TREND MICRO™

Trend Micro™ Threat Intelligence Manager 1

Installation and Deployment Guide

Security Management

Document Part No. ZREM14779/110112

Release Date: June 2011

Protected by U.S. Patent No. not available. Patent pending.

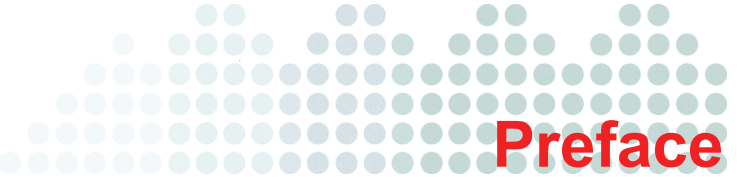
The user documentation of Trend Micro Threat Intelligence Manager is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

Detailed information about how to use specific features within the software are available in the Online Help file and the online Knowledge Base at Trend Micro's Web site.

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

Contents



Preface

Welcome to the *Trend Micro™ Threat Intelligence Manager Installation and Deployment Guide*. This document discusses requirements and procedures for installing the Threat Intelligence Manager on the agents and server.

Topics in the chapter:

Trend Micro™ Threat Intelligence Manager Documentation

The Threat Intelligence Manager documentation includes the following:

TABLE 1-1. Threat Intelligence Manager Documentation

DOCUMENTATION	DESCRIPTION
Trend Micro™ Threat Intelligence Manager Administrator's Guide	A PDF document that discusses getting started information and helps you plan for deployment and configure all product settings.
Online Help	Helps you configure all features through the user interface. You can access the Online Help by opening the Web console and then clicking the Information icon in the top right corner.
Trend Micro™ Threat Intelligence Manager Installation and Deployment Guide	A PDF document that discusses requirements and procedures for installing Trend Micro Threat Intelligence Manager, planning for deployment and configuring product settings.
Readme File	Contains late-breaking product information that might not be found in the other documentation. Topics include a description of features, installation tips, known issues, and product release history. The readme is available at: http://www.trendmicro.com/download
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 Web site: http://esupport.trendmicro.com

Audience

This document is intended to be used by new users of Threat Intelligence Manager, including system administrators, operators, sensitive content contributors, information security staff, executives, and other users with other specific roles.

The audience should have a thorough understanding of the Threat Intelligence Manager system, including general operations and critical concepts.

Document Conventions

To help you locate and interpret information easily, the Threat Intelligence Manager documentation uses the following conventions.

TABLE 1-2. 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 ScanMail tasks
Italics	References to other documentation
`Monospace`	Examples, sample command lines, program code, Web URL, file name, and program output
Tools > Client Tools	A “bread crumb” found at the start of procedures that helps users navigate to the relevant Web console screen. Multiple bread crumbs means that there are several ways to get to the same screen.
<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: text	Provides configuration notes or recommendations

TABLE 1-2. Document Conventions (Continued)

CONVENTION	DESCRIPTION
Tip: text	Provides best practice information and Trend Micro recommendations
WARNING! *text*	Provides warnings about activities that may harm computers on your network

Terminology

The following table provides the official terminology used throughout the Threat Intelligence Manager documentation.

TABLE 1-3. Threat Intelligence Manager Terminology

TERMINOLOGY	DESCRIPTION
Administrator	The person managing the Threat Intelligence Manager server.
Alert	Item of interest generated from a qualifying event or group of events.
Client	The Threat Intelligence Manager client program.
Client computer or endpoint	The computer where the Threat Intelligence Manager client is installed.
Client installation folder	The folder on the computer that contains the Threat Intelligence Manager client files. If you accept the default settings during installation, you will find the installation folder at any of the following locations: `C:\Program Files\Trend Micro\Threat Intelligence Manager Client`
Client user (or user)	The person managing the Threat Intelligence Manager client on the client computer.

TABLE 1-3. Threat Intelligence Manager Terminology (Continued)

TERMINOLOGY	DESCRIPTION
Components	Responsible for collecting, managing, displaying, and investigating event that occur between Trend Micro and third-party products.
Console	The user interface for configuring and managing the Threat Intelligence Manager server and client settings. The console for the Threat Intelligence Manager server program is called the "Web console," while the console for the client program is called the "client console."
Dashboard	UI screen in which Widgets are displayed.
Generated Report	Displays the results of a TMQL query in a given visualization, e.g. pie chart, table, line graph, and so on, in the form of a widget displayed on the Console UI or printable form.
Hibernate	Open source facility that provides relational database table to object mapping. It is the tool used by report management system to interact with the report database.
Investigation Baskets	Collection of report baskets that are available to the user from the Console UI.
Notification	The item sent out to inform a registered user that an event has occurred.
POJO	Acronym for Plain Old Java Objects which is one form of database interface provided by Hibernate.
RBAC	Role-based access control
Report Basket	Collection of reports maintained in the Investigation Baskets UI object.
Report Template	Object which contains the TMQL query and visualization information necessary to generate a report.
Scheduled Report	Generated report that is run at regular time intervals.
Security risk	The collective term for virus/malware, spyware/grayware, and Web threats
Server	The Threat Intelligence Manager server program

TABLE 1-3. Threat Intelligence Manager Terminology (Continued)

TERMINOLOGY	DESCRIPTION
Server computer	The computer
Server installation folder	The folder on the computer that contains the Threat Intelligence Manager server files. If you accept the default settings during installation, you will find the installation folder at any of the following locations: `C:\Program Files\Trend Micro\Threat Intelligence Manager`
Threat Intelligence Manager service	Threat Intelligence Manager is a collection of Windows services that provide the ability to analyze security events generated by other security products.
TIM	Threat Intelligence Manager
TMQL	Trend Micro Query Language. Provides a unified query interface to Threat Intelligence Manager SOLR and DB data stores.
VP	Visibility Platform
Widget	Visual renderings of the report templates. Widgets are contained in the Dashboard.
Workbench	UI screens in which Threat Intelligence Manager logs and event data are queried and analyzed.

Chapter 1

Preparing for the Installation

This chapter guides you through the preparation necessary for a successful installation of the *Trend Micro™ Threat Intelligence Manager*.

Topics include the following:

Overview

The Trend Micro™ Threat Intelligence Manager is designed to be the next generation in Trend Micro's security visibility and central management products. The mission of the first Threat Intelligence Manager is to:

- collect, aggregate, manage, and analyze Trend Micro product event logs into a centralized storage space on a server
- provide advanced visualization and investigation tools that can enable you to monitor, explore, and diagnose security events within your own environment

Threat Intelligence Manager provides unique security visibility based on Trend Micro's proprietary threat analysis and recommendation engines. The flexibility of the Threat Intelligence Manager server enables third-party applications, as well as future Trend Micro products, to seamlessly and easily integrate into Threat Intelligence Manager.

The Threat Intelligence Manager documentation is written for IT administrators and security analysts. The documentation assumes that the readers have an in-depth knowledge of Trend Micro security products from where the security events are generated. The document does not assume the reader has any knowledge of threat intelligence with event correlation.

System Requirements

The installation of Threat Intelligence Manager must be supported by a 64-bit Windows Server 2008 R2 or later (Standard, Enterprise, Datacenter or Web editions) with .NET 3.5 or higher installed to support Microsoft® SQL Server® 2008 R2 Express installation. The .NET 3.5 comes with the Windows 2008 R2 operating system but is not installed by default. Users can install using the Microsoft Server Manager and going to Features > Add Features, checking the .NET Framework 3.5.1, and completing the installation of the software. Hardware requirements are determined by the number of products and events per second that expect support from Threat Intelligence Manager. For additional details about the recommended minimum requirements, refer to the readme.

Installation Prerequisites

The installation of Trend Micro Threat Intelligence Manager requires a connection to an HTTP host site to download the package. You will need access to the binary and download it locally or through a shared directory on the HTTP host site.

Note: Download the product from the Trend Micro download site at: http://downloadcenter.trendmicro.com
For more information, see Installing Threat Intelligence Manager on a Server starting on page 2-6.

Hardware Requirements

- CPU: Core 2 Duo 2.66GHz CPU system or above
- Memory: Minimum 4GB of RAM (Recommended: 16GB or above)
- Hard Disk: At least 250GB of available disk space for storage
- Network Protocol: TCP/IP, UDP for heartbeat, HTTP, HTTPS, TCP over VPN, or TCP port 43 for WhoIs utility.
- Others: .NET Framework 3.5 SP1 or above
- Display: VGA (1280 x 1024/256 color) or higher

Browser Requirements

- Mozilla® Firefox® 3.6.xx and 4.0.xx
- Microsoft® Internet Explorer® 8.0 and 9.0
- Adobe® Flash® Player 10.x or higher

Agent System Requirements

Prior to installation, the agent requires the following:

- Supported Trend Micro products - Agent, installed on 32/64 bit Windows
  - OfficeScan Client/Server Edition (OSCE) 10.0 SP1 Patch 2 and hot fix 2881
  - OSCE 10.5 and hot fix 1286.
  - OSCE 10.5 patch 1 and hot fix 1848.2.

- Supported Trend Micro Products - Agentless
  - Threat Discovery Appliance (TDA) 2.5
  - Deep Security Manager (DSM) 7.0
  - Intrusion Defense Firewall (IDF) 1.2

Product Versions and Keys

Obtain product evaluation keys from your Sales Team.

Deployment Requirements

Along with several useful options you can utilize, there are several requirements necessary to successfully deploy Threat Intelligence Manager. To prepare for the deployment of Threat Intelligence Manager, check that the following conditions are met:

- Network Requirements
- Managed Product Requirements

Network Requirements

The following are the network requirements necessary for successful deployment of Threat Intelligence Manager:

Threat Intelligence Manager Server

The following are among the network ports available for your use:

- Incoming HTTPS (TCP/80) for console access
- Incoming HTTP/HTTPS (TCP/7173/7174) for plain text or SSL log receiving
- Incoming Syslog (UDP/514, TCP/514) for syslog receiving
- Incoming HTTPS (TCP/5118) and Outgoing HTTPS (TCP/5120) for server and agent management
- Outgoing HTTPS (TCP/443) for component and license updates
- Outgoing HTTP (TCP/8080) for general Web services access

Bandwidth Requirements

You should be aware of the following bandwidth requirements:

- Receives compressed logs uploaded from all managed products
- Receives periodic uploads of events from a Webservice API or through UDP Syslog events
- Makes periodic agent management traffic to all agents

Managed Products (Threat Intelligence Manager Agent)

The following are among the network ports available for managed products:

- Outgoing HTTP/HTTPS (TCP/7173/7174) for log uploaded to the Threat Intelligence Manager server or the Threat Intelligence Manager
- Incoming HTTPS (TCP/5118) and Outgoing HTTPS (TCP/5120) for server or agent management of the Threat Intelligence Manager server
- Outgoing HTTPS traffic to manage and collect logs for Web-service-enabled products (optional - port 4119)

Bandwidth Requirements

- Periodically uploads compressed product logs
- Allows the limiting of upload bandwidths in KBs
- Creates periodic server and agent management traffic logs to the server

Managed Product Requirements

The following are the Managed Product requirements necessary for successful deployment of the Threat Intelligence Manager.

Managed Products (Threat Intelligence Manager Agent)

You should have at least one of the following Trend Micro products:

- Supported Trend Micro products - Agent, installed on 32/64 bit Windows
  - OfficeScan Client/Server Edition (OSCE) 10.0 SP1 Patch 2 and hot fix 2881
  - OSCE 10.5 and hot fix 1286.
  - OSCE 10.5 patch 1 and hot fix 1848.2

- Supported Trend Micro Products - Agentless
  - Threat Discovery Appliance (TDA) 2.5 (Managed only for log collection through an agentless syslog channel), 2.55, 2.6
  - Deep Security Manager (DSM) 7.0
  - Intrusion Defense Firewall (IDF) 1.2

Privilege Requirements

- Windows administrator privilege on OSCE servers
- Console administration privilege for TDA.
- List of product's host names or IP addresses
- IDF web service administrator and password
- DSM user and password with WebServiceAPI role enabled

After you have verified the various requirements existing within your environment, you are ready to begin installation as described in Installing and Deploying the Threat Intelligence Manager Server and Agent starting on page 2-1.

Chapter 2

Installing and Deploying the Threat Intelligence Manager Server and Agent

This chapter discusses the steps necessary for successful installation and deployment of the Trend Micro Threat Intelligence Manager server and agent.

Topics include the following:

Deployment Overview

The following diagrams show the expected deployment of the Threat Intelligence Manager as well as the agent/concentrators in an Enterprise environment.

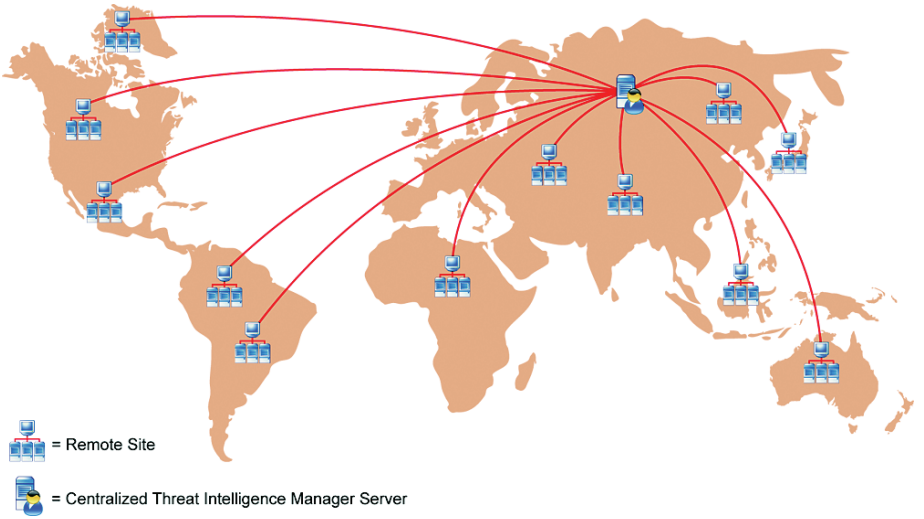


FIGURE 2-1 Standard Expected Deployment

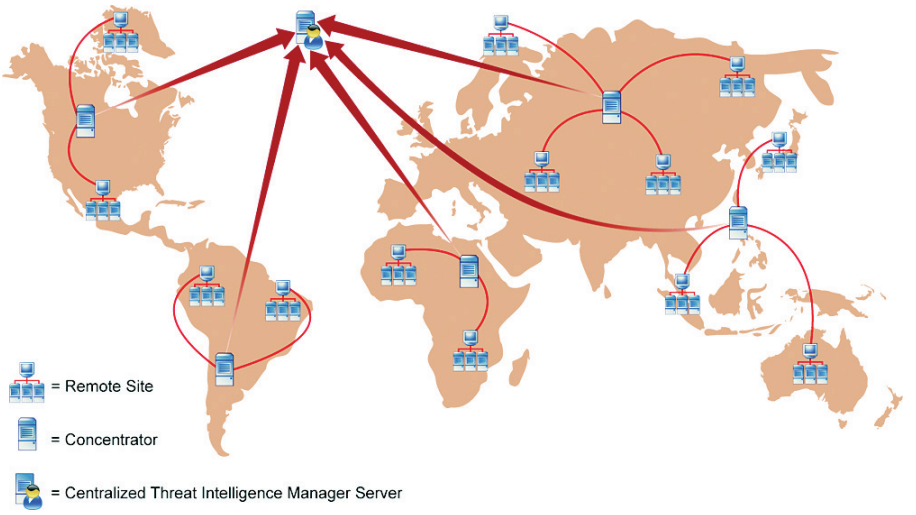


FIGURE 2-2 Expected Deployment Including Agents and Concentrators

When deploying Threat Intelligence Manager, you will need to proceed by working through the following steps:

Deployment Sequence:

1. Deploy the Threat Intelligence Manager server. See Deploying and Installing the Threat Intelligence Manager Server on page 2-6
2. Deploy the Threat Intelligence Manager agent on supported managed products (OSCE). See Deploying and Installing the Threat Intelligence Manager Log Sources on page 2-30
3. Manually add the agent IPs or host names on the Threat Intelligence Manager console.
4. Configure the Threat Discovery Appliance syslog exporting on a Threat Discovery Appliance console.
5. Configure web service to accept events from a Deep Security Manager.
6. Configure web service to accept events from an Office Scan Intrusion Detection Firewall plugin.
7. Import your own corporate tagging configuration.

8. Lastly, verify the deployment. See Verifying the Deployments on page 2-42

Performing a Fresh Installation of the Threat Intelligence Manager Server

Before you begin a Threat Intelligence Manager installation, ensure that you are logged in as a local administrator. To do this, right-click the installation package and select the "Run as administrator" option as shown in the following figure. If you are already logged in as a local administrator, you are not required to do this step.

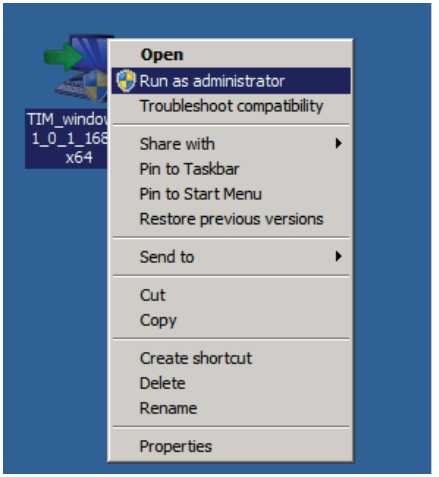


FIGURE 2-3 Run as Administrator option

If you would like to manually edit the configuration files, or run certain programs such as "tm_ctl" and the CDT tool as domain administrators, you should change the user permissions of the Threat Intelligence Manager home directory to allow full-control to

those select users. Only add users that require this level of system maintenance control over the Threat Intelligence Manager. See the following figure as an example.

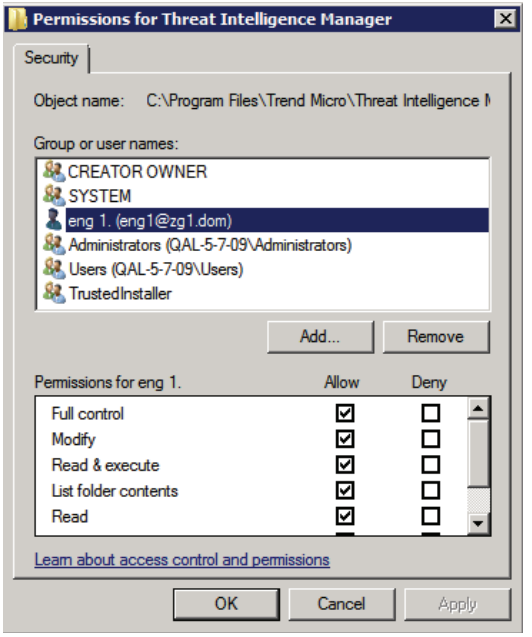


FIGURE 2-4 Permission Settings for Threat Intelligence Manager

To perform a fresh installation, run the installation binary as an administrator on a computer that meets the Trend Micro Threat Intelligence Manager server Fresh Installation Requirements.

For information on the installation screens and configuration options, see the installation screens in the section that follows.

After installing the server, configure the Threat Intelligence Manager server settings from the Web console and then install the Threat Intelligence Manager agents to computers with supported Trend Micro products or add web services for agentless products currently supported by the Threat Intelligence Manager.

Note: To use a remote or existing database, see Appendix A, Using a Remote/Existing Database for Installation on page A-1 before starting the Threat Intelligence Manager installation for the database configurations needed.

Deploying and Installing the Threat Intelligence Manager Server

The first step necessary for a successful installation is to deploy your server.

To do this, complete the following steps:

1. Install and execute the Threat Intelligence Manager package on the Threat Intelligence Manager server.

Note: Silent installations are also supported.

2. Access the Threat Intelligence Manager server console at:

   `https://<server IP or host name>/`

Installing Threat Intelligence Manager on a Server

Before you can install Threat Intelligence Manager, you will need to download the binary from Trend Micro's HTTP server.

Using a Web Browser:

1. Open your Web browser and go to the Trend Micro download site at:
   `http://downloadcenter.trendmicro.com/`
2. Complete the registration process.
3. Click the button right below the header to go to the page where the product kit can be downloaded.

To begin installation:

1. After downloading the binary from the product portal, double-click the `TIM_windows_1_0_0_xxxx_x64.exe` file, where `xxxx` indicates the latest build available from Trend Micro.

Note: You must log in as an Administrator or as a user with Administrator privileges in order to install the Threat Intelligence Manager build.

---

2. The Install Wizard begins. After the Wizard Installation has completed, you should follow the onscreen prompts as shown on the following figures to complete the installation.

FIGURE 2-5 Initiating the Setup

3. Press **Next**.

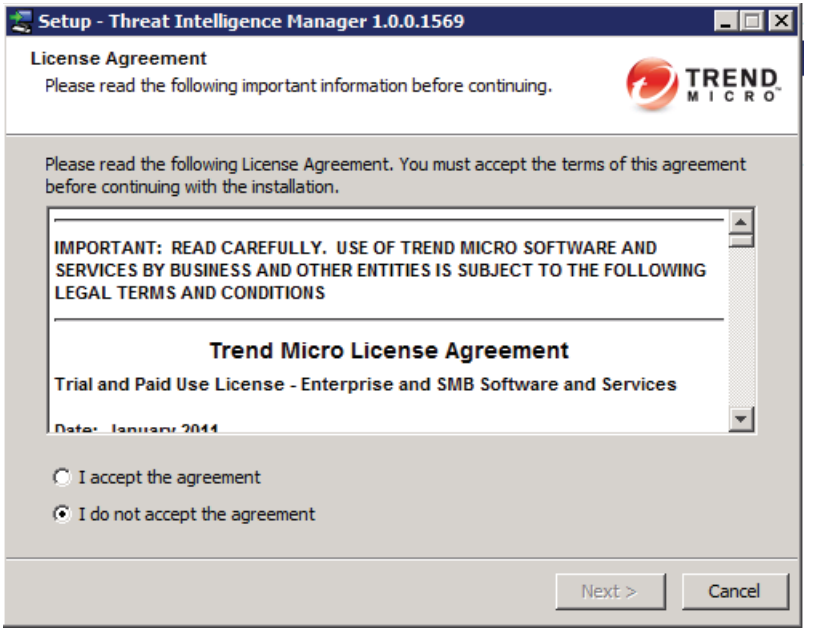


FIGURE 2-6 Accepting the License Agreement

4. To continue, select "I accept the agreement" and click **Next**. Click **Cancel** or "I do not accept the agreement" if you would like to end the installation.
5. Select one of the three types of installation, Standard, Custom, and Demo mode. See Figure 2-7.
   a. Standard installation—Allows user to change destination directory, proxy connection setting, enter a product activation key, set the administrator user name and password, select password policy of strong or weak password and start menu options.
   b. Custom installation—In addition to the configurable options for the standard installation user can configure a remote database connection, management console and web service ports, log receiver ports, and syslog ports. In addition to the steps that follow, see Additional Steps for a Custom Installation.

Note: See Using a Remote/Existing Database for Installation starting on page A-1 for information about using a remote or existing database.

c. Demo mode—If customers only wish to evaluate some of the Threat Intelligence Manager features they can install in demo mode giving the user a way to populate the product with sample data and use that data to simulate features. See Demo Mode Installation.

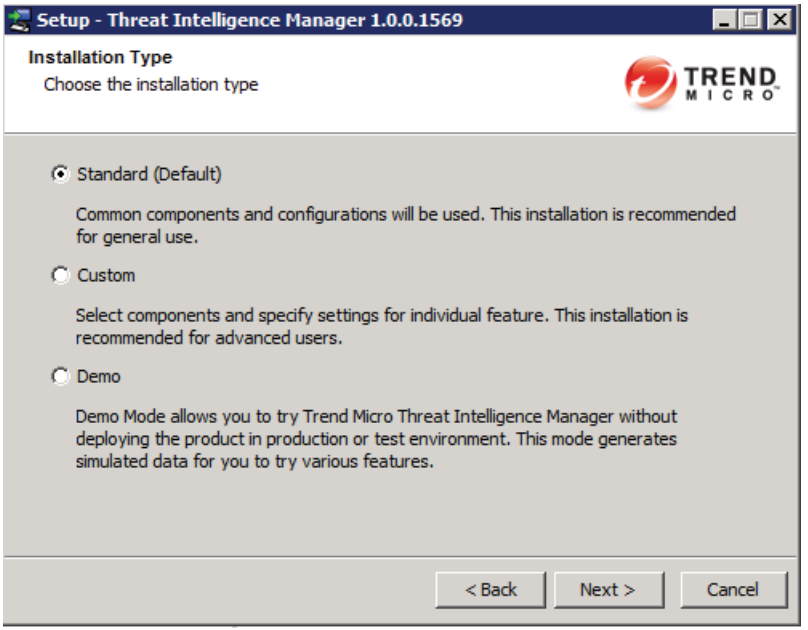


FIGURE 2-7 Select an Installation Type

6. Click **Next**.

7. The default destination directory as shown in Figure 2-8 is sufficient for your installation, but you can browse to other locations based on your organization's requirements.

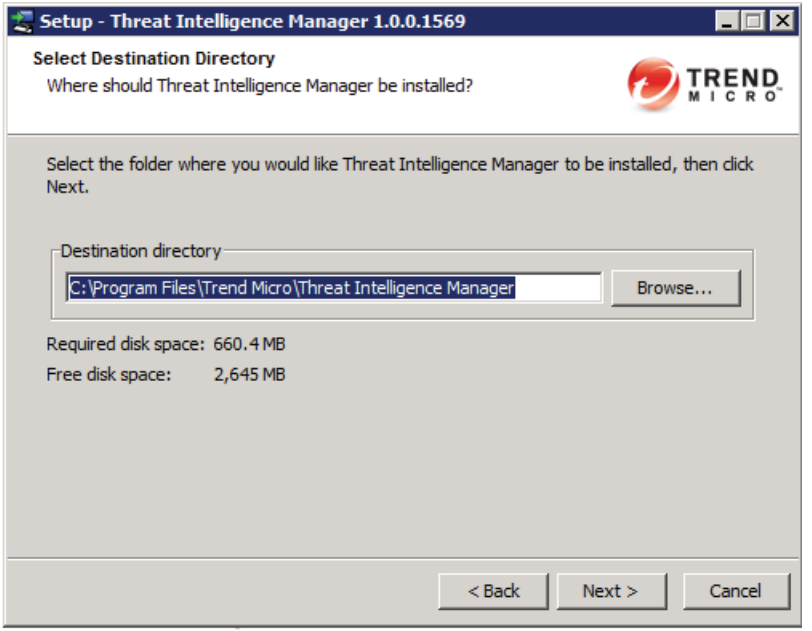


FIGURE 2-8 Select or Assign the Destination Directory

8. Click **Next**. The Connections Settings screen appears See Figure 2-9.

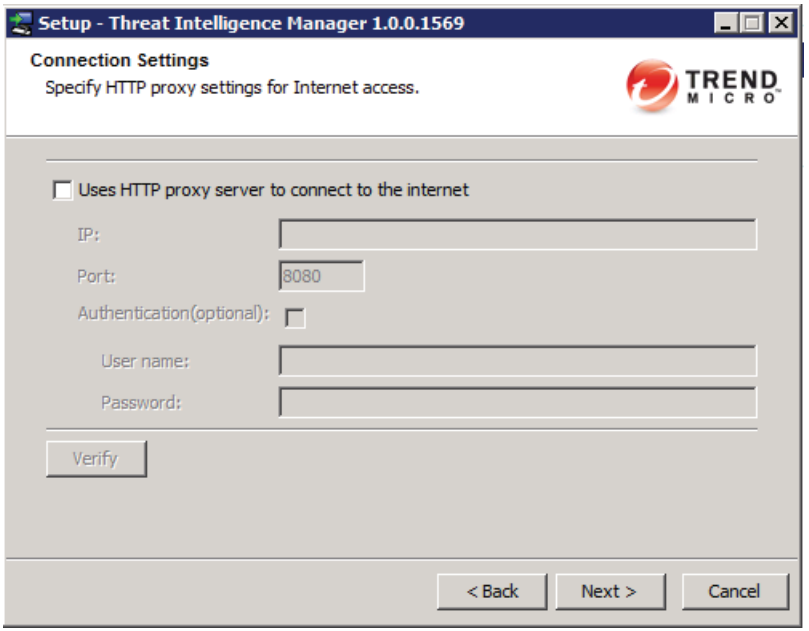


FIGURE 2-9 Configure the Connection Settings

9. You can enable the use of an HTTP proxy server to connect to the Internet., or continue by using the default setting and disabling the use of a proxy server.

Note: The proxy server is used by the Web Reputation Service utility.

10. Click **Next**. The Product Activation screen appears.

11. Enter the product activation key provide by Trend Micro. Users can install the product without the activation key, but the product will have limited functionality until a valid key is activated through the management console.

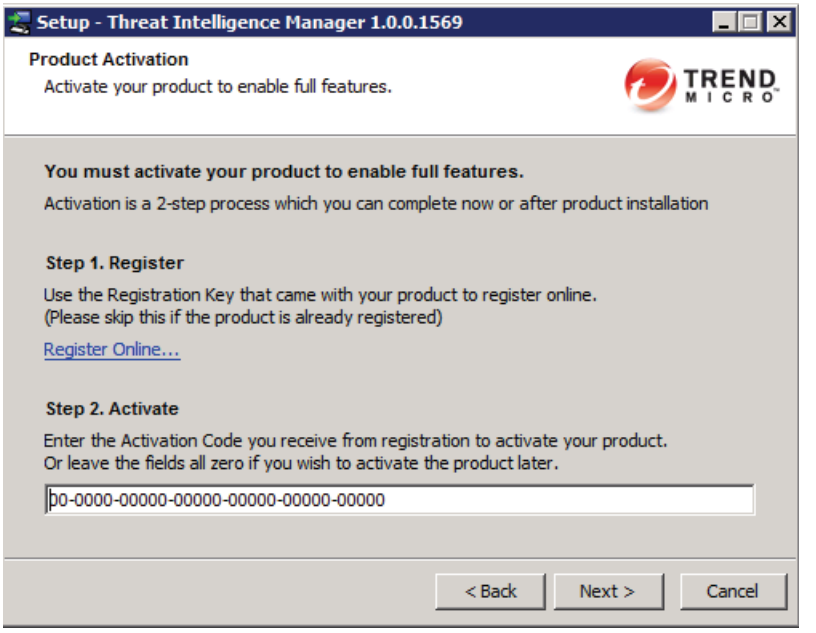


FIGURE 2-10 Enter the Product Activation Key for Full Functionality

12. Click **Next**. The Administrator Account screen appears.

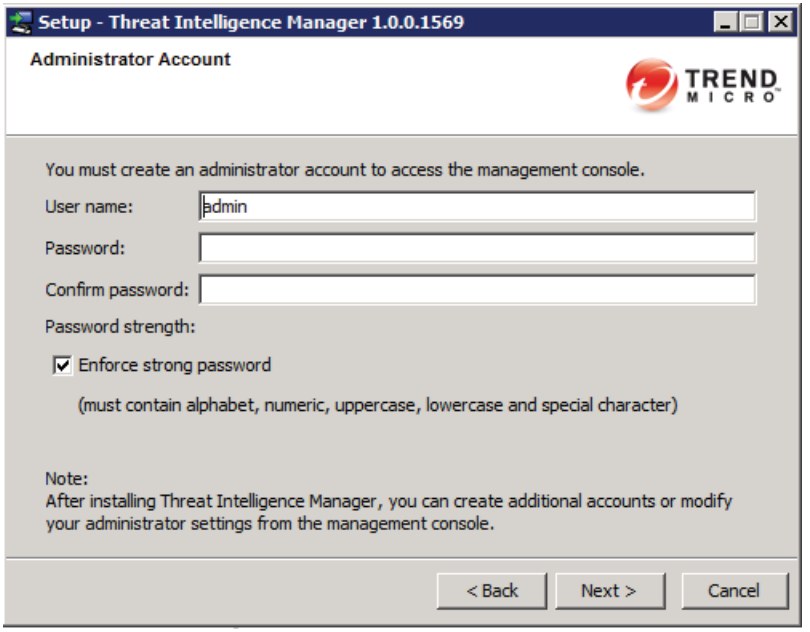


FIGURE 2-11 Creating an Administrator Account

13. To access the management console, you will need to establish an administrator account. You can use the default "admin" as a user name or enter another name.
14. Enter and confirm a password that is at least eight characters in length.

    The password must contain alphabetic, numeric, uppercase, lowercase, and special characters. You must uncheck the "Enforce strong password" check box to use a password that does not contain all the characters listed. Trend Micro recommends using strong passwords for security purposes.

Note: If you are the Administrator, and you have forgotten your Administrator's password after installation, you can reset the password using the "`tmcore_cli`" tool.

For example:
The "`tmcore_cli`" tool will be installed in the "`<install folder>/bin`" location. The command line utility enables Administrators to unlock their account and set up a new password.

Command line example: Usage: `tmcore_cli -action actionname`

Example to unlock and create a new administrator's account password: `tmcore_cli -action unlockout -username USERNAME [-newpassword NEWPASSWORD]`

15. Click **Next**. The Select Start Menu Folder screen appears to help guide you through the establishment of your shortcuts and startup commands. If desired, you can create a variety of shortcuts including one within the Start Menu.

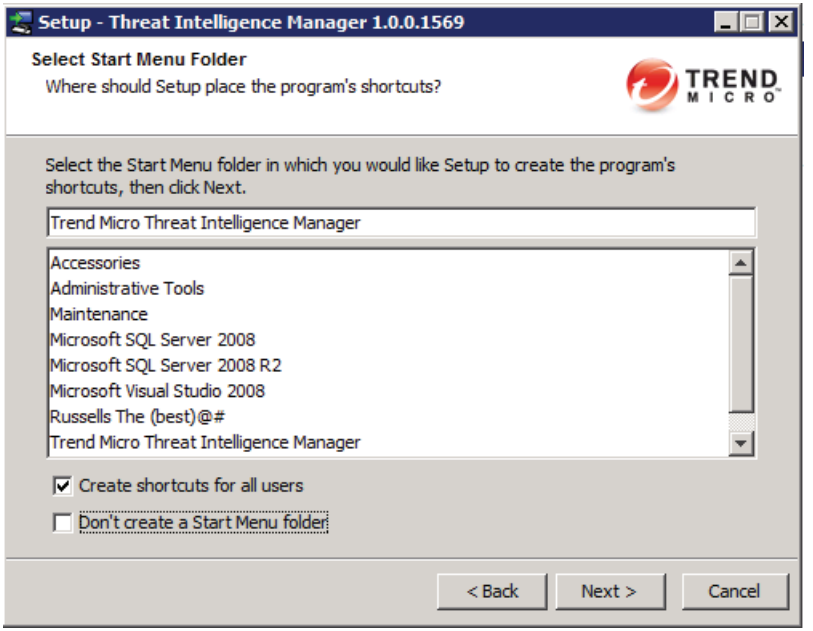


FIGURE 2-12 Start Menu Options

16. Click **Next**. The platform begins to install with the settings you selected in the previous steps.

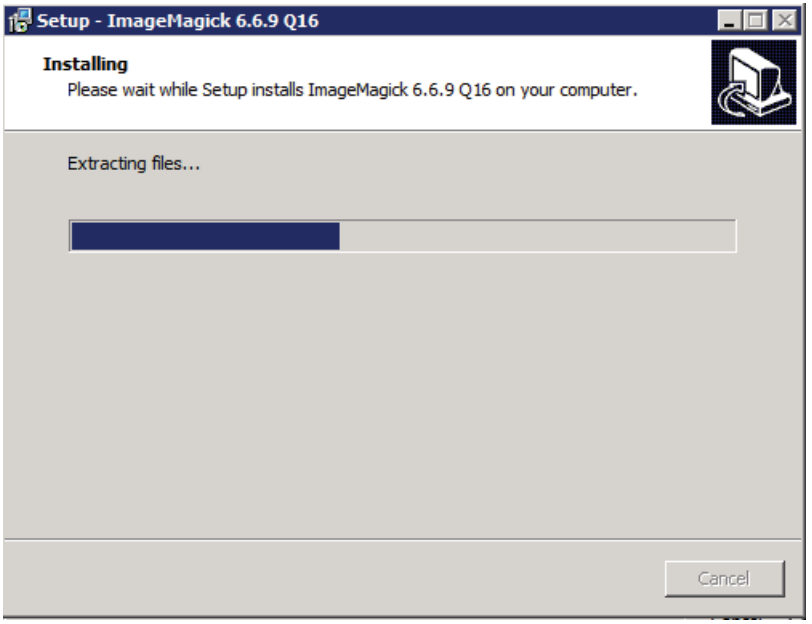


FIGURE 2-13 Installation and Extraction

17. Wait for the Wizard to complete and then click **Finish** to exit the setup.

The application can be launched by selecting the installed icons.

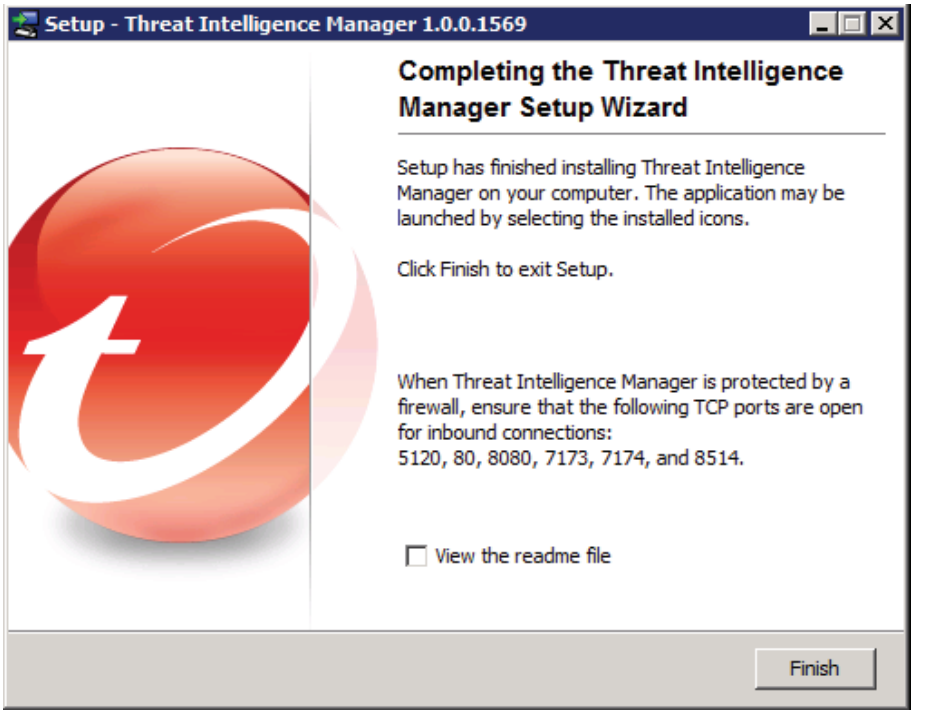


FIGURE 2-14 Finishing the Threat Intelligence Manager Setup Wizard

Additional Steps for a Custom Installation

In addition to the steps required for a standard installation, for a custom installation you must also complete each the following four procedures.

Installing on a Remote or Existing Database

Threat Intelligence Manager can be installed either on a local or remote database server. In addition to the steps required of a standard installation, there are four additional steps (bolded) that you will need to complete for a Custom Installation that include all of the following:

- Installing a Directory
- Defining the Proxy Settings
- Activating the Product
- Defining the Administer Account
- **Installing a Remote or Existing Database**
- **Configuring the Web Console Ports**
- **Configuring the Log Receiver Ports**
- **Configuring the Syslog Receiver Ports**
- Selecting a Start Menu Folder

To configure a database server:

1. You must have selected Custom Installation and completed all the first four processes shown in the previous list.

2. From the Configure Database Server page, select the first box that reads "Use existing database (SQL Server/Express)" as shown in the following figure.

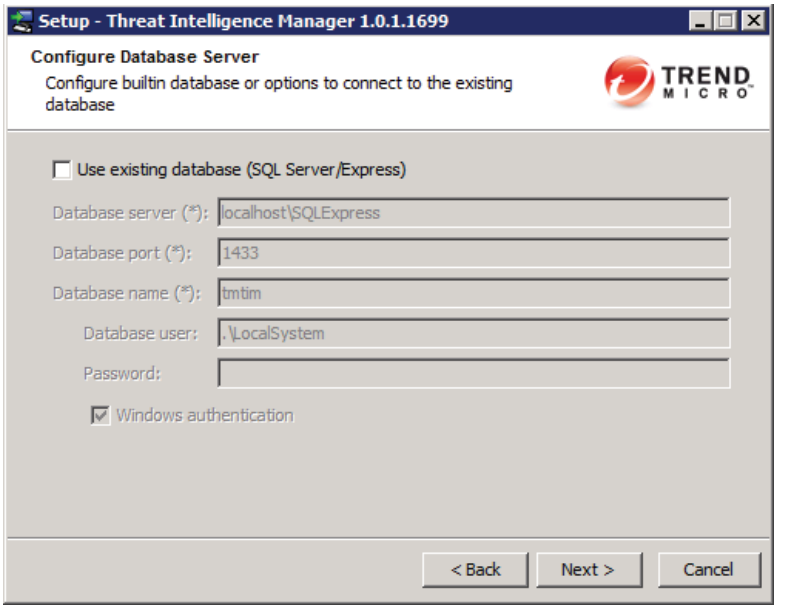


FIGURE 2-15 Configuring a Custom Database Server

The SQL Server Configuration Manager appears.

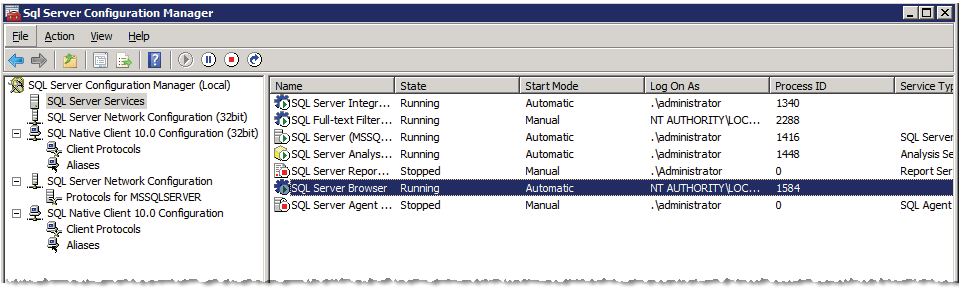


FIGURE 2-16 SQL Server Configuration Manager

3. From the SQL Server Configuration Manager, enable the SQL Server Browser and set the Start Mode to Automatic.
4. Enable the TCP/IP Protocols for MSSQLSERVER, shown in the following figure.

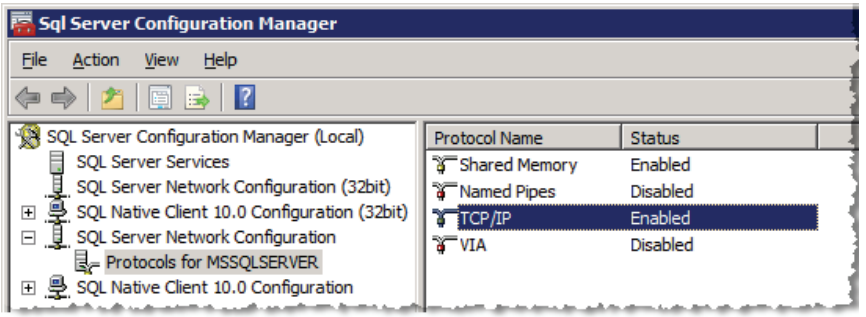


FIGURE 2-17 Enabling the TCP/IP Protocol

5. You can also create an SA or domain user as well. But the SQL server will need to be installed in the Windows Authentication or Mixed Mode for a domain user, and in the Server Authentication or Mixed Mode for an SA user.

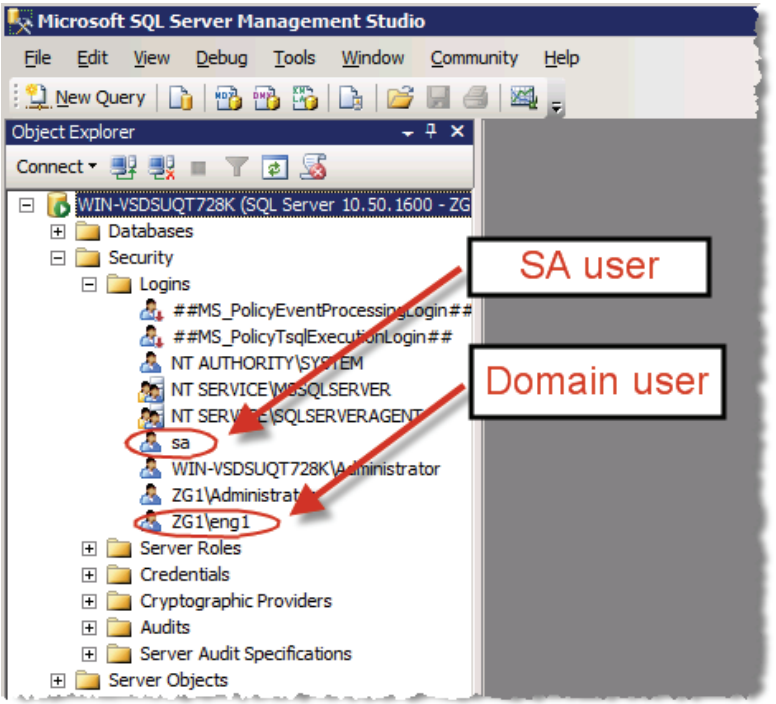


FIGURE 2-18 Windows, Mixed, and Server Authentication Modes

6. In order to set up remote access login properties, you will need to have your **sysadmin** privileges assigned appropriately. Set the server roles similarly to those shown in the following figure.

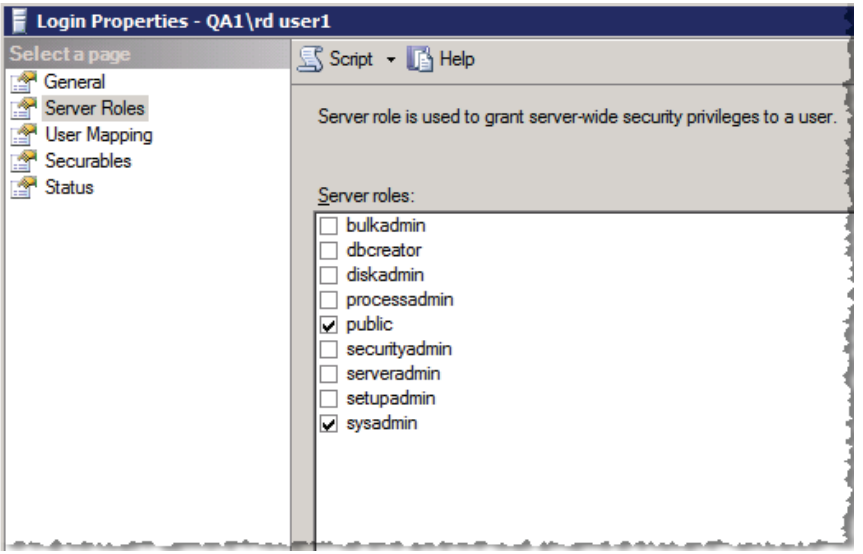


FIGURE 2-19 Security Privileges and Login Properties

7. For Windows Authentication, select the "Windows authentication" button on the Configure Database Server screen. The database server name\Instance might need

to be changed as well, depending on the installed SQL server. See the following figure for more detail.

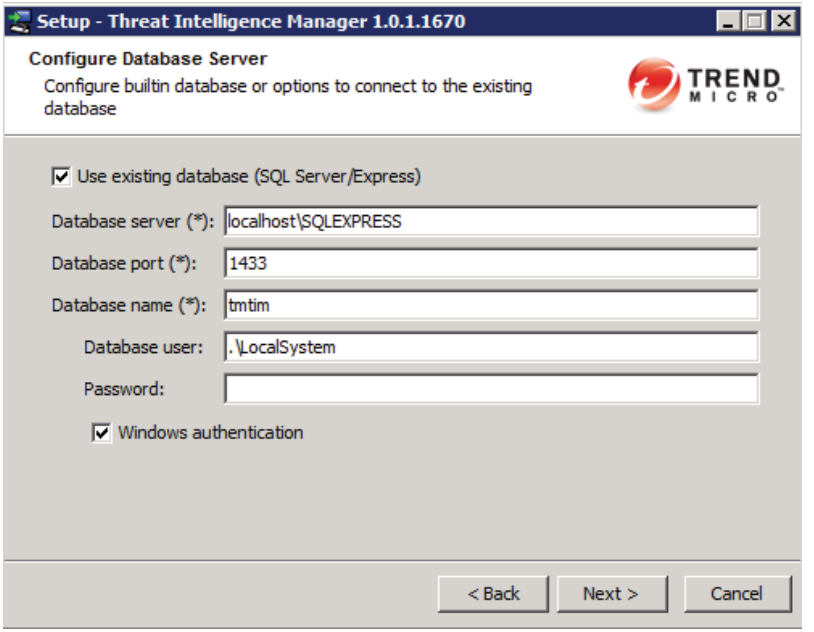


FIGURE 2-20 Windows Authentication Selection

8. For a Server Authentication (SA) user, enter "sa" in the "Database user" box, along with the appropriate user password as shown in the following figure.

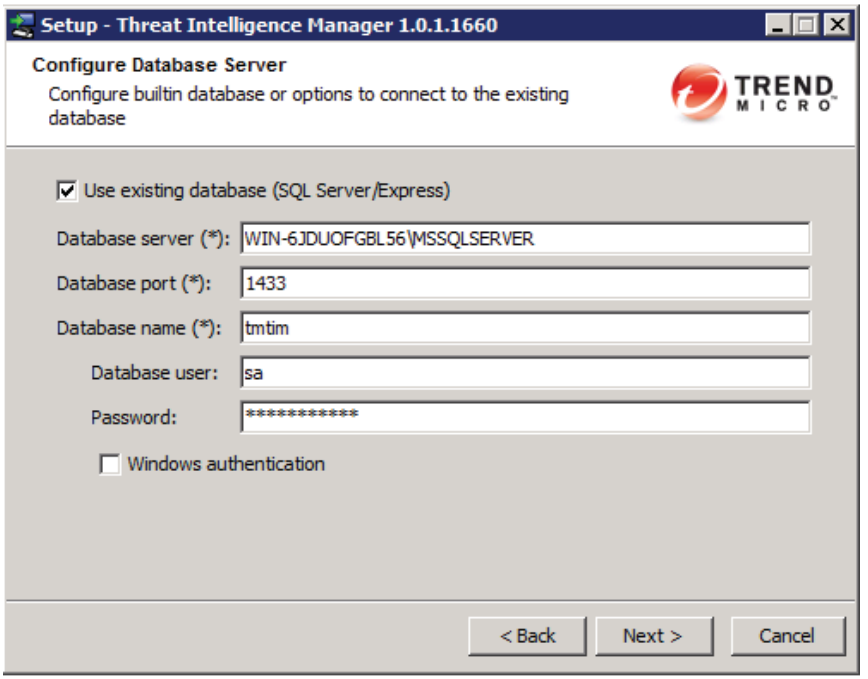


FIGURE 2-21 Server Authentication (SA) Users

The database server name\Instance name might also need to be changed, depending on the installed SQL server.

9. If the database you selected has not yet been created, you can elect to have the installation process create it. The following figure displays the pop-up you will use to create the database.

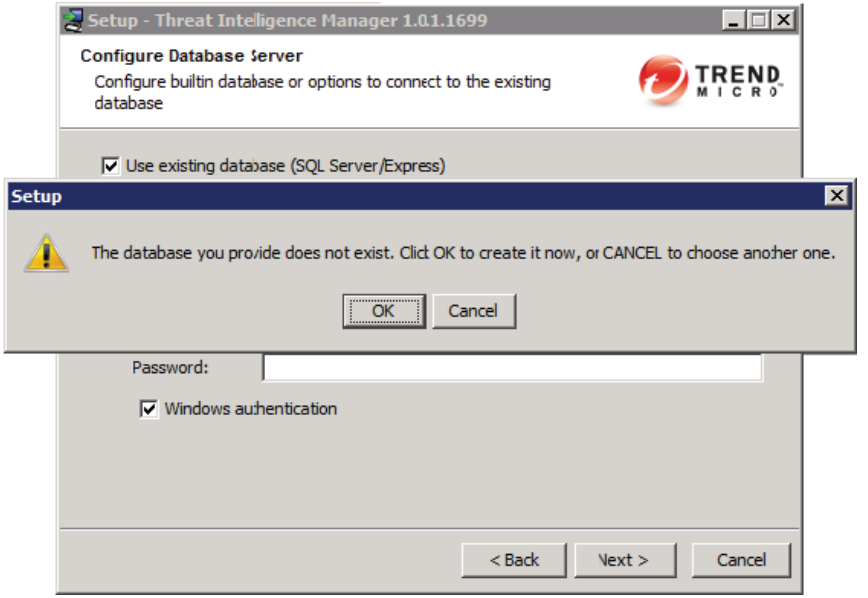


FIGURE 2-22 Creating a New Database

10. If you would like to create a database, click **OK**.

11. The Configure Web Console Port page appears.

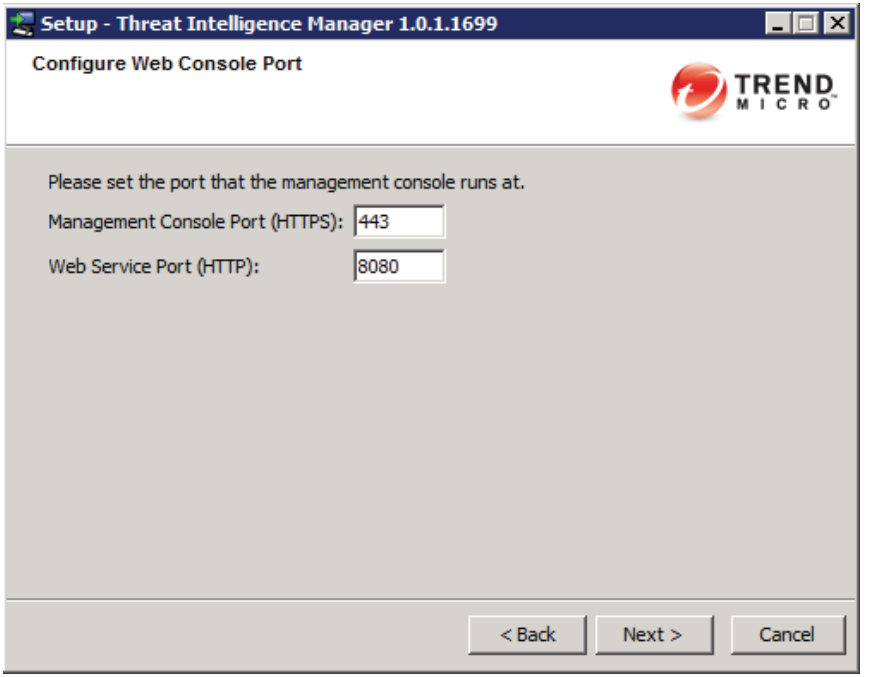


FIGURE 2-23 Configuring the Web Console Port

12. Threat Intelligence Manager supports only the HTTPS protocol in the Web Console. Enter 443 in the first box.
13. The Web Service Port (HTTP) is designed for communication between the front end and the SQL database. Enter 8080 in the second box and click **Next**.

14. The Configure Log Receiver page appears.

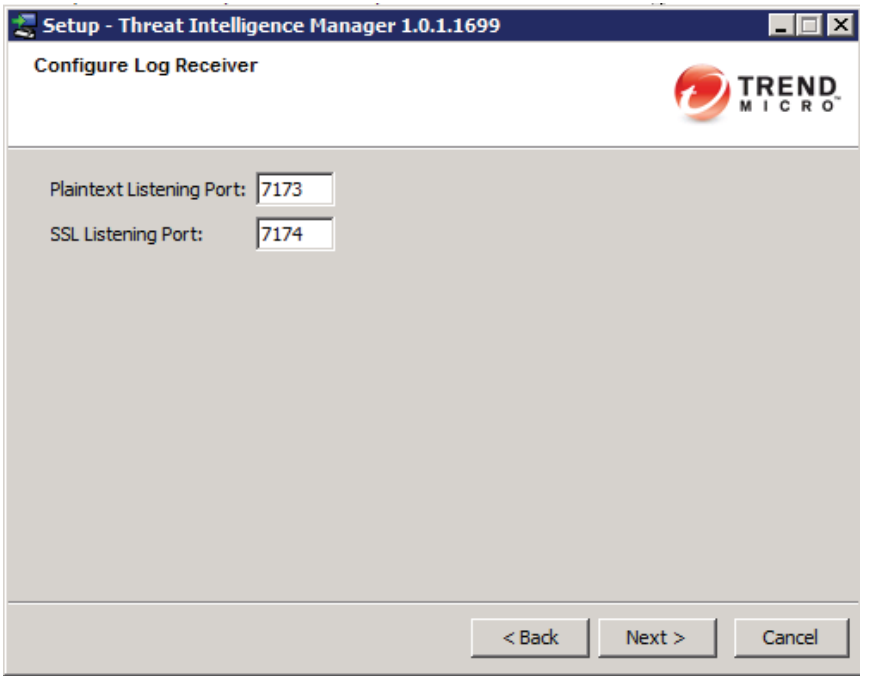


FIGURE 2-24 Configuring the Log Receiver

15. Use the default Plain Text Listening Port of 7173.
16. Use the default SSL Listening Port of 7174. This will create the communication between the agent/concentrator and the server.

17. Click **Next**. The Configure Syslog Receiver page appears.

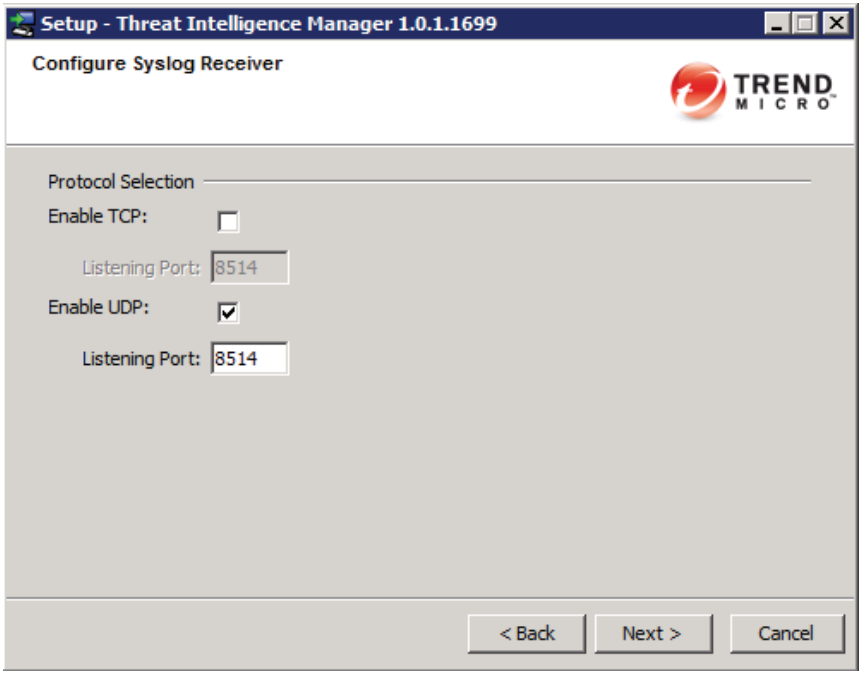


FIGURE 2-25 Configuring the Syslog Receiver

18. Choose between the TCP or UDP protocols depending on your requirements.
19. The default listening port is already set at 8514 for the UDP protocol and will permit communication between your Syslog clients and the server. The UDP port is necessary to upload TDA logs.

20. Click **Next**. The Select Start Menu Folder page appears.

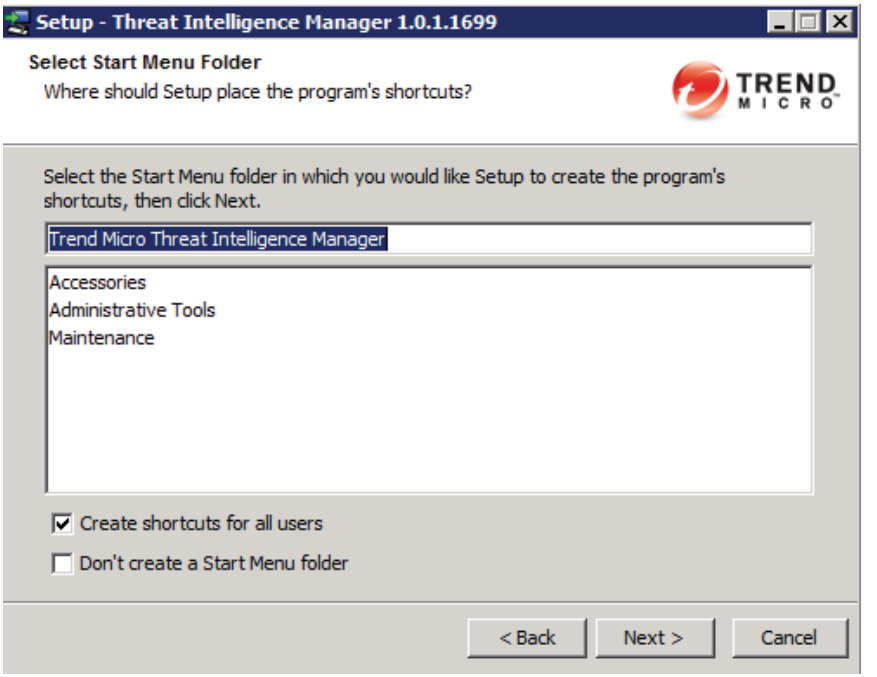


FIGURE 2-26 Selecting the Start Menu Folder

21. Select the Start Menu folder in which you would like Setup to create the program's shortcuts. Click the boxes of the options you would like considered. Click **Next** to continue.

    Setup begins installation on your computer.

Demo Mode Installation

The Installation steps for a Demo Mode Installation are similar to those of the Standard Installation. With the Demo Mode installation, you will complete the following:

- Demo Mode Confirmation
- Install the directory

- Create an administrator account
- Configure a local database if necessary
- Select the Start Menu folder

After selecting the Demo Mode Installation option, you will need to check the agreement box to continue as shown in the following figure.

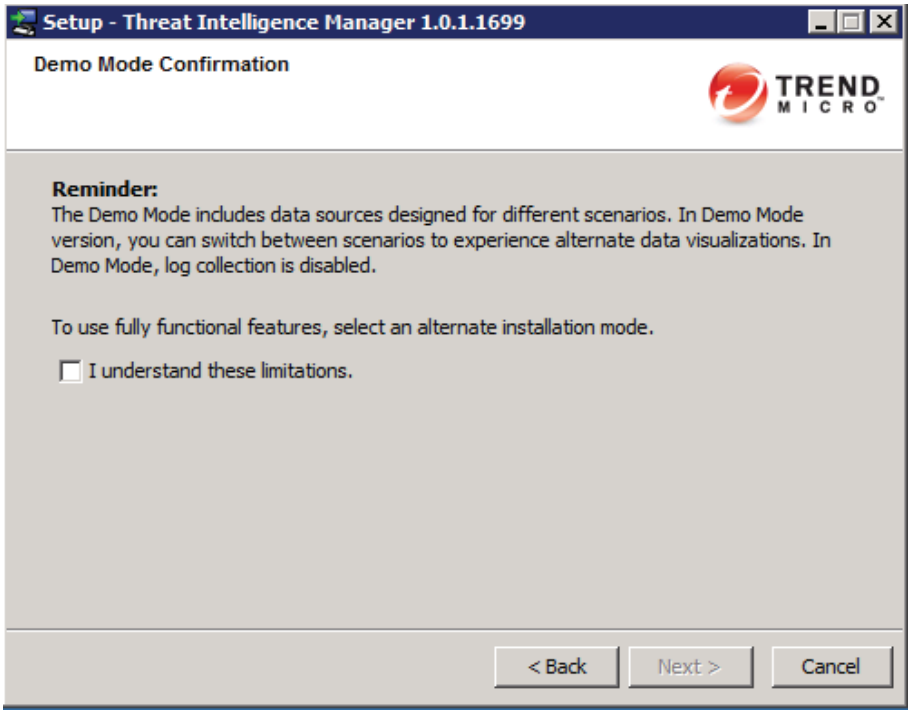


FIGURE 2-27 Demo Mode Confirmation

Click **Next** to continue and step through the Demo Installation as directed.

Configuring the External Ports

External Ports can be accessed externally but you might need to configure a firewall policy for each of them. Most of these ports are configurable during installation, and the

installer will check the port availability during the installation. Some of these ports are L3 documented, however, all ports are manually configurable after installation either through the product console or a .INI file.

The current external ports available are as follows:

- Web Console (installer configurable – default 443)
- Log receiver plain port (installer configurable – default 7173)
- Log receiver SSL port (installer configurable – default 7174)
- Syslog server TCP port (installer configurable – default 8514)
- Syslog server UDP port (installer configurable – default 8514)
- Heartbeat port (L3 configurable – default 5120)

Configuring the Internal Ports

Internal ports are only used on a localhost by Threat Intelligence Manager services and though they are manually configurable, it is not necessary to configure them except for Webservices. For Solr ports, the installer attempts to allocate available port numbers in a predetermined range. For example, the 8900-8910 range is set as the Solr manager ports, and the 8993-9000 range is set for Solr cloud instances.

The current internal ports available are as follows:

- Web services (installer configurable – default 8080)
- Solr Manager port
- SolrCloud instance(s) port
- ZooKeeper port.

Deploying and Installing the Threat Intelligence Manager Log Sources

Log sources can come from several different Trend Products as well as from third-party Syslogs. Depending on the product type, these sources will be handled by different features within the Threat Intelligence Manager, including a standalone agent, a Web

service, or the Syslog server of the Threat Intelligence Manager as shown in the following figure.

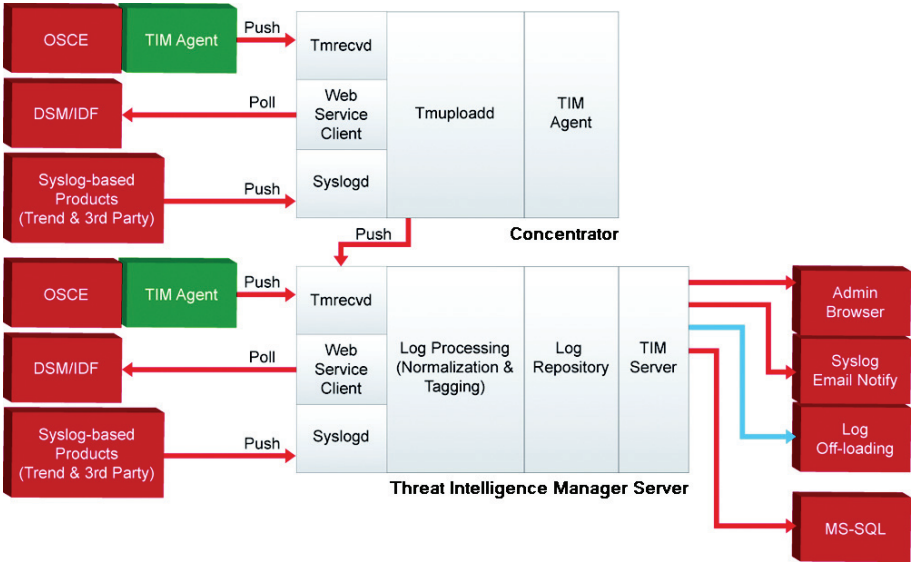


FIGURE 2-28 Overview of Agent/Concentrator/Server

Deploying and Installing the Threat Intelligence Manager Agent

Note: The Threat Intelligence Manager agent will be installed on the same server that the OSCE server resides.

You should next deploy and install the agent on eligible Office Scan products.

Note: Silent installations are supported.

To begin installation, complete the following steps:

1. Execute and install the Threat Intelligence Manager agent package by connecting to the Trend Micro HTTP server, download the Threat Intelligence Manager agent by double-clicking the `TIM-agent-Windows_1_0_0_xxxx_i386.msi` code, where `xxxx` indicates the latest build available from Trend Micro.
2. The Agent Setup Wizard initiates, and the following screen appears.

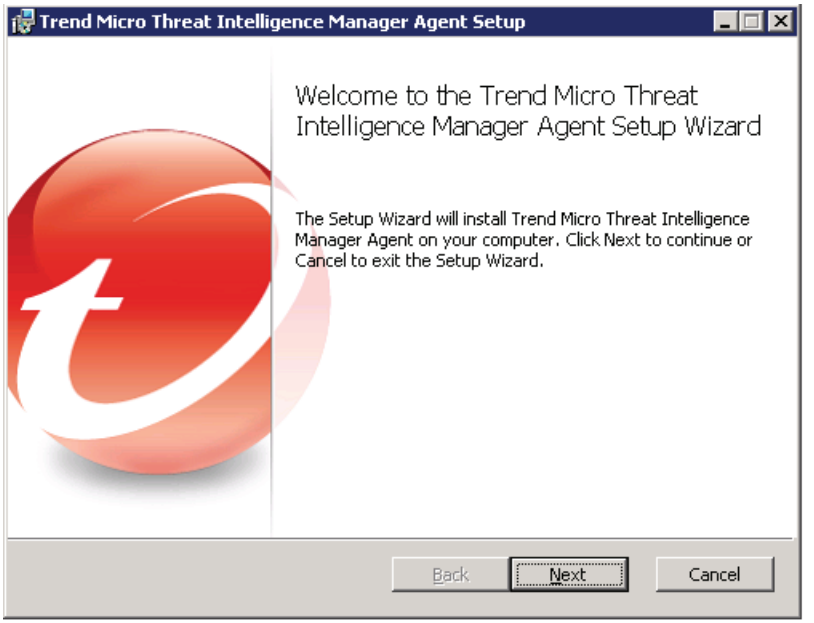


FIGURE 2-29 Agent Setup Wizard

3. Click **Next**.

4. Accept the license agreement by checking the box and the click **Next**.

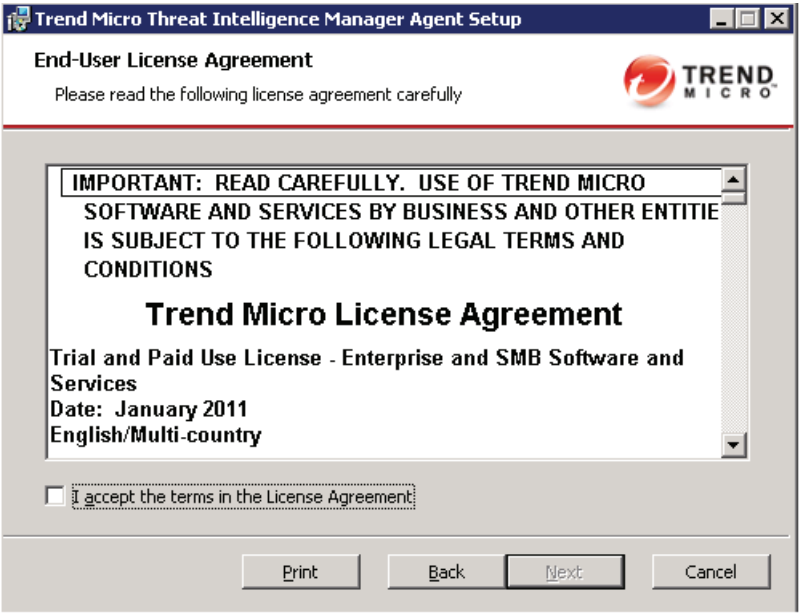


FIGURE 2-30 Accept Agent License Agreement

The Choose Setup Type page appears.

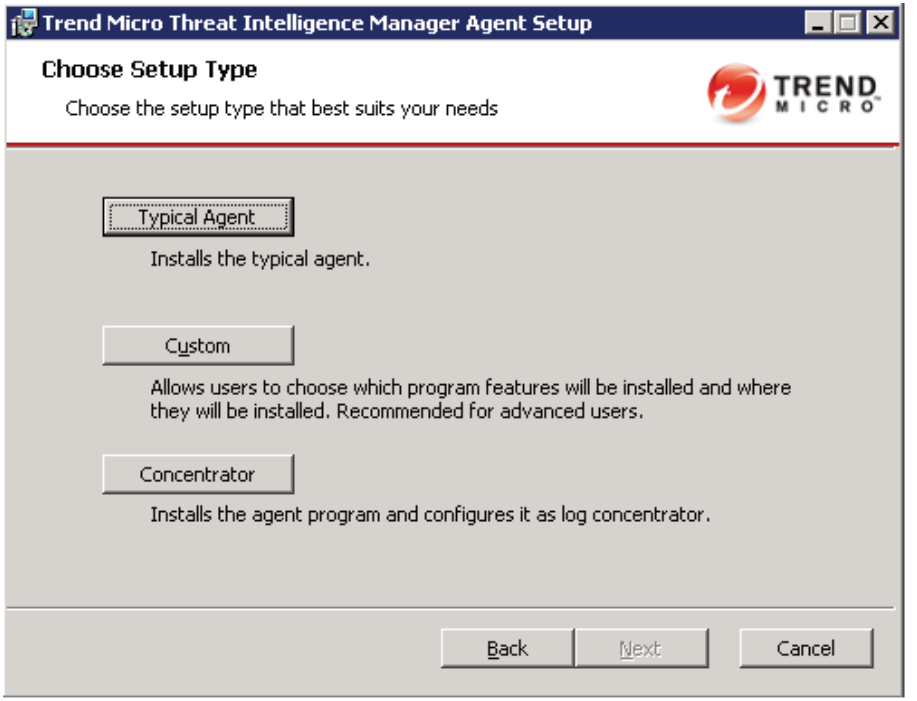


FIGURE 2-31 Choose Setup Type page

5. Select your installment mode from three setup types, depending on your deployment requirements
   a. **Typical Agent**—Agent will be deployed in default location of `C:\Program Files\Trend Micro\Threat Intelligence Manager Agent`.
   b. **Custom Installation**—If this install option is chosen user can install in a non-default location, choose to install agent only, concentrator only or both agent and concentrator.

c. **Concentrator Installation**—Concentrator will be deployed in default location of `C:\Program Files\Trend Micro\Threat Intelligence Manager Agent`.

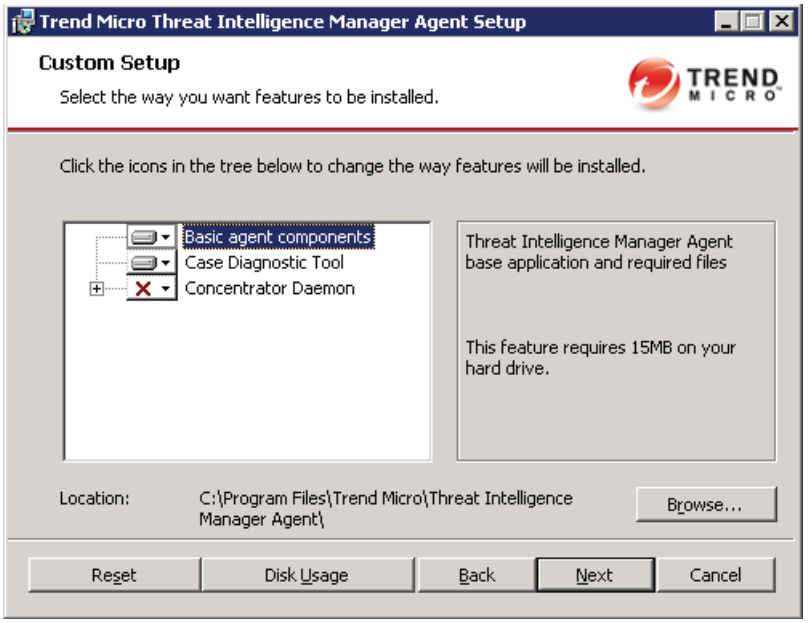


FIGURE 2-32 Custom Installation Selected

6. From Custom Setup screen, users can:
   - Browse to the installation location.
   - Select (or deselect) installation of the agent or concentrator.
   - Reset the screen to default configuration values.
   - Check the Disk Usage to see which available disks have enough space for installation of the agent.
7. Click **Next**.

8. Confirm the installation by clicking **Install**.

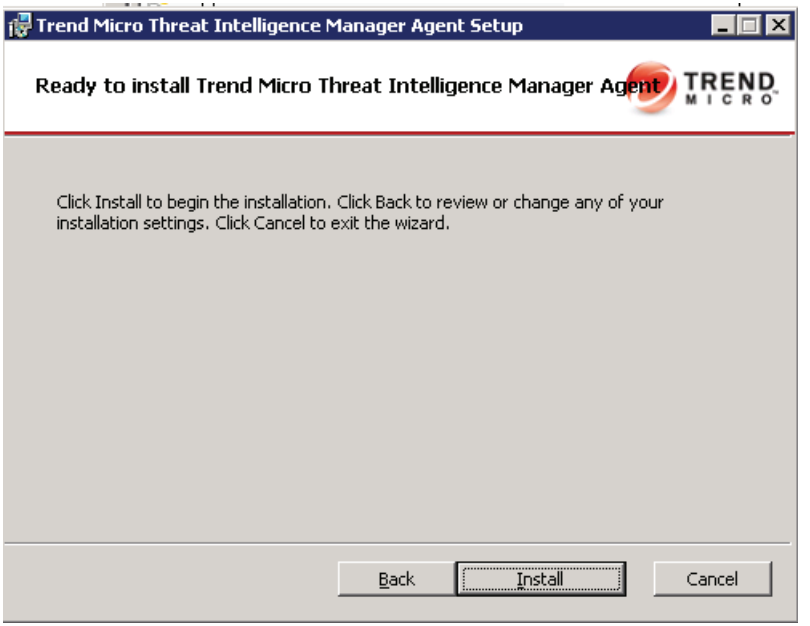


FIGURE 2-33 Click to Confirm the Installation of the Agent

9. Wait while the status screen shows the progress bar for the installation.

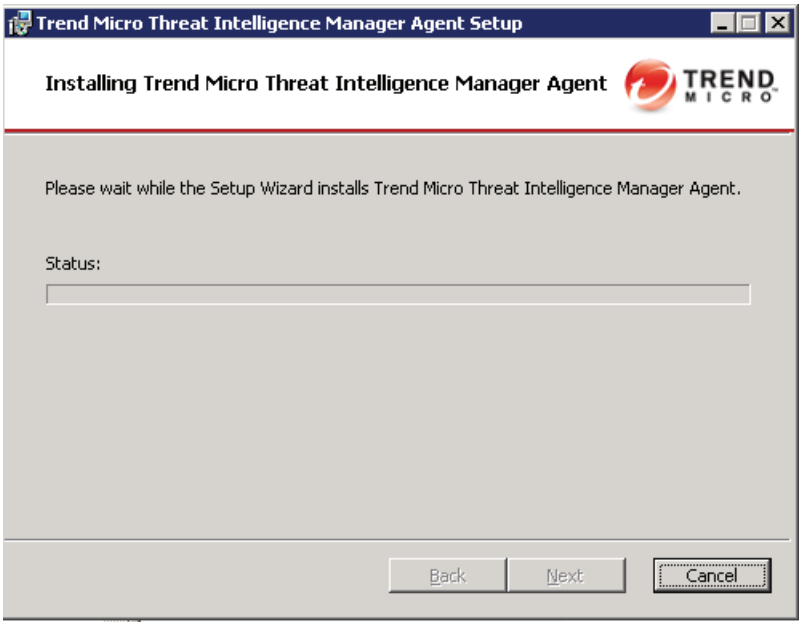


FIGURE 2-34 Status Screen Shows the Agent Installation Progress

Binding the IP Address of Agent

After installing the agent, you may bind the IP addresses for the agent to the Log Receiver ports.

To bind the IP addresses for the agents to the Log Receiver ports (7173/7174):

1. Open the following file:

```
C:\Program Files\Trend Micro\Threat Intelligence
Manager\concentrator\mod\apps\tmrecvd\config\tmrecvd.ini.
```

2. Edit the tmrecvd.ini file as shown in Figure 2-35.

3. Restart the Threat Intelligence Manager Log Receiver.

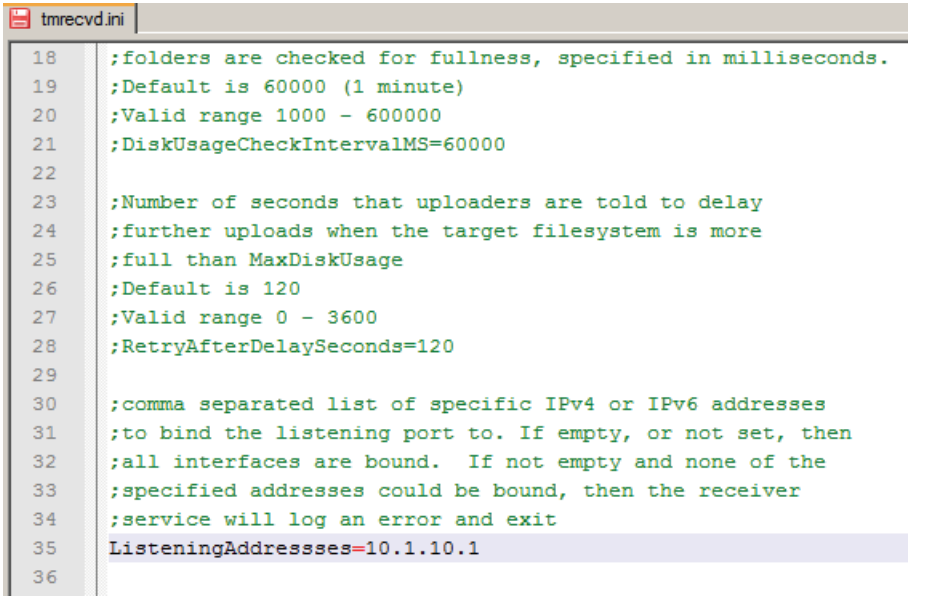


FIGURE 2-35 Binding the IP address of the Log Receiver ports to the agent in the tmrecvd.ini file

Agent Deployment to Managed Products

You can also deploy the agent to other Managed Products through any one of the following methods:

- Manually execute each agent installation individually or use the silent installation with these presets established.
- Use a remote system management tool to distribute and execute the deployment.
- Log on to the managed product machine, and:
  - Insert a CD or USB drive with the Threat Intelligence Manager agent installer.
  - Network transfer the Threat Intelligence Manager agent installer.

Adding Agents to Threat Intelligence Manager

1. Add the agents and managed products as described in the previous sections.
2. Visit **Admin > Log Source**.

To discover an agent:

- Enter an IP to discover installed Threat Intelligence Manager agents.

To activate an agent: (this will detect managed products and start the log collection and management)

The log upload target will be configured during this process.

Enabling and Adding DSM and IDF Web Services

Before adding a Web service, you must enable Web services first on the DSM and/or IDF server.

The following steps describe how to enable and then add Deep Security and IDF Webservices.

To enable the DSM Webservice:

1. Go to the DSM web console at **System > System Settings > System > Web Service API**.
2. Check the **Enabled** radio button.
3. Click **Save**.

To add a Deep Security Webservice:

1. Prior to adding the Deep Security Manager Web service, you must create a Deep Security Manager user that is assigned the WebServiceAPI role. Refer to Deep Security Manager documentation for details on completing this prerequisite.
2. Log in to the Threat Intelligence Management console and go to **Administration > Log Sources**. Select **WebServices**.
3. Define your Webservices clients by clicking **Add**.

   The **Adding New Webservice** window appears.
4. Type and save the required information for:
   - **Type:** DSM
   - **URL:** `https://<hostname/IP>:4119/webservice/Manager`

Note: The default port is 4119. "Manager" must be capitalized. Administrators can configure the DSM port as needed.

- User Name: Previously created on Deep Security Manager. Add the user name and password you use with your Deep Security Manager. The Deep Security role should be configured as a Web Service API user.
- **Password:** Previously created on Deep Security Manager
- **Upload Collected Logs to:** By default, this is the concentrator on the Threat Intelligence Manager server. If you have a collector installed, you can select the location of the collector, and upload your collected logs to that location. The collector concentrator shows the products deployed with DSM.

5. Click **Save**.
6. Check the status column of the Webservices tab to verify the certificate is installed

The connected Webservice Name will appear as an available server source, and include the deployed product, version, and collector used as well as the Webservices status.

To enable the Intrusion Defense Firewall (IDF) Webservice:

1. Open a command prompt window.
2. **cd** to the IDF Add-on installation folder at: `OfficeScan\Addon\Intrusion Defense Firewall`
3. Use the command line to enable IDF Web service.

```
idf_c -action changesetting -name
configuration.webserviceAPIEnabled -value true
```

Note: APIE must be capitalized in the ".webserviceAPIEnabled" portion of the command.

4. Use the username and password under the registry key for the web service.
5. Do the following:
   a. Run: **regedit.**
   b. **HLM > SOFTWARE > Trend Micro > OfficeScan > Addon > IDF**
   c. Value of **IDFUSER** as username.

d. Value of **IDFPASS** as password.

To add the Intrusion Defense Firewall (IDF) Webservice:

1. Prior to adding the Office Scan Intrusion Defense Firewall Web service, the Office Scan server must have installed the Plug-in manager and installed the Intrusion Defense Firewall.
2. Obtain the IDFUSER and IDFPASS from the Office Scan registry key located at:

   `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\Addon\IDF`
3. Log into Threat Intelligence Management console and go to **Administration > Log Sources**. Select **WebServices**.
4. Click **Add**. Type and save the required information for
   - **Type:** IDF
   - **URL:** `https://<hostname/IP>:4119/webservice/Manager`
   - **User Name:** Previously retrieved from the Office Scan registry key in step 3
   - **Password:** Previously retrieved from the Office Scan registry key in step 3
   - **Upload Collected Logs to:** By default, this is the concentrator on the Threat Intelligence Manager server.
5. Check the status column of the Webservices tab to verify the certificate is installed.

Note: If your DSM or IDF accounts are locked out because of multiple login attempts, the steps that follow can be employed to unlock those accounts.

To unlock a DSM account:
Edit the locked out user from the DSM console. Uncheck the lock out option and click Save. See the DSM documentation for additional details if necessary.

To unlock an IDF account:
Use a command prompt to open the IDF installation folder.

Run the following unlock command:

```
idf_c -action unlockout -username Administrator
```

Enabling TDA to Send Logs to Threat Intelligence Manager

Visit the TDA console and configure the TDA Syslog so it is sent to the Threat Intelligence Manager server. Contact your Trend Micro representative to help integrate other third-party Syslogs.

Verifying the Deployments

To verify the various deployments, log on to the Threat Intelligence Manager server console and click the **Investigate** tab. The content on this tab should show all events received over the past few hours including each of the deployments you have configured.

Installation Checklist

Setup prompts you for the following information when you install or upgrade the Threat Intelligence Manager server:

TABLE 2-1. Installation Checklist

INSTALLATION INFORMATION	INFORMATION NEEDED DURING	
	LOCAL/ SILENT FRESH INSTALL	LOCAL/ SILENT UPGRADE
Installation path The default server installation path is: • `C:\Program Files\Trend Micro\Threat Intelligence Manager` Identify the installation path if you choose not to use the default path. If the path does not exist, Setup creates it for you.	Yes	No

TABLE 2-1. Installation Checklist (Continued)

INSTALLATION INFORMATION	INFORMATION NEEDED DURING	
	LOCAL/ SILENT FRESH INSTALL	LOCAL/ SILENT UPGRADE
Proxy server settings If the Threat Intelligence Manager server connects to the Internet through a proxy server, specify the following: • Proxy type (HTTP) • Server name or IP address • Port • Proxy authentication credentials	Yes	No
Administrator account password Setup creates an admin account for Web console logons. Specify the following: • admin account password	Yes	No
Listening Ports **Server: (default)** • TCP 7173 : Log Receiver plain text • TCP 7174 : Log Receiver SSL • TCP/UDP 8514 : Syslog Receiver • TCP 5120 : Server heartbeat • TCP/UDP 8514 : Syslog Receiver • 5119: manager initiates connection **Agent: (default)** • TCP 5118 : Agent heartbeat. • TCP 7173 : Log Receiver plain text. • TCP 7174 : Log Receiver SSL. • TCP/UDP 8514 : Syslog Receiver.		

TABLE 2-1. Installation Checklist (Continued)

INSTALLATION INFORMATION	INFORMATION NEEDED DURING	
	LOCAL/ SILENT FRESH INSTALL	LOCAL/ SILENT UPGRADE
Client installation path Specify the directory on the client computer where the Threat Intelligence Manager client will be installed. Specify the following: • Installation path: The default client installation path is `$ProgramFiles\Trend Micro\Threat Intelligence Manager Client`. Identify the installation path if you choose not to use the default path. If the path does not exist, Setup creates it during client installation. • Client communication port number: Threat Intelligence Manager assigns a fixed port number of 4118.	Yes	No
Program folder shortcut The shortcut to the Threat Intelligence Manager server installation folder displays from the Windows Start menu. The default shortcut name is **Threat Intelligence Manager Server-<Server_name>**. Identify a different name if you do not want to use the default name.	Yes	No

Updating Your Components

Each of the Threat Intelligence Manager components are pocketable. To easily update any one of your components, see any the following sections:

- Updating the Server
- Updating the Agent
- Uninstalling Threat Intelligence Manager
- Uninstalling Threat Intelligence Manager

Updating the Server

To update the server, download and copy the Threat Intelligence Manager server update installer to your Threat Intelligence Manager server and execute the installer file. This update deactivates all services, upgrades the executables, and retains or migrates existing data and logs. To verify the update, access the Threat Intelligence Manager server console and check the current installed version of the Threat Intelligence Manager build number.

Updating the Agent

To update the agent, download and copy the Threat Intelligence Manager agent update installer to your Threat Intelligence Manager server and execute the installer file. This update deactivates all services, upgrades the executables, and retains or migrates existing data and logs. To verify the update, access the Threat Intelligence Manager agent server and check the install version has changed.

Uninstalling Threat Intelligence Manager

To uninstall the Threat Intelligence Management Server product:

1. Use one of the following options:
   a. Go **Control Panel > Programs > Uninstall a program**.

      Locate the Thread Micro Threat Intelligence Manager, click on this program, click on **Uninstall,** and follow the wizard to uninstall.

   b. Go to **Start menu > All Programs > Thread Micro Thread Intelligence Manager - Threat Intelligence Manager Uninstaller** and follow the wizard to uninstall.

WARNING! **If there are Microsoft pending file deletions after uninstall process completes, you may be required to reboot before the Thread Micro Thread Intelligence Manager can be installed on the machine again.**

Chapter 3

Getting Help

This chapter describes troubleshooting issues that might arise and how to contact support for help.

Topics in this chapter:

Troubleshooting Resources

The sections that follow detail some technical information on how and where to obtain general troubleshooting and debug logs for each module. These details should include informative items (such as version and configuration files) as well as controls (such as those found at the control debug level).

The Threat Intelligence Manager server version and build information is available in the following two places:

- In the CurrentVersion registry key found at `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Threat Intelligence Manager`
- In the "`webconf.ini`" file located at `C:\Program Files\Trend Micro\Threat Intelligence Manager\web\htdocs\configs`

The Threat Intelligence Manager server installation path can be obtained by visiting the default Home directory at `C:\Program Files\Trend Micro\Threat Intelligence Manager`. The installation path is also viewable in two locations:

- In the InstallPath registry key found at `HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\Threat Intelligence Manager`
- In the "`webconf.ini`" file located at `C:\Program Files\Trend Micro\Threat Intelligence Manager\web\htdocs\configs`

Installation Logs

Installation logs are located in the Threat Intelligence Manager home directory. There could be one or two logs generated if a failure occurs, or none if the installation completed without failures. The "`install.0.log`" file is created by the "`install4j`" function and if this portion of the installation failed, the "`install.0.log`" file would contain information about that failure. The "`install.1.log`" file would contain error information about failures in the Python script. If the installation was successful, neither of these logs would be present.

If a failure occurs and neither of these logs appear to exist, there is an alternate location where installation logs can be found. In your Temp directory, find either the "`install4j`" file or the Python logs.

For example, go to the location:
`C:\Users\Administrator\AppData\Local\Temp` and search for files with a current time stamp starting with the "`i4j_log`" file.

System and Service Control

The script to stop, start, and check the status of your system services is located in the `C:\Program Files\Trend Micro\Threat Intelligence Manager\bin` directory in a file called the "`tm_ctl`" utility. Using the "`tm_ctl`" utility without parameters produces usage information as follows:

SYNOPSIS

```
[tm_ctl] [ -s service ] [ -h ] [ -v ] command
```

DESCRIPTION

`[tm_ctl]` is a utility for starting, stopping, setting debug levels, or restarting the platform services (Web, DB, Solr, and so on) or displaying the status of running servers. Although the servers can be started manually, `[tm_ctl]` encapsulates tasks such as setting environment variables or work paths.

COMMANDS

`[start] starts the service(s)`

`[stop] stops the service(s)`

`[restart] restarts the service(s) status`

`[status] displays the service(s) status`

`[debug [level]] set/get debug level {OFF, DEBUG, INFO, WARN, ERROR, FATAL}`

OPTIONS

`[-s] service`

Specify the target service name. If the `-s` parameter is used, the command will be performed only for the specified service(s).

`[-h] show this help`

`[-v] verbose mode`

INSTALLED SERVERS

```
['core', 'syslogd', 'web', 'concentrator', 'recvd', 'normd',
'solr']
```

Server Debugging Logs

WARNING! Debugging logs can affect server performance and consume a large amount of disk space. Enable debugging logs only when necessary and promptly disable it if you no longer need debugging data. Remove the log file if the file size becomes huge.

To enable debug logging on a Threat Intelligence Manager server computer, use the `tm_ctl` script previously introduced under System and Service Control on page 3-3.

Option 1: Debugging with the Tomcat Core Service

1. Using the command window, **cd** to **`C:\Program Files\Trend Micro\Threat Intelligence Manager\bin`**

- Run **`tm_ctl -s core debug DEBUG`** or one of the other valid logging levels, which includes: `OFF, DEBUG, INFO, WARN, ERROR, or FATAL` to change to the logging level.

2. Logging level should be returned to `INFO` after debugging is completed.
3. After changing the DebugOption, you should restart the Web service using the **`tm_ctl -s core restart`** command or using Windows services.

Debugging logs for the Apache Tomcat core services can be found in the `C:\Program Files\Trend Micro\Threat Intelligence Manager\tomcat\core\logs` directory.

Option 2: Debugging with the Tomcat Solr Service

To change the debugging level of a Tomcat log:

1. Using the command window, `cd` to **`C:\Program Files\Trend Micro\Threat Intelligence Manager\bin`**
2. Run **`tm_ctl -s solr debug DEBUG`** or one of the other valid logging levels, which include: `OFF, DEBUG, INFO, WARN, ERROR,` or `FATAL` to change to logging level.

3. Logging level should be returned to **INFO** after debugging is completed.
4. After changing the DebugOption, you should restart the Web service using the **tm_ctl –s solr restart** command or restart using windows services.

Debugging logs for the Tomcat Solr services can be found in the `C:\Program Files\Trend Micro\Threat Intelligence Manager\tomcat\solr\logs` directory.

Option 3: Debugging with the Apache Web Service

Using the Apache Web Service, you can debug with any one of the following methods:

- Apache Access/Error Logs

  These logs are located in the `C:\Program Files\Trend Micro\Threat Intelligence Manager\web\logs` folder.
- Apache Debugging Logs

To enable the debugging logs in Apache:

1. Using the command window, **cd** to **C:\Program Files\Trend Micro\Threat Intelligence Manager\bin**
2. Run **tm_ctl -s web debug DEBUG** or one of the other valid logging levels, which include: `OFF, DEBUG, INFO, WARN, ERROR, or FATAL` to change the logging level.
3. Logging level should be returned to `INFO` after debugging is completed.

- Apache Configuration Files

  Apache configuration files are located in the `C:\Program Files\Trend Micro\Threat Intelligence Manager\web\conf` directory.

Option 4: Log Receiver Service (tmrecvd)

Using the Log Receiver Service, you can debug using the following method:

- Log Level Control

To change the debug level for the `tmrecvd` category or the `spnUtil` category:

1. Using the command window, **cd** to **C:\Program Files\Trend Micro\Threat Intelligence Manager\bin**

2. Run **`tm_ctl -s recvd debug DEBUG`** or one of the other valid logging levels, which include: `OFF, DEBUG, INFO, WARN, ERROR, or FATAL` to change the logging level.

- Logging level should be returned to **`INFO`** after debugging is completed.
- After changing the debug level, the `tmrecvd` category needs to be restarted using the "`tm_ctl -s eventd restart`" command. Logs for the `tmrecvd` service can be found in the `C:\Program Files\Trend Micro\Threat Intelligence Manager\log` folder in a file called `tmrecvd.log.0`.

Option 5: Advanced Debugging with a Solr Server

WARNING! **This process should only be attempted by experienced users or by a specific request from the Trend Micro support team.**

- Solr Server

To change the debugging levels of the Solr logs, edit the `logging.properties` file located in the `C:\Program Files\Trend Micro\Threat Intelligence Manager\tomcat\solr\conf` folder.

You can activate logging for respective sections at:

`http://localhost:8983/solr/admin/logging`

If you would like to get the logs for searches or insertions, the following sections should be sufficient:

- `org.apache.solr.search`
- `org.apache.solr.update`
- `org.apache.solr.core`

After changing the debug levels, the Solr service needs to be restarted using the `tm_ctl -s l -s solr restart` command.

Logs for the Solr components can be found in the `C:\Program Files\Trend Micro\Threat Intelligence Manager\tomcat\solr\logs` folder.

- Solr CEF Handler Log

The handler throws exceptions on any errors and does not write any debug log messages. The exceptions are written into Catalina logs. See Option 2: Debugging with the Tomcat Solr Service on page 3-4 for more information.

- Indexer Servelet

The indexer servelet reads configuration information from the `C:\Program Files\Trend Micro\Threat Intelligence Manager\conf\tmplatf.ini` location. The file insert status is maintained in a file located in the `C:\Program Files\Trend Micro\Threat Intelligence Manager\tomcat\solr\indexer_work\UpdateProgress.txt` folder.

The indexer logs are written into the `C:\Program Files\Trend Micro\Threat Intelligence Manager\tomcat\solr\logs` folder.

Option 6: Debugging the Threat Intelligence Manager Server Log with Middleware

You can debug Threat Intelligence Manager with Middleware.

Complete the following steps:

1. Configure the log level in the "`logger.ini`" file located in the `\Trend Micro\Threat Intelligence Manager\web\htdocs\middleware_rev\lib\logger\logger.ini` folder.
2. Find and configure the `zg_middleware.log` file located in the `\Trend Micro\Threat Intelligence Manager\web\logs\` folder.

   You can configure the debugging log manually, as shown in the following configuration file:

   `<Threat Intelligence Manager Installation Root>\Threat Intelligence Manager\web\htdocs\middleware_rev\lib\logger\logger.ini`

   or from the default location at `C:\Program Files\Trend Micro\Threat Intelligence Manager\web\htdocs\middleware_rev\lib\logger`

Middleware Debugging Levels

The Middleware log levels can be used to set the system logging levels. If the log level of a particular message is less than or equal to the system log level, the message can be logged. If it is greater, the message will not be logged.

The following table shows the definition of these log levels.

TABLE 3-2. Middleware Debugging Log Level Definitions

DEFINITION	VALUE	DESCRIPTION
ZG_LOG_EMERG	0	The system is unusable.
ZG_LOG_ALERT	1	Immediate action is required.
ZG_LOG_CRIT	2	Critical conditions
ZG_LOG_ERR	3	Error conditions
ZG_LOG_WARNING	4	Warning conditions
ZG_LOG_NOTICE	5	Normal but significant
ZG_LOG_INFO	6	Informational
ZG_LOG_DEBUG	7	Debug-level messages
ZG_LOG_ALL	0xFFFFFFFF	All messages
ZG_LOG_NONE	0x00000000	No message

You can also set the `level = "ZG_LOG_ALL"` variable in the `logger.ini` file.

Debugging Methods

You can set different debugging methods to log at the same time or disable the log methods you do not want to use by placing semicolons in front of the unwanted method.

For example, in the "`logger.ini`" file, the default method is set to create a log within a file as indicated in the third line:

```
; [Logging Methods]
; The logging methods are used when we log messages.
method[] = "file"
; method[] = "display"
```

```
; method[] = "firebug"
; method[] = "window"
```

Note: The location of the debug file is forced-set in the "<TIM Installation Root>\Threat Intelligence Manager\web\logs\zg_middleware.log" folder for this ETAP release.

WARNING! If you set the file method to debug, the file continues growing until it is deleted.

Debugging the Logs of the Threat Intelligence Manager Map Widget

The Threat Intelligence Manager map widget has its own debugging log. After this widget has been loaded, the debug log generates automatically.

Complete the following steps to locate the Map Widget debugging log:

1. Search for the "Detection_Map_Log" folder under the C:\ directory.
2. You will find the yyyymmdd.txt file (ex. 20110111.txt) within the "Detection_Map_Log" folder. This file contains the debugging log of the Threat Intelligence Manager map.

Agent Debugging Logs

You can also enable debugging logs before installing the Threat Intelligence Manager agent by using msiexec command line options. Visit Microsoft Support for more information on these options.

WARNING! Debugging logs might affect agent performance and consume a large amount of disk space. Enable debugging logs only when necessary and promptly disable it if you no longer need the debugging data. Remove the log file when the file size begins to grow.

Threat Intelligence Manager Agent Debugging Logs

To enable debug logging on a Threat Intelligence Manager agent computer, see the Threat Intelligence Manager agent debug log in the `C:\Program Files\Trend Micro\Threat Intelligence Manager Agent\log\timagent.log.0` folder.

The file to change the debugging level of the Threat Intelligence Manager agent is the "`logging.xml`" file located in the `C:\Program Files\Trend Micro\Threat Intelligence Manager Agent\config\log` folder. The output will appear as follows:

```
<category name="spnSchema" priority="debug"
appender="myrollingfileappender"/>

<category name="spnUtil" priority="debug"
appender="myrollingfileappender"/>

<category name="osce_dll_bridge" priority="debug"
appender="myrollingfileappender"/>

<category name="zgIntegrationMgr" priority="debug"
appender="myrollingfileappender"/>
```

Log Extraction (tmgetlog.exe)

- Log Extraction Logs

The "`tmgetlog.exe`" file is located in the `C:\Program Files\Trend Micro\Threat Intelligence Manager Agent\log\tmgetlog.log.0` folder.

- Log Extraction Configuration

The file to change the debugging level of the "`tmgetlog.exe`" file is the "`tmgetlog.xml`" file located in the `C:\Program Files\Trend Micro\Threat Intelligence Manager Agent\mod\apps\timagent\conf` folder.

```
<category name="tmgetlog" priority="debug"
appender="myrollingfileappender"/>

<category name="spnUtil" priority="debug"
appender="myrollingfileappender"/>

<category name="getlog" priority="debug"
appender="myrollingfileappender"/>
```

Log Uploader (tmupload.exe)

- Uploader Log

The "`tmupload.exe`" log file is located in the `C:\Program Files\Trend Micro\Threat Intelligence Manager Agent\log\tmupload.log.0` folder.

- Uploader Configuration

The file to change debugging level of the "`tmupload.exe`" file is the "`tmupload.xml`" file located in the `C:\Program Files\Trend Micro\Threat Intelligence Manager Agent\mod\apps\timagent\conf` folder.

```
<category name="tmupload" priority="debug"
appender="myrollingfileappender"/>

<category name="spnUtil" priority="debug"
appender="myrollingfileappender"/>
```

Log Uploader Queue (tmupload)

The location of the logs waiting to be uploaded to the Threat Intelligence Manager receiver are located in the `C:\Program Files\Trend Micro\Threat Intelligence Manager Agent\workflow\normlog` folder.

Case Diagnostic Tool

Trend Micro Case Diagnostic Tool (CDT) collects necessary debugging information from a customer's product whenever problems occur. When running the utility, it automatically turns the product's debug status on and off and collects necessary files according to problem categories. Trend Micro uses this information to troubleshoot problems related to the product.

The tool (CaseDiagnosticTool.exe) is located in the <install directory>\cdt folder. Right-click and open the file to start the tool. Follow the directions to completion and send the zip file that is created to Trend Micro support team.

Contacting Trend Micro

Technical Support

Trend Micro provides technical support, pattern downloads, and program updates for one year to all registered users, after which you must purchase renewal maintenance. If you need help or just have a question, feel free to contact us. We also welcome your comments.

Trend Micro Incorporated provides worldwide support to all registered users.

- Get a list of the worldwide support offices at:

  http://www.trendmicro.com/support

- Get the latest Trend Micro product documentation at:

  http://downloadcenter.trendmicro.com/

In the United States, you can reach the Trend Micro representatives by phone, fax, or email:

Trend Micro, Inc.

10101 North De Anza Blvd., Cupertino, CA 95014

Toll free: +1 (800) 228-5651 (sales)

Voice: +1 (408) 257-1500 (main)

Fax: +1 (408) 257-2003

Web address:

http://www.trendmicro.com

Email: support@trendmicro.com

Speeding Up Your Support Call

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

- Microsoft Windows and Service Pack versions
- Network type
- Computer brand, model, and any additional hardware connected to your computer

- Amount of memory and free hard disk space on your computer
- Detailed description of the install environment
- Exact text of any error message given
- Steps to reproduce the problem

The Trend Micro Knowledge Base

The Trend Micro Knowledge Base, maintained at the Trend Micro Web site, has the most up-to-date answers to product questions. You can also use Knowledge Base to submit a question if you cannot find the answer in the product documentation. Access the Knowledge Base at:

http://esupport.trendmicro.com

Trend Micro updates the contents of the Knowledge Base continuously and adds new solutions daily. If you are unable to find an answer, however, you can describe the problem in an email and send it directly to a Trend Micro support engineer who will investigate the issue and respond as soon as possible.

TrendLabs

TrendLabs™ is the global antivirus research and support center of Trend Micro. Located on three continents, TrendLabs has a staff of more than 250 researchers and engineers who operate around the clock to provide you, and every Trend Micro customer, with service and support.

You can rely on the following post-sales service:

- Regular virus pattern updates for all known "zoo" and "in-the-wild" computer viruses and malicious codes
- Emergency virus outbreak support
- Email access to antivirus engineers
- Knowledge Base, the Trend Micro online database of technical support issues

TrendLabs has achieved ISO 9002 quality assurance certification.

Documentation Feedback

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

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

Appendix A

Using a Remote/Existing Database for Installation

This appendix provides information about performing the Threat Intelligence Manager installation with a remote or existing database.

Topics in this appendix include:

Prerequisites

If using a remote or existing database you must first have the database installed and ready to accept TCP/IP connections. The user account used to perform the installation must have been previously created, enabled, and set with the proper permissions.

Configuring a Remote/Existing Database for Threat Intelligence Manager

To use a remote or existing database:

1. Using Microsoft's SQL Server 2008 R2 Management Studio, add the domain or local administrator to control the Thread Micro Threat Intelligence Manager.
2. Add the new login account in the **Security > Logins** folder shown in *Figure A-1*.

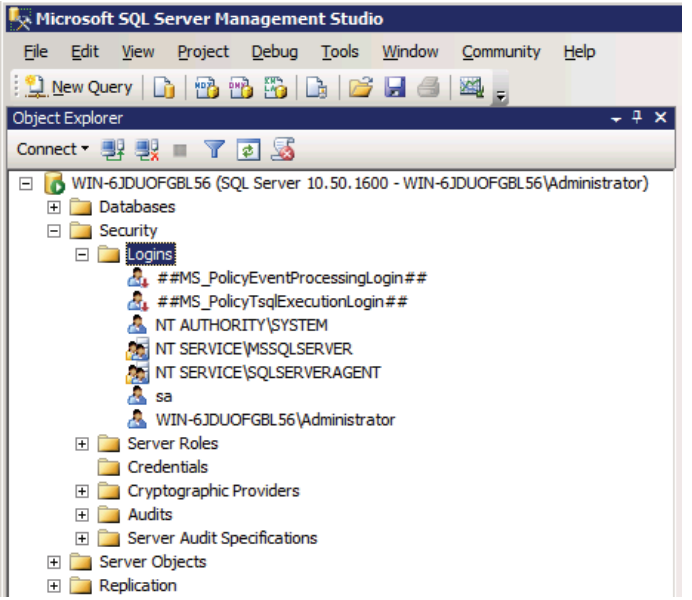


FIGURE A-1. SQL Server Management Studio—Security > Logins folder

3. Give the new login account system administrator privileges under the Server Roles section shown in *Figure A-2*.

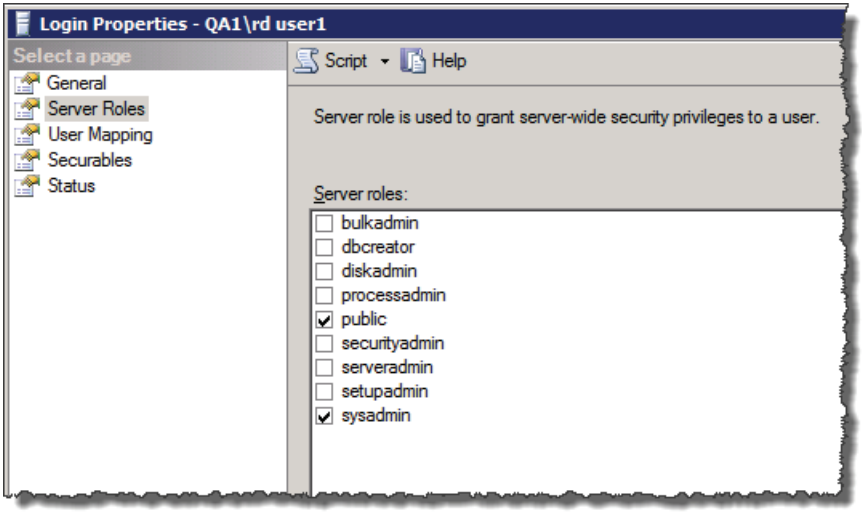


FIGURE A-2. Add System Administrator Privileges

4. Open the Microsoft SQL Server Configuration Manager.

5. Under the SQL Server Services, enable the SQL Server Browser and set the Start Mode to automatic as shown in *Figure A-3*.

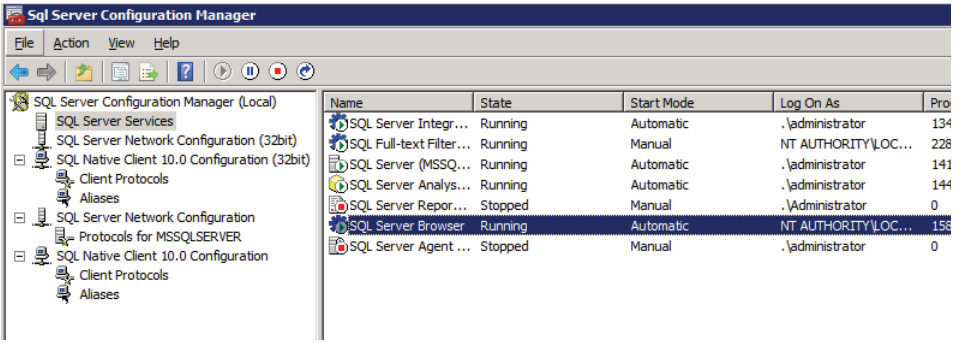


FIGURE A-3. Enable the Browser and Set the Mode

6. Enable all of the TCP/IP protocols as shown in *Figure A-4*.

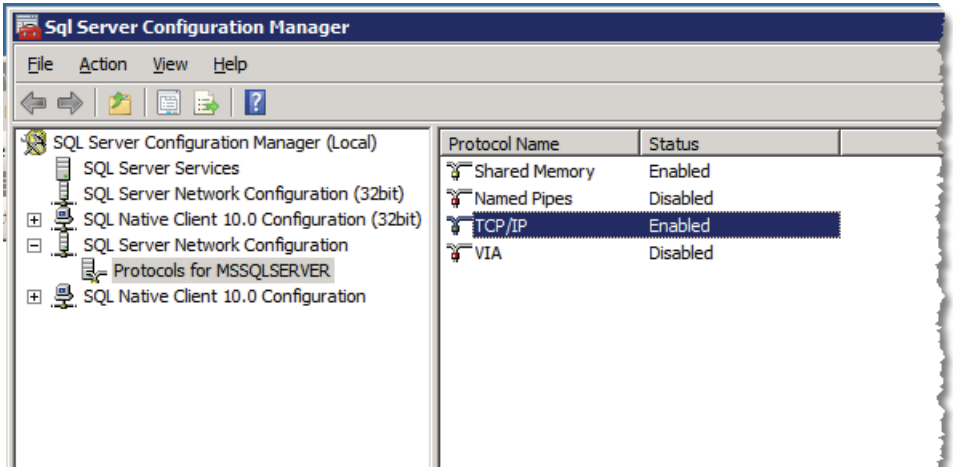


FIGURE A-4. Enable all TCP/IP Protocols

7. Restart the SQL server to ensure changes take effect.

Configuring Your Authentication Method

During a custom installation, select from the following authentication methods for the remote or existing database:

- Windows authentication using LocalSystem
- SQL authentication
- Windows authentication (local or domain user) to connect to a remote or existing database

To configure the authentication method:

1. Check the Windows authentication box and add \LocalSystem as the database user to use a local existing database and Windows authentication. See *Figure A-5*.

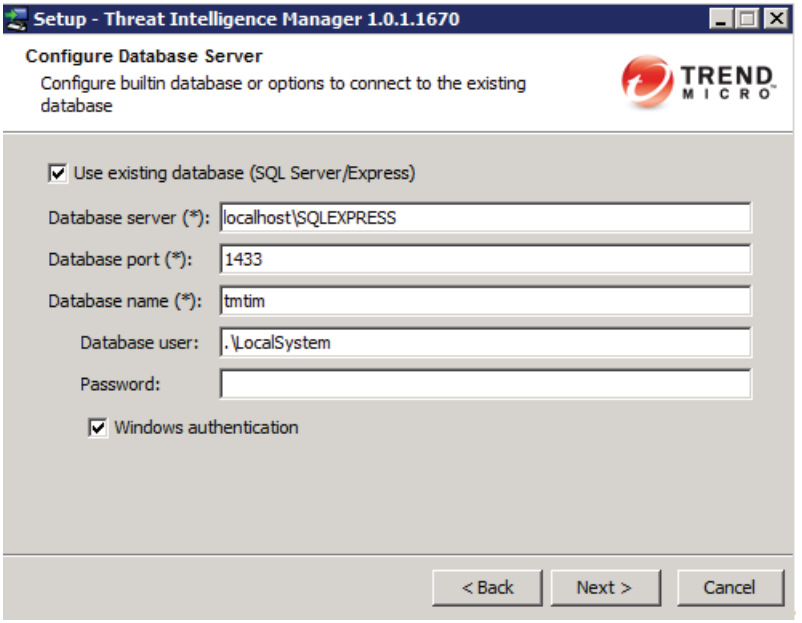


FIGURE A-5. Use a Local Database with Window Authentication

2. For SQL authentication, leave the Windows authentication box unchecked, enter the sa user name and password, and then click **Next**. See *Figure A-6*.

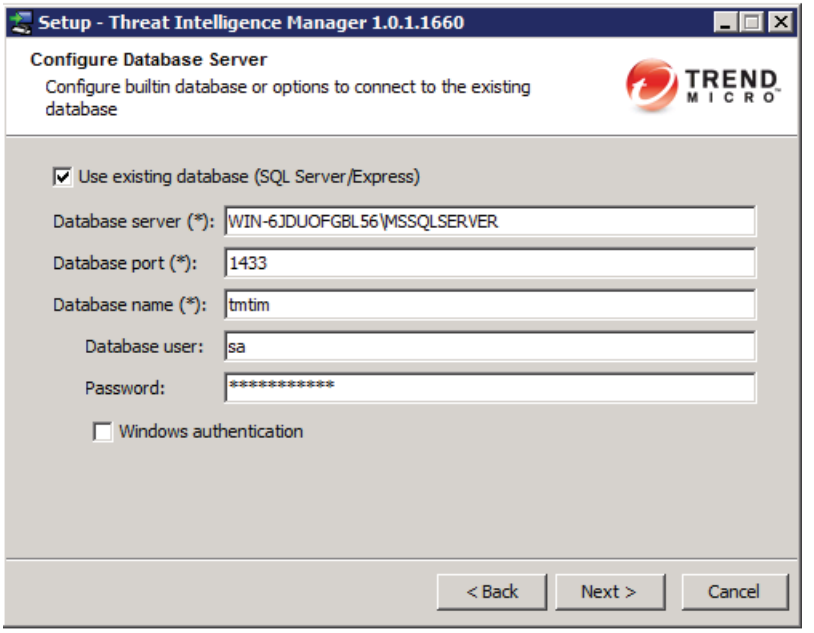


FIGURE A-6. Configuration for Using SQL Authentication

3. To use a domain user, enter the domain name, user name, and password. Check the Windows authentication box, and then click **Next**. See *Figure A-7*.

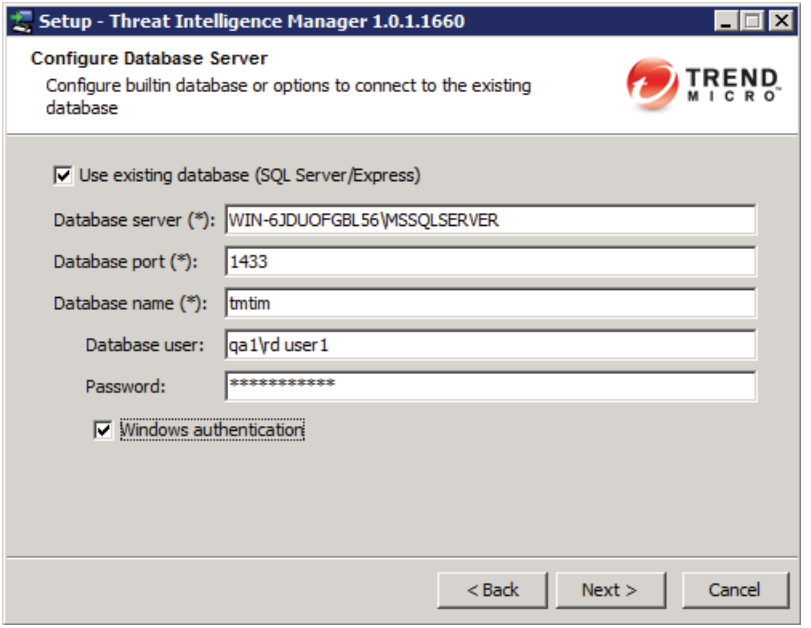


FIGURE A-7. Setting an Authentication Method for a Local User on an Database Existing Locally

4. During a standard installation, if installation detects a database already installed on the local machine, the installation script will ask user to use the local database for installation and require user to provide one of the three installation types shown in *Figure 2-7*.