2.0

TREND MICRO™
Safe Lock Intelligent Manager
Installation Guide

A powerful lockdown solution for fixed-function computers

Endpoint Security

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

http://docs.trendmicro.com/en-us/enterprise/trend-micro-safe-lock.aspx

Document Part No.: SLEM26725/141016

Release Date: December 2014

Protected by U.S. Patent No.: Patents pending.

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

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

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

Evaluate this documentation on the following site:

http://docs.trendmicro.com/en-us/survey.aspx

Table of Contents

Chapter 3: Intelligent Manager Installation

Chapter 4: Intelligent Manager Uninstallation

Chapter 5: Technical Support

Index

Preface

This Installation Guide introduces Trend Micro Safe Lock Intelligent Manager and guides administrators through installation and deployment.

Topics in this chapter include:

About the Documentation

Trend Micro Safe Lock Intelligent Manager documentation includes the following:

TABLE 1. Trend Micro Safe Lock Intelligent Manager Documentation

DOCUMENTATION	DESCRIPTION
Installation Guide	A PDF document that discusses requirements and procedures for installing Safe Lock Intelligent Manager.
Administrator's Guide	A PDF document that discusses getting started information and Safe Lock Intelligent Manager usage and management.
Readme file	Contains a list of known issues. It may also contain late-breaking product information not found in the 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

Audience

Trend Micro Safe Lock Intelligent Manager documentation is intended for administrators responsible for Safe Lock Intelligent Manager management, including agent installation. These users are expected to have advanced networking and server management knowledge.

Document Conventions

The following table provides the official terminology used throughout the Trend Micro Safe Lock Intelligent Manager documentation:

TABLE 2. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
Italics	References to other documents
`Monospace`	Sample command lines, program code, web URLs, file names, and program output
Navigation > **Path**	The navigation path to reach a particular screen For example, **File** > **Save** means, click **File** and then click **Save** on the interface
Note	Configuration notes

CONVENTION	DESCRIPTION
Tip	Recommendations or suggestions
Important	Information regarding required or default configuration settings and product limitations
WARNING!	Critical actions and configuration options

Terminology

The following table provides the official terminology used throughout the Trend Micro Safe Lock Intelligent Manager documentation:

TABLE 3. Safe Lock Intelligent Manager Terminology

TERMINOLOGY	DESCRIPTION
Server	The Safe Lock Intelligent Manager server program
Server endpoint	The host where the Safe Lock Intelligent Manager server is installed
Agents	The hosts running the Safe Lock program
Managed agents Managed endpoints	The hosts running the Safe Lock program that are known to the Safe Lock Intelligent Manager server program
Target endpoints	The hosts where the Safe Lock Intelligent Manager managed agents will be installed
Administrator (or Safe Lock Intelligent Manager administrator)	The person managing the Safe Lock Intelligent Manager server

TERMINOLOGY	DESCRIPTION
Web console	The user interface for configuring and managing Safe Lock Intelligent Manager settings and managed agents
CLI	Command line interface
License activation	Includes the type of Safe Lock Intelligent Manager server installation and the allowed period of usage that you can use the application
Agent installation folder	The folder on the host that contains the Safe Lock Intelligent Manager agent files. If you accept the default settings during installation, you will find the installation folder at the following location: `"c:\Program Files\Trend Micro\Safe Lock"`
Server installation folder	The folder on the host that contains the Safe Lock Intelligent Manager server files. If you accept the default settings during installation, you will find the installation folder at the following location: `"c:\Program Files\Trend Micro\Safe Lock Intelligent Manager"`

Chapter 1

Introduction

Trend Micro Safe Lock Intelligent Manager delivers a simple, no-maintenance solution to lock down and protect fixed-function computers, helping protect businesses against security threats and increase productivity.

Topics in this chapter include:

- *About Trend Micro Safe Lock Intelligent Manager on page 1-2*

- *About Trend Micro Safe Lock on page 1-7*

About Trend Micro Safe Lock Intelligent Manager

Trend Micro Safe Lock Intelligent Manager provides centralized monitoring and management of Trend Micro Safe Lock agent deployment, status, and events. For example, administrators can remotely deploy agents, deploy initial agent Approved Lists, and change agent Application Lockdown states. Additionally, Safe Lock Intelligent Manager performs malware scans and administrators can view root cause information on files blocked from running by Safe Lock agents, reducing the time and effort needed to verify events and allowing quick responses to incidents.

Server Features and Benefits

Trend Micro Safe Lock Intelligent Manager includes the following features and benefits.

TABLE **1-1. Features and Benefits**

FEATURE	BENEFIT
Dashboard	The web console dashboard provides summarized information about monitored Safe Lock agents. Administrators can check deployed Safe Lock agent status easily, and can generate security reports related to Safe Lock agent activity for specified periods.
Centralized Agent Management	Administrators can monitor Safe Lock agent status, examine connection status, view configurations, collect agent logs on-demand or by policy, and remotely turn agent Application Lockdown on or off.
Centralized Event Management	On endpoints protected by Safe Lock agents, administrators can monitor events and status and respond when files are blocked from running. Safe Lock Intelligent Manager provides event management features that let administrators know about blocked file events quickly and allows them to manage these events. For example, events can be marked open or closed for tracking, and the detailed event information needed to resolve events can be collected quickly and easily.

FEATURE	BENEFIT
Root Cause Information Analysis	When blocked file events happen, administrators can determine if they are the result of a significant incident or not. Safe Lock Intelligent Manager provides malware scanning features and root cause information and diagrams to help administrators investigate blocked files quickly. For example, administrators can check if a blocked file is required to launch a mission-critical program, or if the blocked file is detected as malware. Administrators can also learn where blocked files are run from and what process launched them.
Server Event Auditing	Operations performed by Safe Lock Intelligent Manager web console accounts are logged. Safe Lock Intelligent Manager records an operating log for each account, tracking who logs on, who deletes event logs, and more.

Safe Lock Intelligent Manager Requirements

> **Important**
>
> Trend Micro Safe Lock Intelligent Manager has specific requirements that vary based on other software running on the server endpoint.

TABLE 1-2. Required Software for Safe Lock Intelligent Manager

REQUIRED SOFTWARE	SPECIFICATIONS
Operating systems	• Windows XP SP2/SP3 (32-bit)
	• Windows 7 Enterprise (Ultimate) No-SP/SP1 (32-bit and 64-bit)
	• Windows 8 Enterprise No-SP (32-bit and 64-bit)
	• Windows 8.1 Enterprise No-SP (32-bit and 64-bit)
	• Windows Server 2003 No-SP/SP1/SP2 (32-bit and 64-bit)
	• Windows Server 2003 R2 No-SP/SP2 (32-bit and 64-bit)
	• Windows Server 2008 SP1/SP2 (32-bit and 64-bit)
	• Windows Server 2008 R2 No-SP/SP1 (64-bit)
	• Windows Server 2012 No-SP (64-bit)
	• Windows Server 2012 R2 No-SP (64-bit)
Web browser (for Safe Lock Intelligent Manager web console access)	• Microsoft Internet Explorer 7 or later
	• The latest version of Google Chrome
	• The latest version of Mozilla Firefox

TABLE 1-3. Required Hardware for Safe Lock Intelligent Manager (without Safe Lock agent)

REQUIRED HARDWARE	SPECIFICATION
RAM	• 2GB minimum
	• 4GB or more recommended
Processor	• 1 CPU core minimum
	• 1 CPU core or more recommended
Available disk space	• 10GB minimum
	• 20GB or more recommended

TABLE 1-4. Required Hardware for Safe Lock Intelligent Manager (with Safe Lock agent)

REQUIRED HARDWARE	SPECIFICATION
RAM	• 2GB minimum • 4GB or more recommended
Processor	• 1 CPU core minimum • 2 CPU cores or more recommended
Available disk space	• 10GB minimum • 20GB or more recommended

TABLE 1-5. Required Hardware for Safe Lock Intelligent Manager (with or without Safe Lock agent) + SQL Express 2008

REQUIRED HARDWARE	SPECIFICATION
RAM	• 4GB minimum • 8GB or more recommended
Processor	• 1 CPU core minimum • 2 CPU cores or more recommended
Available disk space	• 30GB minimum • 50GB or more recommended

TABLE 1-6. Required Hardware for Safe Lock Intelligent Manager (with or without Safe Lock agent) + SQL Server

REQUIRED HARDWARE	SPECIFICATION
RAM	• 32GB or more required
Processor	• 2 CPU cores minimum • 4 CPU cores or more recommended
Available disk space	• 1TB minimum • 2TB or more recommended

Server Accounts Overview

Trend Micro Safe Lock Intelligent Manager features web console accounts with different privileges and limitations. Use these accounts to configure Safe Lock Intelligent Manager and to monitor or manage Safe Lock agents.

The following table outlines typical Safe Lock Intelligent Manager tasks and the account privileges required to perform them.

	TASK	ACCOUNT PRIVILEGE REQUIRED
1	Add Safe Lock Intelligent Manager accounts.	• admin
2	Use remote deployment tools (`SLrst.exe`) to centrally deploy agents from the server.	• N/A **Note** Using the `SLrst.exe` tool does not require specific account privileges, but does require the Safe Lock agent password to deploy tasks.
3	Use the Safe Lock Intelligent Manager console and remote deployment tools (`SLtasks.exe`) to manage the Approved List and Write Protection List on Safe Lock agents.	• admin • Full Control
4	Monitor Server Event logs.	• admin • Full Control
5	Monitor Agent Event logs.	• admin • Full Control • Read Only

About Trend Micro Safe Lock

Trend Micro Safe Lock protects fixed-function computers like Industrial Control Systems (ICS), Point of Sale (POS) terminals, and kiosk terminals from malicious software and unauthorized use. By using fewer resources and without the need for regular software or system updates, Safe Lock can reliably secure computers in industrial and commercial environments with little performance impact or downtime.

What's New in This Version

This section lists the new features and enhancements available in each release.

Trend Micro Safe Lock 2.0 Features and Enhancements

Trend Micro Safe Lock 2.0 includes the following new features and enhancements.

TABLE 1-7. New Features

FEATURE	DESCRIPTION
Write Protection	Prevents write access to all files in the Approved List and all objects (files, folders, and registry entries) in the Write Protection List
Integrity Monitoring	Monitors file change events system-wide for files, folders, and the registry
Approved List and Trusted Updater support Digital Signatures	Allow to loading or launching files that have pre-defined digital signatures, even if the files are not in the Approved List
Exception Path	Allow to loading or launching files in a pre-defined "exceptions" folder without adding them to the Approved List
Custom Action	Takes action on blocked files, for example Ignore, Quarantine, or Ask Server (requires Safe Lock Intelligent Manager Intelligent Manager)

Agent Features and Benefits

Trend Micro Safe Lock includes the following features and benefits.

Application Lockdown

By preventing programs, DLL files, drivers, and scripts not specifically on the Approved List of applications from running (also known as application white listing), Safe Lock provides both improved productivity and system integrity by blocking malicious software and preventing unintended use.

Exploit Prevention

Known targeted threats like Downad and Stuxnet, as well as new and unknown threats, are a significant risk to ICS and kiosk computers. Systems without the latest operating system updates are especially vulnerable to targeted attacks.

Safe Lock provides both intrusion prevention, which helps prevent threats from spreading to the endpoint, and execution prevention, which helps prevent threats from spreading to the endpoint or from running.

Easy Management

When software needs to be installed or updated, the Trusted Updater and Predefined Trusted Updater List provide an easy way to make changes to the endpoint and automatically add new or modified files to the Approved List, all without having to unlock Trend Micro Safe Lock.

Small Footprint

Compared to other endpoint security solutions that rely on large pattern files that require constant updates, application lockdown uses less memory and disk space, without the need to download updates.

Role Based Administration

Trend Micro Safe Lock provides a separate administrator and Restricted User account, providing full control during installation and setup, as well as simplified monitoring and maintenance after deployment.

Graphical and Command Line Interfaces

Anyone who needs to check the software can use the console, while system administrators can take advantage of the command line interface (CLI) to access all of the features and functions available.

Trend Micro Portable Security Compatible

Out-of-the-box compatibility with Trend Micro Portable Security ensures straightforward removal of any threats that do get on to the endpoint, without the need to update the Approved List or unlock the endpoint.

Safe Lock Agent Requirements

This section introduces Safe Lock system requirements and upgrade limitations.

Agent Requirements

Trend Micro Safe Lock does not have specific hardware requirements beyond those specified by the operating system, with the following exceptions:

TABLE 1-8. Required Hardware for Safe Lock

HARDWARE/SOFTWARE	DESCRIPTION
Available disk space	200MB minimum 300MB recommended
Monitor resolution	640x480

> **Important**
>
> Safe Lock cannot be installed on a system that already runs one of the following:
>
> • Trend Micro OfficeScan
>
> • Trend Micro Titanium
>
> • Another Trend Micro endpoint solution

Agent Operating Systems

See the readme file for the most up-to-date list of supported operating systems for Safe Lock agents.

> **Note**
>
> Memory Randomization, API Hooking Prevention, and DLL Injection Prevention are not supported on 64-bit platforms.

TABLE 1-9. List of Supported Operating Systems

WINDOWS VERSION TYPE	WINDOWS VERSION NAME
Windows Clients	Windows 2000 SP4* (32-bit)
	Note *Without Update Rollup, this version of Windows does not support DLL/Driver Lockdown, Integrity Monitoring, and the Predefined Trusted Updater.
	Windows XP SP1*/SP2/SP3 (32-bit) (except Starter and Home editions)
	Note *This version of Windows does not support DLL/Driver Lockdown, Integrity Monitoring, and the Predefined Trusted Updater. Safe Lock does not support a custom action of "quarantine" on Windows XP or Windows 2003.
	Windows Vista No-SP/SP1/SP2 (32-bit) (except Starter and Home editions)
	Windows 7 No-SP/SP1 (32-bit and 64-bit) (except Starter and Home editions)
	Windows 8 Enterprise No-SP (32-bit and 64-bit)
	Windows 8.1 Enterprise No-SP (32-bit and 64-bit)

WINDOWS VERSION TYPE	WINDOWS VERSION NAME
Windows Server	Windows 2000 Server SP4* (32-bit)
	Note *Without Update Rollup, this version of Windows does not support DLL/Driver Lockdown, Integrity Monitoring, and the Predefined Trusted Updater.
	Windows Server 2003 SP1/SP2 (32-bit)
	Note Safe Lock does not support a custom action of "quarantine" on Windows XP or Windows 2003.
	Windows Server 2003 R2 No-SP/SP2 (32-bit)
	Note Safe Lock does not support a custom action of "quarantine" on Windows XP or Windows 2003.
	Windows Server 2008 SP1/SP2 (32-bit and 64-bit)
	Windows Server 2008 R2 No-SP/SP1 (64-bit)
	Windows Server 2012 No-SP (64-bit)
	Windows Server 2012 R2 No-SP (64-bit)

WINDOWS VERSION TYPE	WINDOWS VERSION NAME
Windows Embedded Standard	Windows (Standard) XP Embedded SP1*/SP2 (32-bit)
	Note
	*This version of Windows does not support DLL/Driver Lockdown, Integrity Monitoring, and the Predefined Trusted Updater.
	Safe Lock does not support a custom action of "quarantine" on Windows XP or Windows 2003.
	Windows Embedded Standard 2009 (32-bit)
	Windows Embedded Standard 7 (32-bit and 64-bit)
	Windows Embedded Standard 8 (32-bit and 64-bit)
	Windows Embedded Standard 8.1 (32-bit and 64-bit)
Windows Embedded POSReady	Windows Embedded POSReady (32-bit)
	Windows Embedded POSReady 2009 (32-bit)
	Windows Embedded POSReady 7 (32-bit and 64-bit)
Windows Embedded Enterprise	Windows Embedded Enterprise XP SP1*/SP2/SP3 (32-bit)
	Note
	*This version of Windows does not support DLL/Driver Lockdown, Integrity Monitoring, and the Predefined Trusted Updater.
	Safe Lock does not support a custom action of "quarantine" on Windows XP or Windows 2003.
	Windows Embedded Enterprise Vista (32-bit)
	Windows Embedded Enterprise 7 (32-bit and 64-bit)

WINDOWS VERSION TYPE	WINDOWS VERSION NAME
Windows Embedded Server	Windows Embedded Server 2003 SP1/SP2 (32-bit)
	Note Safe Lock does not support a custom action of "quarantine" on Windows XP or Windows 2003.
	Windows Embedded Server 2003 R2 (32-bit)
	Note Safe Lock does not support a custom action of "quarantine" on Windows XP or Windows 2003.
	Windows Embedded Server 2008 (32-bit and 64-bit)
	Windows Embedded Server 2008 R2 (64-bit)
	Windows Embedded Server 2012 (64-bit)
	Windows Embedded Server 2012 R2 (64-bit)

Agent Upgrade Preparation

WARNING!

Depending on the installation method you select, Safe Lock versions require different preparation before upgrading.

Before upgrading, take the appropriate action below for your installation method and installed Safe Lock agent version:

TABLE 1-10. Upgrade Actions Required by Installation Method and Installed Agent Version

INSTALLATION METHOD	INSTALLED AGENT VERSION	REQUIRED ACTION	SETTINGS RETAINED
Local installation using Windows Installer	1.0	No preparation needed	No settings retained
	1.1	No preparation needed	Compatible settings retained
	2.0 or later	No preparation needed	No settings retained
Local installation using Command Line Interface Installer	1.0	Manually uninstall	No settings retained
	1.1	No preparation needed	Compatible settings retained
	2.0 or later	Manually uninstall	No settings retained
Remote	1.0	Manually uninstall	No settings retained
	1.1	Manually uninstall	No settings retained
	2.0 or later	Manually uninstall	No settings retained

Agent Use Overview

Trend Micro Safe Lock is a whitelist solution that locks down computers, preventing all applications not on the Approved List from running. Safe Lock can be configured and maintained using the graphical user interface (GUI) agent console or the command line interface (CLI). System updates can be applied without turning off Application Lockdown at the endpoint through the Predefined Trusted Updater List or by using the Trusted Updater.

Consider this typical use case scenario:

1.   Set up the Approved List and turn on Application Lockdown on the endpoint so that unapproved applications cannot be run.

2.   Use the Trusted Updater to update or install software whose installer is not on the Predefined Trusted Updater list.

3.   Configure and enable the Restricted User account for later maintenance.

If someone tries to run an application not specifically on the Approved List, the following message displays:

FIGURE 1-1. Trend Micro Safe Lock blocking message

Chapter 2

Intelligent Manager Deployment Preparation

This chapter introduces Trend Micro Safe Lock Intelligent Manager, deployment recommendations, and system requirements.

Topics in this chapter include:

Server Considerations

This section provides details about what you should consider before installing the Safe Lock Intelligent Manager server.

Database Requirements

Safe Lock Intelligent Manager stores data in a Microsoft SQL database. The database contains collected logs, reports, and agent information for all managed endpoints.

Safe Lock Intelligent Manager requires one of the following to manage its SQL database:

*   Microsoft SQL Server Standard or Enterprise Edition

    > 📝 **Note**
    >
    > For security reasons, Microsoft recommends that you do not install SQL Server on a domain controller.
    >
    > http://msdn.microsoft.com/en-us/library/ms143506.aspx#DC_support

*   Microsoft SQL 2008 Express

    If you install Safe Lock Intelligent Manager on a server that does not have access to Microsoft SQL Server in your environment, Setup provides the option to install Microsoft SQL 2008 Express.

> **!** **Important**
>
> SQL Express 2008 is suitable only for a small number of connections. SQL Express 2008 is suitable for testing purposes, but it is not ideal for larger production environments.Trend Micro recommends using Microsoft SQL Server Standard or Enterprise Edition for large networks monitored by Safe Lock Intelligent Manager.
>
> The following versions of Microsoft Windows support Safe Lock Intelligent Manager but do not support Microsoft .NET Framework 3.5 Service Pack 1 which is a required component of Microsoft SQL Express 2008:
>
> •   Windows Server 2003 No-SP, SP1 (32-bit and 64-bit)
>
> •   Windows Server 2003 R2 No-SP (32-bit and 64-bit)
>
> •   Windows Server 2008 SP1 (32-bit and 64-bit)

For performance information, see *Server Performance on page 2-4*.

Server Host Selection

When selecting an installation target, consider the following:

•   The CPU load the server can handle

•   Other functions that the server performs

    If the target server endpoint has other functions, do one of the following:

    •   Confirm that it does not run critical or resource-intensive applications.

    •   Choose an alternate host that does not run critical or resource-intensive applications.

•   Safe Lock Intelligent Manager must be installed before the Safe Lock agent when installing both on the same endpoint. The Safe Lock agent can be installed after installation of Safe Lock Intelligent Manager is complete.

> **!** **Important**
>
> Safe Lock 1.x agents block and prevent the installation of Safe Lock Intelligent Manager.

Server Performance

Enterprise networks require servers with higher specifications than those required for small and medium-sized businesses.

💡 **Tip**

Trend Micro recommends at least 2GHz dual processors and over 4GB of RAM for the Safe Lock Intelligent Manager server.

The number of agents that a single Safe Lock Intelligent Manager server can manage depends on several factors, such as available server resources and network topology. Contact your Trend Micro representative for help in determining the number of agents that your Safe Lock Intelligent Manager server deployment can manage.

Server Operating Systems and Components

Safe Lock Intelligent Manager supports many specialized and older versions of Microsoft Windows. In order to do this, Safe Lock Intelligent Manager requires different components based on your Windows platform. Manually enable or install the required components to get your environment ready before running Safe Lock Intelligent Manager Setup.

⚠️ **Important**

To use Microsoft SQL Express 2008, confirm that your system meets the requirements for SQL Express 2008. See http://www.microsoft.com/en-US/download/details.aspx?id=1695

To prepare the required components before running Safe Lock Intelligent Manager Setup, use the following table to match your Windows version to the appropriate preparation steps:

TABLE 2-1. List of Supported Operating Systems

WINDOWS VERSION TYPE	WINDOWS VERSION NAME	PREPARATION STEPS
Windows Clients	Windows XP SP2/SP3 (32-bit)	*Preparing Windows XP Components on page 2-13*
	Windows 7 Enterprise (Ultimate) No-SP/SP1 (32-bit and 64-bit)	*Preparing Windows 7 Components on page 2-12*
	Windows 8 Enterprise No-SP (32-bit and 64-bit)	*Preparing Windows 8 Components on page 2-11*
	Windows 8.1 Enterprise No-SP (32-bit and 64-bit)	
Windows Server	Windows Server 2003 No-SP/SP1/SP2 (32-bit and 64-bit)	*Preparing Windows Server 2003 Components on page 2-9*
	Windows Server 2003 R2 No-SP/SP2 (32-bit and 64-bit)	
	Windows Server 2008 SP1/SP2 (32-bit and 64-bit)	*Preparing Windows Server 2008 Components on page 2-6*
	Windows Server 2008 R2 No-SP/SP1 (64-bit)	
	Windows Server 2012 No-SP (64-bit)	*Preparing Windows Server 2012 Components on page 2-5*
	Windows Server 2012 R2 No-SP (64-bit)	

Preparing Windows Server 2012 Components

Before running Safe Lock Intelligent Manager Setup, follow this procedure to prepare components for the following Windows versions:

• Windows Server 2012 R2 No-SP (64-bit)

- Windows Server 2012 No-SP (64-bit)

Procedure

1. Go to **Server Manager** > **Dashboard** > **Add Roles and Features**.

2. In the menu on the left, go to **Server Roles**.

3. In the list, select **Web Server (IIS)**.

4. In the menu on the left, go to **Features**.

5. In the list, select **Message Queuing**.

6. In the menu on the left, go to **Web Server Role (IIS)** > **Role Services**.

7. In the list, select **Web Server**.

8. Under **Web Server**, select **Common HTTP Features**.

9. Under **Web Server** > **Common HTTP Features**, select **Static Content**.

10. Under **Web Server** > **Application Development**, select the following:

    - **Application Initialization**

    - **CGI**

    - **ASP.NET 3.5**

11. Confirm your changes.

Preparing Windows Server 2008 Components

Windows Server 2008 R2 No-SP/SP1 (64-bit)

Before running Safe Lock Intelligent Manager Setup, follow this procedure to prepare components for the following Windows versions:

- Windows Server 2008 R2 No-SP/SP1 (64-bit)

Procedure

• To install Microsoft SQL Server 2008 Express during installation of Safe Lock Intelligent Manager, first download and install Microsoft .NET Framework 3.5 Service Pack 1.

http://www.microsoft.com/en-us/download/details.aspx?id=22

• Before installing Safe Lock Intelligent Manager, first download and install the following components:

One of the following versions of Microsoft .NET Framework:

• 2.0 Service Pack 2.

http://www.microsoft.com/en-us/download/details.aspx?id=1639

• 3.5 Service Pack 1.

http://www.microsoft.com/en-us/download/details.aspx?id=22

Application Initialization 1.0 for IIS 7.5.

• 32-bit: http://go.microsoft.com/fwlink/?LinkID=247816

• 64-bit: http://go.microsoft.com/fwlink/?LinkID=247817

• Before installing Safe Lock Intelligent Manager, enable the following Windows components.

a. Go to **Server Manager** > **Roles** > **Add Roles**.

b. In the menu on the left, go to **Server Roles**.

c. In the list, select **Web Server (IIS)**.

d. In the menu on the left, go to **Web Server (IIS)** > **Role Services**.

e. In the list, under **Web Server** > **Common HTTP Features**, select **Static Content**

f. Under **Web Server** > **Application Development**, select the following:

• **CGI**

•   **ASP.NET 3.5**

g.   Go to **Server Manager** > **Features** > **Add Features**.

h.   In the list, select **Message Queuing**.

i.   Confirm your changes.

Windows Server 2008 SP1/SP2 (32-bit and 64-bit)

Before running Safe Lock Intelligent Manager Setup, follow this procedure to prepare components for the following Windows versions:

•   Windows Server 2008 SP1/SP2 (32-bit and 64-bit)

Procedure

•   To install Microsoft SQL Server 2008 Express during installation of Safe Lock Intelligent Manager, first download and install Microsoft .NET Framework 3.5 Service Pack 1.

    •   http://www.microsoft.com/en-us/download/details.aspx?id=22

> ⚠ **Important**
>
> The following versions of Microsoft Windows support Safe Lock Intelligent Manager but do not support Microsoft .NET Framework 3.5 Service Pack 1 which is a required component of Microsoft SQL Express 2008:
>
>   •   Windows Server 2008 SP1 (32-bit and 64-bit)

•   Before installing Safe Lock Intelligent Manager, first download and install one of the following versions of Microsoft .NET Framework:

    •   2.0 Service Pack 2.

    http://www.microsoft.com/en-us/download/details.aspx?id=1639

    •   3.5 Service Pack 1.

    http://www.microsoft.com/en-us/download/details.aspx?id=22

•   Before installing Safe Lock Intelligent Manager, enable the following Windows components.

   a.   Go to **Server Manager** > **Roles** > **Add Roles**.

   b.   In the menu on the left, go to **Server Roles**.

   c.   In the list, select **Web Server (IIS)**.

   d.   In the menu on the left, go to **Web Server (IIS)** > **Role Services**.

   e.   In the list, under **Web Server** > **Common HTTP Features**, select **Static Content**

   f.   Under **Web Server** > **Application Development**, select the following:

      •   **CGI**

      •   **ASP.NET 3.5**

   g.   Go to **Server Manager** > **Features** > **Add Features**.

   h.   In the list, select **Message Queuing**.

   i.   Confirm your changes.

Preparing Windows Server 2003 Components

Before running Safe Lock Intelligent Manager Setup, follow this procedure to prepare components for the following Windows versions:

•   Windows Server 2003 R2 No-SP/SP2 (32-bit and 64-bit)

•   Windows Server 2003 No-SP/SP1/SP2 (32-bit and 64-bit)

Procedure

•   To install Microsoft SQL Server 2008 Express during installation of Safe Lock Intelligent Manager, first download and install the following components:

   •   Microsoft .NET Framework 3.5 Service Pack 1.

http://www.microsoft.com/en-us/download/details.aspx?id=22

⚠ **Important**

The following versions of Microsoft Windows support Safe Lock Intelligent Manager but do not support Microsoft .NET Framework 3.5 Service Pack 1 which is a required component of Microsoft SQL Express 2008:

- Windows Server 2003 No-SP, SP1 (32-bit and 64-bit)

- Windows Server 2003 R2 No-SP (32-bit and 64-bit)

- Windows Installer 4.5.

  http://www.microsoft.com/en-us/download/details.aspx?id=8483

- Before installing Safe Lock Intelligent Manager, first download and install the following components:

  - One of the following versions of Microsoft .NET Framework:

    - 2.0 Service Pack 2.

      http://www.microsoft.com/en-us/download/details.aspx?id=1639

    - 3.5 Service Pack 1.

      http://www.microsoft.com/en-us/download/details.aspx?id=22

  - Windows Server 2003 Support Tools

    http://www.microsoft.com/en-us/download/details.aspx?id=15326

⚠ **Important**

Safe Lock Intelligent Manager requires that Windows Server 2003 Support Tools be installed to the installer default path.

  - FastCGI 1.5 for IIS

    http://www.iis.net/downloads/microsoft/fastcgi-for-iis

- Before installing Safe Lock Intelligent Manager, enable the following Windows components.

a. Go to **Start** > **Control Panel** > **Add or Remove Programs** > **Windows Components**.

b. In the list, select **Application Server**.

c. Click **Details...**.

d. Select the following:

• **Internet Information Services (IIS)**

• **Message Queuing**

e. Confirm your changes.

• Optionally, to view the Safe Lock Intelligent Manager web console without upgrading Internet Explorer version 6.0, download and install Google Chrome.

http://www.google.co.uk/intl/en_uk/chrome/business/browser/admin/

Preparing Windows 8 Components

Before running Safe Lock Intelligent Manager Setup, follow this procedure to prepare components for the following Windows versions:

• Windows 8.1 Enterprise No-SP (32-bit and 64-bit)

• Windows 8 Enterprise No-SP (32-bit and 64-bit)

Procedure

1. Go to **Start** > **Control Panel** > **Programs** > **Turn Windows features on or off**.

2. In the list, under **Internet Information Services**, select **World Wide Web Services**.

3. Under **Internet Information Services** > **World Wide Web Services** > **Common HTTP Features**, select **Static Content**.

4. Under **Internet Information Services** > **World Wide Web Services** > **Application Development Features**, select the following:

• **Application Initialization**

- **CGI**

- **ASP.NET 3.5**

5. In the list, select **Microsoft Message Queue (MSMQ) Server**.

6. Confirm your changes.

Preparing Windows 7 Components

Before running Safe Lock Intelligent Manager Setup, follow this procedure to prepare components for the following Windows versions:

- Windows 7 Enterprise (Ultimate) No-SP/SP1 (32-bit and 64-bit)

Procedure

- Enable Windows components.

    a. Go to **Start** > **Control Panel**.

    b. Depending on your Windows Control Panel appearance, click one of the following:

    - **Programs** > **Turn Windows features on or off**

    - **Programs and Features** > **Turn Windows features on or off**

    c. In the list, under **Internet Information Services**, select **World Wide Web Services**.

    d. Under **Internet Information Services** > **World Wide Web Services** > **Common HTTP Features**, select **Static Content**.

    e. Under **Internet Information Services** > **World Wide Web Services** > **Application Development Features**, select the following:

    - **CGI**

    - **ASP.NET**

f.   Under **Microsoft .NET Framework 3.5.1**, select **Microsoft Message Queue (MSMQ) Server**.

g.   Confirm your changes.

•   Download and install Application Initialization 1.0 for IIS 7.5.

   •   32-bit: http://go.microsoft.com/fwlink/?LinkID=247816

   •   64-bit: http://go.microsoft.com/fwlink/?LinkID=247817

Preparing Windows XP Components

Before running Safe Lock Intelligent Manager Setup, follow this procedure to prepare components for the following Windows versions:

•   Windows XP SP2/SP3 (32-bit)

Procedure

•   Enable Windows components.

   a.   Go to **Start** > **Control Panel** > **Add or Remove Programs** > **Windows Components**.

   b.   In the list, select the following:

      •   **Internet Information Services (IIS)**

      •   **Message Queuing**

   c.   Confirm your changes.

•   Download and install the following components:

   •   Windows Server 2003 Support Tools

      http://www.microsoft.com/en-us/download/details.aspx?id=15326

> **Important**
>
> Safe Lock Intelligent Manager requires that Windows Server 2003 Support Tools be installed to the installer default path.

- Windows Server 2003 Service Pack 2 Administration Tools Pack for x86 editions

  http://www.microsoft.com/en-us/download/details.aspx?id=6315

- FastCGI 1.5 for IIS

  http://www.iis.net/downloads/microsoft/fastcgi-for-iis

- Microsoft .NET Framework

  - 3.5 Service Pack 1 required when using a local Microsoft SQL Express installation

    http://www.microsoft.com/en-us/download/details.aspx?id=22

  - 2.0 Service Pack 2 required when not using a local Microsoft SQL Express 2008 installation

    http://www.microsoft.com/en-us/download/details.aspx?id=1639

- Optionally, do the following:

  - To install Microsoft SQL Server 2008 Express during installation of Safe Lock Intelligent Manager, download and install Windows Installer 4.5.

    http://www.microsoft.com/en-us/download/details.aspx?id=8483

  - To view the Intelligent Manager web console without upgrading Internet Explorer version 6.0, download and install Google Chrome.

    http://www.google.co.uk/intl/en_uk/chrome/business/browser/admin/

Migrating an Existing Database

Before you begin

A stand-alone Microsoft SQL Server is required for this database migration procedure.

> ⚠️ **WARNING!**
> This procedure moves your existing database between two SQL servers, for example, from a Microsoft SQL Express location previously installed by Safe Lock Intelligent Manager Setup to a stand-alone Microsoft SQL Server. If you will use the same Microsoft SQL Server for this installation as you used in your previous installation, skip this procedure.

If you are reinstalling Safe Lock Intelligent Manager, you may want to migrate data from your old installation. Safe Lock Intelligent Manager stores data in a Microsoft SQL database. The database contains collected logs, reports, and agent information for all managed endpoints.

If you were previously using Microsoft SQL Express to manage your Safe Lock Intelligent Manager database, Trend Micro suggests migrating the database to Microsoft SQL Server using the following procedure.

Procedure

1. Download and install Microsoft SQL Server 2008 Management Studio Express.

   a. Download the installer from Microsoft at http://www.microsoft.com/en-us/download/details.aspx?id=7593.

   b. Install Microsoft SQL Server 2008 Management Studio Express on the endpoint with the source database.

2. Follow the steps to export the script from endpoint with the source Safe Lock Intelligent Manager database.

   See *Exporting an Existing Database on page 2-16*.

   > 📝 **Note**
   > The default name of the Safe Lock Intelligent Manager database is `SafeLock`.

3. Follow the steps to import the database script into the destination SQL server endpoint an connect it to Safe Lock Intelligent Manager.

    See *Importing a Database on page 2-17*.

Exporting an Existing Database

Procedure

1. From the endpoint with the source database, launch Microsoft SQL Server 2008 Management Studio.

    The **Microsoft SQL Server Management Studio** solution window appears.

2. Export the source database script.

    a. Go to **File** > **Export Database Script**.

        Inside the solution window, the **Object Explorer** window appears.

    b. Confirm that the Object Explorer window contains the source database location.

    c. Expand the selection for the source SQL server to display the `SafeLock` database.

    d. Right-click the `SafeLock` database and go to **Tasks** > **Generate Scripts...**

        The **Generate and Publish Scripts** window appears.

    e. In the menu on the left, go to **Choose Objects**.

    f. Select **Select entire database and all database objects**.

    g. Click **Next >**.

    h. Select the following items:

        • **Save scripts to a specific location**

        • **Save to file**

- • **Single file**

- • **Overwrite existing file**

- • **Unicode text**

i.   Set and remember the path to save the file to.

j.   Click **Advanced**.

The **Advanced Scripting Options** window appears.

k.   Under **General**, do the following:

- • Set **ANSI Padding** to **False**.

- • Set **Script for Server Version** to the version of Microsoft SQL your destination SQL server uses. For example, **SQL Server 2012**.

- • Set **Types of data to script** to **Schema and data**.

l.   Click **OK**.

The **Specify how scripts should be saved or published** screen reappears.

m.   Click **Next**.

n.   Review your settings, then click **Next** to begin the export process.

The **Saving or publishing scripts** screen appears. Data from your source SQL database is compiled and saved to a file at the path you specified earlier.

o.   After the process completes successfully, click **Finish**.

3.   Use the resulting export file in the import process.

Importing a Database

Procedure

1.   From the endpoint with the source database, launch Microsoft SQL Server 2008 Management Studio.

The **Microsoft SQL Server Management Studio** solution window appears.

2. Import the database script into the destination endpoint Microsoft SQL Server.

   a. Expand the selection for the destination SQL server to display the `Databases` folder.

   b. Click the `Databases` folder to select it.

   c. Go to **File** > **Open**.

   d. Open the exported script file for the existing Safe Lock Intelligent Manager database you want to import.

      An editor window appears.

   e. Customize the target database full path for the new copy of the database you are creating.

      To change the database path to `e:\SQL_STORE\SafeLock.mdf` in the following script example:

      `NAME = N'SafeLock', FILENAME = N'd:\SafeLock.mdf'`

      Change the "FILENAME" parameter to `N'e:\SQL_STORE \SafeLock.mdf'`.

   f. Customize the target database log full path for the new copy of the database you are creating.

      To change the log path to `e:\SQL_STORE\SafeLock_log.LDF` in the following script example:

      `NAME = N'SafeLock_log', FILENAME = N'd: \SafeLock_log.LDF'`

      Change the "FILENAME" parameter to `N'e:\SQL_STORE \SafeLock_log.LDF'`.

   g. Click **Execute** to run the script, importing the database to the destination SQL server.

3. Depending on if you have already installed Safe Lock Intelligent Manager or not, do the following:

- • If you have not already completed Setup, make a note of the path to the new SQL server location. Complete the Server Installation Checklist before installing. During installation, at the **Database Configuration** Setup screen, select **Use an existing Microsoft SQL Server** and specify the path to the new SQL server location.

    See the following for more information:

    - • *Server Installation Checklist on page 2-21*

    - • *The Database Configuration Screen on page 3-8*

- • If you have already completed Setup, connect Safe Lock Intelligent Manager to the newly imported database.

    See *Connecting to an Existing Database on page 2-19*.

Connecting to an Existing Database

Safe Lock Intelligent Manager can connect to an existing Safe Lock Intelligent Manager database. Use this functionality to connect new installations of Safe Lock Intelligent Manager to old databases, for example, when replacing server endpoint hardware.

⚠️ **WARNING!**

There is a risk of data loss during this process if your current installation of Safe Lock Intelligent Manager has accumulated new data while the migration of your older Safe Lock Intelligent Manager database is being performed.

If you completed Setup and have already started using Safe Lock Intelligent Manager, back up data by exporting newly-collected logs, reports, and agent information for all managed endpoints. Import this data after migrating the older database. See the Safe Lock Intelligent Manager Administrator's Guide for details on exporting and importing data.

Complete Safe Lock Intelligent Manager Setup, then do the following:

Procedure

1. From the Safe Lock Intelligent Manager server endpoint, run the following at the command prompt with Windows administrator privileges:

```
<Safe_Lock_Intelligent_Manager_installation_path>\CmdTools
\Installer\Setup.exe -utility -update_sql_address
<Intelligent_Manager_web_console_administrator_password>
<address_of_target_SQL_server>
<database_user_name_for_target_SQL_server>
<database_password_for_target_SQL_server>
```

Migrating the Intelligent Manager Program to a New Server Endpoint

Before you begin

To migrate the Safe Lock Intelligent Managerprogram to a new server endpoint, no special preparation of Safe Lock agents is needed.

Note

Safe Lock agents cache logs and reports locally until a Safe Lock Intelligent Manager becomes available to collect them. Typically, Safe Lock agents have enough storage to remain separated from a Safe Lock Intelligent Manager for several hours before they begin purging uncollected logs and reports.

To migrate the Safe Lock Intelligent Manager program to a new server endpoint, follow this procedure.

Procedure

1. Uninstall Safe Lock Intelligent Manager from the current server endpoint.

   See *Uninstalling Intelligent Manager on page 4-3*.

2. Install Safe Lock Intelligent Manager on the new server endpoint using identical Server Identification settings as the uninstalled server used.

   See *The Server Identification Screen on page 3-13*.

Server Installation Checklist

Complete the following before running Safe Lock Intelligent Manager Setup.

• Obtain the following from Trend Micro:

PREPARATION
Safe Lock Intelligent Manager Setup installer package
Full or trial version Activation Code
For details about the available Safe Lock Intelligent Manager versions, refer to the documentation available at http://docs.trendmicro.com/en-us/enterprise/trend-micro-safe-lock.aspx

• Do the following to prepare your environment:

ENVIRONMENT
Ensure that all the necessary software components are installed. See *Server Operating Systems and Components on page 2-4*.
Check the required hardware and software specifications. See *Safe Lock Intelligent Manager Requirements on page 1-3*.
Ensure that IP address and DNS settings have been assigned to the target server.

• Gather the following information:

INFORMATION
The installation path for Safe Lock Intelligent Manager files
The database server settings, which Safe Lock Intelligent Manager uses to record collected logs, reports, and agent information See *The Database Configuration Screen on page 3-8*.

INFORMATION
The fully qualified domain name (FQDN), host name, or IP address, which allows agents to identify the Safe Lock Intelligent Manager server See *The Server Identification Screen on page 3-13*.
The web server settings for the Safe Lock Intelligent Manager web console The port numbers, which the Safe Lock Intelligent Manager server uses to communicate with agents See *The Network Configuration Screen on page 3-14*.
The password for the default Safe Lock Intelligent Manager administrator account See *About the Web Console Admin Account Password on page 3-17*. This is the account that you will use to log on to the Safe Lock Intelligent Manager web console.
The port number, which Safe Lock Intelligent Manager uses to deploy remote agent installation packages. See *The Destination Folder and Port for Server Communication Screen on page 3-16*.

After preparations are complete, run Safe Lock Intelligent Manager Setup on the server endpoint.

Chapter 3

Intelligent Manager Installation

This chapter describes Trend Micro Safe Lock Intelligent Manager installation procedures.

Topics in this chapter include:

Setup Flow
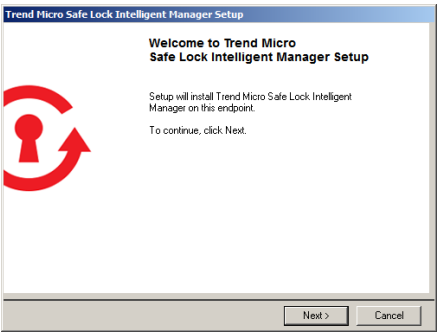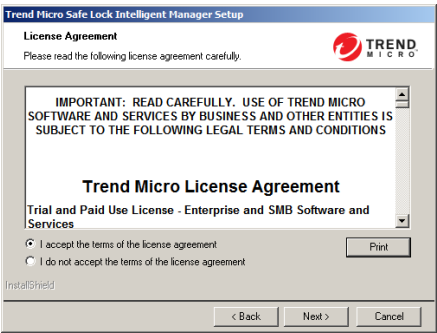
Setup prompts for the following information when installing the Safe Lock Intelligent Manager server.
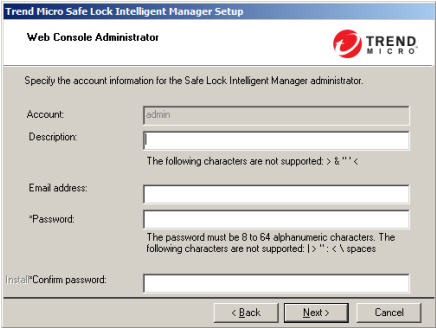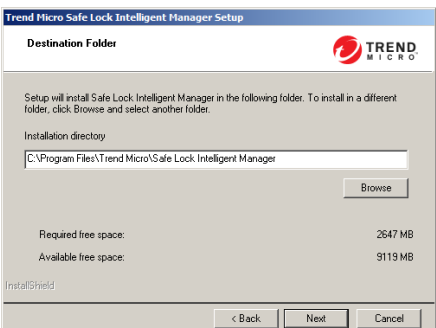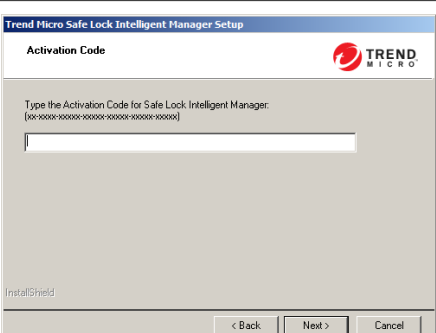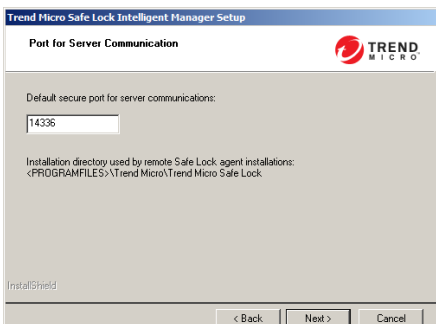

⚠ **Important**
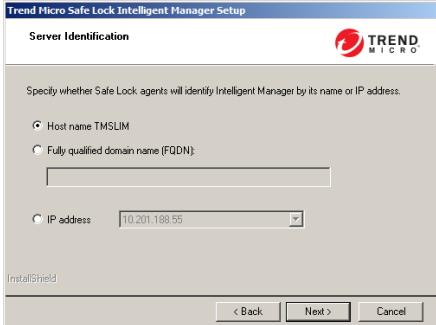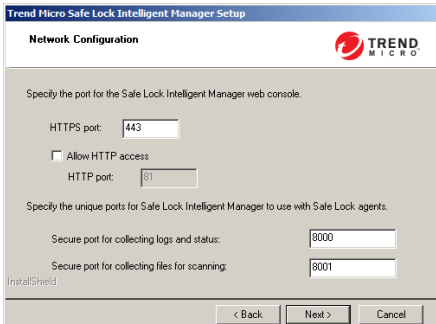
Before running Safe Lock Intelligent Manager Setup, complete the checklist at *Server Installation Checklist on page 2-21*.
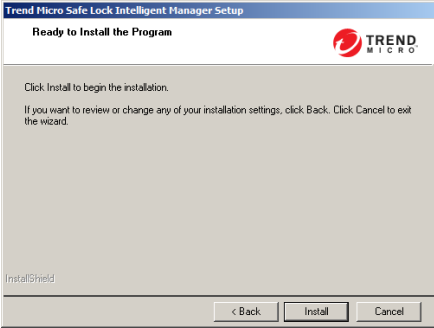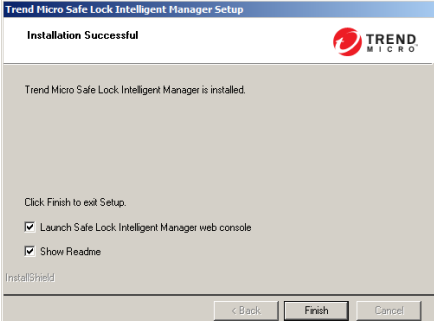

TABLE **3-1. Setup Flow and Required Information**

INSTALLER SCREEN	NEEDED INFORMATION
Trend Micro Safe Lock Intelligent Manager Setup **Welcome to Trend Micro Safe Lock Intelligent Manager Setup** Setup will install Trend Micro Safe Lock Intelligent Manager on this endpoint. To continue, click Next. [Next >] [Cancel]	None
Trend Micro Safe Lock Intelligent Manager Setup **License Agreement** Please read the following license agreement carefully. IMPORTANT: READ CAREFULLY. USE OF TREND MICRO SOFTWARE AND SERVICES BY BUSINESS AND OTHER ENTITIES IS SUBJECT TO THE FOLLOWING LEGAL TERMS AND CONDITIONS **Trend Micro License Agreement** **Trial and Paid Use License - Enterprise and SMB Software and Services** ○ I accept the terms of the license agreement [Print] ○ I do not accept the terms of the license agreement InstallShield [< Back] [Next >] [Cancel]	None

INSTALLER SCREEN	NEEDED INFORMATION
	The database server type, which Safe Lock Intelligent Manager uses to record collected logs, reports, and agent information See *The Database Configuration Screen on page 3-8*.
  	The password for the Safe Lock Intelligent Manager database To use an existing SQL server, specify a server location.

INSTALLER SCREEN	NEEDED INFORMATION

Trend Micro Safe Lock Intelligent Manager Setup
 	
Web Console Administrator   TREND
 	
Specify the account information for the Safe Lock Intelligent Manager administrator.
 	
Account: `admin`
Description:
    The following characters are not supported: > & " ' <
Email address:
*Password:
    The password must be 8 to 64 alphanumeric characters. The following characters are not supported: | > ": < \ spaces
Install*Confirm password:
 	
< Back   Next >   Cancel
	The password for the default Safe Lock Intelligent Manager administrator account
	
	See *About the Web Console Admin Account Password on page 3-17*.
	
	This is the account that you will use to log on to the Safe Lock Intelligent Manager web console.

Trend Micro Safe Lock Intelligent Manager Setup **Destination Folder** TREND Setup will install Safe Lock Intelligent Manager in the following folder. To install in a different folder, click Browse and select another folder. Installation directory `C:\Program Files\Trend Micro\Safe Lock Intelligent Manager` Browse Required free space: 2647 MB Available free space: 9119 MB InstallShield < Back Next Cancel	The installation path for Safe Lock Intelligent Manager files
Trend Micro Safe Lock Intelligent Manager Setup **Activation Code** TREND Type the Activation Code for Safe Lock Intelligent Manager: (xx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx) InstallShield < Back Next > Cancel	The full or trial Activation Code for Safe Lock Intelligent Manager

INSTALLER SCREEN	NEEDED INFORMATION
	The fully qualified domain name (FQDN), host name, or IP address, which allows agents to identify the Safe Lock Intelligent Manager server See *The Server Identification Screen on page 3-13*.
	The web server settings for the Safe Lock Intelligent Manager web console The port numbers, which the Safe Lock Intelligent Manager server uses to communicate with agents See *The Network Configuration Screen on page 3-14*.
	The port number, which Safe Lock Intelligent Manager uses to deploy remote agent installation packages. See *The Destination Folder and Port for Server Communication Screen on page 3-16*.

INSTALLER SCREEN	NEEDED INFORMATION
Trend Micro Safe Lock Intelligent Manager Setup **Ready to Install the Program** — TREND MICRO Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard. InstallShield [< Back] [Install] [Cancel]	None
Trend Micro Safe Lock Intelligent Manager Setup **Installation Successful** — TREND MICRO Trend Micro Safe Lock Intelligent Manager is installed. Click Finish to exit Setup. ☑ Launch Safe Lock Intelligent Manager web console ☑ Show Readme InstallShield [< Back] [Finish] [Cancel]	None

Safe Lock Intelligent Manager Server Installation

Before you begin

For prerequisites, see *Server Installation Checklist on page 2-21*.

Procedure

1. On the target server, launch the Safe Lock Intelligent Manager Setup program (`Setup.exe`).

2. Click **Next >**.

   The Setup program displays the License Agreement screen.

3. Specify the server settings.

   The Setup program confirms that required components are installed and configured correctly. If there is a problem with the configuration of your Windows platform, a message appears listing the issues to resolve before continuing. Click **Installation Troubleshooting** for additional support resolving any detected issues.

4. Complete the *The Database Configuration Screen on page 3-8*.

5. Complete the Web Console Administrator Settings.

   See *About the Web Console Admin Account Password on page 3-17*.

6. Specify the location where the Safe Lock Intelligent Manager program will be installed.

   The following is the default installation path:

   ```
   "c:\Program Files\Trend Micro\Safe Lock Intelligent
   Manager"
   ```

   Identify a new installation path or use the default path. If the path does not exist, Setup creates it automatically.

7. Type the full or trial Activation Code for Safe Lock Intelligent Manager.

   For details about the available Safe Lock Intelligent Manager versions, refer to the documentation available at http://docs.trendmicro.com/en-us/enterprise/trend-micro-safe-lock.aspx

8. Complete the *The Server Identification Screen on page 3-13*.

9. Complete the *The Network Configuration Screen on page 3-14*.

10. Complete the *The Destination Folder and Port for Server Communication Screen on page 3-16*.

11. Click **Install**.

12. Click **Finish**.

Setup launches your default web browser, which allows you to access the Safe Lock Intelligent Manager web console. The web console shortcut appears on the desktop.

FIGURE 3-1. Web Console Shortcut

In addition, Setup displays the Safe Lock Intelligent Manager readme file.

What to do next

Check the IIS configuration to verify if the port is correctly set for each Safe Lock Intelligent Manager channel, and then install agents by following the deployment procedure in the *Safe Lock Intelligent Manager Administrator's Guide*.

The Database Configuration Screen

Before you begin

Check your database requirements and take any needed steps to prepare your environment.

> 📝 **Note**
>
> If you were previously using Microsoft SQL Express to manage your Safe Lock Intelligent Manager database, Trend Micro suggests migrating the database to Microsoft SQL Server.
>
> See *Migrating an Existing Database on page 2-15*.
>
> If you want to continue to use that database instance and that installation of SQL Express, follow the appropriate Tip inline below.

This screen defines how Safe Lock Intelligent Manager stores data for collected logs, reports, and agent information. The Safe Lock Intelligent Manager server installation

establishes this connection as well as the user name and password Safe Lock Intelligent Manager uses to access the database.

Select the type of database you have for your Safe Lock Intelligent Manager environment.
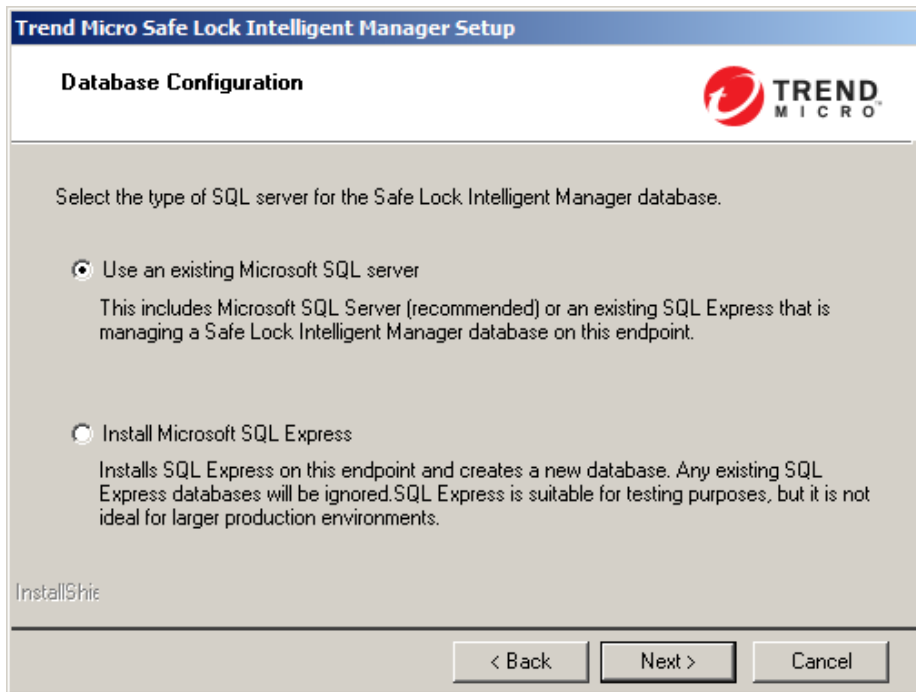

FIGURE 3-2. Configuring the Database Server

Procedure

• **Use an existing Microsoft SQL Server**: Type the SQL Server (\Instance) that you want to use. To specify another SQL server, identify the server using its fully qualified domain name (FQDN), IPv4 address, or NetBIOS name.

> **Tip**
>
> If you previously used Microsoft SQL Express to host your Safe Lock Intelligent Manager database and you want to continue to use that database instance and that installation of SQL Express, select this option. On the next screen, under **Existing SQL server location**, enter the IP address, FQDN, or host name of the endpoint running the earlier installation and append `\SQLEXPRESS`.
>
> > **Important**
> >
> > The endpoint of the earlier installation must remain accessible from the new installation location for the original installation of SQL Express to continue hosting the database. Ideally, use the same endpoint and user account as the previous installation.

- **Install Microsoft SQL Express**: If you do not have Microsoft SQL Server set up in your environment, Safe Lock Intelligent Manager Setup can install Microsoft™ SQL Server™ 2008 R2 SP2 - Express Edition.

  > **Important**
  >
  > SQL Express 2008 is suitable only for a small number of connections. SQL Express 2008 is suitable for testing purposes, but it is not ideal for larger production environments.Trend Micro recommends using Microsoft SQL Server Standard or Enterprise Edition for large networks monitored by Safe Lock Intelligent Manager.
  >
  > The following versions of Microsoft Windows support Safe Lock Intelligent Manager but do not support Microsoft .NET Framework 3.5 Service Pack 1 which is a required component of Microsoft SQL Express 2008:
  >
  > - Windows Server 2003 No-SP, SP1 (32-bit and 64-bit)
  > - Windows Server 2003 R2 No-SP (32-bit and 64-bit)
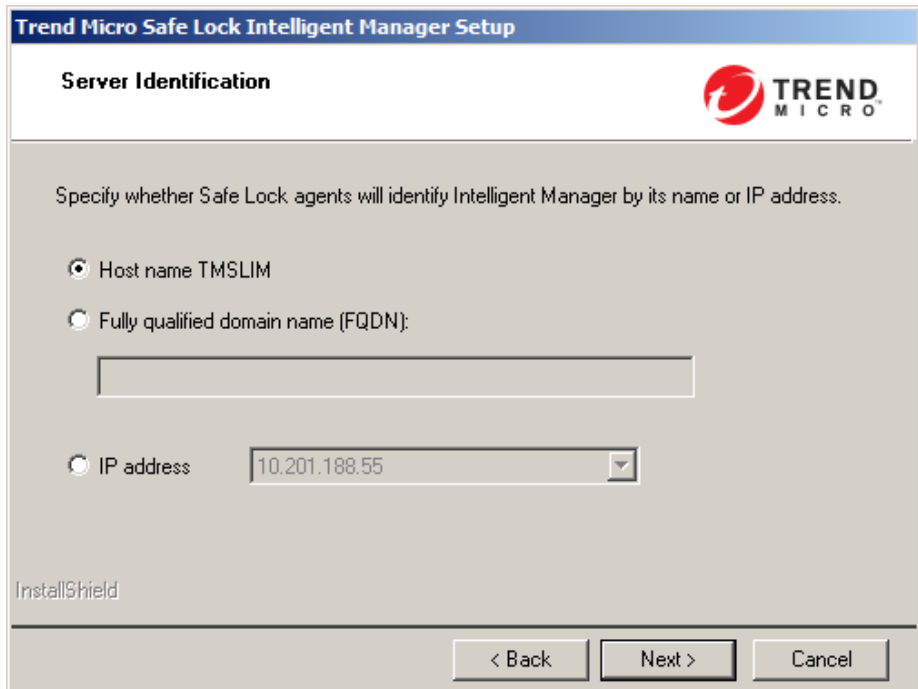 > - Windows Server 2008 SP1 (32-bit and 64-bit)

- Depending on your selection, one of the following screens appears:

SELECTION	RESULTING SCREEN	INFORMATION TO SPECIFY
Use an existing Microsoft SQL Server	**FIGURE 3-3. Configuring the Database Server**	**Existing SQL server location**: Specify the path to the SQL server that hosts the Safe Lock Intelligent Manager database. **User name** and **Password**: Set the password that Safe Lock Intelligent Manager uses to access the database.

SELECTION	RESULTING SCREEN	INFORMATION TO SPECIFY
Install Microsoft SQL Express	 **FIGURE 3-4. Configuring the Database Server**	**User name** and **Password**: The default user name is sa. Set the password that Safe Lock Intelligent Manager uses to access the database. **Tip** Follow the guidelines below to select a secure password: • Use a long password. Trend Micro recommends using a password of at least 10 characters, but longer passwords are preferred. • Use a combination of mixed-case letters, numbers, and other characters. • Avoid names or words in dictionaries. • Avoid simple patterns such as "101010" or "abcde."

The Server Identification Screen

This screen identifies how agents communicate with the Safe Lock Intelligent Manager server.

FIGURE 3-5. Configuring the Server Identification

Select a way for agents to communicate with the server.

> **⚠ Important**
>
> The setting on this screen is irreversible. If there is a need to change the Server Identification at a later time, both the Safe Lock Intelligent Manager server and all registered agents must be reinstalled.
>
> If you are reinstalling Safe Lock Intelligent Manager, use identical settings for Server Identification or your existing managed Safe Lock agents will be unable to communicate with the new Safe Lock Intelligent Manager.

Procedure

- **Fully qualified domain name (FQDN)**: The FQDN of the Safe Lock Intelligent Manager server.

- **Host name**: The host name of the Safe Lock Intelligent Manager server.

- **IP address**: A list of available IPv4 addresses.

The Network Configuration Screen

Before you begin

Install the required IIS server and role services.

See *Server Installation Checklist on page 2-21*.

This screen does the following:

- Defines how the network identifies your Safe Lock Intelligent Manager server connection.

- Identifies the ports which the Safe Lock Intelligent Manager server uses to listen for incoming agent communication.

Accept the default values or specify new ones.

FIGURE 3-6. Configuring the Web Console Settings

Procedure

- **HTTPS port**: Accept the default value (443) or supply a new port number. If changed, access the web console using that port.

- **Allow HTTP access**: If HTTP access is required, select this option.

  By default, the Safe Lock Intelligent Manager web console can be accessed using only HTTPS.

- **HTTP port**: Accept the default value (81) or supply a new port number. If changed, access the web console using that port.

- **Secure port for collecting logs and status**: Accept the default value (8000) or supply a new port number.

•   **Secure port for collecting files for scanning**: Accept the default value (8001) or supply a new port number.

The Destination Folder and Port for Server Communication Screen

This screen identifies the port that Safe Lock agents use to listen for incoming Safe Lock Intelligent Manager communication. In addition, this screen also displays the default agent installation path.
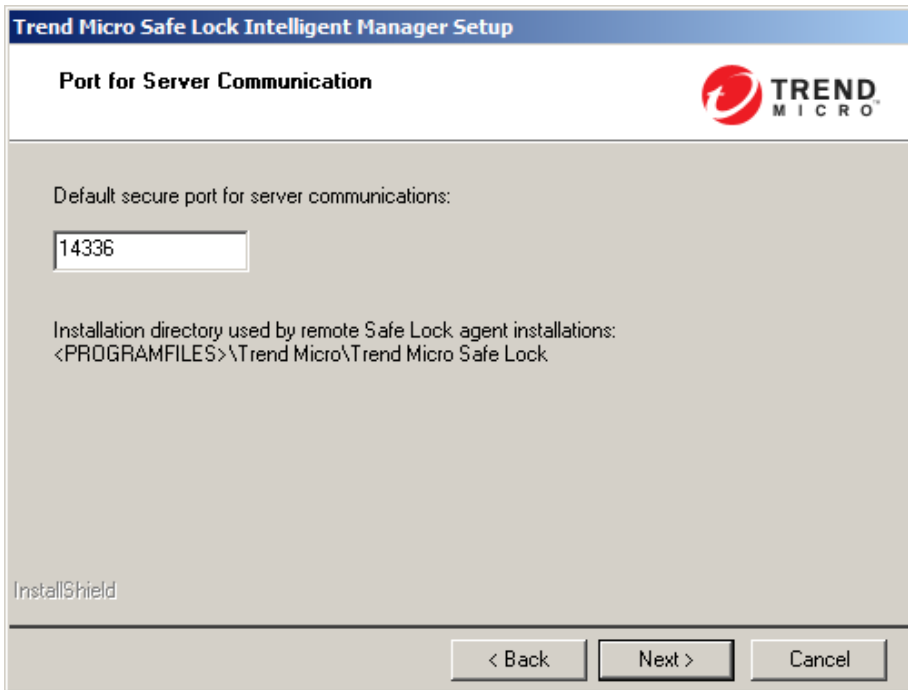

FIGURE 3-7. Setting the Server Communication Port

Procedure

- **Default secure port for server communications**: Accept the default value (14336) or supply a new port number.

About the Web Console Admin Account Password

Safe Lock Intelligent Manager supports the following password characteristics:

- Must be 8 to 64 characters long

- Must be a combination of alphanumeric characters or the following symbols: !@#$
  %^&*()_+=-

- Must not include any of these unsupported symbols: |><\" or space

Record the user name and password for future reference.

> 💡 Tip
>
> Follow the guidelines below to select a secure password:
>
> - Use a long password. Trend Micro recommends using a password of at least 10 characters, but longer passwords are preferred.
>
> - Avoid names or words in dictionaries.
>
> - Use a combination of mixed-case letters, numbers, and other characters.
>
> - Avoid simple patterns such as "101010" or "abcde."

Configuring a Failover Cluster

Deploy Safe Lock Intelligent Manager in a failover cluster.

Procedure

1. Prepare the Active Directory domain network.

Objective: Set up an Active Directory server and prepare two nodes for the cluster.

Reference: http://support.microsoft.com/kb/324753

Expected result:

- Active Directory server: `ad.mycompany.local`

- Node 1: `n1.mycompany.local`

- Node 2: `n2.mycompany.local`

2. Optionally, prepare a SQL Server Failover Cluster.

    Objective: Set up SQL Server Failover Cluster to reduce the risk of a total SQL server failure.

    Reference: http://msdn.microsoft.com/en-us/library/hh231721.aspx

    Expected result:

    - SQL server: `sqlcluster.mycompany.local`

3. Set up Windows Failover Clustering.

    Objective: Enable the Windows Failover Clustering feature and create the cluster for Safe Lock Intelligent Manager.

    Reference: http://technet.microsoft.com/en-us/library/dn505754.aspx

    Expected result:

    - Node 1 and 2 are joined to the newly created Failover Cluster with a Cluster Shared Volume (assume the drive letter is x:).

    - Cluster name: `tmslcluster.mycompany.local`

4. Create the Distributed Transaction Coordinator (DTC) Role.

    Objective: Set up DTC for Safe Lock Intelligent Manager and IIS failover.

    a. Open Failover Cluster Manager.

    b. Connect to the cluster `tmslcluster.mycompany.local`.

    c. Click **Configure Role…** in the cluster configuration panel.

       d.   On the **Before You Begin** screen, click **Next**.

       e.   Select **Distributed Transaction Coordinator (DTC)** and click **Next** on the **Select Role** screen.

       f.   Type `tmslconsole.mycompany.local` as the name of the access point.

       g.   Assign an IP address.

       h.   On the **Client Access Point** screen, click **Next**.

       i.   Select the volume for this DTC and complete the wizard.

    Expected result:

    •   The DTC access point is set up.

5.   Set up Safe Lock Intelligent Manager.

       a.   Select the DTC and click **Move…** to move all resource to Node 1.

       b.   Run the Safe Lock Intelligent Manager installer on Node 1.

       c.   When prompted for the installation destination, change the path to **x:\SafeLock** (assume x: is the drive letter for storage of the DTC).

       d.   When prompted for the database configuration, type the SQL server address.

       e.   When prompted for the server Fully Qualified Domain Name (FQDN), type `tmslconsole.mycompany.local`.

       f.   After installation is done, select the DTC in the Failover Cluster Manager and move the resources to Node 2.

       g.   Run the Safe Lock Intelligent Manager installer on Node 2.

       h.   When prompted for the installation destination on Node 2, change the path to the same one used for the Node 1 installation.

             For example, use **x:\SafeLock** during both Node 1 and Node 2 installations.

       i.   When prompted for the database configuration, type the SQL server address.

             The installer will detect that the database already exists.

       j.   Select the existing database and type the password for validation.

6. Configure Safe Lock Intelligent Manager to be failover ready.

   a. Select the DTC and click **Add resource**.

   b. Add **Generic Service**.

   c. Select **TmslSrvSvc** in the list and complete the wizard.

   d. Right-click **TmslSrvSvc**, then select **Property**.

   e. Go to the **Registry Replication** tab and add `SOFTWARE\TrendMicro`
      `\SafeLockIntelligentManager` to be synced across nodes.

7. Set up IIS Failover.

   Reference: http://support.microsoft.com/kb/970759

   a. Follow the instructions in the Microsoft Knowledge Base article above with
      the following exception:

      In Step 5 of the **Configure high availability for your Web site by creating a
      generic script in Failover Cluster Manager** section, select the DTC and click
      Add resource… instead of the original instruction.

      📝 **Note**

      When copying the script, modify the `SITE_NAME` to the **ConsoleChannel** and
      `APP_POOL_NAME` to the **ConsoleChannel**, so that the script monitors the
      correct IIS site.

      ---

8. Test.

   After you complete the steps above, Safe Lock Intelligent Manager should be
   prepared for failover.

   📝 **Note**

   The console address is `tmslconsole.mycompany.local`.

   You may bring either node offline to test the clustering functionality.

Chapter 4

Intelligent Manager Uninstallation

This chapter describes Trend Micro Safe Lock Intelligent Manager uninstallation procedures.

Topics in this chapter include:

Preparing to Remove Intelligent Manager

Before you begin

To remove Safe Lock Intelligent Manager from your environment, do the following in any order:

Procedure

• Optionally, uninstall managed Safe Lock agents then reinstall them as standalone Safe Lock agents.

> **Note**
>
> Safe Lock agents cache logs and reports locally until a Safe Lock Intelligent Manager becomes available to collect them. Typically, Safe Lock agents have enough storage to remain separated from a Safe Lock Intelligent Manager for several hours before they begin purging uncollected logs and reports.

To preserve the settings from managed endpoints before uninstalling, do the following at each managed Safe Lock agent endpoint:

a. Open the Safe Lock console.

b. Go to **Approved List**.

c. Select all applications.

d. Click **Export** and choose a save location.

The Approved List is exported.

e. Go to **Settings**.

f. Click **Export** and choose a save location.

The settings are exported.

• Uninstall Safe Lock Intelligent Manager.

See *Uninstalling Intelligent Manager on page 4-3*.

Uninstalling Intelligent Manager

Procedure

1. Go to **Start > All Programs > Trend Micro Safe Lock Intelligent Manager > Uninstall Safe Lock Intelligent Manager**.

    Safe Lock Intelligent Manager Setup opens in uninstall mode.

2. Click **Next >**.

3. Optionally, select **Safe Lock Intelligent Manager database** if you do not plan to use the existing database.

    > **Tip**
    >
    > Safe Lock Intelligent Manager is unable to recover any data after the database is deleted. Trend Micro recommends exporting any critical data using the web console before removing the database. See the *Safe Lock Intelligent Manager Administrator's Guide* for more information about exporting data.
    >
    > If you plan to migrate to another Safe Lock Intelligent Manager server endpoint, only select **Safe Lock Intelligent Manager database** if you have already migrated your data.
    >
    > See *Migrating an Existing Database on page 2-15*.

4. Click **Next >**.

    The uninstallation starts and the **Uninstall Progress** screen appears.

    > **Important**
    >
    > Performance may be reduced during uninstallation. Do not stop the uninstallation or shut down the endpoint until uninstallation is complete.

    The uninstallation completes and the **Uninstallation Successful** screen appears.

5. Click **Finish**.

   Safe Lock Intelligent Manager Setup exits.

6. Optionally, uninstall PHP.

   Safe Lock Intelligent Manager Setup installs PHP 5.3.27 if a newer version of PHP is not installed on the endpoint. However, when you uninstall Safe Lock Intelligent Manager, Setup does not remove PHP. If the installed PHP was installed by Setup, you may want to uninstall it.

   📝 **Note**

   Before reinstalling Safe Lock Intelligent Manager on the same endpoint, Trend Micro recommends removing any existing installations of PHP.

Chapter 5

Technical Support

This chapter describes how to find solutions online, use the Support Portal, and contact Trend Micro.

Topics include:

Troubleshooting Resources

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

Using the Support Portal

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

Procedure

1. Go to http://esupport.trendmicro.com.

2. Select a product or service from the appropriate drop-down list and specify any other related information.

   The **Technical Support** product page appears.

3. Use the **Search Support** box to search for available solutions.

4. If no solution is found, click **Submit a Support Case** from the left navigation and add any relevant details, or submit a support case here:

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

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

Trend Community

To get help, share experiences, ask questions, and discuss security concerns with other users, enthusiasts, and security experts, go to:

http://community.trendmicro.com/

Contacting Trend Micro

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

Address	Trend Micro, Inc. 10101 North De Anza Blvd., Cupertino, CA 95014
Phone	Toll free: +1 (800) 228-5651 (sales)
	Voice: +1 (408) 257-1500 (main)
Fax	+1 (408) 257-2003
Website	http://www.trendmicro.com
Email address	support@trendmicro.com

• Worldwide support offices:

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

• Trend Micro product documentation:

  http://docs.trendmicro.com

Related information

↪ *Speeding Up the Support Call*

Speeding Up the Support Call

To improve problem resolution, have the following information available:

• Steps to reproduce the problem

• Appliance or network information

• Computer brand, model, and any additional hardware connected to the endpoint

• Amount of memory and free hard disk space

• Operating system and service pack version

• Endpoint agent version

- Serial number or activation code

- Detailed description of install environment

- Exact text of any error message received

Other Resources

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

Related information

↳ *TrendEdge*
↳ *Download Center*
↳ *TrendLabs*

TrendEdge

Find information about unsupported, innovative techniques, tools, and best practices for Trend Micro products and services. The TrendEdge database contains numerous documents covering a wide range of topics for Trend Micro partners, employees, and other interested parties.

See the latest information added to TrendEdge at:

http://trendedge.trendmicro.com/

Download Center

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

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

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

TrendLabs

TrendLabs℠ is a global network of research, development, and action centers committed to 24x7 threat surveillance, attack prevention, and timely and seamless solutions delivery. Serving as the backbone of the Trend Micro service infrastructure, TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services.

TrendLabs monitors the worldwide threat landscape to deliver effective security measures designed to detect, preempt, and eliminate attacks. The daily culmination of these efforts is shared with customers through frequent virus pattern file updates and scan engine refinements.

Learn more about TrendLabs at:

http://cloudsecurity.trendmicro.com/us/technology-innovation/experts/index.html#trendlabs

About Trend Micro

As a global leader in cloud security, Trend Micro develops Internet content security and threat management solutions that make the world safe for businesses and consumers to exchange digital information. With over 20 years of experience, Trend Micro provides top-ranked client, server, and cloud-based solutions that stop threats faster and protect data in physical, virtualized, and cloud environments.

As new threats and vulnerabilities emerge, Trend Micro remains committed to helping customers secure data, ensure compliance, reduce costs, and safeguard business integrity. For more information, visit:

http://www.trendmicro.com

Trend Micro and the Trend Micro t-ball logo are trademarks of Trend Micro Incorporated and are registered in some jurisdictions. All other marks are the trademarks or registered trademarks of their respective companies.

Index

T

U