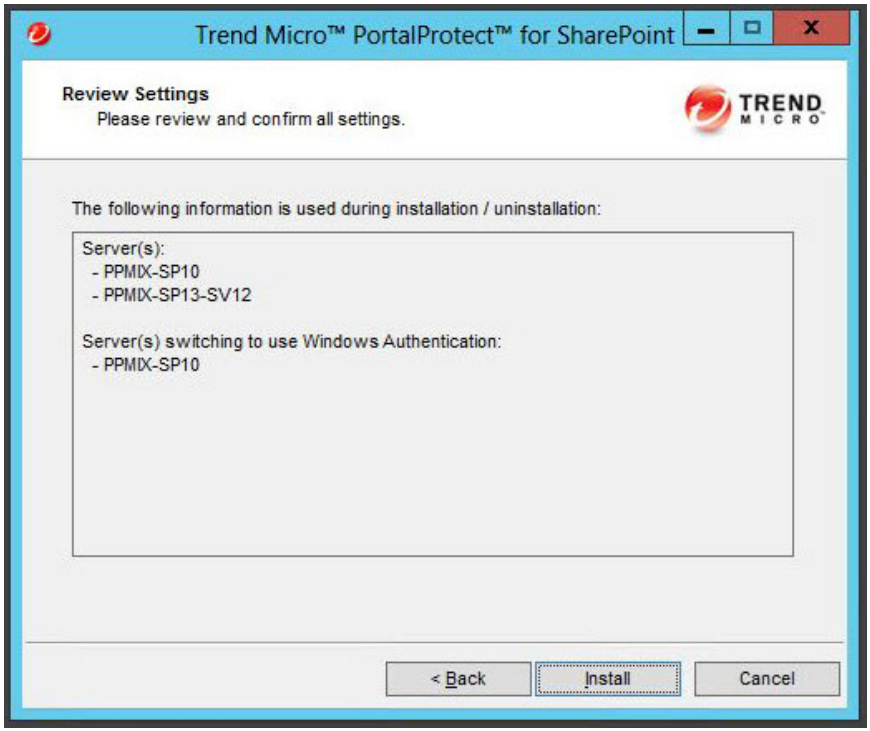
d. Click **Next**.

The **Verifying Windows Authentication Information** screen appears.



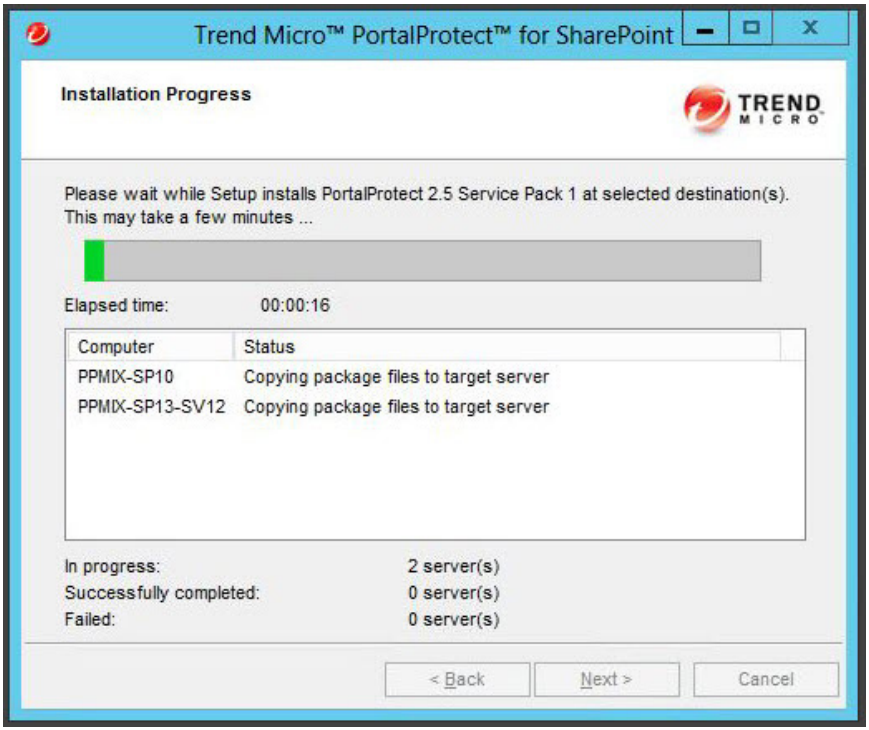
9. Wait until the program completes verifying Windows Authentication information, review the results of each target server, and then click **Next**.

The **Review Settings** screen appears.



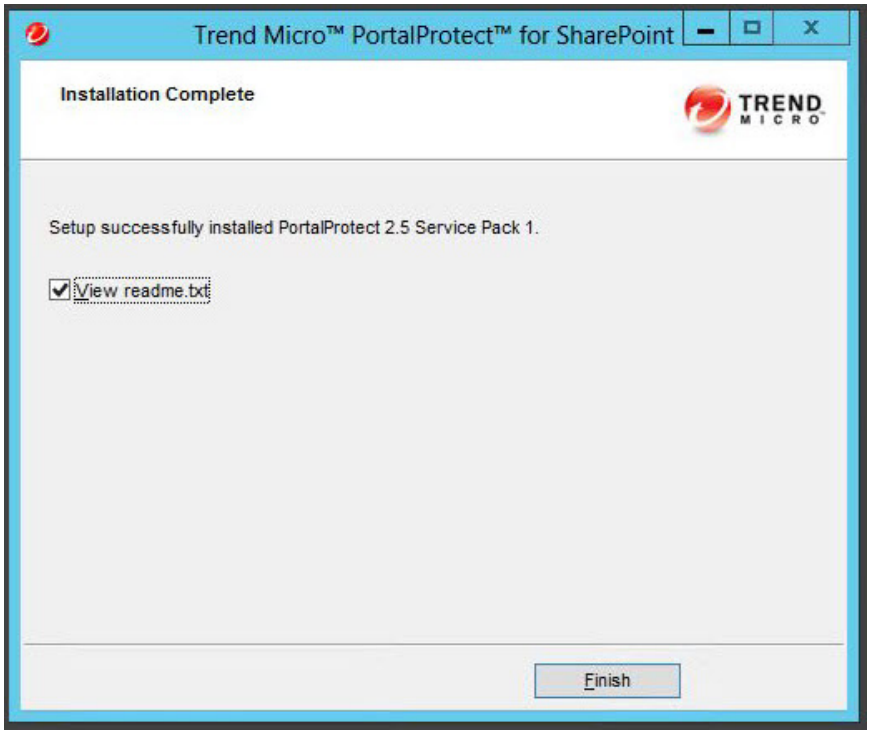
10. Review the server settings and click **Install**.

The **Installation Progress** screen appears.



11. Wait until the installation completes and click **Next**.

The **Installation Complete** screen appears.



12. Click **Finish** to exit the installation program.

    The Readme file displays.

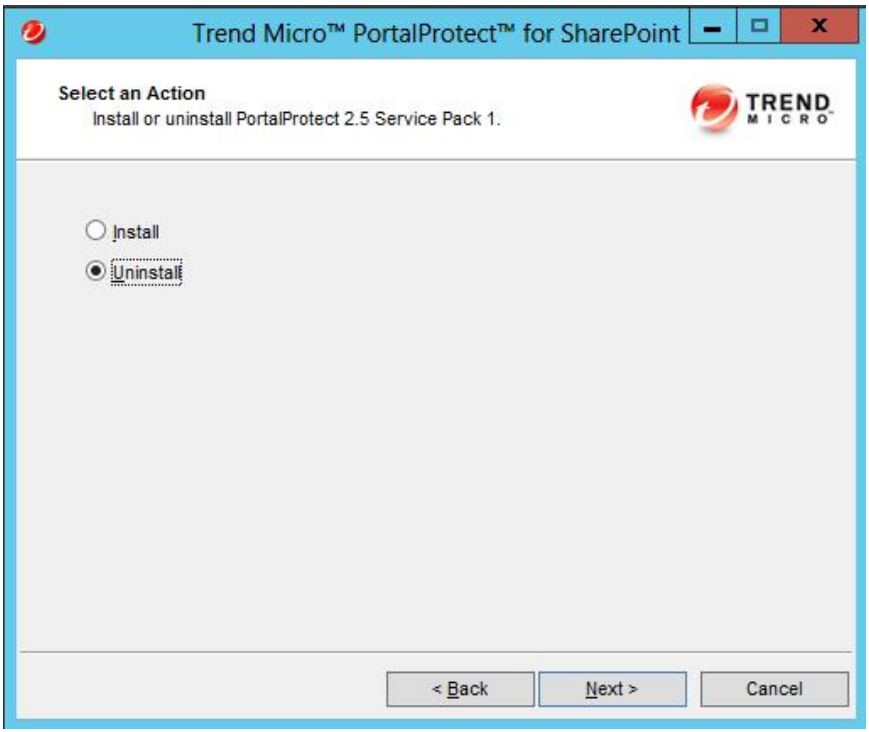
Removing the Service Pack

Removing the Service Pack reverts PortalProtect to the previously installed version.

Procedure

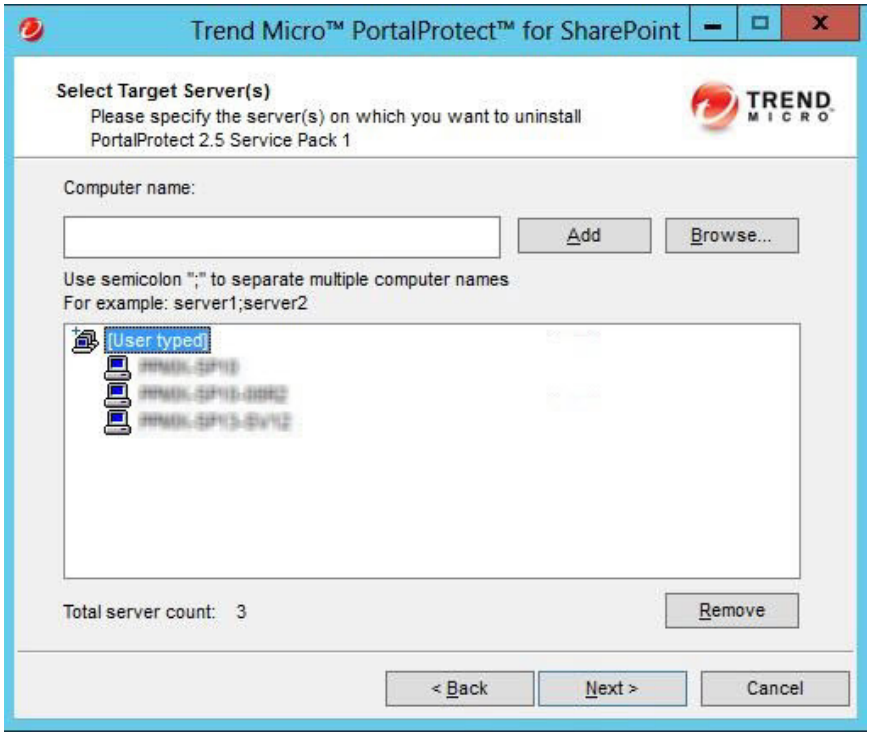
1. Run the Service Pack `setup.exe` program, and click **Next**.
2. Click **I accept the terms in the license agreement**, and click **Next**.

   The **Select an Action** screen appears.



3. Select **Uninstall** and click **Next**.

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



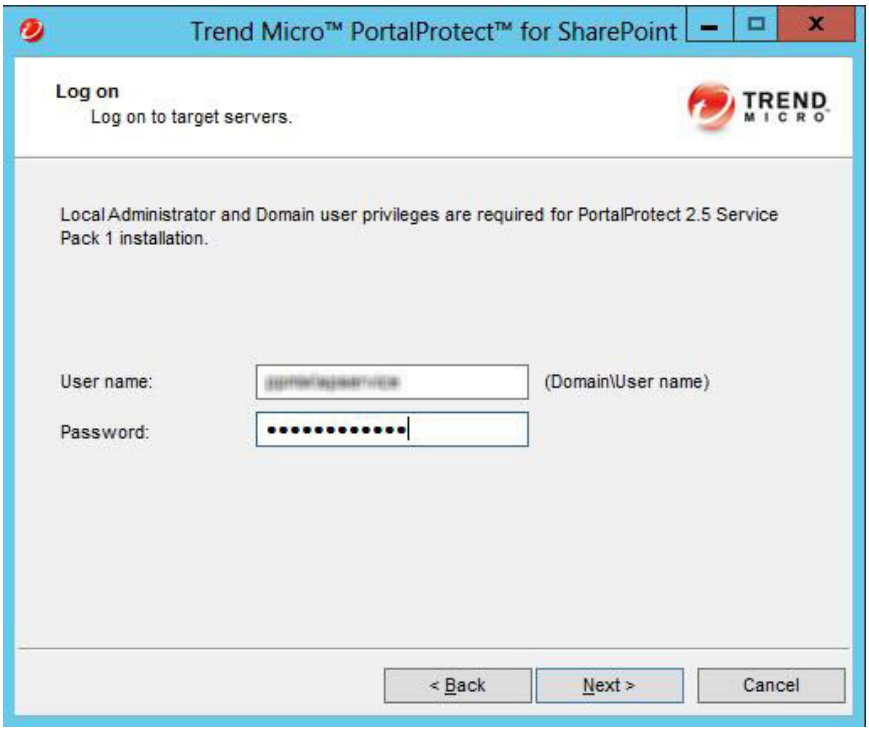
4. Select the servers to which you plan to uninstall PortalProtect.

   a. Perform one of the following:

      - Type the computer name of the server in the **Computer name** text box and click **Add** to add it to the list of servers.
      - Click **Browse** to search for the servers that are available on your network, and then double-click the domain or servers you plan to add to the list.
      - Click **Remove** to remove a server from the list.

b. Click **Next**.

The **Log on** screen appears.

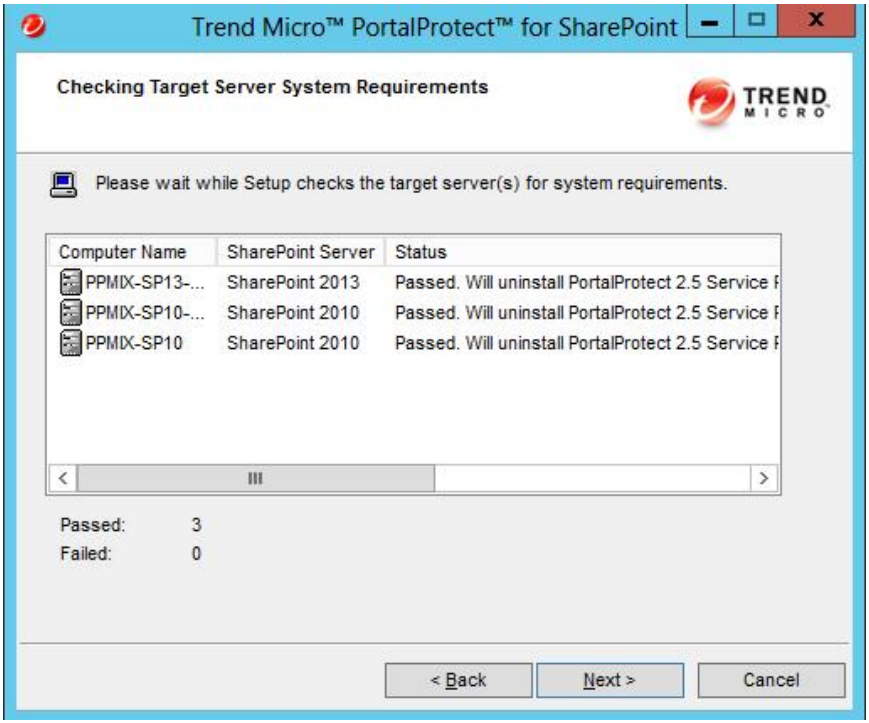


5. Type the PortalProtect program setup account credential to log on to the target server(s), and then click **Next**.

Note

The uninstallation program can uninstall PortalProtect from a number of single servers or from all the servers in a domain. Use an account with the appropriate privileges to access every target server.

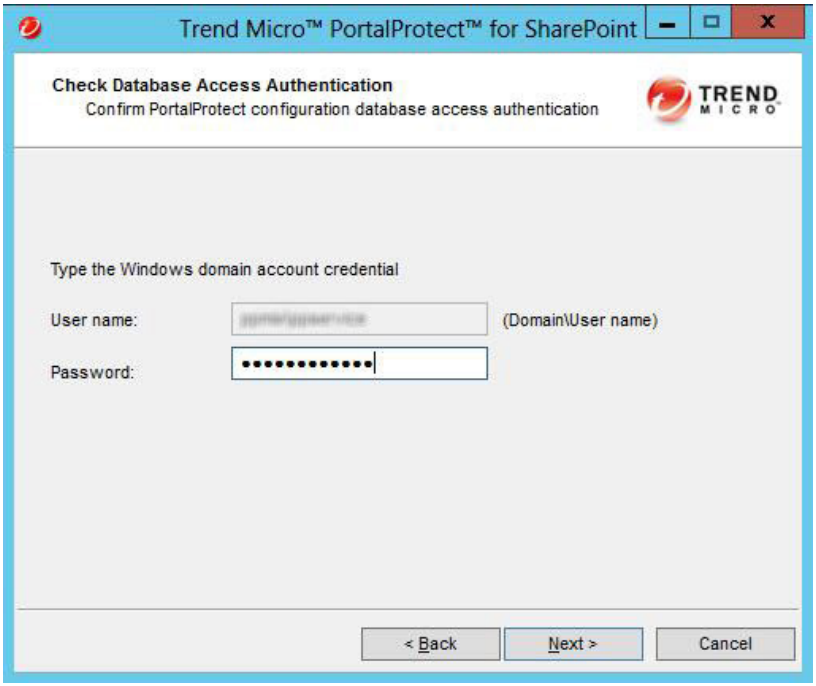
The **Checking Target Server System Requirements** screen appears.



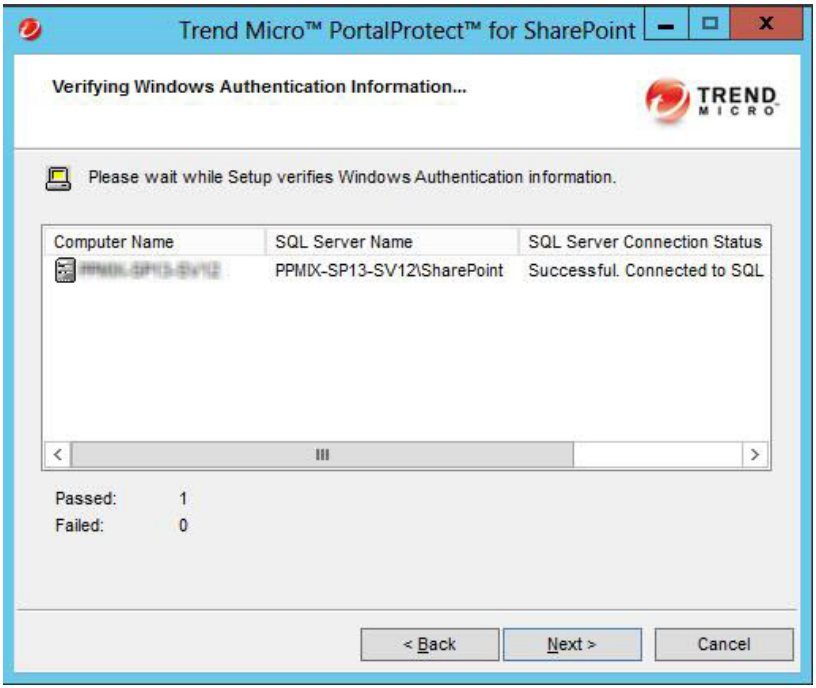
6. If the **Status** of each target server is **Passed**, click **Next**.

7. (Optional) If the program detects at least one server that uses Windows Authentication, the **Check Database Access Authentication** screen appears.

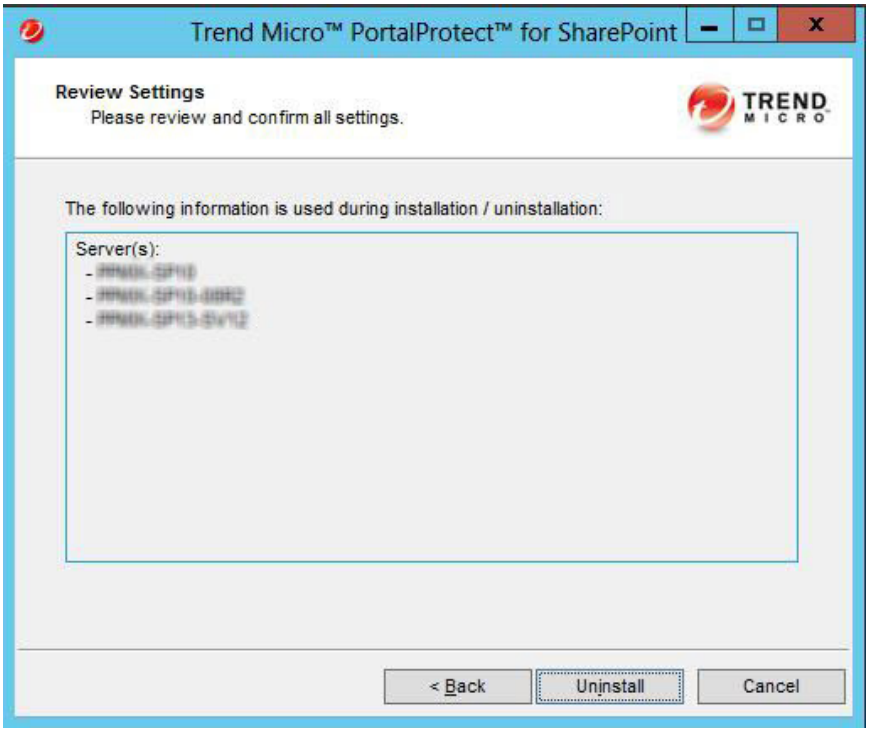
   a. Type the password of the account and click **Next**.



b. Wait until the program completes verifying Windows Authentication information and click **Next**.

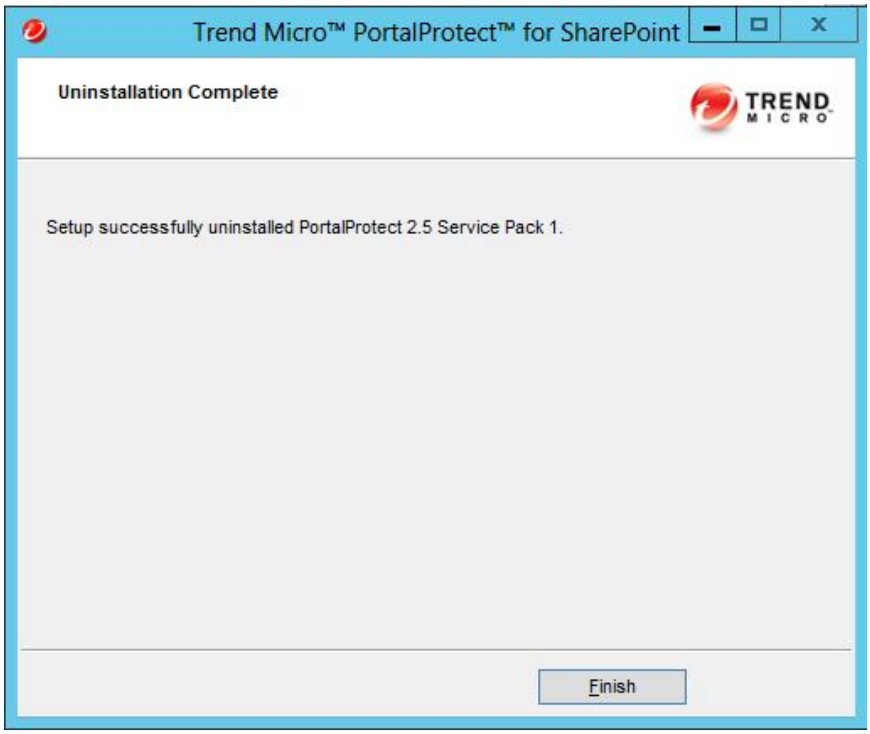


8. On the **Review Settings** screen, confirm all settings and click **Uninstall**.



9. Wait until the uninstallation completes and click **Next**.

The **Uninstallation Complete** screen appears.



10. Click **Finish** to exit the uninstallation program.

PortalProtect is successfully uninstalled from the selected target server(s).

Chapter 3

Technical Support

Learn about the following topics:

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 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.

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 http://about-threats.trendmicro.com/us/threatencyclopedia#malware 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	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

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

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: PPEM28280/180607