TREND MICRO | txOne networks

1.1 Trend Micro Safe Lock™ Intelligent Manager

Installation Guide

A powerful lockdown solution for fixed-function computers

TXOne Edition

Endpoint Security

Document Part No.: SLEM18965/200414

Release Date: April 2020

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

Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that Trend Micro Safe Lock collects and provides detailed instructions on how to disable the specific features that feedback the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Notice:

https://www.trendmicro.com/privacy

Table of Contents

Preface

Chapter 1: Introduction

Chapter 2: Intelligent Manager Deployment Preparation

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
NAT agents	The agents that are built under the routers with the Network Address Translation (NAT) function enabled
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

TERMINOLOGY	DESCRIPTION
Administrator (or Safe Lock Intelligent Manager administrator)	The person managing the Safe Lock Intelligent Manager server
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 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 TXOne Edition 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™

Trend Micro™ Safe Lock Intelligent Manager™ provides centralized monitoring and management of Safe Lock agent deployment, status, and events. For example, administrators can remotely deploy agents, create 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.

What's New

Trend Micro Safe Lock Intelligent Manager TXOne Edition includes the following new features and enhancements:

TABLE 1-1. What's New in Trend Micro Safe Lock Intelligent Manager TXOne Edition

FEATURE	DESCRIPTION
Enhanced Approved List export	The Approved List export feature has been enhanced to include the time a file was added or modified in the list.
Enhanced search filters	Endpoint search filters has been enhanced to include the following: • Support partial search for endpoint names • Display registered agents with a system time that is later than the server system time
New system event logs	This release of Safe Lock Intelligent Manager includes new event logs for Intelligent Manager component updates.

FEATURE	DESCRIPTION
Anti-malware scanning	You can start a manual scan and scheduled scan on agent endpoints from the Intelligent Manager console. **Note** This feature require special licensing. Ensure that you have the correct Activation Code before using this feature. For more information on how to obtain the Activation Code, contact your sales representative.

Server Features and Benefits

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

TABLE 1-2. 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.
Quick Scan	Trend Micro Intelligent Manager provides malware scans of files blocked by application protection and sets actions for the affected files, such as delete, quarantine, or add to Approved List.

FEATURE	BENEFIT
Centralized Agent Management	Trend Micro Intelligent Manager allows administrators to peform the following tasks: • Monitor Safe Lock agent status • Examine connection status • View configurations • Collect agent logs on-demand or by policy • Turn agent Application Lockdown on or off • Enable or disable agent Device Control • Configure agent Maintenance Mode settings • Update agent components • Initialize the Approved List • Deploy agent patches • Add trusted files and USB devices
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.
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.

FEATURE	BENEFIT
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.
Anti-malware scanning	Security risk is the collective term for viruses/malware and spyware/grayware. Safe Lock Intelligent Manager protects endpoints from security risks by scanning files and then performing a specific action for each security risk detected. Notifications and logs help you keep track of security risks and alert you if you need to take immediate action.

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

TABLE 1-3. Required Software for Safe Lock Intelligent Manager

REQUIRED SOFTWARE	SPECIFICATIONS

Operating systems - Windows clients	• Windows 7 No-SP/SP1 (Enterprise/Ultimate) (32-bit and 64-bit)
	• Windows 8 No-SP (Professional/Enterprise) (32-bit and 64-bit)
	• Windows 8.1 No-SP (Professional/Enterprise) (32-bit and 64-bit)
	• Windows 10 (Enterprise/IoT Enterprise) (32-bit and 64-bit)
	  • Anniversary Update (Redstone 1)
	  • Creators Update (Redstone 2)

REQUIRED SOFTWARE	SPECIFICATIONS
Operating systems - Windows server	• Windows Server 2008 SP1/SP2 (Standard/Enterprise/Storage) (32-bit and 64-bit) • Windows Server 2008 R2 No-SP/SP1 (Standard/Enterprise/Storage) (64-bit) • Windows Server 2012 No-SP (Foundation/Essentials/Standard/Datacenter) (64-bit) • Windows Server 2012 R2 No-SP (Foundation/Essentials/Standard/Datacenter) (64-bit) • Windows Server 2012 R2 for Embedded Systems No-SP (64-bit) • Windows Server 2016 (Standard) (64-bit) • Windows Storage Server 2016 • Windows Server 2019 (Standard) (64-bit)
Web browser (for Safe Lock Intelligent Manager web console access)	• Microsoft Internet Explorer 9.0, 10.0, 11.0 (32/64bit) • Microsoft Edge • The latest version of Google Chrome / Chrome Portable • Mozilla Firefox 6 or later **Note** • Older versions of Internet Explorer are unsupported for security enhancement. • When accessed using iOS systems, Safe Lock Intelligent Manager does not support any export functions via the web console.

TABLE 1-4. Required Hardware for Safe Lock Intelligent Manager (without Safe Lock agent)

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

TABLE 1-5. Required Hardware for Safe Lock Intelligent Manager (with Safe Lock agent)

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

TABLE 1-6. Required Hardware for Safe Lock Intelligent Manager (with or without Safe Lock agent) + SQL Express 2008

REQUIRED HARDWARE	SPECIFICATION
RAM	• 4 GB minimum • 8 GB or more recommended
Processor	• 1 CPU core minimum • 2 CPU cores or more recommended

Required Hardware	Specification
Available disk space	• 30 GB minimum • 50 GB or more recommended

Table 1-7. Required Hardware for Safe Lock Intelligent Manager (with or without Safe Lock agent) + SQL Server 2008 / 2012 / 2014 / 2016 / 2017

Required Hardware	Specification
RAM	• 32 GB or more required
Processor	• 2 CPU cores minimum • 4 CPU cores or more recommended
Available disk space	• 1 TB minimum • 2 TB 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

	TASK	ACCOUNT PRIVILEGE REQUIRED
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 • Manage Storage Device Control only • Manage Application Lockdown only
5	Monitor Agent Event logs	• Admin • Full Control • Manage Storage Device Control only • Manage Application Lockdown only • Read Only

	TASK	ACCOUNT PRIVILEGE REQUIRED
6	Download Trend Micro Safe Lock agent installer image	• Admin • Full Control • Manage Storage Device Control only • Manage Application Lockdown only • Read Only
7	Change the administrator password remotely	• Admin
8	Update Safe Lock Intelligent Manager license information	• Admin • Full Control
9	Deploy agent patch	• Admin • Full Control
10	Add trusted files	• Admin • Full Control
11	Manage application lockdown	• Admin • Full Control • Manage Application Lockdown Only
12	Manage storage device control	• Admin • Full Control • Manage Storage Device Control only

	TASK	ACCOUNT PRIVILEGE REQUIRED
13	Check connection	• Admin • Full Control • Manage Storage Device Control only • Manage Application Lockdown only • Read Only
14	Add trusted USB devices	• Admin • Full Control
15	Configure Maitnenance Mode	• Admin • Full Control
16	Update agent components	• Admin • Full Control
17	Agent transfer	• Admin • Full Control

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

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

TABLE 1-8. What's New in Trend Micro Safe Lock TXOne Edition

FEATURE	DESCRIPTION
Enhanced agent-server communication	Safe Lock agent-server communication has been enhanced to support Safe Lock agents with a fixed IP address.
New operating system support	Safe Lock agent installation supports the following operating systems: • Microsoft Windows 10 May 2019 Update (19H1) • Microsoft Windows 10 November 2019 Update (19H2) • Microsoft Windows 10 20H1
Anti-malware scanning	Safe Lock agent provides the scan function that you can start manually on endpoints to scan for malware.
Enhanced event processing	The enhanced Safe Lock data flow and system function processing increase system operation efficiency.

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.

Safe Lock write protection blocks modification and deletion of files, folders, and registry entries.

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.

Approved List Management

When software needs to be installed or updated, you can use one of the following methods 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:

- Maintenance Mode
- Trusted Updater
- Predefined Trusted Updater List
- Command Line Interface (CLI):
    - Trusted hash
    - Trusted certifications

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.

Safe Lock Requirements

This section introduces Safe Lock system requirements and upgrade limitations.

Hardware Requirements

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

TABLE 1-9. 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

Operating Systems

Important

Ensure that the following root certification authority (CA) certificates are installed with intermediate CAs, which are found in `WKSrv.exe`. These root CAs should be installed on the Safe Lock agent environment to communicate with Intelligent Manager.

- Intermediate_Symantec Class 3 SHA256 Code Signing CA
- Root_VeriSign Class 3 Public Primary Certification Authority - G5

To check root CAs, refer to the Microsoft support site:

https://technet.microsoft.com/en-us/library/cc754841.aspx

Note

- Memory Randomization, API Hooking Prevention, and DLL Injection Prevention are not supported on 64-bit platforms.
- See the latest Safe Lock readme file for the most up-to-date list of supported operating systems for agents.

Windows clients:

- Windows 2000 SP4 (32-bit)

  Note

  Safe Lock installed on Windows 2000 SP4 (without update rollup) or Windows XP SP1 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, Maintenance Mode, and Predefined Trusted Updater.

  To support these features, install Filter Manager:

  - For Windows 2000 Service Pack 4, apply the update KB891861 from the Microsoft Update Catalog website.
  - For Windows XP SP1, upgrade to Windows XP SP2.

- Windows XP SP1*/SP2/SP3 (32-bit) (except Starter and Home editions)

Note

- Safe Lock installed on Windows 2000 SP4 (without update rollup) or Windows XP SP1 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, Maintenance Mode, and Predefined Trusted Updater.
- Safe Lock does not support a custom action of "quarantine" on Windows XP.

- 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 No-SP (32-bit and 64-bit)
- Windows 8 No-SP (Professional/Enterprise) (32-bit and 64-bit)
- Windows 8.1 No-SP (Professional/Enterprise with Bing) (32-bit and 64-bit)
- Windows 8.1 No-SP (32-bit and 64-bit)
- Windows 10 (Professional/Enterprise/IoT Enterprise) (32-bit and 64-bit)
  - Anniversary Update (Redstone 1)
  - Creators Update (Redstone 2)
  - Fall Creators Update (Redstone 3)
  - April 2018 Update (Redstone 4)
  - October 2018 Update (Redstone 5)
  - May 2019 Update (19H1)
  - November 2019 Update (19H2)
  - 20H1

Note

- Unlock the endpoint before updating your Windows 10 operating system to the Anniversary Update, Creators Update, Fall Creators Update, April 2018 Update or October 2018 Update.
- OneDrive integration in Windows 10 Fall Creators Update and Spring Creators Update is not supported. Ensure that OneDrive integration is disabled before installing Safe Lock.
- To improve performance, disable the following Windows 10 components:
  - Windows Defender Antivirus. This may be disabled via group policy.
  - Window Update. Automatic updates may require the download of large files which may affect performance.
  - Windows Apps (Microsoft Store) auto-update. Checking for frequent updates may cause performance issues.
- In Windows 10 April 2018 Update (Redstone 4) and later, Safe Lock has the following limitations when working with folders where the `case sensitive` attribute has been enabled:
  - Enabling the `case sensitive` attribute for a folder may prevent Safe Lock from performing certain actions (eg. prescan, quick scan, custom actions) on that folder. Folders that do not have the attribute enabled are not affected.
  - Safe Lock blocks all processes started from folders where the `case sensitive` attribute is enabled. Additionally, Safe Lock is unable to provide any information for the blocked processes, except for file path.
  - The Safe Lock agent cannot verify file signatures of files saved in folders where the `case sensitive` attribute is enabled. As a result, DAC exceptions related to signatures cannot work.

Windows Server:

- Windows 2000 Server SP4* (32-bit)

Note

Safe Lock installed on Windows 2000 SP4 (without update rollup) or Windows XP SP1 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, Maintenance Mode, and Predefined Trusted Updater.

- Windows Server 2003 SP1/SP2 (32-bit)

Note

- Safe Lock installed on Windows 2000 SP4 (without update rollup) or Windows XP SP1 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, Maintenance Mode, and Predefined Trusted Updater.
- Safe Lock does not support a custom action of "quarantine" on Windows XP.

- Windows Server 2003 R2 No-SP/SP2 (Standard/Enterprise/Storage) (32-bit)

Note

- Safe Lock installed on Windows 2000 SP4 (without update rollup) or Windows XP SP1 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, Maintenance Mode, and Predefined Trusted Updater.
- Safe Lock does not support a custom action of "quarantine" on Windows XP.

- 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 Server 2016 (Standard) (64-bit)
- Windows Server 2019 (Standard) (64-bit)

Windows Embedded Standard:

- Windows (Standard) XP Embedded SP1*/SP2 (32-bit)

Note

- Safe Lock installed on Windows 2000 SP4 (without update rollup) or Windows XP SP1 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, Maintenance Mode, and Predefined Trusted Updater.
- Safe Lock does not support a custom action of "quarantine" on Windows XP.

- 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 8 Standard No-SP (32-bit and 64-bit)
- Windows Embedded Standard 8.1 (32-bit and 64-bit)
- Windows Embedded 8.1 Standard (Professional/Industry Pro) (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

- Safe Lock installed on Windows 2000 SP4 (without update rollup) or Windows XP SP1 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, Maintenance Mode, and Predefined Trusted Updater.
- Safe Lock does not support a custom action of "quarantine" on Windows XP.

- Windows Embedded Enterprise Vista (32-bit)
- Windows Embedded Enterprise 7 (32-bit and 64-bit)

Windows Embedded Server:

- Windows Embedded Server 2003 SP1/SP2 (32-bit)

Note

- Safe Lock installed on Windows 2000 SP4 (without update rollup) or Windows XP SP1 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, Maintenance Mode, and Predefined Trusted Updater.
- Safe Lock does not support a custom action of "quarantine" on Windows XP.

- Windows Embedded Server 2003 R2 (32-bit)

Note

- Safe Lock installed on Windows 2000 SP4 (without update rollup) or Windows XP SP1 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, Maintenance Mode, and Predefined Trusted Updater.
- Safe Lock does not support a custom action of "quarantine" on Windows XP.

- 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)

Windows Storage Server

- Windows Storage Server 2016

Agent Upgrade Preparation

Note

This version of Safe Lock supports upgrade from the following versions:

- Safe Lock TXOne Edition

WARNING!

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

Download the latest updates from the Trend Micro Software Download Center. Go to http://downloadcenter.trendmicro.com/.

TABLE 1-10. Fresh Installation of the Safe Lock agent

INSTALLATION METHOD	INSTALLED AGENT VERSION	REQUIRED ACTION	SETTINGS RETAINED
Local installation using Windows Installer	TXOne Edition 1.1	No preparation needed	No settings retained
Local installation using Command Line Interface Installer	TXOne Edition 1.1	Manually uninstall	No settings retained

Installation Method	Installed Agent Version	Required Action	Settings Retained
Remote installation **Note** Safe Lock supports remote installation using Safe Lock Intelligent Manager Intelligent Manager Remote Setup Tool (SLrst).	TXOne Edition 1.1	Manually uninstall	No settings retained

Table 1-11. Post-installation agent upgrade

Installation Method	Installed Agent Version	Required Action	Settings Retained
Patch package For example, running `tmsl_txone_11_win_en.exe`	• TXOne Edition 1.0 • TXOne Edition 1.1	No preparation needed	Compatible settings retained
Remote installation **Note** Safe Lock supports remote patch deployment from Safe Lock Intelligent Manager Intelligent Manager.	• TXOne Edition 1.0 • TXOne Edition 1.1	No preparation needed	Compatible settings retained

Supported Methods for Updating Safe Lock Agents

Safe Lock agents can be updated using the local or remote methods .

Note

The TXOne Edition installation package does not support Safe Lock agent upgrade from previous versions to TXOne Edition. You must install a fresh copy of the Safe Lock TXOne Edition agent on endpoints.

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:

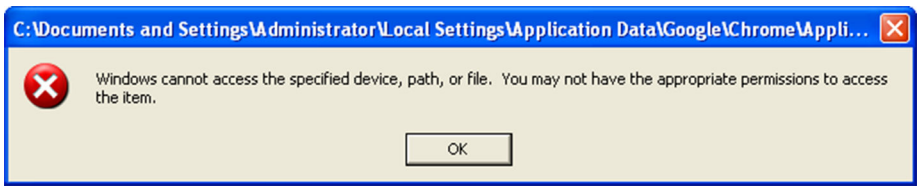


FIGURE 1-1. Trend Micro Safe Lock blocking message

Chapter 2

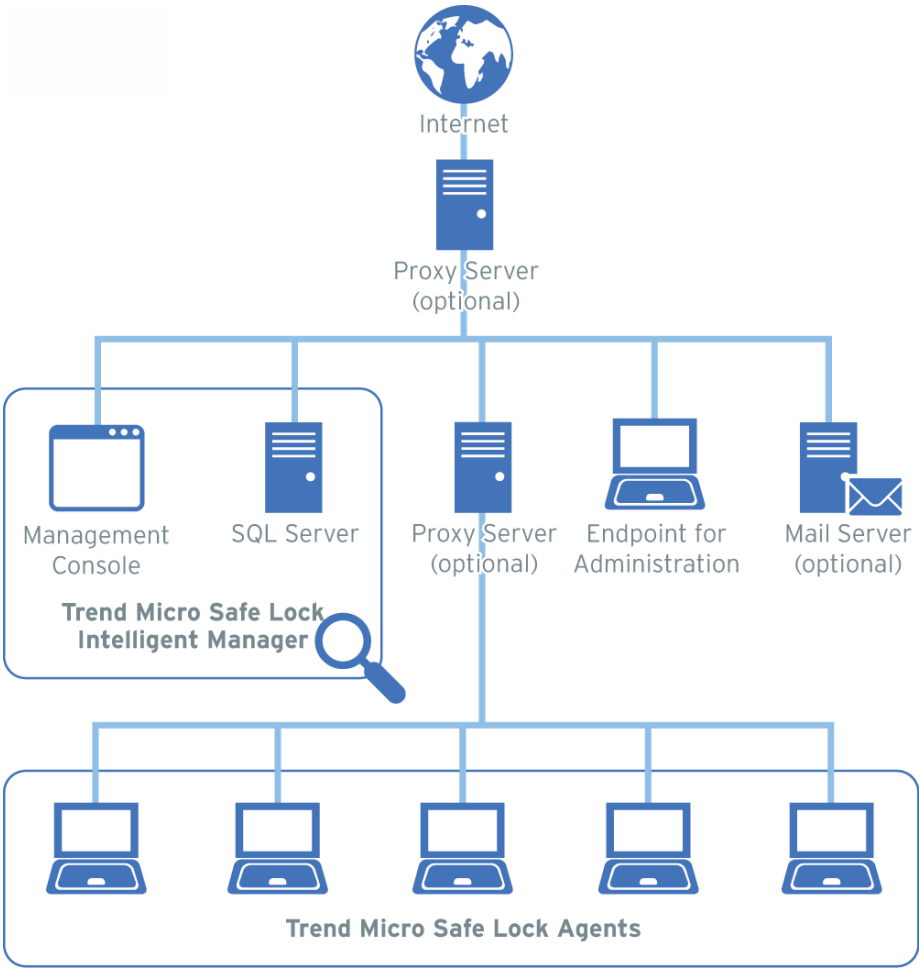
Intelligent Manager Deployment Preparation

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

Topics in this chapter include:

Installation Overview

The following figure displays an example network topology for Safe Lock Intelligent Manager and Trend Micro Safe Lock endpoints:



The following list provides an overview of typical tasks and steps to take during a new installation of Safe Lock Intelligent Manager and Trend Micro Safe Lock endpoints:

Tasks	Steps
To set up Safe Lock Intelligent Manager	1. Prepare for Safe Lock Intelligent Manager installation. See *Server Considerations on page 2-4*. 2. Install Safe Lock Intelligent Manager. See *Intelligent Manager Installation on page 3-1*.
To prepare customizations for Trend Micro Safe Lock installations (optional)	• Prepare customized Setup.ini files. See Trend Micro Safe Lock Intelligent Manager Administrator's Guide > Installation Customization using a Setup.ini File.
To remotely install Trend Micro Safe Lock	1. Prepare for remote installations. See Trend Micro Safe Lock Intelligent Manager Administrator's Guide > Remote Installation Considerations. 2. Remotely install. See Trend Micro Safe Lock Intelligent Manager Administrator's Guide > The Remote Setup Tool (SLrst). 3. Create initial Approved Lists. See Trend Micro Safe Lock Intelligent Manager Administrator's Guide > Updating the Approved List on Safe Lock Agents. 4. Turn on Application Lockdown. See Trend Micro Safe Lock Intelligent Manager Administrator's Guide > The Remote Tasks Tool (SLtasks).

Tasks	Steps
To locally install Trend Micro Safe Lock	1. Download the installer. See Trend Micro Safe Lock Intelligent Manager Administrator's Guide > Downloading an Up-to-Date Agent Installer Package. 2. Install. See Trend Micro Safe Lock Intelligent Manager Administrator's Guide > Local Agent Installation. 3. Create initial Approved Lists. See Trend Micro Safe Lock Intelligent Manager Administrator's Guide > Setting Up the Approved List. 4. Turn on Application Lockdown. See Trend Micro Safe Lock Intelligent Manager Administrator's Guide > About the Agent Console.

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

- Safe Lock Intelligent Manager supports the Mixed Mode Authentication of SQL Server. However, Windows Authentication Mode is not supported.

- 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.

Windows Server 2008 SP1 (32-bit and 64-bit) supports Safe Lock Intelligent Manager, but do not support Microsoft .NET Framework 3.5 Service Pack 1 (a required component of Microsoft SQL Express 2008).

For performance information, see *Server Performance on page 2-6*.

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.

A single Safe Lock Intelligent Manager server can support up to 100,000 agents.

However, the performance of a single Safe Lock Intelligent Manager server still depends on several factors, such as available server resources and network topology. Contact your Trend Micro representative for help in determining the optimal 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. For more details, go to the following site:

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 7 No-SP/SP1 (32-bit and 64-bit)	*Preparing Windows 7 Components on page 2-14*
	Windows 8 No-SP (32-bit and 64-bit)	*Preparing Windows 8 and Windows 10 Components on page 2-13*
	Windows 8.1 No-SP (32-bit and 64-bit)	
	Windows 10 Enterprise (32-bit and 64-bit)	
	Windows 10 IoT Enterprise (32-bit and 64-bit)	

WINDOWS VERSION TYPE	WINDOWS VERSION NAME	PREPARATION STEPS
Windows Server	Windows Server 2008 SP1/SP2 (32-bit and 64-bit)	*Preparing Windows Server 2008 Components on page 2-10*
	Windows Server 2008 R2 No-SP/SP1 (64-bit)	
	Windows Server 2012 No-SP (64-bit)	*Preparing Windows Server 2012, 2016, and 2019 Components on page 2-8*
	Windows Server 2012 No-SP (Foundation/Essentials/Standard/ Datacenter) (64-bit)	
	Windows Server 2012 R2 No-SP (Foundation/Essentials/Standard/ Datacenter) (64-bit)	
	Windows Server 2012 R2 No-SP (64-bit)	
	Windows Server 2012 R2 for Embedded Systems No-SP (64-bit)	
	Windows Server 2016 (Standard) (64-bit)	
	Windows Storage Server 2016	
	Windows Server 2019 (Standard) (64-bit)	

Preparing Windows Server 2012, 2016, and 2019 Components

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

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

- Windows Server 2012 No-SP (Foundation/Essentials/Standard/Datacenter) (64-bit)
- Windows Server 2012 R2 No-SP (Foundation/Essentials/Standard/Datacenter) (64-bit)
- Windows Server 2012 R2 No-SP (64-bit)
- Windows Server 2012 R2 for Embedded Systems No-SP (64-bit)
- Windows Server 2016 (Standard) (64-bit)
- Windows Storage Server 2016
- Windows Server 2019 (Standard) (64-bit)

Procedure

1. Go to **Server Manager** > **Dashboard** > **Add Roles and Features**.
2. On the **Select installation type** screen, select **Role-based or feature-based installation**.
3. In the menu on the left, go to **Server Roles**.
4. In the list, select **Web Server (IIS)**.
5. In the menu on the left, go to **Features**.
6. In the list, select **Message Queuing**.
7. In the menu on the left, go to **Web Server Role (IIS)** > **Role Services**.
8. Enable the following features in the list:
   - Select **Web Server**
   - Under **Web Server**, select **Common HTTP Features**
   - Under **Web Server** > **Common HTTP Features**, select **Static Content**
   - Under **Web Server** > **Application Development**, select the following:

     - **Application Initialization**

- **CGI**

- **ASP.NET 3.5**

9. Click **Install**, and then click **Close** after the process is complete.

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

1. 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

   Note

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

2. 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

3. 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. Enable the following features in the list:

      - Under **Web Server** > **Common HTTP Features**, select **Static Content**
      - Under **Web Server** > **Application Development**, select the following:

        - **CGI**

        - **ASP.NET**

   f. Click **Install**, and then click **Close** after the process is complete.

   g. Back in **Server Manager** again, click **Features** > **Add Features**.

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

   i. Click **Install**, and then click **Close** after the process is complete.

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

1. 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

Important

Windows Server 2008 SP1 (32-bit and 64-bit) supports Safe Lock Intelligent Manager, but do not support Microsoft .NET Framework 3.5 Service Pack 1 (a required component of Microsoft SQL Express 2008).

2. 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. Enable the following features in the list:

- Under **Web Server** > **Common HTTP Features**, select **Static Content**
- Under **Web Server** > **Application Development**, select the following:

  - **CGI**

  - **ASP.NET 3.5**

f. Click **Install**, and then click **Close** after the process is complete.

g. Back in **Server Manager** again, click **Features** > **Add Features**.

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

i. Click **Install**, and then click **Close** after the process is complete.

Preparing Windows 8 and Windows 10 Components

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

- Windows 8.1 No-SP (32-bit and 64-bit)
- Windows 8 No-SP (32-bit and 64-bit)
- Windows 10 Enterprise (32-bit and 64-bit)
- Windows 10 IoT Enterprise (32-bit and 64-bit)

Procedure

1. Press the **Windows key** and **R** to open the **Run** dialog box, and type the following command:

   ```
   Control Panel
   ```

   The **Control Panel** opens in classic mode.

   Note

   For details on other ways to open the **Control Panel**, refer to the following URL:

   https://support.microsoft.com/en-us/help/13764/windows-where-is-control-panel

2. Depending on the current **View by** selected, click one of the following:
   - For **Category** view, click **Programs**.
   - For **Large icons** or **Small icons** view, click **Programs and Features**.
3. Click **Turn Windows features on or off**.
4. In the new window, enable the following features in the list:
   - Select **Microsoft Message Queue (MSMQ) Server**
   - Under **Internet Information Services**, select **World Wide Web Services**
   - Under **Internet Information Services** > **World Wide Web Services** > **Common HTTP Features**, select **Static Content**

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

  - **Application Initialization**

  - **CGI**

  - **ASP.NET**

5. Click **OK** and wait for the process to complete.

Preparing Windows 7 Components

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

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

Procedure

1. 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

2. Press the **Windows key** and **R** to open the **Run** dialog box, and type the following command:

   ```
   Control Panel
   ```

   The **Control Panel** opens in classic mode.

   Note

   For details on other ways to open the **Control Panel**, refer to the following URL:

   https://support.microsoft.com/en-us/help/13764/windows-where-is-control-panel

3. Depending on the current **View by** selected, click one of the following:

- For **Category** view, click **Programs**.
- For **Large icons** or **Small icons** view, click **Programs and Features**.

4. Click **Turn Windows features on or off**.
5. In the new window, enable the following features in the list:
   - Select **Microsoft Message Queue (MSMQ) Server**
   - Under **Internet Information Services**, select **World Wide Web Services**
   - Under **Internet Information Services** > **World Wide Web Services** > **Common HTTP Features**, select **Static Content**
   - Under **Internet Information Services** > **World Wide Web Services** > **Application Development Features**, select the following:

     - **CGI**

     - **ASP.NET**
6. Click **OK** and wait for the process to complete.

Ports Used by the Server

The following table shows the ports that are used by the Safe Lock Intelligent Manager server.

TABLE 2-2. Ports used by the server

PORT	PURPOSE
25	SMTP server connection for sending notifications and reports
443 (default)	Management console access through HTTPS
514	Syslog sever connection for log forwarding
3128	Proxy server connection for component updates and server-agent communication

PORT	PURPOSE
8000 (default)	Agent status update and log collection
8001 (default)	Agent file collection for scanning
14336 (default)	Remote agent installation

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 2-17*.

   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 2-19*.

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 2-22*.
     - *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 2-20*.

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 command with Windows administrator privileges and follow the on-screen instructions:

   ```
   <Safe_Lock_Intelligent_Manager_installation_path>CmdTools
   \Installer\Commands\ConfigSQLSetting.bat
   ```

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 :
  - 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:
  - Ensure that all the necessary software components are installed.

    See *Server Operating Systems and Components on page 2-6*.
  - Check the required hardware and software specifications.

    See *Safe Lock Intelligent Manager Requirements on page 1-5*.
  - Ensure that IP address and DNS settings have been assigned to the target server.

- Gather the following 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*.
  - 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:

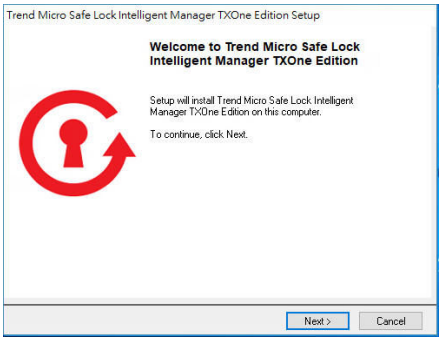
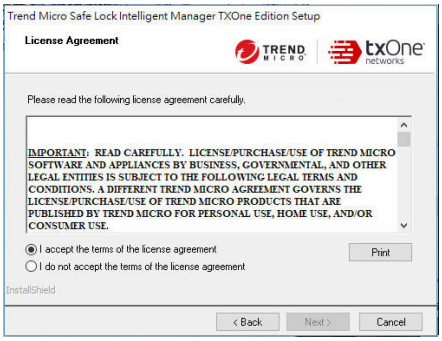
Setup Flow

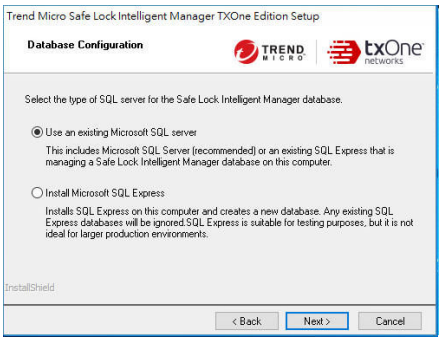
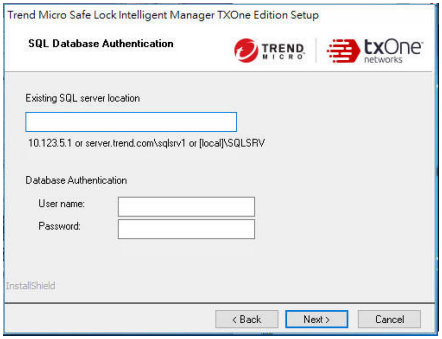
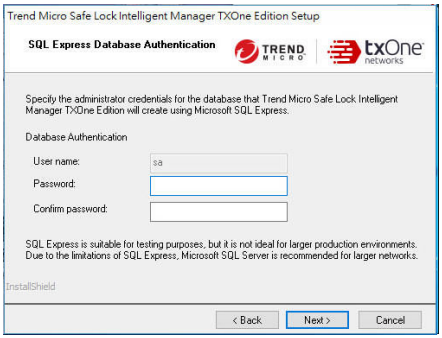
Setup prompts for the following information when installing the Safe Lock Intelligent Manager server.

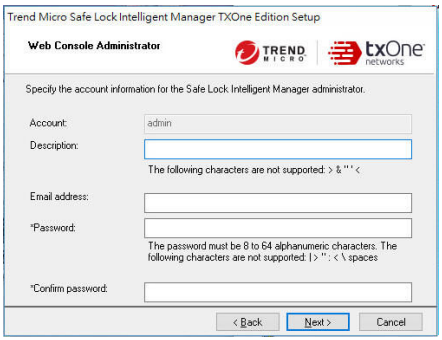
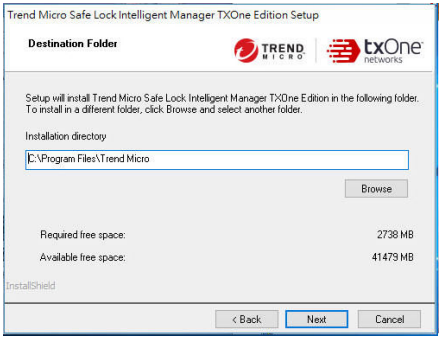
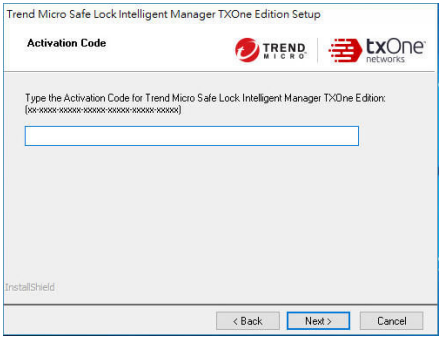
Important

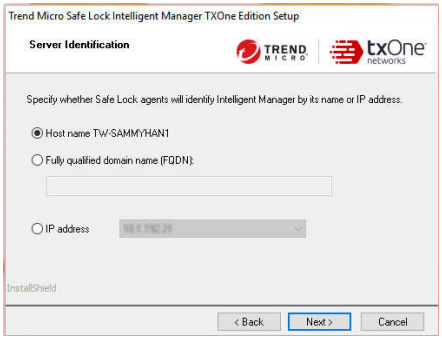
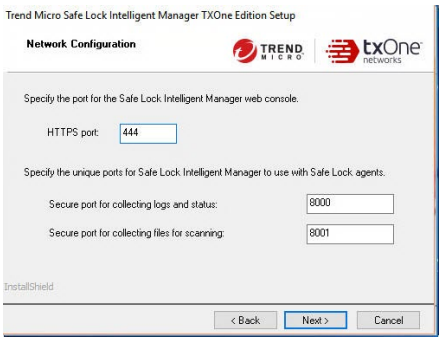
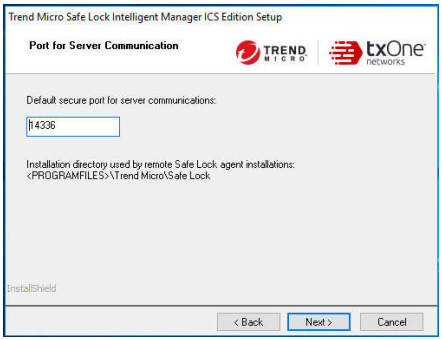
Before running Safe Lock Intelligent Manager Setup, complete the checklist at *Server Installation Checklist on page 2-22*.

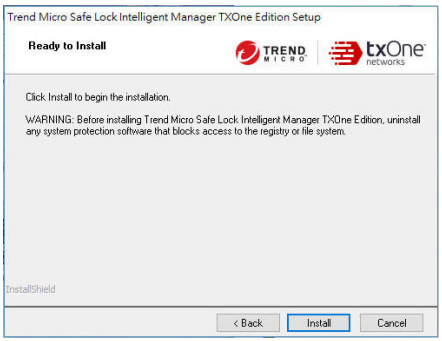
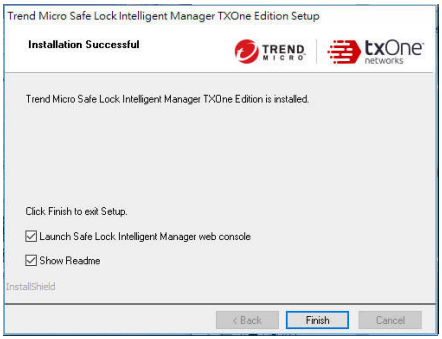
TABLE 3-1. Setup Flow and Required Information

INSTALLER SCREEN	NEEDED INFORMATION
	None
	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
	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 installation path for Safe Lock Intelligent Manager files
	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*. **Tip** For easier migration later, select the host name or specify a fully qualified domain name (FQDN) for this server.
	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
	None
	None

Safe Lock Intelligent Manager Server Installation

Before you begin

For prerequisites, see *Server Installation Checklist on page 2-22*.

Procedure

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

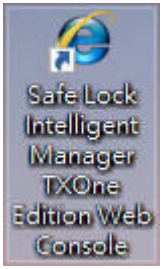


FIGURE 3-1. Web Console Shortcut

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 2-16*.

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.

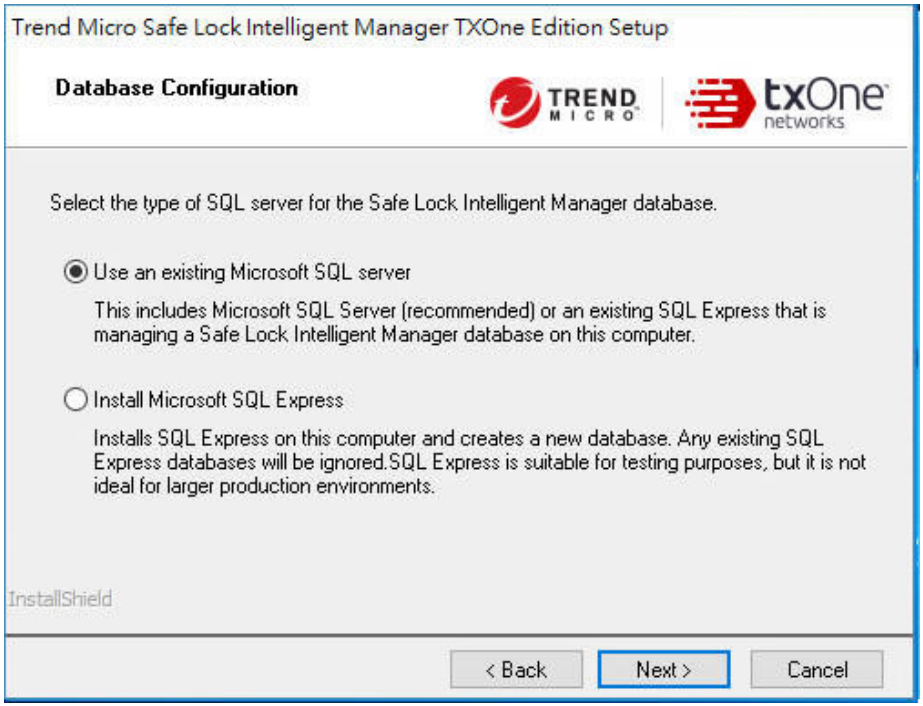


FIGURE 3-2. Configuring the Database Server

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.

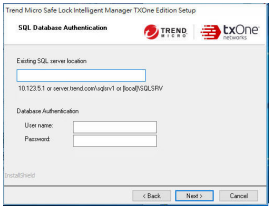
- **Install Microsoft SQL Express**: If you do not have Microsoft SQL Server set up in your environment, Safe Lock Intelligent Manager Setup can install Microsoft™ SQL Server™ 2008 R2 SP2 - Express Edition.

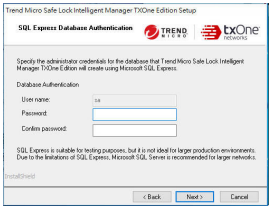
Important

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.

Windows Server 2008 SP1 (32-bit and 64-bit) supports Safe Lock Intelligent Manager, but do not support Microsoft .NET Framework 3.5 Service Pack 1 (a required component of Microsoft SQL Express 2008).

- 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.

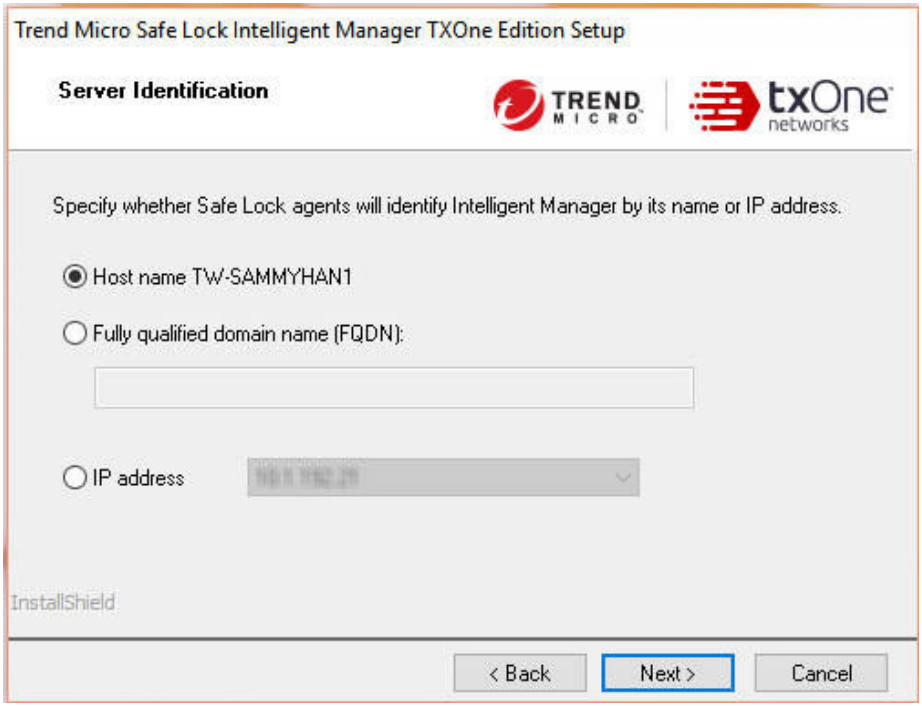


FIGURE 3-5. Configuring the Server Identification

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 2-22*.

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.

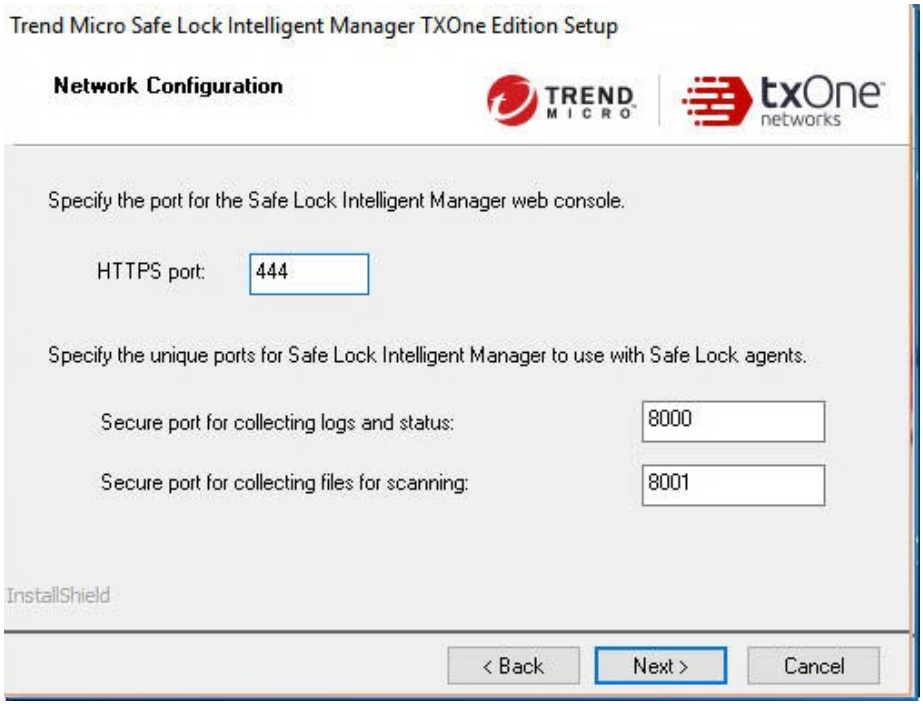


FIGURE 3-6. Configuring the Web Console Settings

Procedure

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

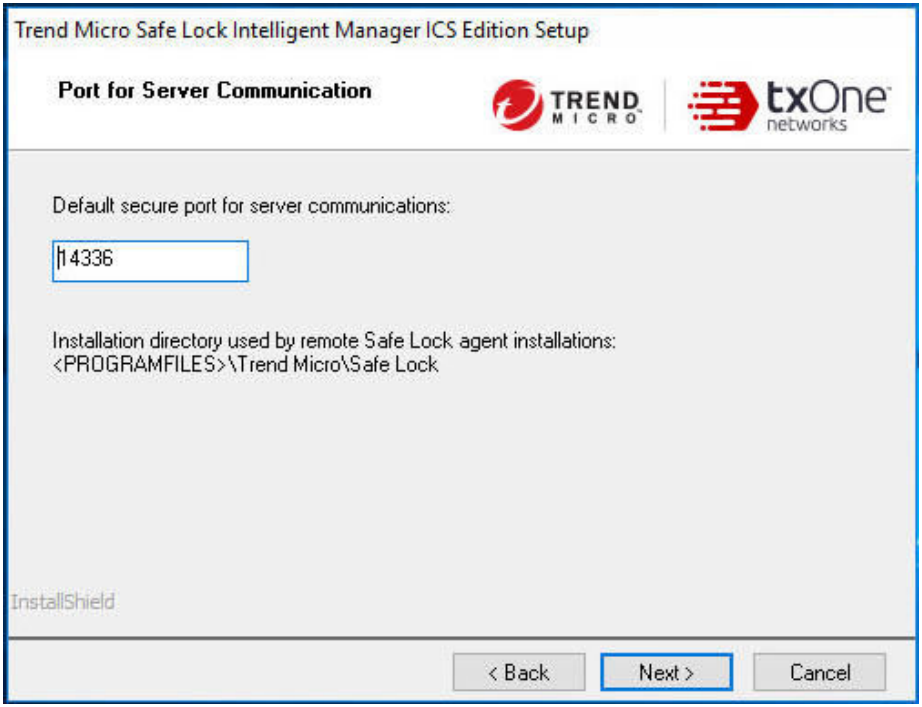


FIGURE 3-7. Setting the Server Communication Port

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. Safe Lock Intelligent Manager 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 2-16*.

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 5.3.29 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

Learn about the following topics:

Troubleshooting Resources

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

Using the Support Portal

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

Procedure

1. Go to http://esupport.trendmicro.com.
2. Select from the available products or click the appropriate button to search for solutions.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Contact Support** and select the type of support needed.

Tip

To submit a support case online, visit the following URL:

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

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

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia

provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to http://about-threats.trendmicro.com/us/threatencyclopedia#malware to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports

Contacting Trend Micro

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

Address	Trend Micro, Incorporated 225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A.
Phone	Phone: +1 (817) 569-8900 Toll-free: (888) 762-8736
Website	http://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:

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

- Trend Micro product documentation:

  http://docs.trendmicro.com

Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional connected hardware or devices
- Amount of memory and free hard disk space
- Operating system and service pack version
- Version of the installed agent
- Serial number or Activation Code
- Detailed description of install environment
- Exact text of any error message received

Sending Suspicious Content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

https://ers.trendmicro.com/

Refer to the following Knowledge Base entry to send message samples to Trend Micro:

http://esupport.trendmicro.com/solution/en-US/1112106.aspx

File Reputation Services

Gather system information and submit suspicious file content to Trend Micro:

http://esupport.trendmicro.com/solution/en-us/1059565.aspx

Record the case number for tracking purposes.

Web Reputation Services

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and malware):

http://global.sitesafety.trendmicro.com/

If the assigned rating is incorrect, send a re-classification request to Trend Micro.

Other Resources

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

Download Center

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

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

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

Documentation Feedback

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

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

Index

T

U

W