TREND MICRO™

2.0 Vulnerability Protection

Installation Guide

Advanced Vulnerability Shielding for Endpoints

Endpoint Security

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

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

Document Part No. APEM26305_140210

Release Date: April 2014

Document Version No.: 1.0

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

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 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

Chapter 1: Introduction

Chapter 2: Preparing for Installation

Chapter 3: Installation

Appendix A: Ports Used by Trend Micro Vulnerability Protection

Appendix B: Configuring the Settings.Properties File

Appendix C: Installation Output

Appendix D: Trend Micro Vulnerability Protection Memory Usage

Appendix E: Performance Profiles

Appendix F: SSL Authentication Certificate

Appendix G: Frequently Asked Questions (FAQs)

Appendix H: Troubleshooting

Index

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

To help you locate and interpret information easily, the Trend Micro Vulnerability Protection documentation uses the following conventions:

Table 2. Document Conventions

Convention	Description
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and tasks
Italics	References to other documentation or new technology components
<Text>	Indicates that the text inside the angle brackets should be replaced by actual data. For example, `C:\Program Files\<file_name>` can be `C:\Program Files\sample.jpg`.
Note	Provides configuration notes or recommendations
Tip	Provides best practice information and Trend Micro recommendations
WARNING!	Provides warnings about activities that may harm endpoints on your network

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 • Automatically shields newly discovered vulnerabilities within hours through a rapid deployment of rules to thousands of 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

The following table lists the requirements for the installation.

Table 2-1. Installation Requirements

Installation Information	Description
Installer packages	Place the installer 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) **Note** Trend Micro recommends allocating 13 GB of disk space when installing Vulnerability Protection Manager with the embedded Microsoft SQL Server Express database.
Operating system	• Microsoft Windows 2012 R2 (64-bit) • Microsoft Windows 2012 (64-bit) • Windows Server 2008 R2 (64-bit) • Windows Server 2008 (32-bit and 64-bit) • Windows 2003 Server SP2 (32-bit and 64-bit) • Windows 2003 Server R2 SP2 (32-bit and 64-bit)

Hardware/Software	**Specifications**
Database	• Oracle 11g • Oracle 10g • Microsoft SQL Server 2012 (All Service Packs) • Microsoft SQL Server 2008 (All Service Packs) • Microsoft SQL Express 2008 R2 SP2 embedded **Tip** Installing SQL Express 2008 R2 SP2 requires the .NET Framework 2.0 SP2 and Windows installer 4.5. On Windows 2008 and above, Trend Micro recommends using .NET Framework 3.5 SP1.
Web browser	• Firefox 12+ • Internet Explorer 11.x • Internet Explorer 10.x • Internet Explorer 9.x • Chrome 20+ **Note** Cookies must be enabled on all browsers.

Table 2-3. Vulnerability Protection Agent System Requirements

Hardware/Software	**Specifications**
Memory	128 MB
Disk space	500 MB

HARDWARE/SOFTWARE	SPECIFICATIONS
Operating system	• Windows 8.1 (32-bit and 64-bit) • Windows Server 2012 R2 (64-bit) • Windows 8 (32-bit and 64-bit) • Windows Server 2012 (64-bit) • Windows 7 (32-bit and 64-bit) • Windows Server 2008 R2 (64-bit) • Windows Server 2008 (32-bit and 64-bit) • Windows Vista (32-bit and 64-bit) • Windows Server 2003 SP1 (32-bit and 64-bit) patched with "Windows Server 2003 Scalable Networking Pack" • Windows Server 2003 SP2 (32-bit and 64-bit) • Windows Server 2003 R2 SP2 (32-bit and 64-bit) • Windows XP (32-bit and 64-bit)

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

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 3-14*.

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.

The following table lists the recommended databases for enterprise deployments.

Table 3-1. Databases for Enterprise Deployment

Database	Version
Microsoft™ SQL Server	• 2012 • 2008 R2 • 2008
Microsoft™ SQL Server Express™	• 2008 R2 SP2
Oracle Database	• 11g • 10g

Tip

If you only plan to test or evaluate Trend Micro Vulnerability Protection in a small-scale environment, you may also use the embedded Apache Derby database.

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

Procedure

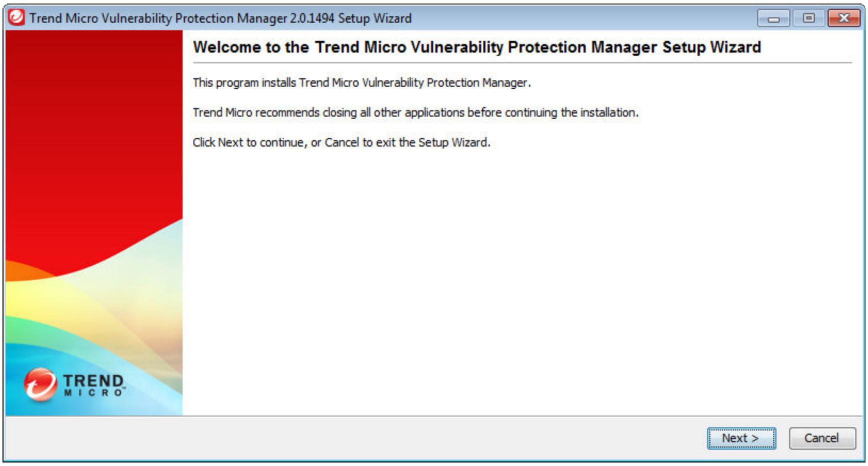
1. Run any of the following installation packages:

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 for 32-bit operating systems
`VP-Windows-2.0.<XXXX>.x64-sqlexp`	Installer embedded with Microsoft SQL Server Express for 64-bit operating systems

Note

<XXXX> is the installer build number.

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



Trend Micro Vulnerability Protection Manager 2.0.1494 Setup Wizard

Welcome to the Trend Micro Vulnerability Protection Manager Setup Wizard

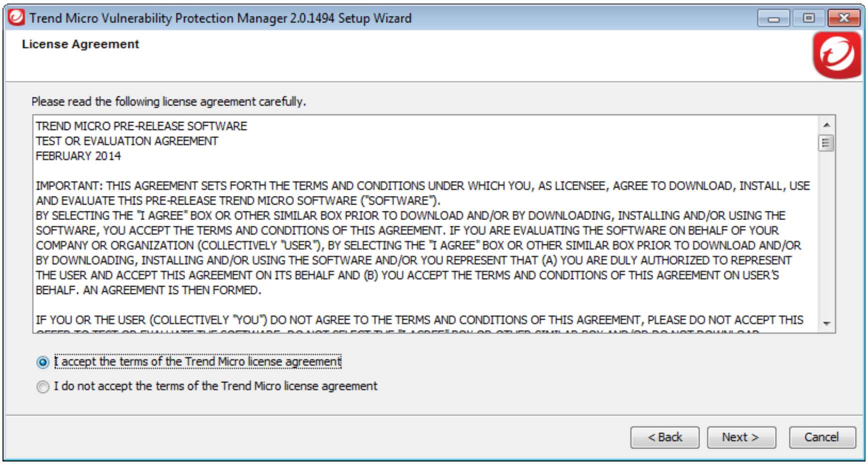
This program installs Trend Micro Vulnerability Protection Manager.

Trend Micro recommends closing all other applications before continuing the installation.

Click Next to continue, or Cancel to exit the Setup Wizard.

2. Click **Next**.

The **License Agreement** screen appears.



Trend Micro Vulnerability Protection Manager 2.0.1494 Setup Wizard

License Agreement

Please read the following license agreement carefully.

TREND MICRO PRE-RELEASE SOFTWARE
TEST OR EVALUATION AGREEMENT
FEBRUARY 2014

IMPORTANT: THIS AGREEMENT SETS FORTH THE TERMS AND CONDITIONS UNDER WHICH YOU, AS LICENSEE, AGREE TO DOWNLOAD, INSTALL, USE AND EVALUATE THIS PRE-RELEASE TREND MICRO SOFTWARE ("SOFTWARE").
BY SELECTING THE "I AGREE" BOX OR OTHER SIMILAR BOX PRIOR TO DOWNLOAD AND/OR BY DOWNLOADING, INSTALLING AND/OR USING THE SOFTWARE, YOU ACCEPT THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU ARE EVALUATING THE SOFTWARE ON BEHALF OF YOUR COMPANY OR ORGANIZATION (COLLECTIVELY "USER"), BY SELECTING THE "I AGREE" BOX OR OTHER SIMILAR BOX PRIOR TO DOWNLOAD AND/OR BY DOWNLOADING, INSTALLING AND/OR USING THE SOFTWARE AND/OR YOU REPRESENT THAT (A) YOU ARE DULY AUTHORIZED TO REPRESENT THE USER AND ACCEPT THIS AGREEMENT ON ITS BEHALF AND (B) YOU ACCEPT THE TERMS AND CONDITIONS OF THIS AGREEMENT ON USER'S BEHALF. AN AGREEMENT IS THEN FORMED.

IF YOU OR THE USER (COLLECTIVELY "YOU") DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, PLEASE DO NOT ACCEPT THIS

● I accept the terms of the Trend Micro license agreement

○ I do not accept the terms of the Trend Micro license agreement

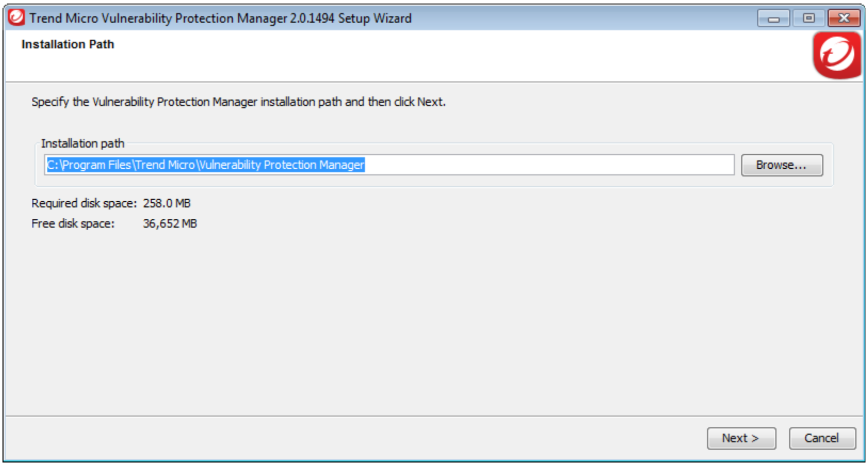
3. Click **I accept the terms of the Trend Micro license agreement** to continue the installation.

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.



Trend Micro Vulnerability Protection Manager 2.0.1494 Setup Wizard

Installation Path

Specify the Vulnerability Protection Manager installation path and then click Next.

Installation path: C:\Program Files\Trend Micro\Vulnerability Protection Manager

Required disk space: 258.0 MB

Free disk space: 36,652 MB

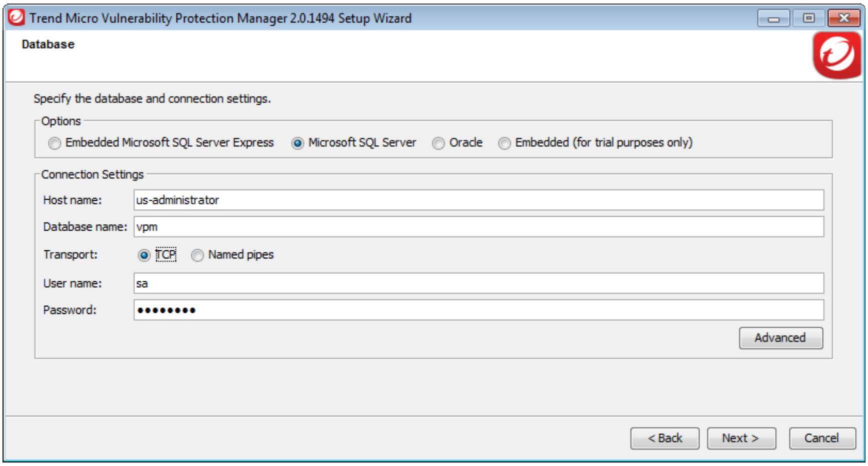
5. Specify a location for the Vulnerability Protection Manager files.

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.



Trend Micro Vulnerability Protection Manager 2.0.1494 Setup Wizard

Database

Specify the database and connection settings.

Options

○ Embedded Microsoft SQL Server Express ● Microsoft SQL Server ○ Oracle ○ Embedded (for trial purposes only)

Connection Settings

Host name: us-administrator

Database name: vpm

Transport: ● TCP ○ Named pipes

User name: sa

Password: ••••••••

7. Select from the following database options:

Type	Description
Embedded Microsoft SQL Server Express	The Vulnerability Protection Manager installs the Microsoft SQL Express 2008 R2 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. **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	The Vulnerability Protection Manager accesses the previously installed Oracle database.

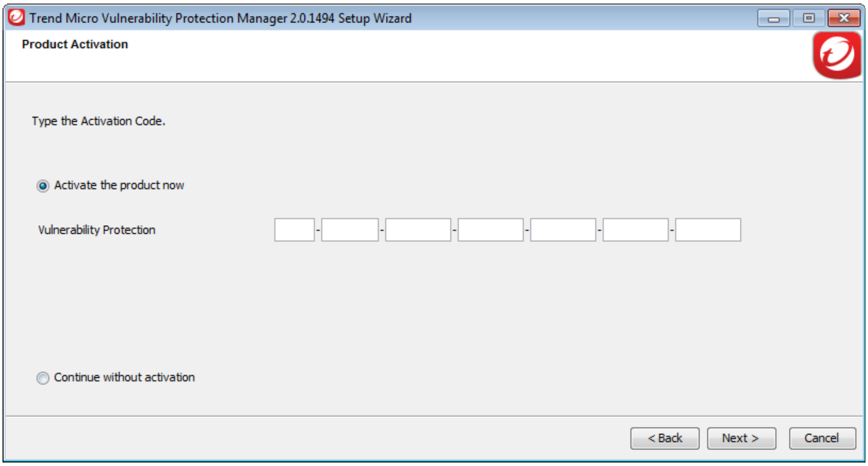
Type	Description
	Important If you select Oracle, you must first create the database before installing Vulnerability Protection Manager. For more information, see *Installing the Database on page 3-2*.
Embedded (Trial and demonstration)	The Vulnerability Protection Manager installs the Apache Derby included in the installation package.

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.


Trend Micro Vulnerability Protection Manager 2.0.1494 Setup Wizard

Product Activation

Type the Activation Code.

● Activate the product now

Vulnerability Protection

○ Continue without activation

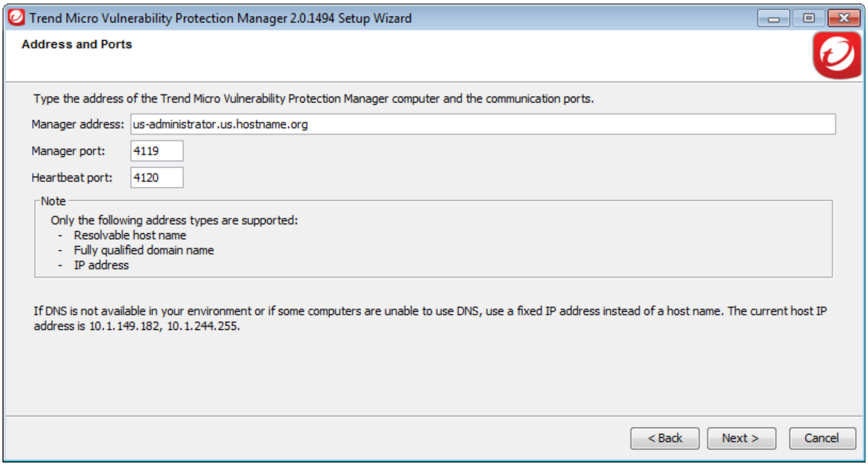
10. Type your Activation Code.

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.



Trend Micro Vulnerability Protection Manager 2.0.1494 Setup Wizard

Address and Ports

Type the address of the Trend Micro Vulnerability Protection Manager computer and the communication ports.

Manager address: us-administrator.us.hostname.org

Manager port: 4119

Heartbeat port: 4120

Note

Only the following address types are supported:
- Resolvable host name
- Fully qualified domain name
- IP address

If DNS is not available in your environment or if some computers are unable to use DNS, use a fixed IP address instead of a host name. The current host IP address is 10.1.149.182, 10.1.244.255.

12. Provide the following:

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

      Note

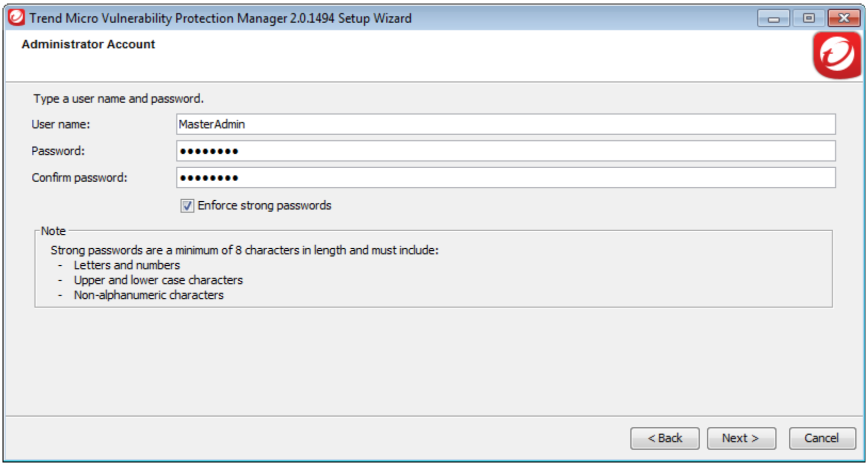
      If DNS is not available in your environment, or if some endpoints are unable to use DNS, use a fixed IP address instead of a host name.

    - **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.



Trend Micro Vulnerability Protection Manager 2.0.1494 Setup Wizard

Administrator Account

Type a user name and password.

User name: MasterAdmin

Password: ••••••••

Confirm password: ••••••••

☑ Enforce strong passwords

Note

Strong passwords are a minimum of 8 characters in length and must include:

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

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

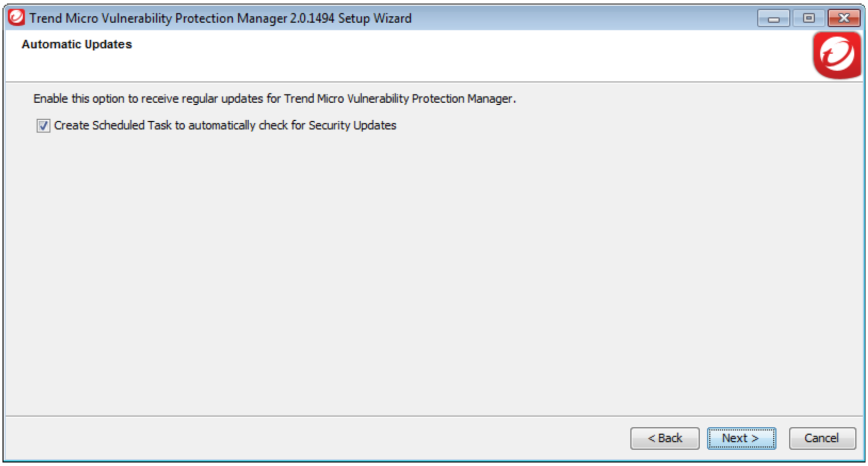
Tip

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 **Automatic Updates** screen appears.



Trend Micro Vulnerability Protection Manager 2.0.1494 Setup Wizard

Automatic Updates

Enable this option to receive regular updates for Trend Micro Vulnerability Protection Manager.

☑ Create Scheduled Task to automatically check for Security Updates

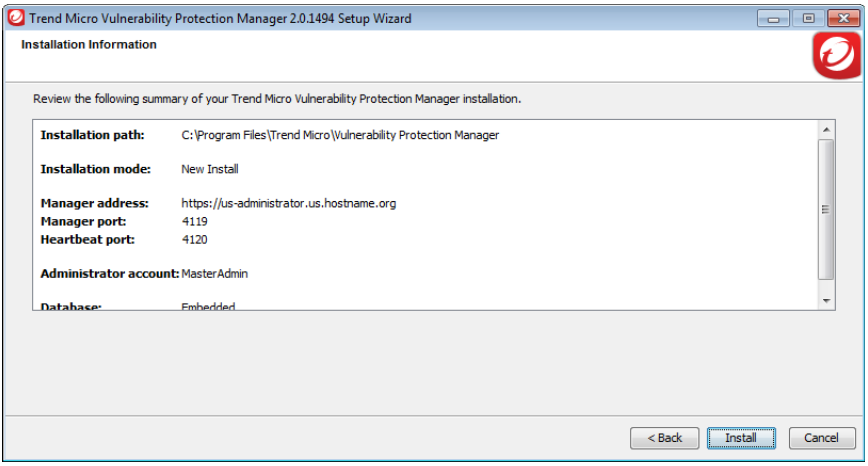
16. Accept the **Create Scheduled Task to automatically check for Security Updates** option (enabled by default).

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. Click **Next**.

The **Installation Information** screen appears.



Trend Micro Vulnerability Protection Manager 2.0.1494 Setup Wizard

Installation Information

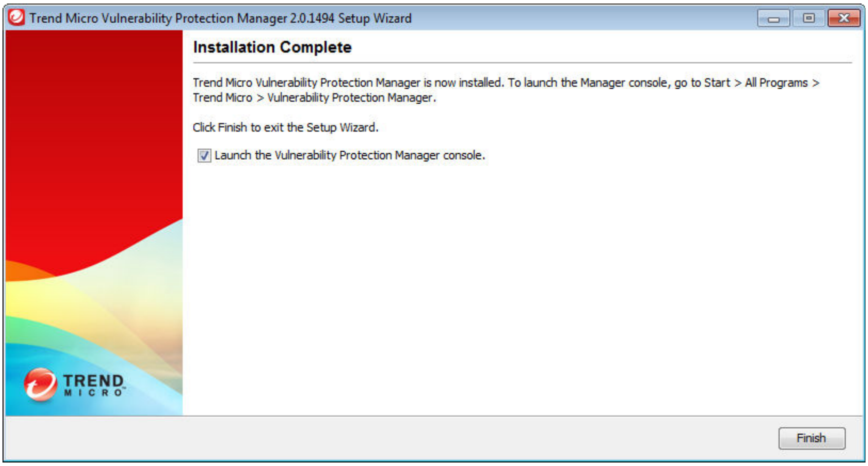
Review the following summary of your Trend Micro Vulnerability Protection Manager installation.

Installation path:	C:\Program Files\Trend Micro\Vulnerability Protection Manager
Installation mode:	New Install
Manager address:	https://us-administrator.us.hostname.org
Manager port:	4119
Heartbeat port:	4120
Administrator account:	MasterAdmin
Database:	Embedded

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

    The installation process begins.

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



Trend Micro Vulnerability Protection Manager 2.0.1494 Setup Wizard

Installation Complete

Trend Micro Vulnerability Protection Manager is now installed. To launch the Manager console, go to Start > All Programs > Trend Micro > Vulnerability Protection Manager.

Click Finish to exit the Setup Wizard.

☑ Launch the Vulnerability Protection Manager console.

Installing Vulnerability Protection Agent

Procedure

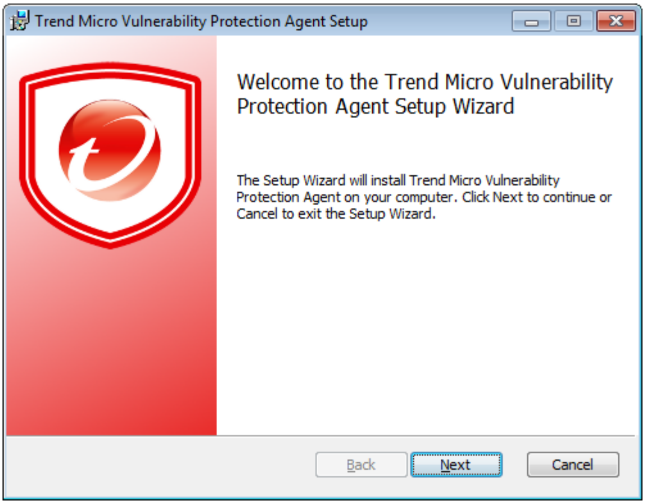
1. Run any of the following installation packages:

INSTALLER	DESCRIPTION
`VPAgent-Windows-2.0.0-<XXXX>.i386`	Standard installer for 32-bit operating systems
`VPAgent-Windows-2.0.0-<XXXX>.x86_64`	Standard installer for 64-bit operating systems

Note

<XXXX> is the installer build number.

The **Welcome** screen appears.

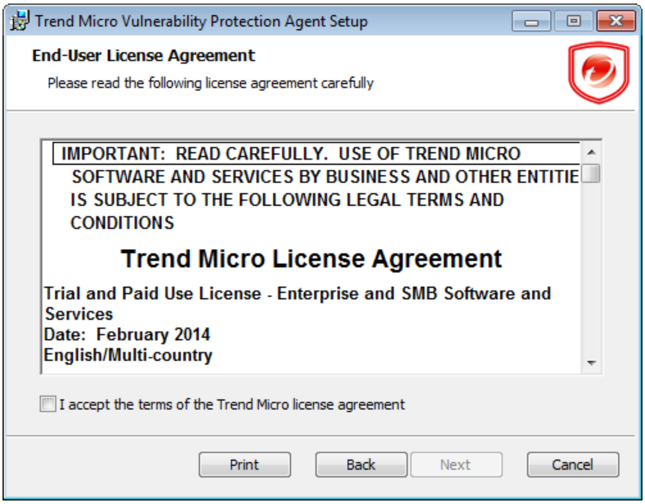


Welcome to the Trend Micro Vulnerability Protection Agent Setup Wizard

The Setup Wizard will install Trend Micro Vulnerability Protection Agent on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

2. Click **Next**.

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



End-User License Agreement

Please read the following license agreement carefully

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

Trend Micro License Agreement

Trial and Paid Use License - Enterprise and SMB Software and Services
Date: February 2014
English/Multi-country

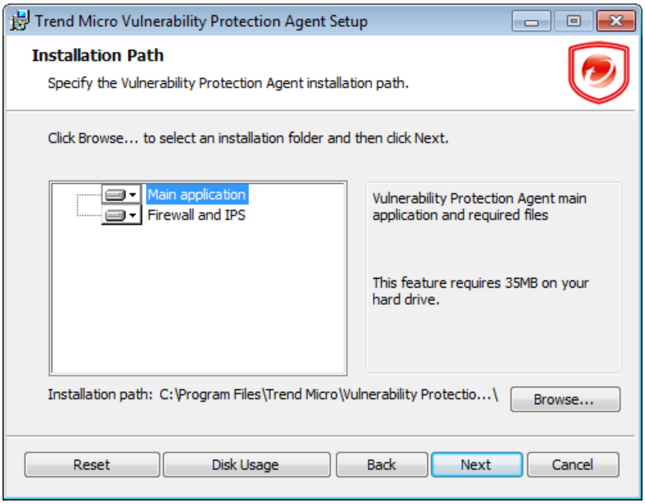
□ I accept the terms of the Trend Micro license agreement

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 **Installation Path** screen appears.



Trend Micro Vulnerability Protection Agent Setup

Installation Path

Specify the Vulnerability Protection Agent installation path.

Click Browse... to select an installation folder and then click Next.

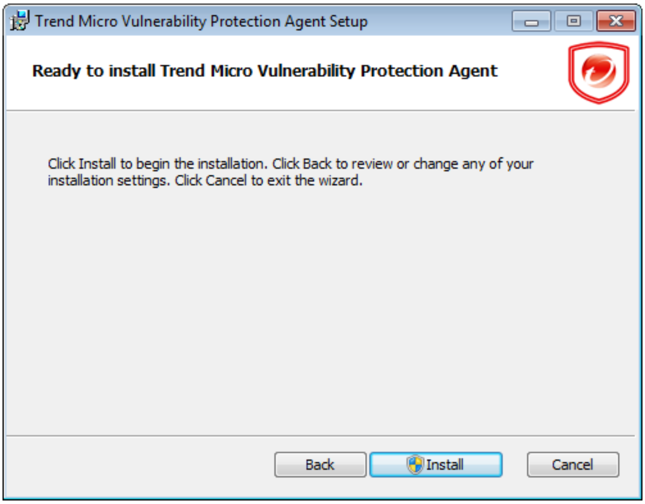
Vulnerability Protection Agent main application and required files

This feature requires 35MB on your hard drive.

Installation path: C:\Program Files\Trend Micro\Vulnerability Protectio...\

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

A confirmation screen appears.



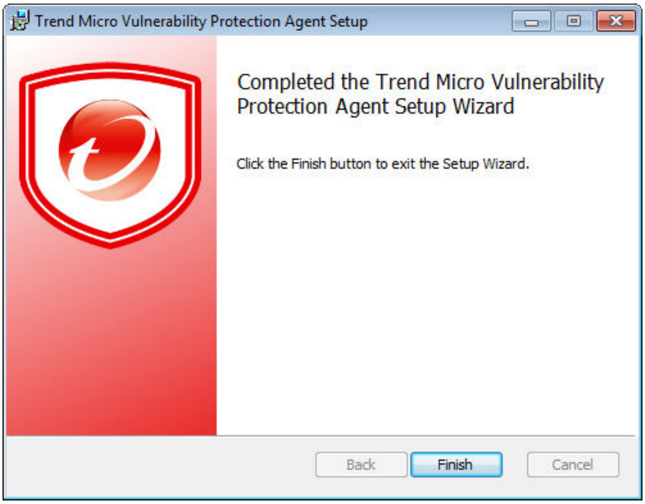
Ready to install Trend Micro Vulnerability Protection Agent

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

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.


Trend Micro Vulnerability Protection Agent Setup

Completed the Trend Micro Vulnerability Protection Agent Setup Wizard

Click the Finish button to exit the Setup Wizard.

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

To verify the installation, right-click **Computer** from the Start menu. Go to **Manage** > **Services and Applications** > **Services** and locate "Vulnerability Protection Agent".

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

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

Port	Purpose
25	Communication to a SMTP Server to send email alerts (configurable)
53	For DNS Lookup
389	Connection to an LDAP Server for Active Directory integration (configurable)
636	Connection to an LDAP Server for Active Directory integration (configurable)
1433	Bi-directional Microsoft SQL Server Database port
1434	Bi-directional Microsoft SQL Server Database port
1521	Bi-directional Oracle Database server port
3268	Connection to an LDAP Server for Active Directory integration (configurable)
4119	Used by your browser to connect to the manager
4120	The "heartbeat" port, used by agents to communicate with manager (configurable)

Vulnerability Protection Agent Ports

Ports	Purpose
4118	Manager-to-Agent communication
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.Database Type=<value>	Embedded Microsoft SQL Server Express Microsoft SQL Server Oracle	DatabaseScreen.Database Type=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 - Apache Derby	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 default instance. This setting is required for: • Microsoft SQL Server	DatabaseScreen.SQLServer.Instance=MSSQLSERVER
DatabaseScreen.SQLServer.Domain=<value>	<database domain> **Note** This setting is required for: • Microsoft SQL Server	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** `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** `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 Vulnerability Protection Manager.

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`.

2. Create a new folder called `Backupkeystore`.

3. Copy `.keystore` and `configuration.properties` to the newly created folder `Backupkeystore`.

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

5. 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*.

6. Type a password.

   Note

   The default name for the certificate is `-dname`. Some Certification Authorities (CAs) require a particular certificate name to sign the Certificate Signing Request (CSR). Consult your CA Admin to confirm your specific requirements.

   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`.

7. Run the following commands from a command line editor:

a. To view the newly generated certificate: `C:\Program Files\Trend Micro\Vulnerability Protection Manager\jre\bin>keytool -list -v`

b. To create a CSR file for your CA to sign: `C:\Program Files\Trend Micro\Vulnerability Protection Manager\jre\bin>keytool -certreq -keyalg RSA -alias tomcat -file certrequest.csr`

> **Note**
>
> Follow the CSR submission guidelines specified by your CA when submitting the CSR file.

c. To import the CA cert in JAVA trusted keystore: `C:\Program Files\Trend Micro\Vulnerability Protection Manager\jre\bin>keytool -import -alias root -trustcacerts -file cacert.crt -keystore "C:/Program Files/Trend Micro/Vulnerability Protection Manager/jre/lib/security/cacerts"`

d. To import the CA cert in JAVA trusted keystore: `C:\Program Files\Trend Micro\Vulnerability Protection Manager\jre\bin>keytool -import -alias root -trustcacerts -file cacert.crt -keystore "C:/Program Files/Trend Micro/Vulnerability Protection Manager/jre/lib/security/cacerts"`

e. To import the certificate response to your keystore: `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`.

f. To view the certificate chain in you keystore: `C:\Program Files\Trend Micro\Vulnerability Protection Manager\jre\bin>keytool -list -v`

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

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

> **Note**
>
> It will look something like: `keystoreFile=C\:\\\\Program Files\\\\Trend Micro\\\\Vulnerability Protection Managertrend_manager_program_cap\\\\.keystore port=4119 keystorePass= $1$85ef650a5c40bb0f914993ac1ad855f48216fd0664ed2544bbec6de80160b2fe9800f79f913f28e80381c8e71f2fed96a2aa522ada039a7abfa01542d42dbe3installed=true serviceName= Trend Micro Vulnerability Protection Manager.`

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

11. Save and close the file.

12. Restart the Vulnerability Protection Manager service.

13. Connect to the Vulnerability Protection Manager with your browser to see the new SSL certificate signed by your CA.

Appendix G

Frequently Asked Questions (FAQs)

This appendix answers various Frequently Asked Questions.

Frequently Asked Questions

Question	Answer
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.
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...**.

QUESTION	ANSWER
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.
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 2008 R2 Express	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>\MSSQL10_50.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.

Index

TREND MICRO INCORPORATED
10101 North De Anza Blvd. Cupertino, CA., 95014, USA
Tel:+1(408)257-1500/1-800 228-5651 Fax:+1(408)257-2003 info@trendmicro.com

www.trendmicro.com

Item Code: APEM26305/140210