TREND MICRO™

2.0 TREND MICRO™ Vulnerability Protection

Service Pack 2

Installation Guide

Advanced Vulnerability Shielding for Endpoints

Endpoint Security

Document Part No. APEM26977/150527

Release Date: August 2015

Document Version No.: GM

Product Name and Version No.: Trend Micro Vulnerability Protection 2.0 SP2

Protected by U.S. Patent Nos.: 7,630,982; 8,220,041; 8,505,092; 8,549,282; 7,930,747; 8,510,791; 7,996,896; 8,171,547; 8,230,508

The user documentation for Trend Micro Vulnerability Protection 2.0 SP2 is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

Detailed information about how to use specific features within the software are available in the online help file and the Knowledge Base at Trend Micro website.

Trend Micro is always seeking to improve its documentation. Your feedback is always welcome. Please evaluate this documentation on the following site:

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

Table of Contents

Preface

Preface v

Trend Micro Vulnerability Protection Documentation vi

Audience vi

Document Conventions vii

Chapter 1: Introduction

About Vulnerability Protection 1-2

Vulnerability Protection Components 1-2

Features 1-2

Chapter 2: Preparing for Installation

Installation Requirements 2-2

Performance Recommendations 2-3

System Requirements 2-4

Multi-Node Manager 2-7

Co-Located Relay-enabled Agent 2-8

Scaling for Large Installations 2-8

Chapter 3: Installation

Installation Tasks 3-2

Installing the Database 3-2

- Account Details 3-3
- Communication with SQL Server 3-3

Installing Vulnerability Protection Manager 3-4

- Installing Vulnerability Protection Manager 3-4

Installing Vulnerability Protection Agent 3-15
Importing Agent Software 3-15
Exporting the Agent Installer 3-16
Installing Vulnerability Protection Agent 3-17

Uninstallation 3-20
Uninstalling Manager Using the Uninstallation Program 3-21
Uninstalling Vulnerability Protection Agent Using the Uninstallation Program 3-21
Uninstalling from the Command Line 3-22

Chapter 4: Upgrading

Upgrading Vulnerability Protection Manager 4-2

Upgrading Agents from Vulnerability Protection Manager 4-5

Chapter 5: Post-Installation Tasks

Verifying a Successful Installation 5-2

Managing Multiple Nodes 5-3
Adding a Manager Node 5-3
Viewing Nodes 5-3
Decommissioning Nodes 5-6

Activating the Vulnerability Protection Agent 5-6

Enabling Relay Functionality 5-7

Configuring a Software Update Server 5-8
Web Server Requirements 5-8
Folder Structure 5-9
Using the New Software Repository 5-10

Appendix A: Ports Used by Trend Micro Vulnerability Protection

Vulnerability Protection Manager Ports A-2

Vulnerability Protection Agent Ports A-2

Appendix B: Configuring the Settings.Properties File

Format B-2
Required Values B-2
Optional Values B-2

Appendix C: Installation Output

Successful Installation C-2
Unsuccessful Installation C-3

Appendix D: Trend Micro Vulnerability Protection Memory Usage

Configuring the Installer's Maximum Memory Usage D-2
Configuring the Manager's Maximum Memory Usage D-2

Appendix E: Performance Profiles

Changing the Performance Profile E-2

Appendix F: SSL Authentication Certificate

Creating an SSL Authentication Certificate F-2

Appendix G: Frequently Asked Questions (FAQs)

Frequently Asked Questions G-2

Appendix H: Troubleshooting

Troubleshooting H-2

Appendix I: Intrusion Defense Firewall Migration Tool

About Intrusion Defense Firewall Migration Tool I-2
System Requirements I-2
Using the Migration Tool I-5
Converting Intrusion Defense Firewall Clients I-13

Troubleshooting I-15
Error “Unable to locate the database backup file” I-15
Error “Unable to install a new database instance” I-16
Error “Unable to uninstall Intrusion Defense Firewall” I-16
Error “Unable to configure Vulnerability Protection. Unable to access the database. Installation cannot continue.” I-17
Error “Unable to install Microsoft SQL Express 2012 on hosts running Microsoft Server 2003, Microsoft Server 2008 (RTM), Microsoft Server 2008 R2 (RTM)…” I-17
Restoring the Intrusion Defense Firewall Plug-in After an Unsuccessful Migration I-18

Appendix J: Vulnerability Protection Deployment Tool

About Vulnerability Protection Deployment Tool J-2

System Requirements J-2

Installing Vulnerability Protection Deployment Tool J-3

Vulnerability Protection Deployment Tool Tasks J-5

Configuring Server Settings J-6

Working with Logs J-8

Troubleshooting J-9
Errors when Deploying the Install Agent Task J-9
Errors when Deploying the Uninstall Agent Task J-11
Unable to Check Status when Deploying the Activate Agent or Check Status Task J-12

Preface

Preface

Welcome to the Trend Micro™ Vulnerability Protection *Installation Guide*. This document discusses requirements and procedures for installing the Vulnerability Protection Manager and Agents.

Topics in this chapter:

- *Trend Micro Vulnerability Protection Documentation on page vi*
- *Audience on page vi*
- *Document Conventions on page vii*

Trend Micro Vulnerability Protection Documentation

Trend MicroVulnerability Protection documentation includes the following:

TABLE 1. Vulnerability Protection Documentation

DOCUMENTATION	DESCRIPTION
Installation Guide	A PDF document that discusses requirements and procedures for installing Trend Micro Vulnerability Protection Manager and Agents.
Administrator's Guide	A PDF document that provides information on the main product tasks, usage advice, reference data, and field-specific information such as valid parameter ranges and optimal values.
Help	HTML files compiled in WebHelp or CHM format that provide "how to's", usage advice, and field-specific information. The Help is accessible from Trend Micro Vulnerability Protection Manager and Agents.
Readme file	Contains a list of known issues and basic installation steps. It may also contain late-breaking product information not found in the Help or printed documentation
Knowledge Base	An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following website: http://esupport.trendmicro.com

Download the latest version of the PDF documents and readme at:

http://docs.trendmicro.com/en-us/enterprise/vulnerability-protection.aspx

Audience

Trend Micro Vulnerability Protection documentation is intended for the following users:

- Trend Micro Vulnerability Protection Administrators: Responsible for installing and managing the manager and agents. These users are expected to have advanced networking and server management knowledge.
- End users: Users who have Trend Micro Vulnerability Protection Agent installed on their endpoints. The skill level of these individuals ranges from beginner to power user.

Document Conventions

The documentation uses the following conventions.

TABLE 2. 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

CONVENTION	DESCRIPTION
 **WARNING!**	Critical actions and configuration options

Chapter 1

Introduction

This chapter introduces Trend Micro™ Vulnerability Protection and provides an overview of its features and capabilities.

Topics in this chapter:

- *About Vulnerability Protection on page 1-2*
- *Vulnerability Protection Components on page 1-2*
- *Features on page 1-2*

About Vulnerability Protection

Trend Micro Vulnerability Protection provides advanced vulnerability shielding against zero-day threats and blocks exploits before a patch can even be deployed. Trend Micro Vulnerability Protection is a standalone product replacement for Intrusion Defense Firewall (OfficeScan module) and works in conjunction with other complete user protection solutions including Control Manager for central management.

Vulnerability Protection Components

Trend Micro Vulnerability Protection consists of the following components:

TABLE 1-1. Trend Micro Vulnerability Protection Components

COMPONENT	DESCRIPTION
Vulnerability Protection Manager	The centralized web-based management console used by administrators for configuring security policy and deploying protection to the Vulnerability Protection Agent
Vulnerability Protection Agent	The security agent deployed directly on endpoints to provide Intrusion Prevention and Firewall protection

Features

The following table lists the features of Trend Micro Vulnerability Protection.

TABLE 1-2. Trend Micro Vulnerability Protection Features

FEATURES	DESCRIPTION
Firewall	• Centralizes management of the server firewall policy • Supports virtual machine zoning and prevents Denial of Service (DoS) attacks **Note** Running both OfficeScan firewall and Trend Micro Vulnerability Protection firewall, regardless of whether Vulnerability Protection firewall is active, may lead to unpredictable behavior on some Windows XP/2003 systems. Trend Micro recommends uninstalling the OfficeScan firewall driver to resolve the issue. For more information, see http://esupport.trendmicro.com/solution/en-us/0122179.aspx.
Intrusion Prevention	• Uses vulnerability rules to shield known vulnerabilities from an unlimited number of exploits • With the enforcement of periodic recommendation scans, automatically shields newly discovered vulnerabilities through a deployment of rules to servers without requiring a system restart • Enables compliance with PCI Requirement 6.6 for the protection of web applications and the data that they process • Defends against SQL injection attacks, cross-site scripting attacks, and other web application vulnerabilities • Shields vulnerabilities until code fixes are available • Increases visibility into, or control over, applications accessing the network • Identifies malicious applications accessing the network and reduces the vulnerability exposure of your servers

Chapter 2

Preparing for Installation

This chapter provides the information necessary before installing Trend Micro Vulnerability Protection.

Topics in this chapter:

- *Installation Requirements on page 2-2*
- *Performance Recommendations on page 2-3*
- *System Requirements on page 2-4*
- *Co-Located Relay-enabled Agent on page 2-8*
- *Scaling for Large Installations on page 2-8*

Installation Requirements

The following table lists the requirements for the installation.

TABLE 2-1. Installation Requirements

INSTALLATION INFORMATION	DESCRIPTION
Installation packages	Place the installation package for the Vulnerability Protection Manager and the Vulnerability Protection Agent on the target endpoints.
Administrator privileges	You need to have Administrator privileges on the endpoints on which you will install Trend Micro Vulnerability Protection software components.
License (Activation codes)	During installation, the Setup Wizard prompts you to type an Activation Code. You can use the Registration Key that came with the product to obtain an Activation Code online from the Trend Micro website. **Note** If you do not activate your product during registration, you can do so at a later time from the product console. However, Vulnerability Protection provides a limited feature set until the activation process is complete.

Installation Information	Description
Network communication	Communication between the manager and its agents uses DNS host names by default. In order for a successful agent deployment, you must ensure that each endpoint can resolve the host name of the manager. This may require the Vulnerability Protection Manager endpoint to have a DNS entry or an entry in the agent endpoint's host file. **Note** The Setup Wizard requires the host name during the Vulnerability Protection Manager installation procedure. If you do not have DNS, type an IP address instead.
Ports	Trend Micro Vulnerability Protection requires several dedicated ports that must remain open. For more information, see *Ports Used by Trend Micro Vulnerability Protection on page A-1*.
Reliable time stamps	All endpoints on which Trend Micro Vulnerability Protection software is running should be synchronized with a reliable time source such as a Network Time Protocol (NTP) server.

Performance Recommendations

Many Vulnerability Protection Manager operations require high CPU and memory resources. Trend Micro recommends that the Vulnerability Protection Manager endpoint should have four cores and sufficient RAM in high scale environments.

The database should be installed on hardware that is equal to or better than the specifications of the Vulnerability Protection Manager endpoint. For optimal performance, the database should have 8 to 16 GB of RAM and fast access to local or network storage. Trend Micro recommends consulting a database administrator on the best database configuration and the ideal maintenance plan.

System Requirements

The following tables list the system requirements for installing Trend Micro Vulnerability Protection Manager and Agent.

TABLE 2-2. Vulnerability Protection Manager System Requirements

HARDWARE/ SOFTWARE	SPECIFICATIONS
Memory	4 GB (8 GB recommended)
Disk space	1.5 GB (5 GB recommended)
Number of CPU	2 (4 recommended) **Note** Trend Micro recommends allocating 4 CPUs and 13 GB of disk space when installing Vulnerability Protection Manager with the embedded Microsoft SQL Server Express database.
Operating system	• Microsoft™ Windows Server® 2012 R2 (64-bit) • Microsoft™ Windows Server® 2012 (64-bit) • Microsoft™ Windows Server® 2008 R2 with SP1 (64-bit) • Microsoft™ Windows Server® 2008 with SP2 (32-bit and 64-bit) • Microsoft™ Windows Server® 2003 R2 with SP1 or SP2 (32-bit and 64-bit) • Microsoft™ Windows Server® 2003 with SP2 (32-bit and 64-bit)

HARDWARE/ SOFTWARE	SPECIFICATIONS
Database	• Oracle™ Database11g • Oracle™ Database 12c • Microsoft™ SQL Server® 2014 • Microsoft™ SQL Server® 2014 Express • Microsoft™ SQL Server® 2012 • Microsoft™ SQL Server® 2012 Service Pack 2 (SP2) Express embedded • Microsoft™ SQL Server® 2012 Express (all service packs) • Microsoft™ SQL Server® 2008 (all service packs) • Microsoft™ SQL Server® 2008 Express (all service packs) **Tip** Installing SQL Server 2012 SP2 Express requires the .NET Framework 3.5 SP1 and Windows Installer 4.5. on Windows 2008 SP2 or later.

Hardware/ Software	Specifications
Web browser	• Mozilla® Firefox® 12+ • Microsoft™ Internet Explorer® 11.x • Microsoft™ Internet Explorer® 10.x • Microsoft™ Internet Explorer® 9.x • Google Chrome™ 20+ **Note** Cookies must be enabled on all browsers. Internet Explorer Support Policy: Microsoft has announced a new browser-support policy that will take effect after January 12, 2016. After this date, only the most recent version of Internet Explorer available for a supported operating system will receive technical support and security updates from Microsoft. Trend Micro works very closely with Microsoft to ensure that its products are compatible with new Internet Explorer browser versions as quickly as possible after public release. Older versions of Internet Explorer may continue to function with Trend Micro products, but support may be limited if a technical issue is found to be directly related to Internet Explorer. In these cases, due to limited support from Microsoft, users may be asked to upgrade to the latest version of Internet Explorer or change browsers to resolve the issue. In addition, users are advised to first check with Trend Micro for known compatibility issues or special instructions before upgrading to a new version of Internet Explorer. More information on Microsoft's new Internet Explorer Support Policy can be found here.

Table 2-3. Vulnerability Protection Agent System Requirements

Hardware/Software	Specifications
Memory	128 MB

HARDWARE/SOFTWARE	SPECIFICATIONS
Disk space	500 MB
Operating system	• Microsoft™ Windows® 10 (32-bit and 64-bit) • Microsoft™ Windows® 8.1 (32-bit and 64-bit) • Microsoft™ Windows Server® 2012 R2 (64-bit) • Microsoft™ Windows® 8 (32-bit and 64-bit) • Microsoft™ Windows Server® 2012 (64-bit) • Microsoft™ Windows® 7 with SP1 (32-bit and 64-bit) • Microsoft™ Windows Server® 2008 R2 with SP1 (64-bit) • Microsoft™ Windows Server® 2008 (32-bit and 64-bit) • Microsoft™ Windows® Vista with SP2 (32-bit and 64-bit) • Microsoft™ Windows Server® 2003 with SP1 (32-bit and 64-bit) and patched with "Windows Server 2003 Scalable Networking Pack" • Microsoft™ Windows Server® 2003 with SP2 (32-bit and 64-bit) • Microsoft™ Windows Server® 2003 R2 with SP2 (32-bit and 64-bit) • Microsoft™ Windows® XP with SP2 or SP3 (32-bit) • Microsoft™ Windows® XP with SP2 (64-bit)

Multi-Node Manager

Vulnerability Protection Manager can be run as multiple nodes operating in parallel using a single database. Running the manager as multiple nodes provides increased reliability, redundant availability, virtually unlimited scalability, and better performance.

Each node is capable of all tasks and no node is more important than any of the others. Users can sign into any node to carry out their tasks. When one node becomes unavailable, this does not lead to the loss of any data nor does it prevent the manager from completing any task.

Each node must be running the same version of the manager software. When performing an upgrade of the manager software, the first manager to be upgraded takes over all Vulnerability Protection Manager duties and shuts down all other Vulnerability Protection Manager nodes. The other nodes appear as *Offline (Upgrade Required)* on the **Network Map with Activity Graph** of the **System Activity** panel under **System Information**. After each node is upgraded, the node goes back online and resumes all manager tasks.

For more information, see *Managing Multiple Nodes on page 5-3*.

Co-Located Relay-enabled Agent

A Vulnerability Protection deployment requires at least one Vulnerability Protection Relay. Relays distribute Software Updates to agents which keep your protection up to date. Trend Micro recommends installing a Relay-enabled agent on the same endpoint as the Vulnerability Protection Manager to protect the host computer and to function as a local Relay.

During the installation of the Vulnerability Protection Manager, the installer will look in its local directory for an agent installation package.

If an agent installation package is unavailable, the installation of the Vulnerability Protection Manager proceeds without the agent. The Relay-enabled agent may be installed at a later time.

For more information, see *Installing Vulnerability Protection Agent on page 3-15* and *Activating the Vulnerability Protection Agent on page 5-6*.

Scaling for Large Installations

To improve the performance of Trend Micro Vulnerability Protection installations with more than 1,000 managed endpoints, Trend Micro recommends the following measures:

- Install the manager on an endpoint with a minimum of a quad-core processor and 8 GB of available memory

Note

Installing Microsoft SQL Server Express on an endpoint with a 32-bit dual-core processor and 4 GB of available memory causes high CPU usage issues. As a result, completing resource-intensive tasks such as recommendation scans can take as long as four days.

- Upgrade the server hardware

Note

For example, upgrading to 64-bit dual node 8-core processors increases processing speeds.

- Use an external database

Note

For more information on installing a standalone database, see *Installing the Database on page 3-2*.

Chapter 3

Installation

This chapter describes the installation steps for Trend Micro Vulnerability Protection.

Topics in this chapter:

- *Installation Tasks on page 3-2*
- *Installing the Database on page 3-2*
- *Installing Vulnerability Protection Manager on page 3-4*
- *Installing Vulnerability Protection Agent on page 3-17*

Installation Tasks

The following are the primary installation tasks:

1. Install the database if you intend to use a standalone server.

   For more information, see *Installing the Database on page 3-2*.

2. Install Vulnerability Protection Manager.

   For more information, see *Installing Vulnerability Protection Manager on page 3-4*.

3. Install Vulnerability Protection Agent.

   For more information, see *Installing Vulnerability Protection Agent on page 3-17*.

Installing the Database

If you intend to use a standalone server, you must first install the database software, create a database, and create a user account before installing Vulnerability Protection Manager.

Important

Vulnerability Protection does not support special characters in the database user name.

The following table lists the recommended databases for enterprise deployments.

TABLE 3-1. Databases for Enterprise Deployment

DATABASE	VERSION
Microsoft™ SQL Server	• 2014 • 2012 • 2008 R2 • 2008

DATABASE	VERSION
Microsoft™ SQL Server Express™	• 2014 • 2012 SP2 • 2008 R2 SP2
Oracle Database	• 11g • 12c

Account Details

The following table lists the recommended configuration settings for the standalone database.

TABLE 3-2. Database Configuration Settings

DATABASE	ROLES	PERMISSIONS
Microsoft SQL Server	• DB_Creator Server Roles • DB_Owner (of Vulnerability Protection Manager)	N/A
Oracle Database	• CONNECT • RESOURCE	• CREATE TABLE • CREATE SEQUENCE • CREATE TRIGGER

Note

Take note of the database account details. The Setup Wizard requires the database account details during the Vulnerability Protection Manager installation process.

Communication with SQL Server

When using named pipes to connect to SQL Server, a properly authenticated Microsoft Windows communication channel must be available between the Vulnerability

Protection Manager's host and the SQL Server host. If no such communication channel is available, Vulnerability Protection Manager cannot communicate with SQL Server over named pipes.

For more information on using named pipes, see http://technet.microsoft.com/en-us/library/ms189307(v=sql.105).aspx.

Installing Vulnerability Protection Manager

This section describes how to install Vulnerability Protection Manager.

Installing Vulnerability Protection Manager

Procedure

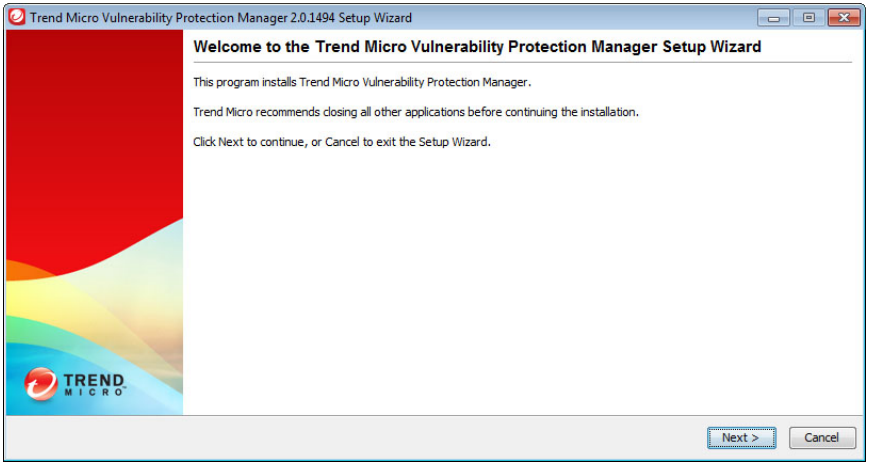
1. Run any of the following installation packages:

INSTALLER	DESCRIPTION
VP-Windows-2.0.<XXXX>.i386	Standard installer for 32-bit operating systems
VP-Windows-2.0.<XXXX>.x64	Standard installer for 64-bit operating systems
VP-Windows-2.0.<XXXX>.i386-sqlexp	Installer embedded with Microsoft SQL Server Express and Vulnerability Protection Agent installation package for 32-bit operating systems
VP-Windows-2.0.<XXXX>.x64-sqlexp	Installer embedded with Microsoft SQL Server Express and Vulnerability Protection Agent installation package with Relay option for 64-bit operating systems

Note

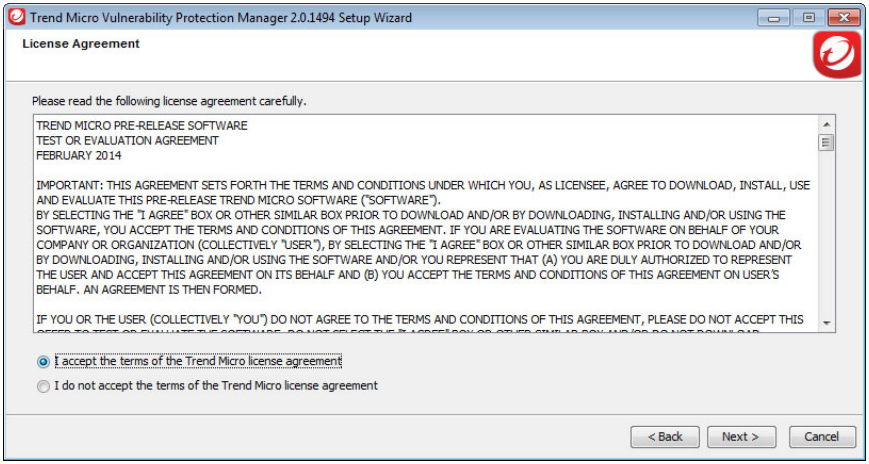
<XXXX> is the installer build number.

The **Trend Micro Vulnerability Protection Manager Setup Wizard** screen appears.



2. Click **Next**.

The **License Agreement** screen appears.



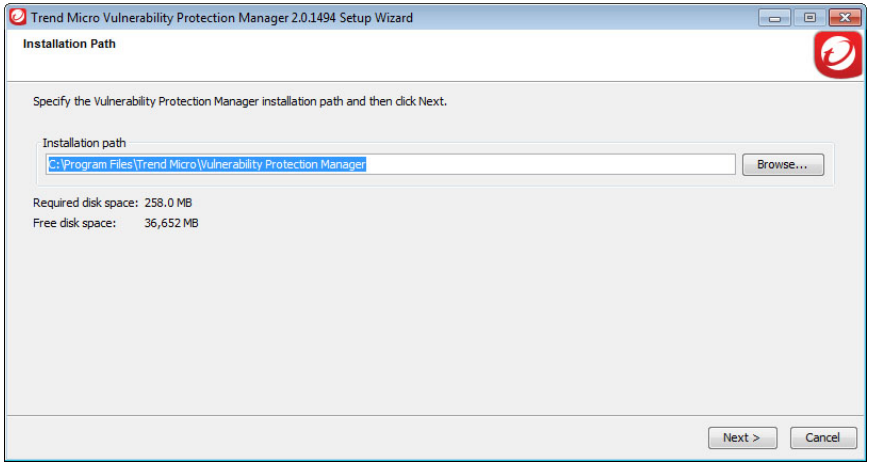
3. Click **I accept the terms of the Trend Micro license agreement** to continue the installation.

Note

If you do not accept the terms, select **I do not accept the terms of the Trend Micro license agreement** and click **Cancel**. This terminates the installation without modifying your operating system.

4. Click **Next**.

The **Installation Path** screen appears.



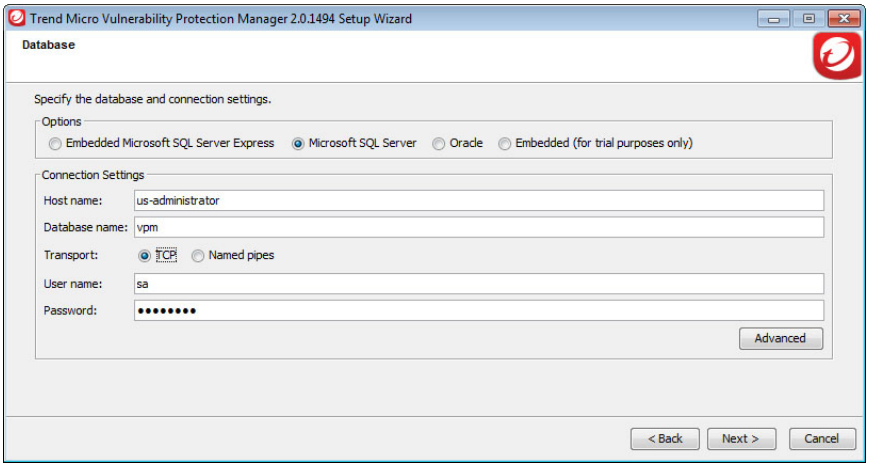
5. Specify a location for the Vulnerability Protection Manager files.

Note

When selecting a folder, the installer appends the suggested folder name at the end of the selected path. To avoid duplication, review the folder path when using the **Browse** button.

6. Click **Next**.

The **Database** screen appears.



Note

The **Embedded Microsoft SQL Server Express** option is only available when using an installer embedded with Microsoft SQL Server Express.

7. Select from the following database options:

TYPE	DESCRIPTION
Embedded Microsoft SQL Server Express	The Vulnerability Protection Manager installs SQL Server 2012 Service Pack 2 (SP2) Express, which is included in the installation package. **Note** This option is only available when using either of the installer packages embedded with Microsoft SQL Server Express.
Microsoft SQL Server	The Vulnerability Protection Manager accesses the previously installed Microsoft SQL Server.

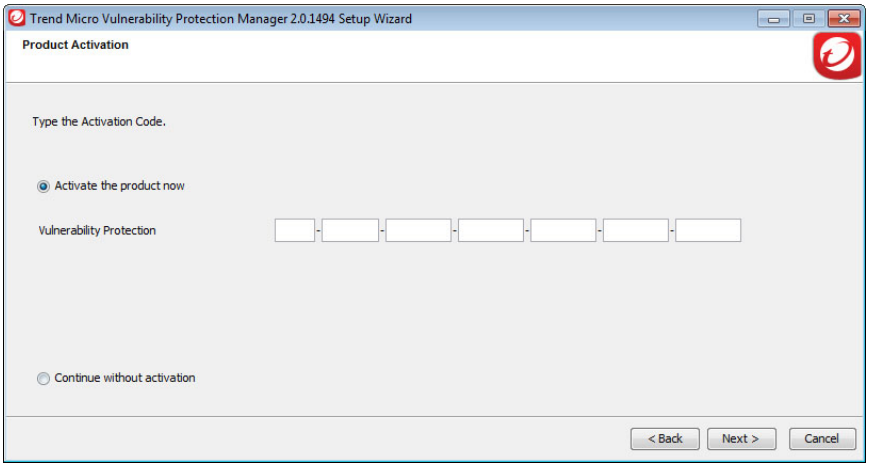
TYPE	DESCRIPTION
	Important If you select Microsoft SQL Server, you must first create the database before installing Vulnerability Protection Manager. For more information, see *Installing the Database on page 3-2*.
Oracle Database	The Vulnerability Protection Manager accesses the previously installed Oracle database. **Important** If you select Oracle, you must first create the database before installing Vulnerability Protection Manager. For more information, see *Installing the Database on page 3-2*.

8. Depending on the selected database, provide the following in the **Connection Settings** section:

ITEM	DESCRIPTION
Host name	The label assigned to a single endpoint connected to a network
Database name	The name assigned to a specific database
Transport	Select one of the following: • **Transmission Control Protocol (TCP)** • **Named Pipe** **Note** These options are only available for Microsoft SQL Server
User name	The user name for the System Administrator (sa) account
Password	The password for the System Administrator (sa) account

9. Click **Next**.

The **Product Activation** screen appears.

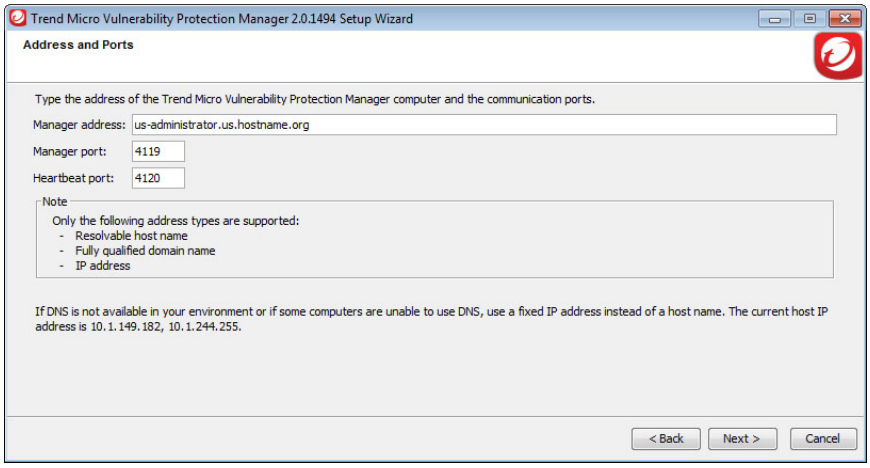


10. Type your **Activation Code**.

> **Note**
>
> If you select **Continue without activation**, you can activate your product at a later time using the web console by going to **Administration** > **Licenses**.

11. Click **Next**.

The **Address and Ports** screen appears.



12. Provide the following:

    - **Manager address**: A resolvable host name, fully-qualified domain name (FQDN), or IP address

      Note

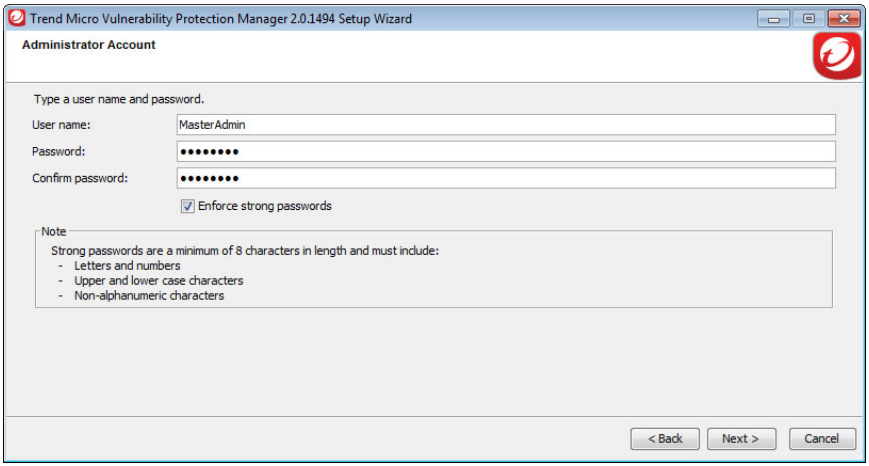
      If DNS is not available in your environment, or if some endpoints are unable to use DNS, use a fixed IP address instead of a host name.

    - **Manager port**: The HTTPS port responsible for the Vulnerability Protection Manager web console

    - **Heartbeat port**: The port on which the Manager listens for communication from agents

13. Click **Next**.

The **Administrator Account** screen appears.



14. Type the user name and password for the administrator account. Retype the password to confirm.

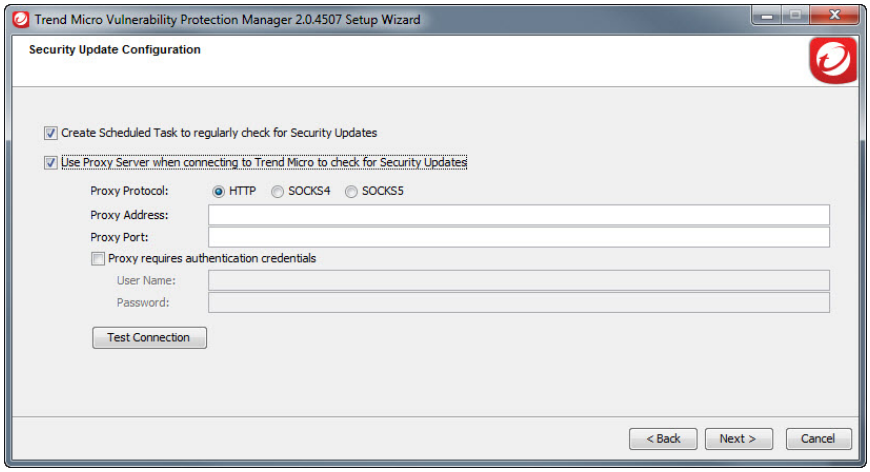
Tip

Trend Micro recommends selecting **Enforce strong passwords**. Strong passwords are a minimum of 8 characters in length and must include:

- Letters and numbers
- Upper and lower case characters
- Non-alphanumeric characters

15. Click **Next**.

The **Security Update Configuration** screen appears.



16. Accept the **Create Scheduled Task to regularly check for Security Updates** option (enabled by default).

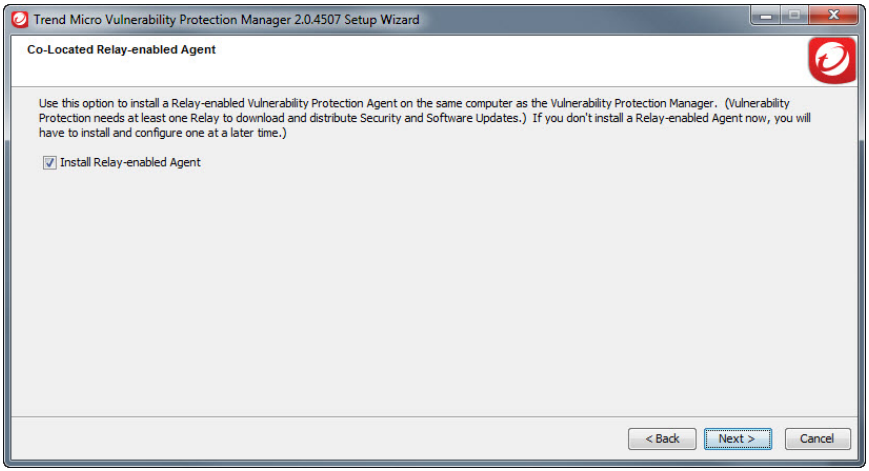
Tip

Trend Micro recommends enabling this feature to automatically retrieve the latest components or check for new software. You can configure updates at any time using the web console by going to **Administration** > **Updates**.

17. If the network requires that Vulnerability Protection uses a proxy server, select **Use Proxy Server when connecting to Trend Micro for Security Updates** and configure the proxy settings.

18. Click **Next**.

The **Co-Located Relay-enabled Agent** screen appears.

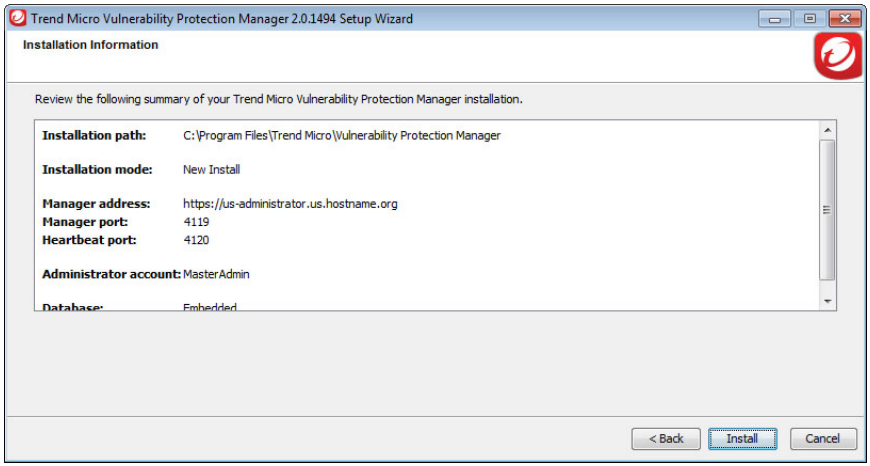


Note

This option is only available when installing on endpoints running 64-bit operating systems.

19. Select **Install Relay-enabled Agent**.
20. Click **Next**.

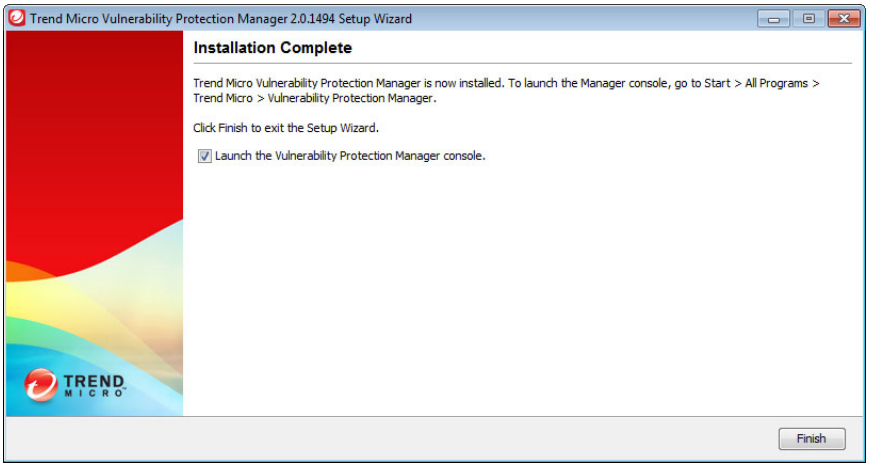
The **Installation Information** screen appears.



21. Verify the information and click **Install** to start installing Vulnerability Protection Manager.

    The installation process begins.

22. On the **Installation Complete** screen, click **Finish** to exit the Setup Wizard.



Installing Vulnerability Protection Agent

This section describes how to install Vulnerability Protection Agents.

Importing Agent Software

The Vulnerability Protection Agent installer may be downloaded from the Download Center. However, Trend Micro recommends importing the installation package into Vulnerability Protection Manager first, and then exporting the Vulnerability Protection Agent installation package.

Completing this step ensures that the Agent installer is readily available from the Vulnerability Protection Manager web console.

Procedure

1. Download an agent installation package and save to a local folder.
2. On the Vulnerability Protection Manager web console, go to **Administration** > **Updates** > **Software** > **Local**.

The **Local Software** screen appears.

3. Click **Import**.
4. The **Import Software** screen appears.
5. Click **Choose File** and locate the agent installation package from the local folder.
6. Click **Next**.
7. Click **OK** if a confirmation screen appears.
8. Click **Finish**.

   The import progress bar appears.
9. Click **Close**.

Exporting the Agent Installer

After importing the Vulnerability Protection Agent into Vulnerability Protection Manager, you need to export and save the installation package to a local folder.

Procedure

1. On the Vulnerability Protection Manager web console, go to **Administration** > **Updates** > **Software** > **Local**.
2. Select the agent.
3. From the menu bar, click **Export** > **Export Installer**.

   The installer is exported into an installer package.
4. Save the agent to a local folder.

Installing Vulnerability Protection Agent

Procedure

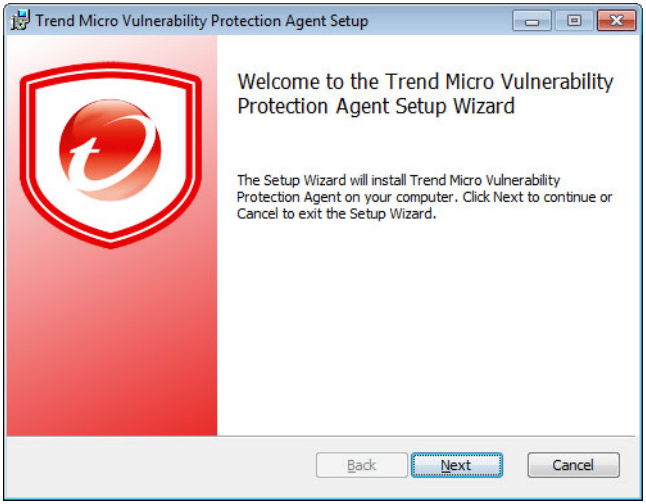
1. Run any of the following installation packages:

INSTALLER	DESCRIPTION
VPAgent-Windows-2.0.2-<XXXX>.i386	Standard installer for 32-bit operating systems
VPAgent-Windows-2.0.2-<XXXX>.x86_64	Standard installer for 64-bit operating systems

Note

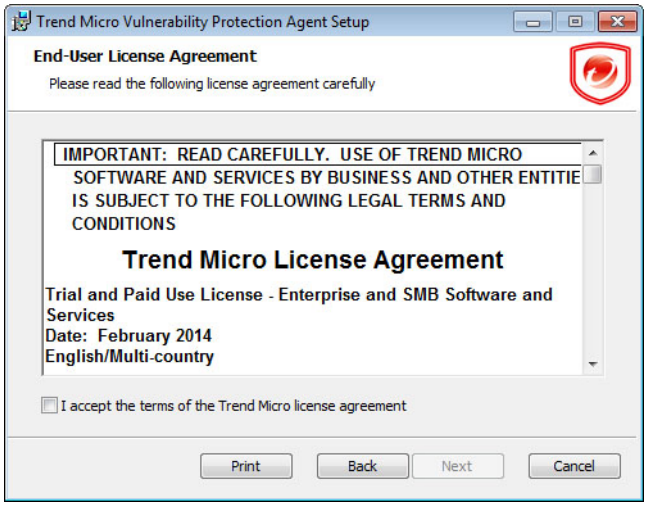
<XXXX> is the installer build number.

The **Welcome** screen appears.



2. Click **Next**.

The **End-User License Agreement** screen appears.



3. Click **I accept the terms of the Trend Micro license agreement** to continue the installation.

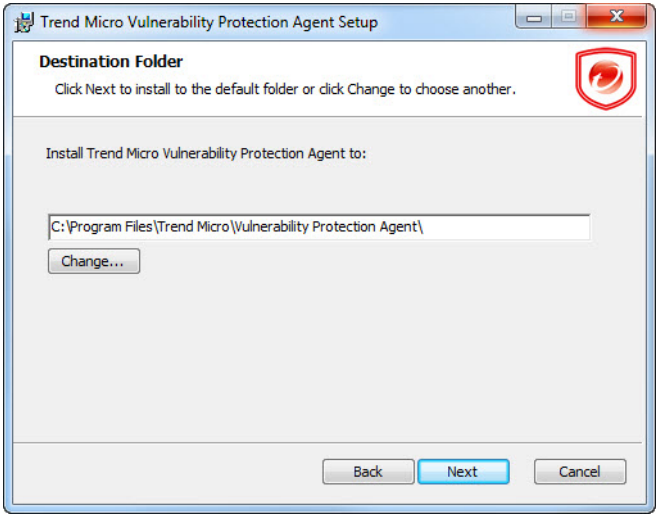
Note

If you do not accept the terms, click **Cancel**. This terminates the installation without modifying your operating system.

---

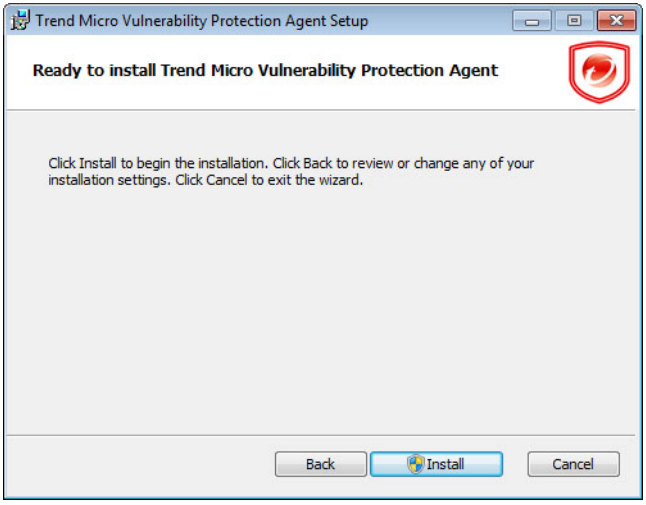
4. Click **Next**.

The **Destination Folder** screen appears.



5. Specify a location for the Vulnerability Protection Agent files and click **Next**.

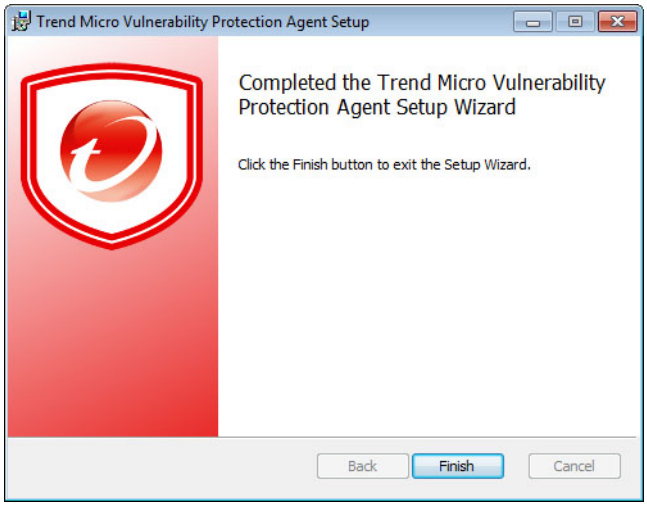
   A confirmation screen appears.



6. Click **Install** to start installing Vulnerability Protection Agent.

   The installation process begins.

7. On the **Completed the Trend Micro Vulnerability Protection Agent Setup Wizard** screen, click **Finish** to exit the Setup Wizard.



   The Vulnerability Protection Agent installs and runs immediately after the installation completes.

Uninstallation

The following section explains how to uninstall Trend Micro Vulnerability Protection Manager and Agent.

Uninstalling Manager Using the Uninstallation Program

Procedure

1. Uninstall Vulnerability Protection Manager in one of the following ways:

   - From the Start menu:

     a. On the Vulnerability Protection Manager endpoint, click **Start** > **Programs** > **Trend Micro** > **Trend Micro Vulnerability Protection Manager Uninstaller**.

        A confirmation screen appears.

     b. Click **Yes** to verify the uninstallation.

     c. Click **Next** to begin uninstalling Vulnerability Protection Manager.

        A confirmation screen appears.

     d. Click **Finish** to close the manager uninstallation program.

   - From Windows Control Panel:

     a. From the Windows Control Panel, click **Add/Remove Programs**.

     b. Click **Control Panel** > **Add or Remove Programs**.

     c. Locate and double-click "Vulnerability Protection Manager" and follow the on-screen instructions.

Uninstalling Vulnerability Protection Agent Using the Uninstallation Program

Procedure

1. From the Windows Control Panel, click **Add/Remove Programs**.
2. Select **Trend Micro Vulnerability Protection Agent** from the list, and click **Change/Remove**.

Important

When you uninstall an activated agent from a managed endpoint, Vulnerability Protection Manager does not automatically detect the uninstallation. The endpoint remains listed in the Computers list and its status appears as **Managed (Offline)**. To avoid this, either deactivate the agent from the web console before uninstallation, or delete the endpoint from the Computers list.

Uninstalling from the Command Line

You can uninstall both the Vulnerability Protection Manager and Vulnerability Protection Agent using a command line editor (for example, cmd.exe).

To uninstall Vulnerability Protection Manager, use the following commands:

- `Uninstall.exe`

  Performs a normal uninstallation

- `Uninstall.exe -q`

  Performs a silent uninstallation

To uninstall Vulnerability Protection Agent, use the following commands:

- `msiexec /x <package_name_including_extension>`

  Performs a normal uninstallation

- `msiexec /x <package_name_including_extension> /quiet`

  Performs a silent uninstallation

Chapter 4

Upgrading

The following are the steps for upgrading a basic Agent-based Vulnerability Protection installation:

1. Upgrade the Vulnerability Protection Manager to version 2.0 SP2.

   For more information, see *Upgrading Vulnerability Protection Manager on page 4-2*.

2. Install at least one Vulnerability Protection Agent with Relay functionality enabled.

   For more information, see *Installing Vulnerability Protection Agent on page 3-15* and *Enabling Relay Functionality on page 5-7*.

3. Upgrade the Vulnerability Protection Agents and Relays to version 2.0 SP2.

   For more information, see *Upgrading Agents from Vulnerability Protection Manager on page 4-5*.

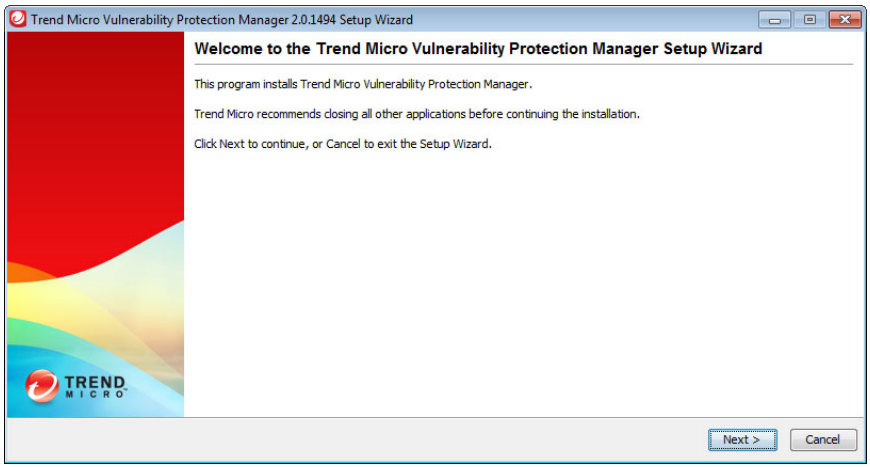
Upgrading Vulnerability Protection Manager

This section describes the steps for upgrading to Vulnerability Protection 2.0 SP2.

Procedure

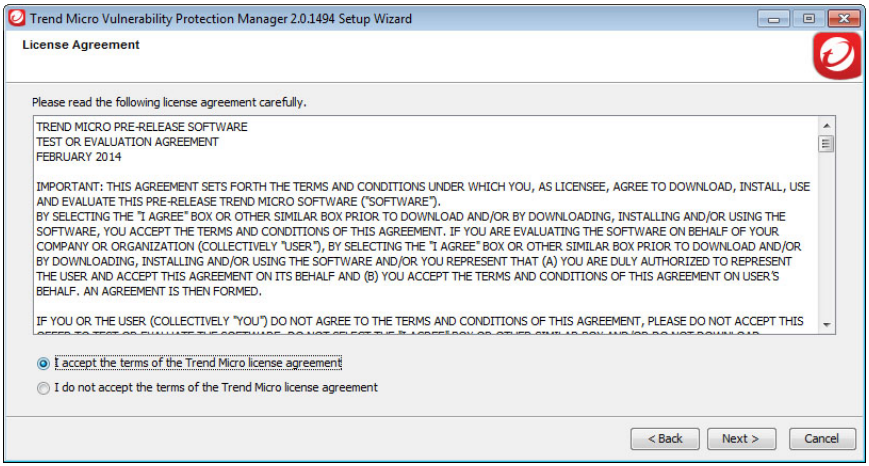
1. Download the Vulnerability Protection Manager 2.0 SP2 installation package from the Trend Micro Download Center (http://downloadcenter.trendmicro.com/).
2. Save the installation package to a local folder.
3. Run the installation package.

   The **Trend Micro Vulnerability Protection Manager Setup Wizard** screen appears.



4. Click **Next**.

The **License Agreement** screen appears.



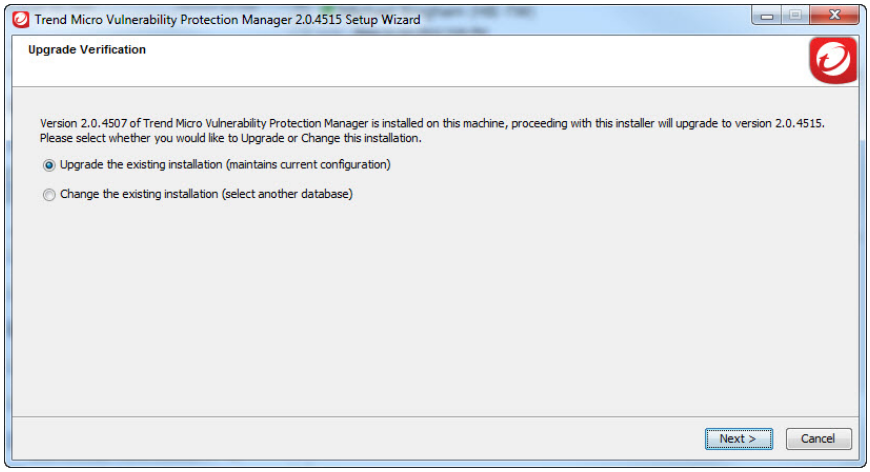
5. Click **I accept the terms of the Trend Micro license agreement** to continue the installation.

Note

If you do not accept the terms, select **I do not accept the terms of the Trend Micro license agreement** and click **Cancel**. This terminates the installation without modifying your operating system.

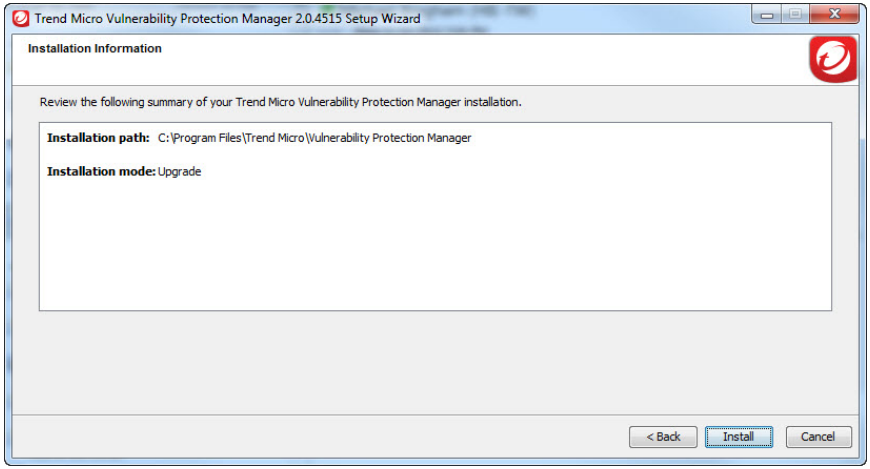
6. Click **Next**.

The **Upgrade Verification** screen appears.



7. Select **Upgrade the existing installation (maintains current configuration)**.
8. Click **Next**.

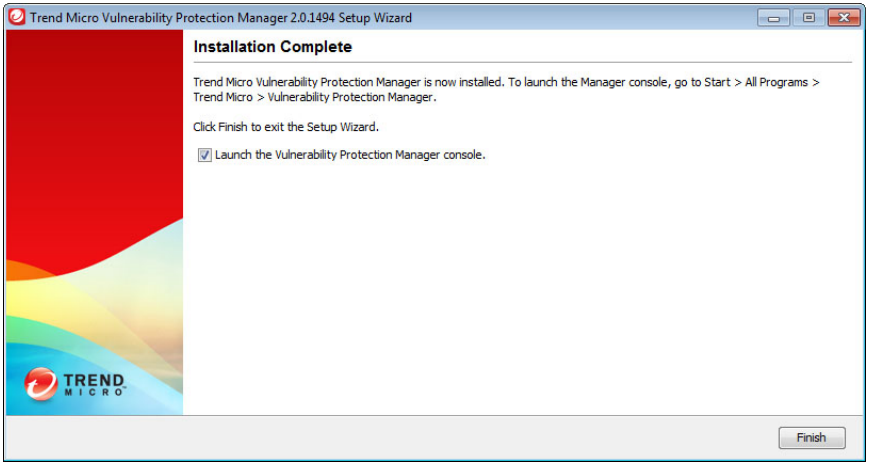
   The **Installation Information** screen appears.



9. Verify the information and click **Install** to start installing Vulnerability Protection Manager.

   The installation process begins.

10. On the **Installation Complete** screen, click **Finish** to exit the Setup Wizard.



Upgrading Agents from Vulnerability Protection Manager

This section describes the steps in deploying software upgrades to Agents.

Note

You may also update each agent manually using the steps for installing agents.

For more information, see *Installing Vulnerability Protection Agent on page 3-15*.

Procedure

1. On the Vulnerability Protection Manager web console, go to **Computers**.
2. Locate the agent that you want to upgrade from the **Computers** list.
3. Right-click the endpoint name and select **Actions** > **Upgrade Agent Software**.

   The **Upgrade Agent Software** screen appears.
4. Select the software version from the **Agent Version** drop-down list.
5. Select an upgrade schedule.
6. Click **OK**.

   The agent software is upgraded to the selected version.

Chapter 5

Post-Installation Tasks

This chapter describes the post-installation steps for Trend Micro Vulnerability Protection.

Topics in this chapter:

- *Verifying a Successful Installation on page 5-2*
- *Managing Multiple Nodes on page 5-3*
- *Activating the Vulnerability Protection Agent on page 5-6*
- *Enabling Relay Functionality on page 5-7*
- *Configuring a Software Update Server on page 5-8*

Verifying a Successful Installation

To verify the installation, follow the appropriate steps for your operating system.

Procedure

- For Windows 7 (32- and 64-bit), Windows XP (64-bit), and Windows Server 2003 (32-bit)

  a. Right-click **Computer** from the Start menu.

  b. Go to **Manage** > **Services and Applications** > **Services**.

  c. Locate "Trend Micro Vulnerability Protection Manager" or "Vulnerability Protection Agent".

- For Windows Server 2008 (32- and 64-bit) and Windows Server 2008 R2 (64-bit)

  a. Right-click **Computer** from the Start menu.

  b. Go to **Programs** > **Administraive Tools** > **Services**.

  c. Locate "Trend Micro Vulnerability Protection Manager" or "Vulnerability Protection Agent".

- For Windows 8 (32- and 64-bit), Windows 8.1 (32- and 64-bit), Windows Server 2012 (64-bit), Windows Server 2012 R2 (64-bit)

  a. Click the **Desktop** tile from the **Start** screen.

  b. From the Desktop, right-click **Start**.

  c. Go to **Computer Management** > **Services and Applications** > **Services**.

  d. Locate "Trend Micro Vulnerability Protection Manager" or "Vulnerability Protection Agent".

Managing Multiple Nodes

Note

You must be using either a Microsoft SQL Server or an Oracle database to run multiple nodes.

Adding a Manager Node

To run the Vulnerability Protection Manager as multiple nodes, you must first add a node to an existing database.

Important

At no point should more than one instance of the installer be running at the same time. Doing so can lead to unpredictable results, including corruption of the database.

Procedure

1. Follow Steps 1 to 6 of the Vulnerability Protection Manager installation procedure.

   Note

   For more information, see *Installing Vulnerability Protection Manager on page 3-4*.

2. Type the account details of the database currently in use.

   The new node connects to the database.

Viewing Nodes

The **Network Map with Activity Graph** of the **System Activity** panel under **System Information** displays all Vulnerability Protection Manager nodes along with their status, combined activity, and jobs being processed.

Note

The Vulnerability Protection Manager processes many concurrent activities in a distributed pool that is executed by all online manager nodes. All activity not derived from user input is packaged as a job and can thus be run on any manager, except for some local jobs that are executed on each node, such as clearing the cache.

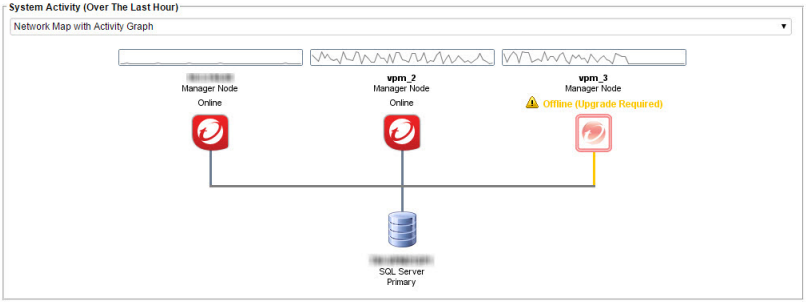
Procedure

1. On the Vulnerability Protection Manager web console, go to **Administration** > **System Information**.

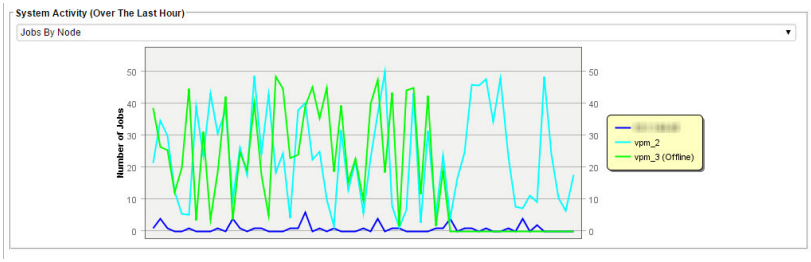
   The **System Information** screen appears.

2. Use the **System Activity** drop-down list to view the following information.

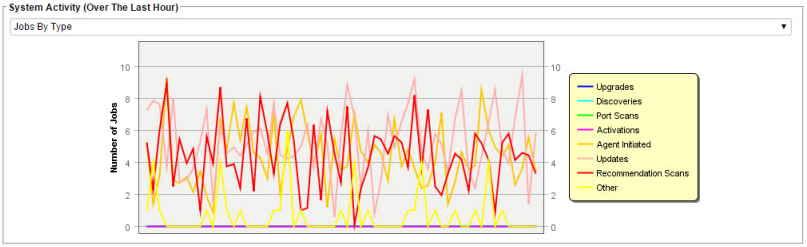
   - **Network Map with Activity Graph**: Displays an overview of the manager nodes in the network and a graphical representation of node activities over the last hour



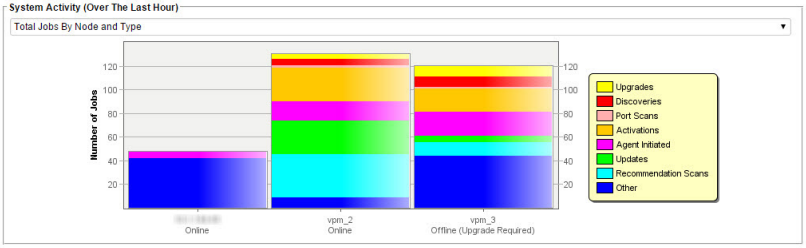
- **Jobs By Node**: Breaks down the number of jobs carried out by each node over the last hour



- **Jobs By Type**: Displays the job types completed by all the nodes over the last hour



- **Total Jobs By Node and Type**: Displays the total number of jobs and job types for each node over the last hour



Decommissioning Nodes

This section describes how to remove or decommission a manager node.

Note

A node must be offline before it can be decommissioned.

Procedure

1. Go to **Administration** > **System Information** > **System Activity (Over The Last Hour)** > **Network Map with Activity Graph**.

   The **Network Map with Activity Graph** appears.

2. Click the Manager Node icon of the node you want to decommission.

   The **Properties** screen appears.

3. Under **Options**, click **Decommission**.

   A confirmation screen appears.

4. Click **OK**.

   The decomissioned node is removed from the **Manager Node** screen.

Activating the Vulnerability Protection Agent

Trend Micro Vulnerability Protection automatically installs and activates the agent if you use the all-in-one Vulnerability Protection Manager package.

You may also choose to install the agent separately. For more information, see *Installing Vulnerability Protection Agent on page 3-17*.

When using the standalone installation package, you must activate the agent after installation.

Procedure

1. On the Vulnerability Protection Manager web console, go to **Computers** > **New** > **New Computer**.

   The **New Computer Wizard** appears.

2. Type the host name or IP address of the computer where an agent is installed in the **Hostname** field.

3. Select a policy based on the operating system from the **Policy** drop-down list.

4. Leave the default setting for the **Download Software Updates From** field.

5. Click **Next**.

   Vulnerability Protection Manager verifies that an agent is installed on the specified computer.

6. Click **Finish**.

Enabling Relay Functionality

You need to manually enable the relay functionality of an agent in any of the following scenarios:

- If you did not choose to install the relay-enabled agent during the Vulnerability Protection Manager installation process.
- If you are using a 32-bit server and you need to install the agent separately on a 64-bit endpoint.

Important

If you are running Windows Firewall, you also need to add a Firewall Rule that allows TCP/IP traffic on port 4122 on the Relay.

Procedure

1. On the Vulnerability Protection Manager web console, go to **Computers**.
2. Locate the agent from the **Computers** list and double-click the agent name.

   The **Computer Editor** screen appears.
3. On the **Computer Editor** screen, go to **Overview** > **Actions** > **Software**.
4. Click **Enable Relay**.

   Vulnerability Protection Manager installs the required plug-ins to enable the Relay Module on the agent.

Configuring a Software Update Server

Vulnerability Protection Software Updates are normally hosted and distributed by Relay-enabled agents. To deploy a Vulnerability Protection Agent on an endpoint, you must first import the software package for the platform into Vulnerability Protection Manager.

If you already have web servers deployed throughout your network, you may choose to let those servers perform the task of Software Update distribution instead of deploying Relays for that purpose. To do so, you will have to mirror the software repository of the Vulnerability Protection Relay on your web servers.

The following information describes how to set up your own software repository on a local web server.

Important

This is a required step for all endpoints running 32-bit operating systems.

Web Server Requirements

The following table lists the requirements for the web server.

TABLE 5-1. Web Server Requirements

ITEM	SPECIFICATION
Disk space	8 GB
Ports	• 4122: Agent-to-Relay communication (TCP) • 4123: Internal Relay communication to localhost (TCP)

Folder Structure

You must create a folder on the software web server which will mirror the structure of the software repository folder of a Trend Micro Vulnerability Protection Relay.

Note

The procedures for mirroring folders depend on your IT environemnt and are beyond the scope of this documentation.

The default location for the software repository folder on a Windows Relay is `C:\ProgramData\Trend Micro\Deep Security Agent\relay\www\dsa\`.

Note

This folder is a hidden folder by default. To display this folder in Windows Explorer, type `%ProgramData%` in **Start** > **Run**.

Below is the folder structure:

```
|-- dsa
| |-- <Platform>.<Architecture>
| |-- <Filename>
| |-- <Filename>
| |-- ...
```

For example:

```
|-- dsa
|     |-- Windows.x86_64
|     |-- Agent-Core-Windows-9.5.1-1532.x86_64.msi
|     |-- Agent-Core-Windows-9.5.1-1534.x86_64.msi
|     |-- Feature-DPI-Windows-9.5.1-1532.x86_64.dsp
|     |-- Feature-DPI-Windows-9.5.1-1534.x86_64.dsp
|     |-- ...
|     |-- Plugin-Filter-Windows-9.5.1-1532.x86_64.dsp
|     |-- Plugin-Filter-Windows-9.5.1-1534.x86_64.dsp
|     |-- ...
```

Note

The dsa folder on the Trend Micro Vulnerability Protection Relay contains more files and folders than those illustrated in the example above. However, the only folders you need to mirror when hosting a functioning software repository are the ones containing the files associated with the platform and architecture of the agents in use. You may also choose to mirror the entire dsa folder.

Using the New Software Repository

Configure Trend Micro Vulnerability Protection to start using the web server as a software update repository.

Procedure

1. On the Vulnerability Protection Manager web console, go to **Administration** > **System Settings** > **Updates**.
2. Under **Software Updates**, type the URL(s) of the folder(s) on your web server(s) containing the mirrored software repository.
3. Click **Add**.
4. Click **Save**.

Appendix A

Ports Used by Trend Micro Vulnerability Protection

This appendix lists the ports required by Trend Micro Vulnerability Protection Manager and Agent.

Vulnerability Protection Manager Ports

TABLE A-1. Vulnerability Protection Manager

PORT	DIRECTION	PURPOSE
4118 (TCP)	Manager to Agent	Agent listening port. Manager-to-Agent communication
4120 (TCP)	From Agent to Manager	The "heartbeat" port, used by Vulnerability Protection agents to communicate with Vulnerability Protection Manager
4119 (TCP)	Connection to the Vulnerability Protection Manager console	Used by a browser to connect to Vulnerability Protection Manager
25 (TCP)	From Manager to SMTP server	Communication to an SMTP Server for sending email alerts (configurable)
53 (TCP)	From Manager to DNS	For DNS lookup
389, 636 (TCP)	From Manager to LDAP server	Connection to an LDAP Server for Active Directory integration (configurable)
1433 (TCP)	Bi-directional	Microsoft SQL server
1521 (TCP)	Bi-directional	Oracle SQL Server
514 (UDP)	Bi-directional	Communication with a syslog server (configurable)

Vulnerability Protection Agent Ports

PORTS	PURPOSE
4118	Manager-to-agent communication
4122	Relay-to-agent communication

PORTS	PURPOSE
4123	Used for internal communication and should not be accessible from outside

Appendix B

Configuring the Settings.Properties File

This section contains information about the contents of the Settings.Properties file that you can use during a command line installation of Vulnerability Protection Manager.

Format

Use the following format for each entry in the Settings.Properties file:

```
<Screen Name>.<Property Name>=<Property Value>
```

Required Values

The following tables list the required values for the Settings.Properties file.

TABLE B-1. "LicenseScreen" Settings

PROPERTY	POSSIBLE VALUES	EXAMPLE
LicenseScreen.License.1=<value>	<AC for Vulnerability Protection>	LicenseScreen.License.1=XX-XXXX-XXXXX-XXXXX-XXXX-XXXX-XXXX

TABLE B-2. "CredentialsScreen" Settings

PROPERTY	POSSIBLE VALUES	EXAMPLE
CredentialsScreen.Administrator.Username=<value>	<user name for master administrator>	CredentialsScreen.Administrator.Username=MasterAdmin
CredentialsScreen.Administrator.Password=<value>	<password for the master administrator>	CredentialsScreen.Administrator.Password=12345678

Optional Values

The following tables list the optional values for the Settings.Properties file.

TABLE B-3. "UpgradeVerificationScreen" Settings

PROPERTY	POSSIBLE VALUES	EXAMPLE
UpgradeVerificationScreen.Overwrite=<value>	True False **Note** The default value is `False`. Setting this value to `True` will overwrite any existing data in the database without further prompting.	UpgradeVerificationScreen.Overwrite=False

Note
This screen/setting is not referenced unless an existing installation is detected.

TABLE B-4. "DatabaseScreen" Settings

PROPERTY	POSSIBLE VALUES	EXAMPLE
DatabaseScreen.DatabaseType=<value>	Microsoft SQL Server Express (only the installer included in the SQL Server Express package) Microsoft SQL Server Oracle	DatabaseScreen.DatabaseType=Microsoft SQL Server Express

PROPERTY	POSSIBLE VALUES	EXAMPLE
DatabaseScreen.Hostname =<value>	The name or IP address of the database host Current host name **Note** This setting is required for: • Oracle • Microsoft SQL Server	DatabaseScreen.Hostname =us-administrator
DatabaseScreen.Database Name=<value>	Any string **Note** This setting is required for: • Oracle • Microsoft SQL Server	DatabaseScreen.Database Name=vpm
DatabaseScreen.Transport =<value>	Named Pipes TCP **Note** This setting is required for: • Microsoft SQL Server	DatabaseScreen.Transport =TCP

PROPERTY	POSSIBLE VALUES	EXAMPLE
DatabaseScreen.Password =<value>	<password for database> **Note** This setting is required for: • Oracle • Microsoft SQL Server • Microsoft SQL Server Express	DatabaseScreen.Password =12345678
DatabaseScreen.SQLServer.Instance=<value>	<database instance> **Note** Leave this value blank to use the current instance. This setting is required for Microsoft SQL Server.	DatabaseScreen.SQLServer.Instance=MSSQLSERVER
DatabaseScreen.SQLServer.Domain=<value>	<database domain> **Note** This setting is required to use Windows Authentication on Microsoft SQL Server. To use SQL Server Authentication, leave the value blank.	DatabaseScreen.SQLServer.Domain=hostname.org

PROPERTY	POSSIBLE VALUES	EXAMPLE
DatabaseScreen.Username=<value>	<user name for database> **Note** This setting is required for: • Oracle • Microsoft SQL Server	DatabaseScreen.Username=sa
DatabaseScreen.SQLServer.UseDefaultCollation=<value>	True False **Note** The default value is `False`. This setting is required for: • Microsoft SQL Server	DatabaseScreen.SQLServer.UseDefaultCollation=False

TABLE B-5. "AddressAndPortsScreen" Settings

PROPERTY	POSSIBLE VALUES	EXAMPLE
AddressAndPortsScreen.ManagerAddress=<value>	<host name, URL or IP address of the manager host>	AddressAndPortsScreen.ManagerAddress=us-administrator
AddressAndPortsScreen.ManagerPort=<value>	<valid port number> **Note** The default value is `4119`.	AddressAndPortsScreen.ManagerPort=4119

PROPERTY	POSSIBLE VALUES	EXAMPLE
AddressAndPortsScreen.HeartbeatPort=<value>	<valid port number> **Note** The default value is `4120`.	AddressAndPortsScreen.HeartbeatPort=4120

TABLE B-6. "CredentialsScreen" Settings

PROPERTY	POSSIBLE VALUES	EXAMPLE
CredentialsScreen.UseStrongPasswords=<value>	True False **Note** The default value is `False`. `True` indicates that you want Vulnerability Protection Manager to enforce strong passwords.	CredentialsScreen.UseStrongPasswords=True

TABLE B-7. "SecurityUpdateScreen" Settings

PROPERTY	POSSIBLE VALUES	EXAMPLE
SecurityUpdateScreen.UpdateComponents=<value>	True False **Note** The default value is `True`. `True` indicates that you want Vulnerability Protection Manager to automatically retrieve the latest components.	SecurityUpdateScreen.UpdateComponents=False

Appendix C

Installation Output

The following are sample outputs from successful and unsuccessful command line installations.

Successful Installation

```
Stopping Trend Micro Vulnerability
                                Protection Manager Service...
Detecting previous versions of Trend Micro Vulnerability
                                Protection Manager...
Upgrade Verification Screen settings accepted...
Database Screen settings accepted...
License Screen settings accepted...
Address And Ports Screen settings accepted...
Credentials Screen settings accepted...
All settings accepted, ready to execute...
Uninstalling previous version
Stopping Services Extracting files...
Setting Up...
Connecting to the Database...
Creating the Database Schema...
Updating the Database Data...
Creating MasterAdmin Account...
Recording Settings...
Creating Temporary Directory...
Installing Reports...
Creating Help System...
Setting Default Password Policy...
Importing Example Security Profiles...
Applying Security Update...
Assigning IPS Filters to Example Security Profiles...
Correcting the Port for the Manager Security Profile...
Correcting the Port List for the Manager...
Creating IP List to Ignore...
Creating Scheduled Tasks...
Creating Asset Importance Entries...
Creating Auditor Role...
Auditing...
Optimizing...
Recording Installation...
Creating Properties File...
Creating Shortcut...
Configuring SSL...
Configuring Service...
Configuring Java Security...
```

```
Configuring Java Logging...
Cleaning Up...
Starting Vulnerability
                                Protection Manager...
Finishing installation...
```

Unsuccessful Installation

This example shows the output generated when the properties file contains an invalid license string.

Note

The [Error] tag in the trace indicates an unsuccessful attempt.

```
Stopping Trend Micro Vulnerability
                                Protection Manager Service...
Detecting previous versions of Trend Micro Vulnerability
                                Protection Manager...
Upgrade Verification Screen settings accepted...
Database Screen settings accepted...
Database Options Screen settings accepted...
[ERROR] The license code you have entered is invalid.
[ERROR] License Screen settings rejected...
Rolling back changes...
```

Appendix D

Trend Micro Vulnerability Protection Memory Usage

This section provides information on how to configure the maximum memory usage for Trend Micro Vulnerability Protection components.

Configuring the Installer's Maximum Memory Usage

The installer uses 1 GB of contiguous memory by default. If the installer is unable to run, you can configure the installer to use less memory.

Procedure

1. Go to the directory where the installer is located.
2. Create a new text file called VP-Windows-2.0.<xxxx.xxx>.vmoptions where <xxxx.xxx> is the build number of the installer and the platform.

   Note

   For more information on installation package file names, see *Installing Vulnerability Protection Manager on page 3-4*.

3. Edit the file by adding the line `-Xmx<xxxy>` where <xxxy> is the amount of memory allocated for the installer.

   Note

   <y> is the unit of measurement. Use `m` for MB and `g` for GB.

   For example, adding the line `-Xmx800m` configures the installer to use 800MB.

4. Save the file and launch the installer.

Configuring the Manager's Maximum Memory Usage

The Vulnerability Protection Manager default setting for heap memory usage is 4 GB. For enterprise environments with more managed endpoints, Trend Micro recommends changing the heap memory setting to at least 8 GB.

Procedure

1. Go to the Vulnerability Protection Manager directory.

   Note

   The default directory location is C:\Program Files\Trend Micro\Vulnerability Protection Manager.

2. Create a new file called Vulnerability Protection.vmoptions.

3. Edit the file by adding the line `-Xmx<xxxy>` where <xxxy> is the amount of memory allocated for the manager.

   Note

   <y> is the unit of measurement. Use `m` for MB and `g` for GB.

   For example, adding the line `-Xmx10g` configures the manager to use 10 GB.

4. Save the file and restart the Trend Micro Vulnerability Protection Manager service.

5. You can verify the new setting by going to **Administration** > **System Information** and in the **System Details** area, expand **Manager Node** > **Memory**. The Maximum Memory value should indicate the new configuration setting.

Appendix E

Performance Profiles

By default, new installations use the Aggressive Performance Profile which is optimized for a dedicated manager. If Vulnerability Protection Manager is installed on a system with other resource-intensive software it may be preferable to use the Standard Performance Profile.

The Performance Profile also controls the amount of agent-initiated connections that the manager accepts. The default settings for each of the Performance Profiles are designed to keep the number of accepted, delayed, and rejected heartbeats balanced.

Changing the Performance Profile

Procedure

1. On the Vulnerability Protection Manager dashboard, go to to **Administration** > **System Information**.
2. Under **System Activity**, click the **Manager Node** button.

   The **Properties** screen appears.
3. Select your preferred **Performance Profile** from the drop-down list.
4. Click **OK**.

Appendix F

SSL Authentication Certificate

The Vulnerability Protection Manager creates a 10-year self-signed certificate for the web browser-to-manager connections. If required, you can replace this certificate with a real certificate.

Once generated, import the certificate into the .keystore in the root of the Vulnerability Protection Manager installation directory and have an alias of tomcat. The manager uses the certificate in subsequent browser connections.

Creating an SSL Authentication Certificate

Procedure

1. Go to the Vulnerability Protection Manager installation directory located at C:\Program Files\Trend Micro\Vulnerability Protection Manager, and then create a new folder called Backupkeystore.

2. Copy the following files to the newly created Backupkeystore folder.

   - C:\Program Files\Trend Micro\Vulnerability Protection Manager\.keystore
   - C:\Program Files\Trend Micro\Vulnerability Protection Manager\configuration.properties
   - C:\Program Files\Trend Micro\Vulnerability Protection Manager\jre\lib\security\cacerts

3. Open the command prompt and go to the following location: C:\Program Files\Trend Micro\Vulnerability Protection Manager\jre\bin

4. Run the following command to create a self-signed certificate:

   ```
   C:\Program Files\Trend Micro\Vulnerability Protection
   Manager\jre\bin>keytool -genkey -alias tomcat -keyalg RSA -
   dname cn=vpmserver
   ```

Note

For more information on generating the certificate, see Thawte Tomcat Support.

-dname is the common name of the certificate your CA will sign. Some Certification Authorities (CAs) require a specific name to sign the Certificate Signing Request (CSR). Consult your CA Admin to see if you have that particular requirement.

dname example:

```
-dname "cn=<server name or IP
address>,ou=Name_of_your_Department, o=Company_Name,
L=Your_Location, ST=State_Name, C=Country”
```

To view the newly generated certificate, run this command:

```
C:\Program Files\Trend Micro\Vulnerability Protection
Manager\jre\bin>keytool -list -v
```

If you encounter issue *"keytool error: java.lang.Exception: Key pair not generated, alias <tomcat> already exists"* when generating a key, run the following command to delete any previous entries:

```
C:\Program Files\Trend Micro\Vulnerability Protection
Manager\jre\bin>keytool -delete
```

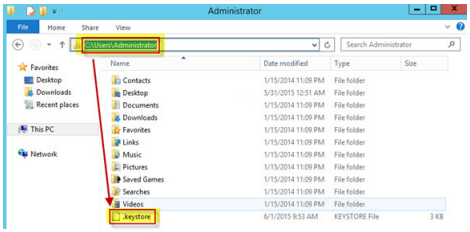
Then, type the alias name `tomcat` and the keystore password to delete.

5. Choose a password when prompted.

   A new keystore file is automatically created under the user home directory.

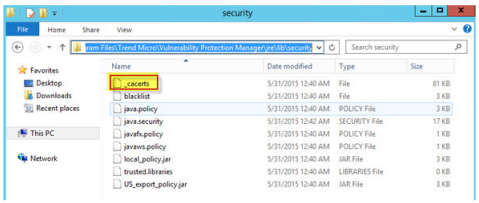
   To view the .keystore file, log on as Administrator and go to C:\Documents and Settings\Administrator.

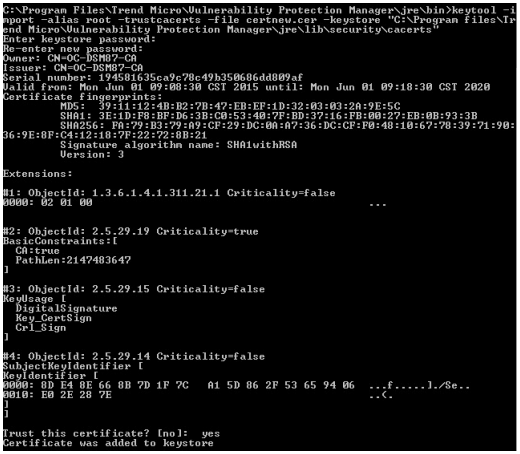
   For example:



6. To perform any of the following tasks, run the corresponding commands from a command line editor:

TABLE F-1. Available Commands

TASK	COMMAND AND SUB-STEPS
Create a CSR file for your CA to sign	**Important** Follow the CSR submission guidelines specified by your CA when submitting the CSR file. Go to https://technet.microsoft.com/en-us/library/cc770607.aspx as a reference. `C:\Program Files\Trend Micro\Vulnerability Protection Manager\jre\bin>keytool -certreq -keyalg RSA -alias tomcat -file certrequest.csr` a. Send the certrequest.csr to your CA to sign. In return you will get two files. One is a "CA certificate itself" (for example, cacert.crt or certnew.cer) and the second is the “certificate reply” (for example, certresponse.txt). b. Copy these files to C:\Program Files\Trend Micro\Vulnerability Protection Manager\jre\bin. c. Navigate to C:\Program Files\Trend Micro\Vulnerability Protection Manager\jre\lib\security\ folder, and then rename cacerts file to _cacerts. For example: 

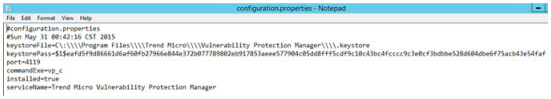
TASK	COMMAND AND SUB-STEPS
Import the CA cert in JAVA trusted keystore	`C:\Program Files\Trend Micro\Vulnerability Protection Manager\jre\bin>keytool -import -alias root -trustcacerts -file certnew.cer -keystore "C:\Program Files\Trend Micro\Vulnerability Protection Manager\jre\lib\security\cacerts""` For example: 
Import the CA cert in your keystore	`C:\Program Files\Trend Micro\Vulnerability Protection Manager\jre\bin>keytool -import -alias root -trustcacerts -file certnew.cer` For example: 

TASK	COMMAND AND SUB-STEPS
Import the certificate response to your keystore (optional)	`C:\Program Files\Trend Micro\Vulnerability Protection Manager\jre\bin>keytool -import -alias tomcat -file certresponse.txt` **Note** A prompt asks if you trust the certificate. Type `Yes`. Some CA will not provide any response file. Skip this command if there is no such response file. If you are signing using another CA, rename the file certnew.cer to cacert.crt using the above import command.

7. Copy the .keystore file from your user home directory C:\Documents and Settings \Administrator to C:\Program Files\ Trend Micro \Vulnerability Protection Manager\.

8. Open the configuration.properties file in folder C:\Program Files\Trend Micro \Vulnerability Protection Manager.

   For example:



9. Locate the string `keystorePass=<xxxx>` and replace `<xxxx>` with the password you previously supplied.

   Original:

   ```
   keystorePass=
   $1$eafd5f9d86661d6af60fb27966e844e372b077789802eb917853aeee
   577904c05dd8fff5cdf9c10c43bc4fcccc9c3e0cf3bdbbe528d604dbe6f
   75acb43e54faf
   ```

   Change to:

   ```
   keystorePass=Password
   ```

   After restarting the Vulnerability Protection Manager service, the RAW data will be encrypted following the original format.

10. Save and close the file.
11. Restart the Vulnerability Protection Manager service.
12. Connect to the Vulnerability Protection Manager with your browser to see the new SSL certificate signed by your CA.

For example:

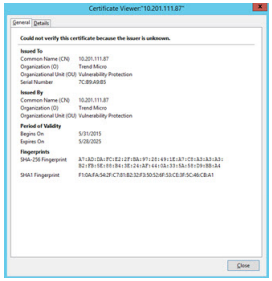


FIGURE F-1. Original SSL

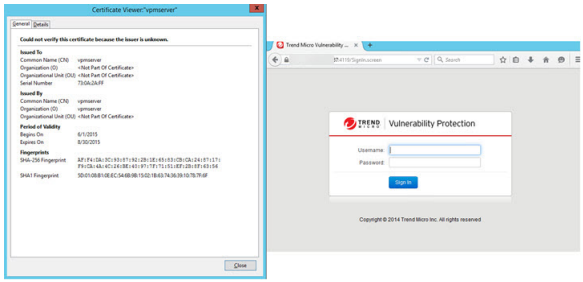


FIGURE F-2. Newly-created SSL

Appendix G

Frequently Asked Questions (FAQs)

This appendix answers various Frequently Asked Questions.

Frequently Asked Questions

Question	Answer
What are the benefits of converting from Intrusion Defense Firewall and migrating its settings to Vulnerability Protection?	Take advantage of the following features that Vulnerability Protection offers: • Support for IPv6, enhanced policy management • Standalone installation • Integration with Trend Micro™ Control Manager™ or Trend Micro™ Complete User Protection, which offers interconnected suite of security. For details about Complete User Protection, see http://www.trendmicro.com/us/business/complete-user-protection/index.html#compare-enterprise-suites. • Recommendation Scan performance improvement To get started, refer to *Intrusion Defense Firewall Migration Tool on page I-1* for instructions.
Where can I download the installer packages for Trend Micro Vulnerability Protection?	The Trend Micro Download Center: http://downloadcenter.trendmicro.com.
Where can I download the technical documents for Trend Micro Vulnerability Protection?	The Trend Micro Documentation Center: http://docs.trendmicro.com.
Why am I experiencing problems when installing two Vulnerability Protection Managers on the same machine?	Only one instance of the Vulnerability Protection Manager can be installed on any given machine.

QUESTION	ANSWER
What is the default user name and password to log on the Vulnerability Protection Manager console?	You are prompted for a user name and password during installation. The default user name for the manager console is “MasterAdmin”. There is no default password. The user name and password are both set during the installation. **Note** The user name is not case-sensitive.
How can I reset the manager console password?	Go to **Administration** > **User Management** > **Users**, right-click on the User and select **Set Password...**.
How can I unlock a locked out user?	On the manager console, go to **Administration** > **User Management** > **Users**, right-click on the User and select **Unlock User(s)**. To unlock a user from the manager, type the following from the Vulnerability Protection Manager's install directory in a command line editor: `vp_c -action unlockout -username <username> [-newpassword NEWPASSWORD]` <username> is the user name. Optionally, use `-newpassword` to set a new password for the user.
How can I use my domain account credentials when logging on to the manager console?	Go to **Administration** > **User Management** > **Users** and select **Synchronize with Directory**.
How can I mass-deploy the agents to the endpoints?	Organizations typically use existing enterprise software distribution systems such as Microsoft® System Center or Novell® ZENworks® to install agents.

Question	Answer
Can I uninstall the Vulnerability Protection Agent from the manager console?	No. You can deactivate the agent from the Vulnerability Protection Manager console, but you must uninstall the agent locally.
How do I deactivate the Vulnerability Protection Agent from the command line?	See “Manually Deactivate/Stop/Start the Agent” in the Administrator's Guide or online help.
How can I manually update the Vulnerability Protection Agent that has no connection with the Vulnerability Protection Manager?	Updating the agent is not possible when disconnected from the manager since the manager must send the security configuration details to the agent.

Appendix H

Troubleshooting

This chapter describes how to troubleshoot issues that may arise with Trend Micro Vulnerability Protection.

Troubleshooting

TABLE H-1. Vulnerability Protection Manager

ISSUE	SOLUTION
Unable to install the Vulnerability Protection Manager	During installation of the Vulnerability Protection Manager, the service may be unable to install properly if the **Services** screen is open. Close the services screen before installing Vulnerability Protection Manager. If the problem persists, restart the endpoint.
Unable to re-install the Vulnerability Protection Manager on the same endpoint after manually uninstalling Vulnerability Protection Manager and Microsoft SQL Server 2012 Service Pack 2.	This issue occurs because uninstalling Vulnerability Protection Manager and Microsoft SQL Server Express manually does not delete the Vulnerability Protection Manager database. To re-install the manager, users must perform the following steps: 1. Click **Cancel** to end the database installation. 2. Go to the <SQL Server>\MSSQL11.TMVUNPROTECT\MSSQL\DATA\ folder. **Note** <SQL Server> is the name of the user-defined Microsoft SQL Server Express database. 3. Delete vpm.mdf and vpm_log.ldf . 4. Restart the Vulnerability Protection Manager Setup Wizard.

TABLE H-2. Vulnerability Protection Agent

ISSUE	SOLUTION
Vulnerability Protection Agent is unable to start	There are several conditions that can prevent the vp_agent service from starting. The problem may be caused by: • Invalid credentials (not valid yet, corrupt, expired, or bad digital signature), • Unable to read the private key (corrupt or hardware was radically changed), or • The listening port already in use. In cases where the Vulnerability Protection Agent is unable to start, it is unable to report to the Vulnerability Protection Manager, so it writes to the Windows Event Log. You should check the Windows Event log to diagnose the problem.
Vulnerability Protection Agent is installed but the user interface displays blank fields	If the manager URL, manager certificate name, and manager certificate fingerprint fields are blank, the agent has not been activated. These fields are blank until the agent has been activated by Vulnerability Protection Manager. Locate the endpoint in the Vulnerability Protection Manager's Computers list, right-click on the endpoint name and select **Actions** > **Activate/ Reactivate**.

Issue	Solution
Getting the following error message in an "Agent Activate Failed" system event: "A client error occurred in the VPM to VPA protocol: HTTP client error received: certificate is not yet valid"	The clock on a Vulnerability Protection Agent machine must be synchronized with the Vulnerability Protection Manager to within 24 hours. If the Vulnerability Protection Agent clock is behind the Vulnerability Protection Manager clock then an agent activatation operation will be unsuccessful because the certificate generated for the manager by the Vulnerability Protection Manager is not yet be valid.

Appendix I

Intrusion Defense Firewall Migration Tool

Learn how to use Intrusion Defense Firewall Migration Tool in the following topics:

- *About Intrusion Defense Firewall Migration Tool on page I-2*
- *System Requirements on page I-2*
- *Using the Migration Tool on page I-5*
- *Converting Intrusion Defense Firewall Clients on page I-13*
- *Troubleshooting on page I-15*

About Intrusion Defense Firewall Migration Tool

Trend Micro™ Intrusion Defense Firewall Migration Tool, also known as *IDF Migration Support Wizard* or *migration tool*, is a tool that allows Intrusion Defense Firewall users to convert Intrusion Defense Firewall and migrate its server settings to Trend Micro™ Vulnerability Protection.

For information about the benefits of Trend Micro™ Vulnerability Protection, see *About Vulnerability Protection on page 1-2*.

System Requirements

Before running Intrusion Defense Firewall Migration Tool, make sure that target servers meet the following system requirements:

TABLE I-1. System Requirements

HARDWARE/SOFTWARE	SPECIFICATION
OfficeScan server version	10.6, 11, or 11 Service Pack 1
Intrusion Defense Firewall version	The target server should be running any of the following supported versions: • 1.5.0.1229 • 1.5.2331 • 1.5.2373 **Important** Intrusion Defense Firewall 1.5.1210 cannot be used to perform migration.

HARDWARE/SOFTWARE	SPECIFICATION
Operating system	The target server should be running any of the following supported operating systems: • Microsoft Windows Server™ 2012 R2 (64-bit) • Microsoft Windows Server™ 2012 (64-bit) • Microsoft Windows Server™ 2008 R2 (64-bit) • Microsoft Windows Server™ 2008 (32- and 64-bit) • Microsoft Windows Server™ 2003 SP2 or 2003 R2 SP2 (32- and 64-bit) **Note** For Windows Server 2003 SP2 or 2003 R2 SP2, the migration tool will use Microsoft SQL Server 2008 R2 Express.

HARDWARE/SOFTWARE	SPECIFICATION
Database	If Intrusion Defense Firewall uses a remote database, you must manually configure a database following the steps available in the Intrusion Defense Firewall *Administrator's Guide* pages 11-3 to 11-5. For details, see http://docs.trendmicro.com/all/ent/idf/v1.5/en-us/idf_1.5_ag.pdf. **Note** • For servers running Windows Server 2003, you can opt to choose either Microsoft™ SQL Server™ Express 2008 to install a built-in database or allow the migration tool to port Intrusion Defense Firewall settings into the new database instance for Vulnerability Protection Manager. • For servers running Windows Server 2008 or Windows Server 2008 R2, you can opt to use SQL Server 2008 R2 or update Windows to the latest service pack before running the migration tool. • Microsoft SQL Server 2012 Service Pack 2 Express cannot be installed on hosts running Microsoft Windows Server 2003, Windows Server 2008 (RTM), Windows Server 2008 SP2, or Windows Server 2008 R2 (RTM). You can manually configure a database following the steps available in the Intrusion Defense Firewall Administrator's Guide pages 11-3, section *Migrating to a Larger Database*. Alternatively, manually change the Microsoft SQL Server Express 2012 installer to Microsoft SQL Server Express 2008 installer, and then run the IDF Migration Tool. Follow these steps: 1. Download Microsoft SQL Server Express R2 Service Pack 2, version 10.50.4000.0 from the Microsoft website. 2. Rename the SQL Server Express installer as SQLEXPR_x86_ENU.exe for 32-bit platform or SQLEXPR_x64_ENU.exe for 64-bit platform. 3. Copy installer that you renamed in *Step b.* to the IDF Migration Tool directory to replace the original SQL Server installer.

Using the Migration Tool

Using the Intrusion Defense Firewall Migration Tool allows you to complete the following tasks automatically:

- Uninstall Intrusion Defense Firewall
- Install the Vulnerability Protection Manager plug-in and agent
- Import Intrusion Defense Firewall settings into the new Vulnerability Protection database (VUNprotect)

  The migration tool installs a new Microsoft™ SQL Server™ 2012 instance, VUNprotect, if the original Intrusion Defense Firewall server uses a built-in database.

Important

Back up your Intrusion Defense Firewall to help restore your original settings in case an issue occurs during migration.

To use the migration tool:

Procedure

1. Download the corresponding package and extract to a directory on your Intrusion Defense Firewall server.
   - 32-bit: IDFMigrateWizard-x.x.xxxx.i386.zip
   - 64-bit: IDFMigrateWizard-x.x.xxxx.x86_64.zip
2. Navigate to the directory where you extracted the tool package, and then double-click IdfMigrateWizard.exe.

The **Welcome** screen appears.

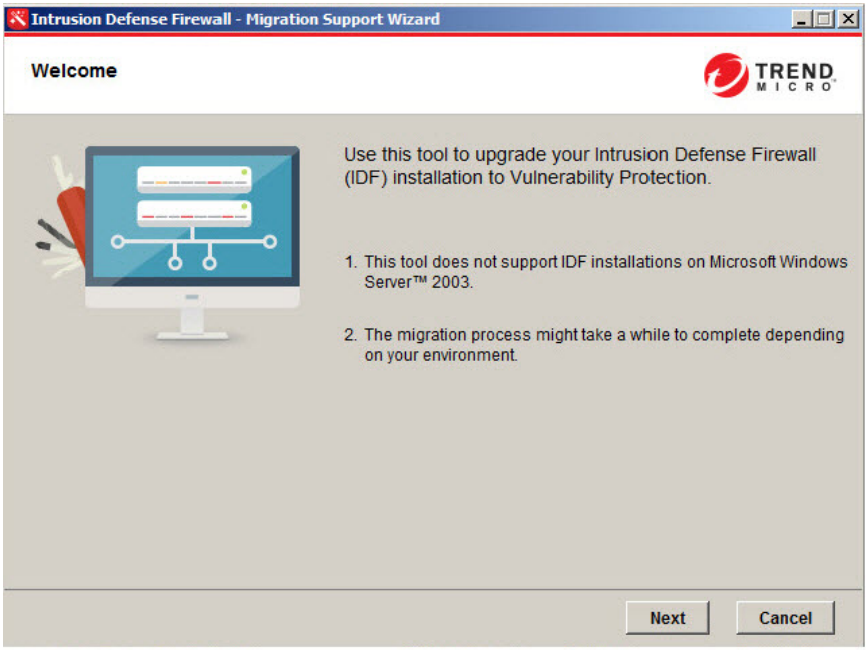


FIGURE I-1. Intrusion Defense Firewall Migration Tool Welcome Screen

3. On the **Welcome** screen, click **Next**.

The **Installation Path** screen appears.

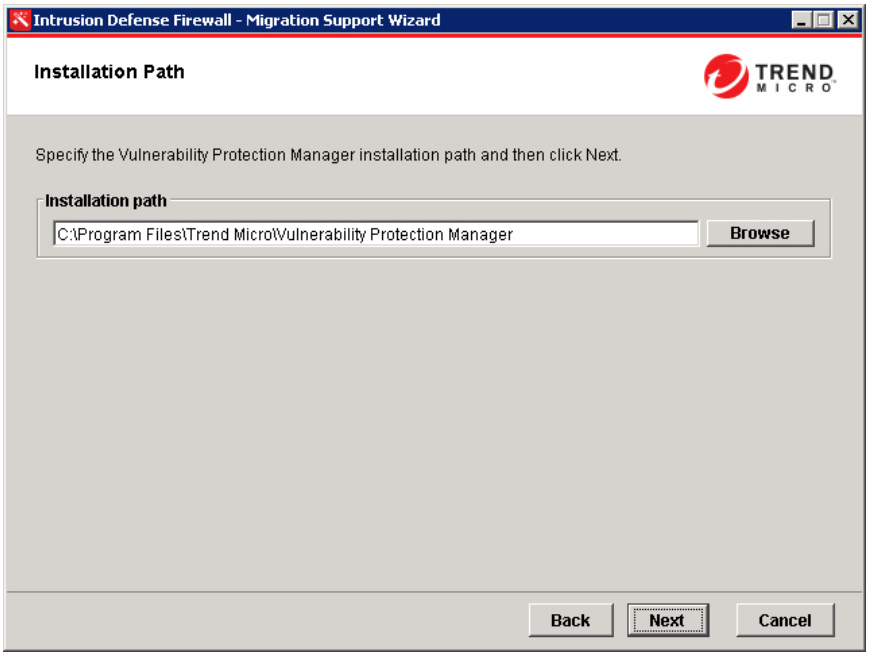


FIGURE I-2. Intrusion Defense Firewall Migration Tool Installation Path Screen

4. On the **Installation Path** screen, browse to locate a new installation path or accept the default path, and then click **Next**.

The **Database** screen appears.

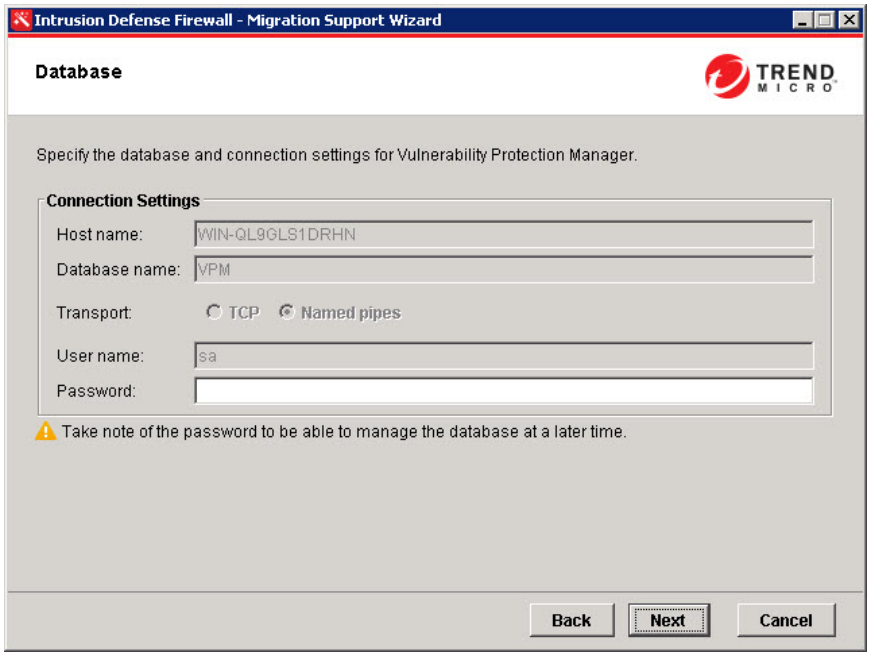


FIGURE I-3. Intrusion Defense Firewall Migration Tool Database Screen

5. On the **Database** screen, type the **password** for the *sa* account.

   The migration tool determines if a built-in/local or remote SQL server is used in conjunction with your Intrusion Defense Firewall setup. If a built-in database is used, the **host name** value set under **Connection Settings** is name of the local server. Otherwise, the **host name** value is an IP address corresponding to the remote SQL server.

Tip

Schedule regular database backups using **Scheduled Task Wizard** of the Intrusion Defense Firewall Server Plug-in web-based interface through the OfficeScan Web console. Access the IDF Server Plug-in interface through the OfficeScan console.

Go to **System** > **Scheduled Tasks** and click **New** in the toolbar to start the **Scheduled Task Wizard**. Select **Backup** from the drop-down list and then use the next two screens to specify how often you want a backup to be performed. When you are prompted for the output location, specify the SQL Server backup directory which is typically located at C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Backup \. The next step of the Wizard will prompt you to name the new Scheduled Task and give you the option to run task after closing the **Scheduled Task Wizard**.

The **Administrator Account** screen appears.

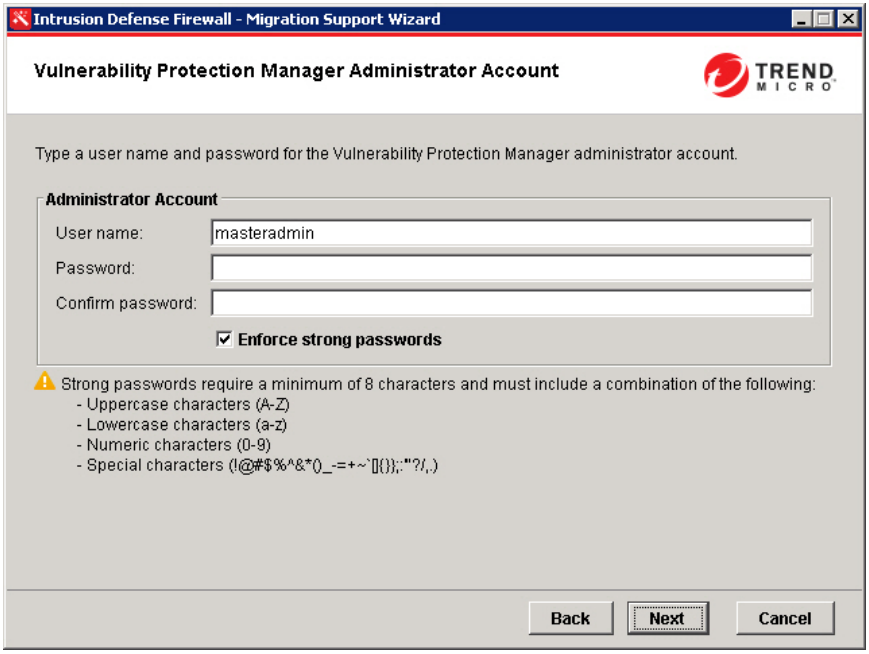


FIGURE I-4. Intrusion Defense Firewall Migration Tool Administrator Account Screen

6. On the **Administrator Account** screen, you may opt to change the default administrator **user name** and set the **password** that you will use to access the Vulnerability Protection Manager web console.

Tip

To help ensure secure access, enforce a strong password.

The migration tool creates a backup of the Intrusion Defense Firewall database, creates a new Vulnerability Protection database that will be used to import and save Intrusion Defense Firewall settings, and then uninstalls the plug-in.

The migration tool starts the Vulnerability Protection installation, as shown by the following screen:

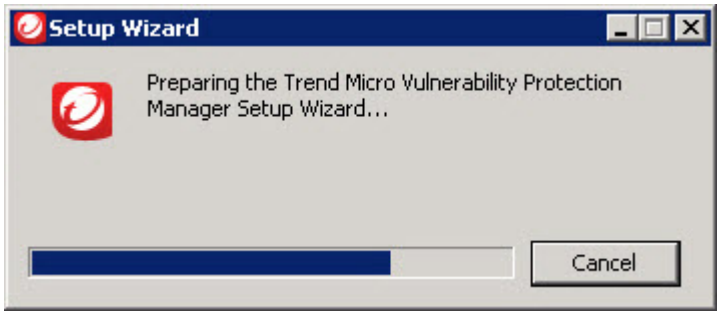


FIGURE I-5. Launching the Vulnerability Protection Installation

7. Install Vulnerability Protection Manager and agent on the server.

Follow the on-screen instructions.

Note

A Vulnerability Protection agent, also known as a relay-enabled agent, must be installed on same host as Vulnerability Protection Manager. Vulnerability Protection needs an agent to download and distribute updates.

The steps involve when installing Vulnerability Protection when migrating from Intrusion Defense Firewall are minimal and straightforward . You are expected to

accept the license agreement, install a VP agent, and review the installation summary. Compared to the normal VP setup, steps that prompt you to set the installation path, database connection, and product license are omitted.

Refer to the applicable steps listed in *Installing Vulnerability Protection Manager on page 3-4* and *Installing Vulnerability Protection Agent on page 3-17*.

Vulnerability Protection is installed successfully. A screen similar to the following appears:

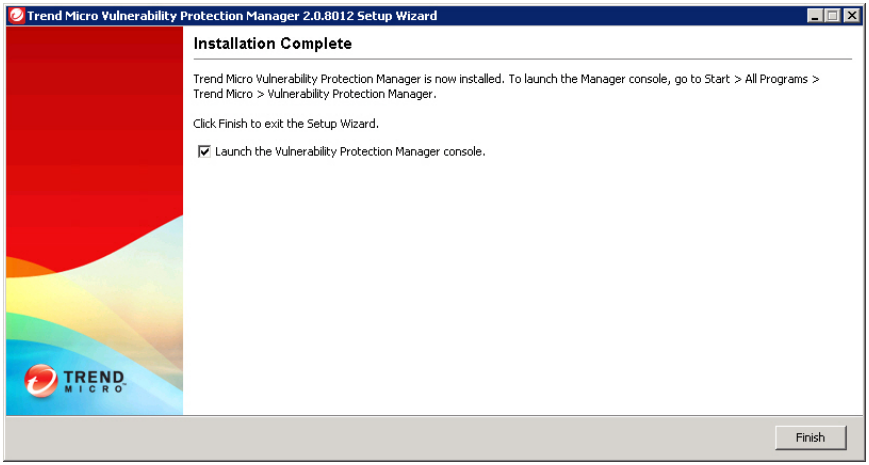


FIGURE I-6. Vulnerability Protection Successfully Installed

8. Click Finish.

A screen similar to the following appears:

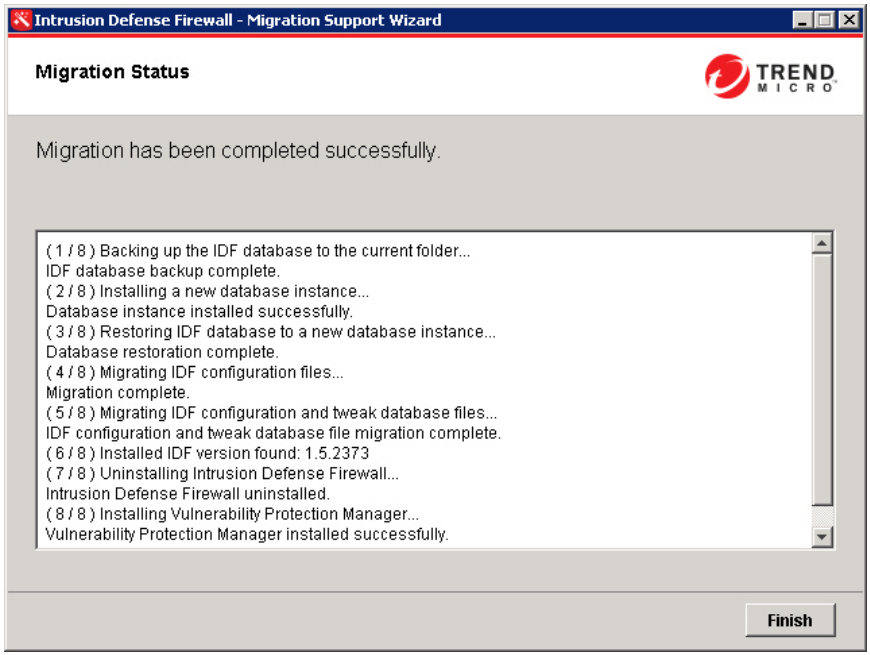


FIGURE I-7. Migration Status - Successfully Completed

9. On the **Migration Status** screen, click **Finish**.

   The migration tool saves installation logs (for example, install.log, log_migration_process.txt, and other related files) in the working directory where you run IdfMigrateWizard.exe.

Intrusion Defense Firewall settings are imported into the new Vulnerability Protection database. Vulnerability Protection Manager and agent are installed in place of Intrusion

Defense Firewall. The following example shows an OfficeScan installation with a Vulnerability Protection plug-in program:

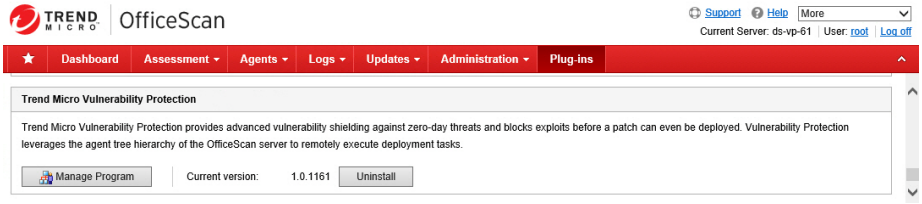


FIGURE I-8. Vulnerability Protection from the OfficeScan Web Console

Converting Intrusion Defense Firewall Clients

Convert existing IDF clients to become Vulnerability Protection agents. Otherwise, the IDF plug-in program will be uninstalled automatically if the OfficeScan agent is uninstalled. As a result, you will not be able to manage such clients through the OfficeScan console and avail of the features offered in the latest release.

Procedure

1. Log on to the Vulnerability Protection Manager web console using the *Administrator* account, which is previously specified when running the migration tool.
2. Import the upgrade installer for Vulnerability Protection agent.
   a. Go to the **Administration** tab.
   b. In the tree view of the left panel, go to **Updates** > **Software** > **Local**.

      The **Local Software** page appears.
   c. Click **Import...** to display the **Import Software** dialog.
   d. Click **Browse...** to locate the installer for Vulnerability Protection agent listed below, and then click **Next**.
      - 32-bit: VPAgent-Windows-2.0.2-2409.i386.zip

- 64-bit: VPAgent-Windows-2.0.2-2409.x86_64.zip

e. Click **Start** and wait for the software package import process to complete.

3. Upgrade the agent.

a. Go to the **Computers** tab.

b. Select any number of computers in the list for upgrade.

c. Right-click, and then select **Actions** > **Upgrade Agent Software...**.

What to do next

Note

If the conversion to Vulnerability Protection is unsuccessful, it is possible that the IDF uninstallation process did not run properly.

As a workaround, perform the following steps to completely uninstall IDF from any of the target computers:

1. Open the command prompt by clicking the **Start** button and typing `Command Prompt` in the search box.

2. Navigate to the IDF installation path by issuing the `cd` command (for example, `cd C:\Program Files (X86)\Trend Micro\IDF Client`)

3. Uninstall IDF by issuing the following command:

```
rundll32 IdfClientAgent.dll,Uninstall
```

After uninstalling IDF successfully, the IDF folder is completely removed. Use the Vulnerability Protection Agent installer (Agent-Core-Windows-9.5.2-2409.x86_64.msi or Agent-Core-Windows-9.5.2-2409.i386.msi) to manually install Vulnerability Protection Agent.

After installation, log on to the Vulnerability Protection Manager web console to add and activate the agent. For details, see *Activating the Vulnerability Protection Agent on page 5-6*.

Troubleshooting

Learn the possible reasons and available workarounds for the following issues:

- *Error "Unable to locate the database backup file" on page I-15*
- *Error "Unable to install a new database instance" on page I-16*
- *Error "Unable to uninstall Intrusion Defense Firewall" on page I-16*
- *Error "Unable to configure Vulnerability Protection. Unable to access the database. Installation cannot continue." on page I-17*
- *Error "Unable to install Microsoft SQL Express 2012 on hosts running Microsoft Server 2003, Microsoft Server 2008 (RTM), Microsoft Server 2008 R2 (RTM)…" on page I-17*
- *Restoring the Intrusion Defense Firewall Plug-in After an Unsuccessful Migration on page I-18*

Error "Unable to locate the database backup file"

This error message appears if the Intrusion Defense Firewall server is using a built-in database. The Intrusion Defense Firewall Migration Tool automatically generates a backup of the Intrusion Defense Firewall database (IDFBackup.bak) in the default installation directory (for example, C:\Program Files\Trend Micro\OfficeScan\Addon \Intrusion Defense Firewall).

If this action is unsuccessful, perform the following workaround:

1. Back up the Intrusion Defense Firewall database manually.

   For details, see the Intrusion Defense Firewall *Administrator's Guide* pages 11-11 to 11-12. (http://docs.trendmicro.com/all/ent/idf/v1.5/en-us/idf_1.5_ag.pdf).

2. Copy the backup file (for example, C:\dbbackup\IDFBackup.bak) to the target server where the migration tool is going to be executed.

3. Run the migration tool again.

Error "Unable to install a new database instance"

This error message appears if any of the conditions below is triggered:

- The SQL server instance installation process is unexpectedly terminated.
- An instance of the new VP database instance, Vunprotect, is created (from a previous migration or plug-in installation).

Consider the following workaround:

1. Check whether Vunprotect exists. If so, remove the instance through the SQL Server.
    - Windows Server 2003:

      Go to the **Control Panel** > **Add or Remove Programs**, and then select **Microsoft SQL Server 2008 R2 (64-bit)**. Click **Remove** twice.
    - Windows Server 2008 or later:

      Go to the **Control Panel** > **Program and Features**, and then select **Microsoft SQL Server 2012 (64-bit)**. Click **Uninstall/Change**, and then click **Remove**.
2. Verify that the instance folder is completed removed. Otherwise, delete the folder manually.
3. Run the migration tool again.

Error "Unable to uninstall Intrusion Defense Firewall"

This error message appears when any of the conditions below is triggered:

- The Intrusion Defense Firewall uninstall process is terminated unexpectedly.
- The Intrusion Defense Firewall settings and saved data are not deleted completely.

Perform the following workaround:

1. Go to the Intrusion Defense Firewall installation directory (for example, C:\Program Files\Trend Micro\OfficeScan\Addon\Intrusion Defense Firewall).

If idfSeveruninstall.exe exists, double-click to uninstall Intrusion Defense Firewall automatically. Otherwise, delete all files and folders manually.

2. Open the command line (cmd.exe), and then execute the following commands:

```
cd C:\Program Files\Trend Micro\OfficeScan\Addon\Intrusion Defense Firewall
VP-Windows-2.0.xxxx.x64.exe  -varfile  migration.properties
```

Note

For Japanese version, use the following command:

```
VP-Windows-2.0.xxxx.x64.exe  -Dinstall4j.language=ja  -varfile migration.properties
```

Error “Unable to configure Vulnerability Protection. Unable to access the database. Installation cannot continue.”

This error message appears when Intrusion Defense Firewall uses a remote database. Make sure that connection to the remote IDF database is normal before running the migration tool.

Error “Unable to install Microsoft SQL Express 2012 on hosts running Microsoft Server 2003, Microsoft Server 2008 (RTM), Microsoft Server 2008 R2 (RTM)…”

Depending on the operating system running on the target server, consider one of the following workarounds:

- Windows 2003:

  Use SQLEXPR_X64_EU.exe or SQLEXPR_X86_EU.exe when installing Microsoft SQL Server 2008 Express.

- Windows Server 2008 or Windows Server 2008 R2:

Upgrade your operating system to the latest hot fix. Alternatively, use SQLEXPR_X64_EU.exe or SQLEXPR_X86_EU.exe when installing Microsoft SQL Server 2008 Express.

Restoring the Intrusion Defense Firewall Plug-in After an Unsuccessful Migration

Procedure

1. Reinstall Intrusion Defense Firewall.
2. Stop the *Intrusion Defense Firewall* service from the Services Microsoft Management Console snap-in.
3. Copy the database backup file to SQL Server backup directory (for example, C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Backup\).
4. Run IDFRestore.bat from the Intrusion Defense Firewall root directory (typically C:\Program Files\Trend Micro\OfficeScan\Addon\Intrusion Defense Firewall).
5. Start the *Intrusion Defense Firewall* service.

Appendix J

Vulnerability Protection Deployment Tool

Learn how to use Vulnerability Protection Deployment Tool in the following topics:

- *About Vulnerability Protection Deployment Tool on page J-2*
- *System Requirements on page I-2*
- *Installing Vulnerability Protection Deployment Tool on page J-3*
- *Vulnerability Protection Deployment Tool Tasks on page J-5*
- *Configuring Server Settings on page J-6*
- *Working with Logs on page J-8*
- *Troubleshooting on page J-9*

About Vulnerability Protection Deployment Tool

Trend Micro™ Vulnerability Protection provides advanced vulnerability shielding against zero-day threats and blocks exploits before a patch can even be deployed.

Vulnerability Protection Deployment Tool provides the following functionalities:

- Serves as a plug-in program that synchronizes agent information between OfficeScan, Vulnerability Protection Manager, and Vulnerability Protection agents
- Deploys commands to managed endpoints and records events viewable as system logs

Vulnerability Protection Deployment Tool leverages the agent tree hierarchy of the OfficeScan server to remotely execute deployment tasks.

System Requirements

Before installing Vulnerability Protection Deployment Tool, make sure that target servers meet the following system requirements:

TABLE J-1. System Requirements

HARDWARE/SOFTWARE	SPECIFICATION
OfficeScan server version	10.6, 11, or 11 Service Pack 1
Vulnerability Protection Manager version	2.0 or 2.0 Service Pack 1
Plug-in Manager version	2.0 or later

For detailed specifications related to Vulnerability Protection requirements, see *Preparing for Installation on page 2-1*.

Installing Vulnerability Protection Deployment Tool

Procedure

1. Log on to the OfficeScan web console, and then go to **Plug-ins** (OfficeScan 11 or later) or **Plug-in Manager** (OfficeScan 10.6).
2. On the **Plug-ins** or **Plug-in Manager** screen, go to **Trend Micro Vulnerability Protection Deployment Tool** and then click **Download**.
3. After download completes, click **Install** .

   A prompt similar to the following appears:

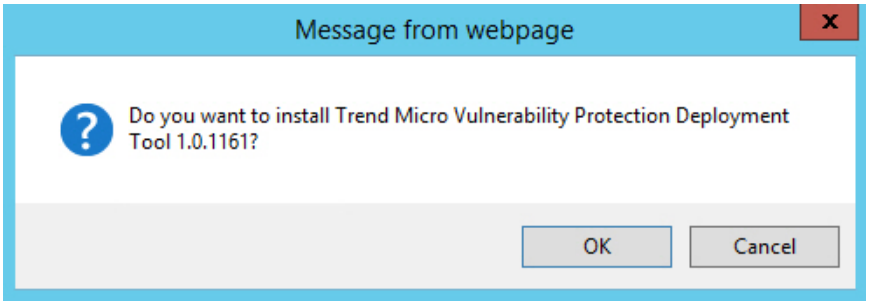


FIGURE J-1. Installation Prompt

4. Click **OK** to install the deployment tool.

The License Agreement screen appears.

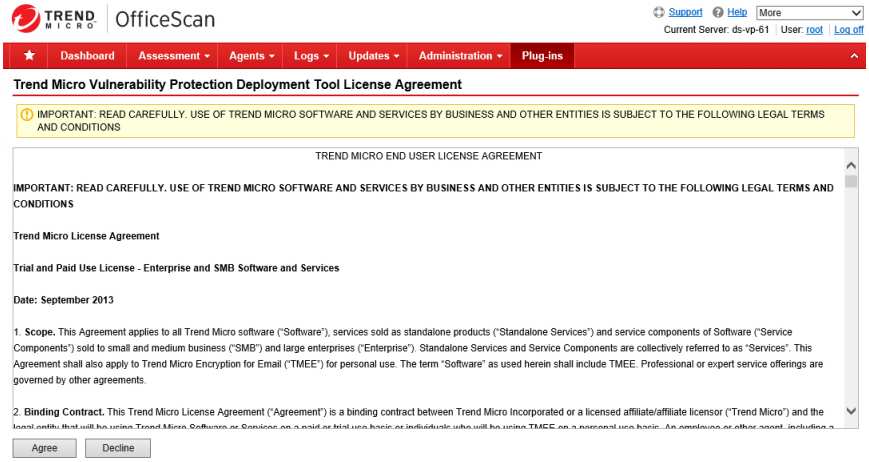


FIGURE J-2. Vulnerability Protection Deployment Tool License Agreement Screen

5. Click **Agree**.

After a successful installation, a screen similar to the following appears:

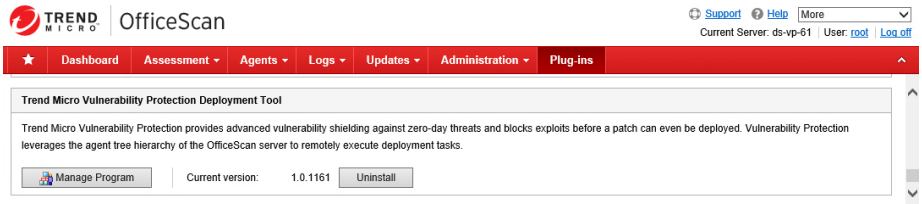


FIGURE J-3. Vulnerability Protection Deployment Tool Manage Program Screen

Vulnerability Protection Deployment Tool Tasks

The **Agent Management** screen accessible from **OfficeScan console** > **Plug-ins** > **Vulnerability Protection Deployment Tool** allows you to issue the following tasks:

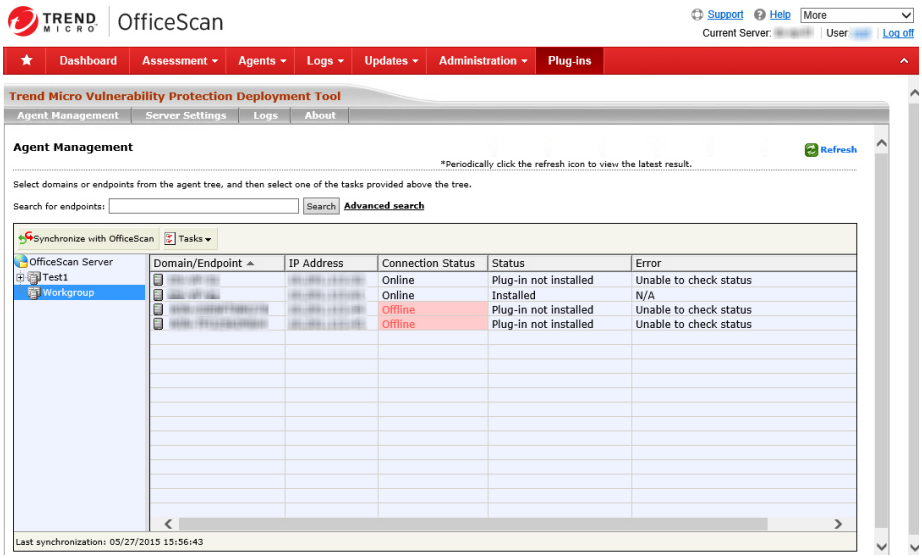


FIGURE J-4. Agent Management Screen

- **Install Agent**

  Installs the Vulnerability Protection agent on a target endpoint.

- **Uninstall Agent**

  Removes the Vulnerability Protection agent from a target endpoint.

- **Activate Agent**

  Activates the connection between Vulnerability Protection Manager, Agent, and OfficeScan. When activated, VPM communicates with an agent by sending it a

unique "fingerprint". The agent will then use this fingerprint to uniquely identify the Vulnerability Protection Manager and will not accept instructions from any other VP Manager servers that might try to contact it.

- **Check Status**

  Determines whether an endpoint is online or offline. See *Troubleshooting on page J-9* for errors and possible workarounds.

Configuring Server Settings

Use the **Server Settings** screen to configure the connection details used to establish communication to and from a Vulnerability Protection server and its agents.

Procedure

1. On the OfficeScan console, go to the **Plug-ins** screen, and click **Manage Program**.

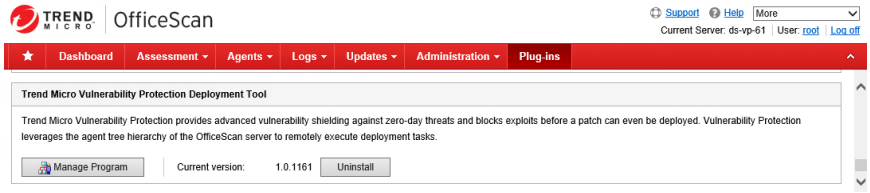


FIGURE J-5. Manage Program

   The **Agent Management** screen opens.

2. Click **Server Settings**.

The **Server Settings** screen appears.

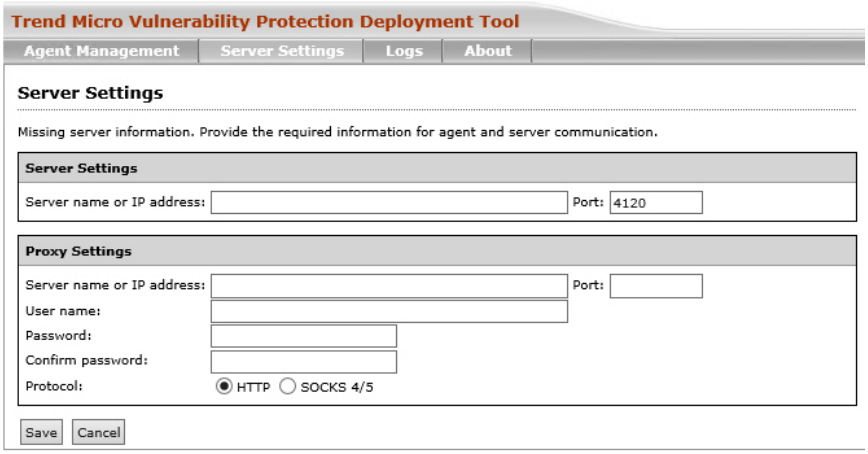


FIGURE J-6. Server Settings Screen

3. Set the settings that OfficeScan and Plug-in Manager will use to communicate with Vulnerability Protection server.

   - **Server name** or **IP address** of the server hosting Vulnerability Protection Manager
   - **Port number** used by agents to communicate with manager

4. Set the proxy server settings if one is required in your network:

   - **Server name** or **IP address** of the proxy server
   - **User name** and **password** combination used to authenticate with the proxy server
   - **HTTP** or **SOCKS 4/5 protocol**

5. Click **Save**.

OfficeScan and related services should be able to communicate with the registered Vulnerability Protection server and its client. Otherwise, make sure that the settings configured are correct and normal network connection exists.

Working with Logs

Vulnerability Protection Deployment Tool maintains logs that provide summaries of events related to the issued tasks.

Procedure

- View logs

  View logs to gather information about the status of all issued commands.

  On the OfficeScan console, go to the Vulnerability Protection Deployment Tool **Agent Management** screen, and then click **Logs**. A result similar to the following appears:

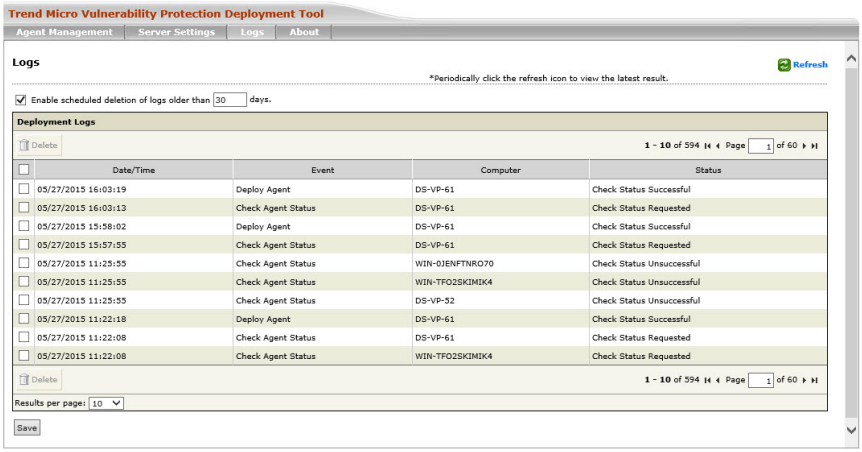
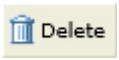


FIGURE J-7. Logs Screen

- Delete logs

Manually delete logs on a regular basis to manage hard disk space.

1. On the **Logs** screen, select multiple logs to delete, and then click 

.
2. Click **OK** to confirm.

Deleted logs are permanently removed from the storage.

Troubleshooting

Learn the possible reasons and available workarounds for the following issues:

- *Errors when Deploying the "Install Agent" Task on page J-9*
- *Errors when Deploying the Uninstall Agent Task on page J-11*
- *Unable to Check Status when Deploying the Activate Agent or Check Status Task on page J-12*

Errors when Deploying the Install Agent Task

The following compilation resulted from having endpoints displayed on the **Agent Management** screen as having an *Online* **Connection Status**. Depending on the endpoint status, there are various reasons and possible workarounds in place.

TABLE J-2. Install Agent Errors

ENDPOINT STATUS	ERROR / POSSIBLE REASON	POSSIBLE WORKAROUND
Not activated	Wrong address used by the VPM server or agent-initiated activation is enabled **Note** For details about agent-initiated activation, refer to the Vulnerability Protection *Administrator's Guide*.	Issue **Activate Agent** from the OfficeScan console **Agent Management** screen. This changes the status to *Installed* if the agent is activated successfully. Issue the *Reactivate* command from the Vulnerability Protection Manager console **Computer** screen, and then go back to the OfficeScan console **Agent Management** screen to issue **Check Status**.
Vulnerability Protection agent plug-in not installed	Installation timeout	Check if the agent status via the OfficeScan console is *Online*. If so, click **Install Agent** again to try and refresh the status. Otherwise, check for reasons why the agent is offline. Refer to the OfficeScan documentation for details. If clicking **Install Agent** results to the same error, check if the Vulnerability Protection plug-in program is installed. If so, remove the program by running the following command: `C:\Program Files (x86)\TrendMicro\VPPLSClient\Regutil.exe -uc C:\Program Files (x86)\TrendMicro\VPPLSClient\Regutil.exe`
Vulnerability Protection agent plug-in not installed	The Deep Security or Intrusion Defense Firewall agent program is installed	1. Check which agent program is installed on the endpoint. 2. Uninstall Deep Security agent or Intrusion Defense Firewall agent. 3. Issue **Install Agent** to install Vulnerability Protection agent.

Endpoint Status	Error / Possible Reason	Possible Workaround
Vulnerability Protection agent plug-in not installed	Unable to unregister Vulnerability Protection agent	Issue **Install Agent** from the OfficeScan console. If the issue persists, contact your support provider for assistance.
Not activated	Agent activated by another server	Make sure that both Plug-in Manager and Vulnerability Protection Manager servers apply the same settings. For example, if an IP address is set as the server address in Vulnerability Protection Manager, the same should be applied in Plug-in Manager.
Not activated	Agent-initiated activation is disabled or incorrect server address	Check if agent-initiated activation is disabled. If so, enable this option via the Vulnerability Protection Manager console. Then, issue **Activate Agent** again.

Errors when Deploying the Uninstall Agent Task

The following compilation resulted from having endpoints that meet all these conditions:

- The **Agent Management** screen displays such endpoints with an *Online* **Connection Status**.
- The Vulnerability Protection agent program is installed on the endpoints.

Table J-3. Uninstall Agent Errors

Error / Possible Reason	Possible Workaround
Self-protect enabled	Change the endpoint setting of “Agent Self Protection” in Vulnerability Protection Manager console from **Yes** to **No**, then issue **Uninstall Agent**from the OfficeScan **Agent Management** screen.

Error / Possible Reason	Possible Workaround
Timeout during uninstall	Verify that the connection between the server and agent is normal. Then try to uninstall. If the issue persist, contact your support provider.

Unable to Check Status when Deploying the Activate Agent or Check Status Task

If you are unable to check status even if the connection status of an endpoint on the Agent Management screen is *Online* and the Vulnerability Protection agent program is installed, try any of the following workarounds:

- Check if the agent is installed and running properly. If not, issue **Install Agent**. The agent should be installed.
- Verify that the connection between the server and agent is normal.
- Contact your support provider if the issue persists.

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: APEM26977/150527