TREND MICRO™
Safe Lock™ Intelligent Manager
Service Pack 1 Patch 3
Installation Guide
A powerful lockdown solution for fixed-function computers
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:


© 2018 Trend Micro Incorporated. All Rights Reserved.Trend Micro, the Trend Micro t-ball logo, Trend Micro Safe Lock, Safe Lock Intelligent Manager, Trend Micro Portable Security, Trend Micro Portable Security 2, and TrendLabs are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Document Part No.: SLEM28240/180418

Release Date: July 2018

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:

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.


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

# Table of Contents

## Preface

Preface .................................................................................................................. v  
About the Documentation ................................................................................ v  
Audience ............................................................................................................. vi  
Document Conventions ................................................................................... vi  
Terminology ...................................................................................................... vii

## Chapter 1: Introduction

About Trend Micro Safe Lock Intelligent Manager ................................. 1-2  
  What’s New .............................................................................................  1-2  
  Server Features and Benefits ...............................................................  1-4  
  Safe Lock Intelligent Manager Requirements ......................................  1-6  
  Server Accounts Overview ...................................................................  1-9

About Trend Micro Safe Lock ...................................................................  1-11  
  What’s New ........................................................................................... 1-11  
  Agent Features and Benefits ...............................................................  1-13  
  Safe Lock Requirements ......................................................................  1-15  
  Agent Use Overview ............................................................................  1-23

## Chapter 2: Intelligent Manager Deployment Preparation

Installation Overview ..................................................................................... 2-2

Server Considerations .................................................................................... 2-4  
  Database Requirements ........................................................................ 2-4  
  Server Host Selection ............................................................................. 2-5  
  Server Performance ................................................................................ 2-6

Server Operating Systems and Components ............................................. 2-6  
  Preparing Windows Server 2012 and 2016 Components ..................... 2-8  
  Preparing Windows Server 2008 Components ....................................  2-10  
  Preparing Windows 8 and Windows 10 Components .........................  2-12
Preparing Windows 7 Components .................................................. 2-14
Migrating an Existing Database .......................................................... 2-15
   Exporting an Existing Database ...................................................... 2-16
   Importing a Database ..................................................................... 2-18
   Connecting to an Existing Database .............................................. 2-20
Migrating the Intelligent Manager Program to a New Server Endpoint .................................................................................. 2-21
Server Installation Checklist ....................................................................... 2-21

Chapter 3: Intelligent Manager Installation

Setup Flow ....................................................................................................... 3-2
Safe Lock Intelligent Manager Server Installation ..................................... 3-6
   The Database Configuration Screen .............................................. 3-8
   The Server Identification Screen ................................................. 3-13
   The Network Configuration Screen .............................................. 3-14
   The Destination Folder and Port for Server Communication Screen .................................................................................. 3-16
   About the Web Console Admin Account Password ...................... 3-17
   Configuring a Failover Cluster ....................................................... 3-17

Chapter 4: Intelligent Manager Uninstallation

Preparing to Remove Intelligent Manager .................................................. 4-2
Uninstalling Intelligent Manager ............................................................. 4-3

Chapter 5: Technical Support

Troubleshooting Resources ........................................................................ 5-2
   Using the Support Portal ................................................................... 5-2
   Threat Encyclopedia ........................................................................... 5-2
Contacting Trend Micro ............................................................................ 5-3
   Speeding Up the Support Call ....................................................... 5-4
Sending Suspicious Content to Trend Micro ............................................. 5-4
   Email Reputation Services ............................................................. 5-4
   File Reputation Services ................................................................... 5-5
Web Reputation Services ................................................................. 5-5
Other Resources ...................................................................................... 5-5
Download Center ...................................................................................... 5-5
Documentation Feedback ......................................................................... 5-6

Index

Index .............................................................................................................. IN-1
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 on page v*
- *Audience on page vi*
- *Document Conventions on page vi*
- *Terminology on page vii*

About the Documentation

Trend Micro Safe Lock Intelligent Manager documentation includes the following:

**TABLE 1. Trend Micro Safe Lock Intelligent Manager Documentation**

<table>
<thead>
<tr>
<th>DOCUMENTATION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation Guide</td>
<td>A PDF document that discusses requirements and procedures for installing Safe Lock Intelligent Manager.</td>
</tr>
<tr>
<td>Administrator's Guide</td>
<td>A PDF document that discusses getting started information and Safe Lock Intelligent Manager usage and management.</td>
</tr>
<tr>
<td>Readme file</td>
<td>Contains a list of known issues. It may also contain late-breaking product information not found in the printed documentation.</td>
</tr>
<tr>
<td>Knowledge Base</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td><a href="http://esupport.trendmicro.com">http://esupport.trendmicro.com</a></td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>CONVENTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPPER CASE</td>
<td>Acronyms, abbreviations, and names of certain commands and keys on the keyboard</td>
</tr>
<tr>
<td><strong>Bold</strong></td>
<td>Menus and menu commands, command buttons, tabs, and options</td>
</tr>
<tr>
<td><strong>Italics</strong></td>
<td>References to other documents</td>
</tr>
<tr>
<td>Monospace</td>
<td>Sample command lines, program code, web URLs, file names, and program output</td>
</tr>
<tr>
<td>Navigation &gt; Path</td>
<td>The navigation path to reach a particular screen</td>
</tr>
<tr>
<td></td>
<td>For example, <strong>File &gt; Save</strong> means, click <strong>File</strong> and then click <strong>Save</strong> on the interface</td>
</tr>
</tbody>
</table>

**Note**
Configuration notes
<table>
<thead>
<tr>
<th>CONVENTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tip</td>
<td>Recommendations or suggestions</td>
</tr>
<tr>
<td>Important</td>
<td>Information regarding required or default configuration settings and product limitations</td>
</tr>
<tr>
<td>WARNING!</td>
<td>Critical actions and configuration options</td>
</tr>
</tbody>
</table>

## 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

<table>
<thead>
<tr>
<th>TERMINOLOGY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>The Safe Lock Intelligent Manager server program</td>
</tr>
<tr>
<td>Server endpoint</td>
<td>The host where the Safe Lock Intelligent Manager server is installed</td>
</tr>
<tr>
<td>Agents</td>
<td>The hosts running the Safe Lock program</td>
</tr>
<tr>
<td>NAT agents</td>
<td>The agents that are built under the routers with the Network Address Translation (NAT) function enabled</td>
</tr>
<tr>
<td>Managed agents</td>
<td>The hosts running the Safe Lock program that are known to the Safe Lock Intelligent Manager server program</td>
</tr>
<tr>
<td>Managed endpoints</td>
<td></td>
</tr>
<tr>
<td>Target endpoints</td>
<td>The hosts where the Safe Lock Intelligent Manager managed agents will be installed</td>
</tr>
<tr>
<td><strong>TERMINOLOGY</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Administrator (or Safe Lock Intelligent Manager administrator)</td>
<td>The person managing the Safe Lock Intelligent Manager server</td>
</tr>
<tr>
<td>Web console</td>
<td>The user interface for configuring and managing Safe Lock Intelligent Manager settings and managed agents</td>
</tr>
<tr>
<td>CLI</td>
<td>Command line interface</td>
</tr>
<tr>
<td>License activation</td>
<td>Includes the type of Safe Lock Intelligent Manager server installation and the allowed period of usage that you can use the application</td>
</tr>
</tbody>
</table>
| 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" |
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 1-11*
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 2.0 Service Pack 1 Patch 3 includes the following new features and enhancements:
TABLE 1-1. What's New in Trend Micro Safe Lock Intelligent Manager 2.0 Service Pack 1 Patch 3

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fileless Attack Prevention</td>
<td>Safe Lock Intelligent Manager introduces Fileless Attack Prevention to this release, and provides the following features:</td>
</tr>
<tr>
<td></td>
<td>• Monitors processes, process chains and command line arguments commonly associated with fileless attacks</td>
</tr>
<tr>
<td></td>
<td>• Manage events based on the last 5 parent processes involved in the process chain</td>
</tr>
<tr>
<td></td>
<td>• Manage events based on the command line arguments used</td>
</tr>
<tr>
<td></td>
<td>• Apply action to other endpoints with the same blocked process chains and command line arguments</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Since Fileless Attack Prevention blocks the execution of all target processes by default, ensure that the Fileless Attack Prevention feature has been properly configured to allow the execution of processes required in your environment.</td>
</tr>
<tr>
<td>Agent Management enhancements</td>
<td>Safe Lock Intelligent Manager introduces the following enhancements for agent management:</td>
</tr>
<tr>
<td></td>
<td>• Apply update patch to selected agents remotely</td>
</tr>
<tr>
<td></td>
<td>• Sort agents according to agent version</td>
</tr>
</tbody>
</table>
Audit Log enhancements

Safe Lock Intelligent Manager introduces the following enhancements for the audit logs:

- Support for multiple filters on the Agent Event and Server Event screens
- Export list of deployed endpoints and trusted hashes in the Server Events screen
- Improved deployment details screen:
  - Easier access from the Server Events screen
  - Filter and export of deployment details
  - Inclusion of IP address information

Installer flag for trusted hash list import/export

Safe Lock Intelligent Manager adds the installer flag to the resulting .txt file when importing or exporting the trusted hash list.

Server Features and Benefits

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

**TABLE 1-2. Features and Benefits**

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>BENEFIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>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.</td>
</tr>
<tr>
<td>Quick Scan</td>
<td>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.</td>
</tr>
</tbody>
</table>
Centralized Agent Management
Trend Micro Intelligent Manager allows administrators to perform the following tasks:
- Monitor Safe Lock agent status
- Examine connection status
- View configurations
- Collect agent logs on-demand or by policy
- Remotely turn agent Application Lockdown on or off
- Initialize the Approved List
- Deploy agent patches
- Add trusted files

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.

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

<table>
<thead>
<tr>
<th>Required Software</th>
<th>Specifications</th>
</tr>
</thead>
</table>
| 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) |
<table>
<thead>
<tr>
<th>Required Software</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating systems - Windows server</td>
<td>Windows Server 2008 SP1/SP2 (Standard/Enterprise/Storage) (32-bit and 64-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 R2 No-SP/SP1 (Standard/Enterprise/Storage) (64-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 No-SP (Foundation/Essentials/Standard/Datacenter) (64-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 R2 No-SP (Foundation/Essentials/Standard/Datacenter) (64-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 R2 for Embedded Systems No-SP (64-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2016 (Standard) (64-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows Storage Server 2016</td>
</tr>
</tbody>
</table>

**Note**

Safe Lock Intelligent Manager Intelligent Manager 2.0 SP1 Patch 2 or later no longer supports installation on Windows XP or Windows Server 2003. To update existing installations of Safe Lock Intelligent Manager Intelligent Manager 2.0 SP1 Patch 1 or earlier on these platforms, please install the SP1 Patch 2 or later cumulative patch module.

<table>
<thead>
<tr>
<th>Web browser (for Safe Lock Intelligent Manager web console access)</th>
<th>Microsoft Internet Explorer 9.0, 10.0, 11.0 (32/64bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The latest version of Google Chrome / Chrome Portable</td>
</tr>
<tr>
<td></td>
<td>Mozilla Firefox 6 or later</td>
</tr>
</tbody>
</table>

**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)

<table>
<thead>
<tr>
<th>Required Hardware</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>• 2 GB minimum</td>
</tr>
<tr>
<td></td>
<td>• 4 GB or more recommended</td>
</tr>
<tr>
<td>Processor</td>
<td>• 1 CPU core minimum</td>
</tr>
<tr>
<td></td>
<td>• 1 CPU core or more recommended</td>
</tr>
<tr>
<td>Available disk space</td>
<td>• 10 GB minimum</td>
</tr>
<tr>
<td></td>
<td>• 20 GB or more recommended</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Required Hardware</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>• 2 GB minimum</td>
</tr>
<tr>
<td></td>
<td>• 4 GB or more recommended</td>
</tr>
<tr>
<td>Processor</td>
<td>• 1 CPU core minimum</td>
</tr>
<tr>
<td></td>
<td>• 2 CPU cores or more recommended</td>
</tr>
<tr>
<td>Available disk space</td>
<td>• 10 GB minimum</td>
</tr>
<tr>
<td></td>
<td>• 20 GB or more recommended</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Required Hardware</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>• 4 GB minimum</td>
</tr>
<tr>
<td></td>
<td>• 8 GB or more recommended</td>
</tr>
<tr>
<td>Processor</td>
<td>• 1 CPU core minimum</td>
</tr>
<tr>
<td></td>
<td>• 2 CPU cores or more recommended</td>
</tr>
</tbody>
</table>
### Required Hardware

<table>
<thead>
<tr>
<th></th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available disk space</td>
<td>• 30 GB minimum</td>
</tr>
<tr>
<td></td>
<td>• 50 GB or more recommended</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Required Hardware</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>• 32 GB or more required</td>
</tr>
<tr>
<td>Processor</td>
<td>• 2 CPU cores minimum</td>
</tr>
<tr>
<td></td>
<td>• 4 CPU cores or more recommended</td>
</tr>
<tr>
<td>Available disk space</td>
<td>• 1 TB minimum</td>
</tr>
<tr>
<td></td>
<td>• 2 TB or more recommended</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Task</th>
<th>Account Privilege Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>• Admin</td>
</tr>
</tbody>
</table>
### Trend Micro Safe Lock™ Intelligent Manager Installation Guide

<table>
<thead>
<tr>
<th>Task</th>
<th>Account Privilege Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Use remote deployment tools (<a href="#">SLrst.exe</a>) to centrally deploy agents from the server.</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Using the <a href="#">SLrst.exe</a> tool does not require specific account privileges, but does require the Safe Lock agent password to deploy tasks.</td>
</tr>
<tr>
<td>3. Use the Safe Lock Intelligent Manager console and remote deployment tools (<a href="#">SLtasks.exe</a>) to manage the Approved List and Write Protection List on Safe Lock agents.</td>
<td>Admin, Full Control</td>
</tr>
<tr>
<td>4. Monitor Server Event logs.</td>
<td>Admin, Full Control</td>
</tr>
<tr>
<td>5. Monitor Agent Event logs.</td>
<td>Admin, Full Control, Storage Device Control, Read Only</td>
</tr>
<tr>
<td>6. Download Trend Micro Safe Lock agent installer image.</td>
<td>Admin, Full Control, Storage Device Control, Read Only</td>
</tr>
<tr>
<td>7. Change the administrator password remotely</td>
<td>Admin</td>
</tr>
<tr>
<td>8. Update Safe Lock Intelligent Manager license information</td>
<td>Admin, Full Control</td>
</tr>
</tbody>
</table>
### Introduction

<table>
<thead>
<tr>
<th>Task</th>
<th>Account Privilege Required</th>
</tr>
</thead>
</table>
| 9 Deploy agent patch | • Admin  
• Full Control |
| 10 Add trusted files     | • 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 2.0 Service Pack 1 Patch 3 includes the following new features and enhancements.
### Table 1-8. What’s New in Trend Micro Safe Lock 2.0 Service Pack 1 Patch 3

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform support enhancements</td>
<td>Safe Lock adds support for the following platforms:</td>
</tr>
<tr>
<td></td>
<td>• Windows 10 Professional</td>
</tr>
<tr>
<td></td>
<td>• Windows 10 Fall Creators Update (Redstone 3)</td>
</tr>
<tr>
<td></td>
<td>• Windows 10 April 2018 Update (Redstone 4)</td>
</tr>
<tr>
<td></td>
<td>• Windows Storage Server 2016</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>For more information, see <a href="#">Operating Systems on page 1-16</a>.</td>
</tr>
<tr>
<td>Fileless Attack Prevention</td>
<td>Safe Lock adds Fileless Attack Prevention to this release, and provides the following features:</td>
</tr>
<tr>
<td></td>
<td>• Monitors processes, process chains and command line arguments commonly associated with fileless attacks</td>
</tr>
<tr>
<td></td>
<td>• Manage events based on the last 5 parent processes involved in the process chain</td>
</tr>
<tr>
<td></td>
<td>• Manage events based on the command line arguments used</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Since Fileless Attack Prevention blocks the execution of all target processes by default, ensure that the Fileless Attack Prevention feature has been properly configured to allow the execution of processes required in your environment.</td>
</tr>
</tbody>
</table>
## Windows Event Log enhancements

Safe Lock introduces the following enhancements for the Windows Event Log:

- Default log size increased from 1 MB to 10 MB
- Hash value of the blocked file added to the Windows Event Log

## Support Secure Boot option

Safe Lock adds support for the Secure Boot feature of Windows 10.

## Compatibility with Microsoft BitLocker

Safe Lock adds support for Microsoft BitLocker to ensure compatibility with the Safe Lock agents.

## Trend Micro signature check enhancements

Safe Lock adds an option in setup.ini to enable/disable the Trend Micro signature check for remote patch.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Event Log enhancements</td>
<td>Safe Lock introduces the following enhancements for the Windows Event Log:</td>
</tr>
<tr>
<td></td>
<td>• Default log size increased from 1 MB to 10 MB</td>
</tr>
<tr>
<td></td>
<td>• Hash value of the blocked file added to the Windows Event Log</td>
</tr>
<tr>
<td>Compatibility with Microsoft BitLocker</td>
<td>Safe Lock adds support for Microsoft BitLocker to ensure compatibility with</td>
</tr>
<tr>
<td></td>
<td>the Safe Lock agents.</td>
</tr>
<tr>
<td>Trend Micro signature check enhancements</td>
<td>Safe Lock adds an option in setup.ini to enable/disable the Trend Micro</td>
</tr>
<tr>
<td></td>
<td>signature check for remote patch.</td>
</tr>
</tbody>
</table>

## 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.

**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 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**

<table>
<thead>
<tr>
<th>HARDWARE/SOFTWARE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available disk space</td>
<td>200MB minimum</td>
</tr>
<tr>
<td></td>
<td>300MB recommended</td>
</tr>
<tr>
<td>Monitor resolution</td>
<td>640x480</td>
</tr>
</tbody>
</table>

**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:

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), Windows XP SP1, or Windows Server 2003 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, and Predefined Trusted Updater.

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

- Safe Lock installed on Windows 2000 SP4 (without update rollup), Windows XP SP1, or Windows Server 2003 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, and 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 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)
Note

- Unlock the endpoint before updating your Windows 10 operating system to the Anniversary Update, Creators Update, Fall Creators Update or April 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.
  - Windows 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.

Windows Server:

- Windows 2000 Server SP4* (32-bit)

Note

Safe Lock installed on Windows 2000 SP4 (without update rollup), Windows XP SP1, or Windows Server 2003 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, and Predefined Trusted Updater.

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

Note

- Safe Lock installed on Windows 2000 SP4 (without update rollup), Windows XP SP1, or Windows Server 2003 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, and Predefined Trusted Updater.

- Safe Lock does not support a custom action of “quarantine” on Windows XP or Windows 2003.
- Windows Server 2003 R2 No-SP/SP2 (Standard/Enterprise/Storage) (32-bit)

**Note**
- Safe Lock installed on Windows 2000 SP4 (without update rollup), Windows XP SP1, or Windows Server 2003 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, and Predefined Trusted Updater.
- 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 Server 2016 (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), Windows XP SP1, or Windows Server 2003 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, and 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 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), Windows XP SP1, or Windows Server 2003 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, and 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 Embedded Server:
• Windows Embedded Server 2003 SP1/SP2 (32-bit)
Introduction

Note

- Safe Lock installed on Windows 2000 SP4 (without update rollup), Windows XP SP1, or Windows Server 2003 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, and Predefined Trusted Updater.

- 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 installed on Windows 2000 SP4 (without update rollup), Windows XP SP1, or Windows Server 2003 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, and Predefined Trusted Updater.

- 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)

Windows Storage Server

- Windows Storage Server 2016

Agent Upgrade Preparation

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. Upgrade Actions Required by Installation Method and Installed Agent Version**

<table>
<thead>
<tr>
<th>INSTALLATION METHOD</th>
<th>INSTALLED AGENT VERSION</th>
<th>REQUIRED ACTION</th>
<th>SETTINGS RETAINED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local installation using Windows Installer</td>
<td>1.0</td>
<td>No preparation needed</td>
<td>No settings retained</td>
</tr>
<tr>
<td></td>
<td>1.1</td>
<td>No preparation needed</td>
<td>Compatible settings retained</td>
</tr>
<tr>
<td></td>
<td>2.0 or later</td>
<td>No preparation needed</td>
<td>No settings retained</td>
</tr>
<tr>
<td>Local installation using Command Line Interface Installer</td>
<td>1.0</td>
<td>Manually uninstall</td>
<td>No settings retained</td>
</tr>
<tr>
<td></td>
<td>1.1</td>
<td>No preparation needed</td>
<td>Compatible settings retained</td>
</tr>
<tr>
<td></td>
<td>2.0 or later</td>
<td>Manually uninstall</td>
<td>No settings retained</td>
</tr>
<tr>
<td>Remote installation</td>
<td>1.0</td>
<td>Manually uninstall</td>
<td>No settings retained</td>
</tr>
<tr>
<td></td>
<td>1.1</td>
<td>Manually uninstall</td>
<td>No settings retained</td>
</tr>
<tr>
<td></td>
<td>2.0 or later</td>
<td>Manually uninstall</td>
<td>No settings retained</td>
</tr>
</tbody>
</table>

**Note**
Safe Lock supports remote installation using Safe Lock Intelligent Manager.

**Supported Methods for Updating Safe Lock Agents**

Safe Lock agents can be updated using various methods depending on its current version.
### TABLE 1-11. Supported Methods for Updating Safe Lock Agents

<table>
<thead>
<tr>
<th>CURRENT VERSION</th>
<th>TARGET VERSION</th>
<th>SUPPORTED METHOD FOR UPDATING SAFE LOCK AGENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>LOCAL INSTALLATION</td>
</tr>
<tr>
<td></td>
<td></td>
<td>USING AN INSTALLER</td>
</tr>
<tr>
<td>1.1</td>
<td>Latest version</td>
<td>✓</td>
</tr>
<tr>
<td>2.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.0 Patch 1</td>
<td></td>
<td>✓  ✓</td>
</tr>
<tr>
<td>2.0 SP 1</td>
<td></td>
<td>✓  ✓  ✓</td>
</tr>
<tr>
<td>2.0 SP 1 Patch 1</td>
<td></td>
<td>✓  ✓  ✓</td>
</tr>
<tr>
<td>2.0 SP 1 Patch 2</td>
<td></td>
<td>✓  ✓  ✓  ✓</td>
</tr>
</tbody>
</table>

**Note**

If you are running Safe Lock Intelligent Manager on Windows 2003 or earlier versions, we recommend applying the hotfix for enforcing TLSv10 (tmsl_20_win_en_hfb_enforce_TLSv10.exe) to avoid possible communication issues between the Intelligent Manager and the agent. Refer to the Product Patch tab on the Trend Micro Download Center for details.

---

### 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:

![Trend Micro Safe Lock blocking message](image)

**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 on page 2-2
• Server Considerations on page 2-4
• Server Operating Systems and Components on page 2-6
• Migrating an Existing Database on page 2-15
• Migrating the Intelligent Manager Program to a New Server Endpoint on page 2-21
• Server Installation Checklist on page 2-21
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:

<table>
<thead>
<tr>
<th>TASKS</th>
<th>STEPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>To set up Safe Lock Intelligent Manager</td>
<td>1. Prepare for Safe Lock Intelligent Manager installation.</td>
</tr>
<tr>
<td></td>
<td>See <em>Server Considerations on page 2-4</em>.</td>
</tr>
<tr>
<td></td>
<td>2. Install Safe Lock Intelligent Manager.</td>
</tr>
<tr>
<td></td>
<td>See <em>Intelligent Manager Installation on page 3-1</em>.</td>
</tr>
<tr>
<td>To prepare customizations for Trend Micro</td>
<td>• Prepare customized Setup.ini files.</td>
</tr>
<tr>
<td>To remotely install Trend Micro Safe Lock</td>
<td>1. Prepare for remote installations.</td>
</tr>
<tr>
<td></td>
<td>2. Remotely install.</td>
</tr>
<tr>
<td></td>
<td>3. Create initial Approved Lists.</td>
</tr>
<tr>
<td></td>
<td>4. Turn on Application Lockdown.</td>
</tr>
</tbody>
</table>
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.


- 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 (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 2-6.

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.

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**

<table>
<thead>
<tr>
<th>WINDOWS VERSION TYPE</th>
<th>WINDOWS VERSION NAME</th>
<th>PREPARATION STEPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Clients</td>
<td>Windows 7 No-SP/SP1 (32-bit and 64-bit)</td>
<td>Preparing Windows 7 Components on page 2-14</td>
</tr>
<tr>
<td></td>
<td>Windows 8 No-SP (32-bit and 64-bit)</td>
<td>Preparing Windows 8 and Windows 10 Components on page 2-12</td>
</tr>
<tr>
<td></td>
<td>Windows 8.1 No-SP (32-bit and 64-bit)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows 10 Enterprise (32-bit and 64-bit)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows 10 IoT Enterprise (32-bit and 64-bit)</td>
<td></td>
</tr>
<tr>
<td>WINDOWS VERSION TYPE</td>
<td>WINDOWS VERSION NAME</td>
<td>PREPARATION STEPS</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 R2 No-SP/SP1 (64-bit)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 No-SP (64-bit)</td>
<td>Preparing Windows Server 2012 and 2016 Components on page 2-8</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 No-SP (Foundation/Essentials/Standard/Datacenter) (64-bit)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 R2 No-SP (Foundation/Essentials/Standard/Datacenter) (64-bit)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 R2 No-SP (64-bit)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 R2 for Embedded Systems No-SP (64-bit)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows Server 2016 (Standard) (64-bit)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows Storage Server 2016</td>
<td></td>
</tr>
</tbody>
</table>

**Preparing Windows Server 2012 and 2016 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

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
   - 3.5 Service Pack 1

   **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](http://go.microsoft.com/fwlink/?LinkID=247816)
   - 64-bit: [http://go.microsoft.com/fwlink/?LinkID=247817](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
   - 3.5 Service Pack 1
Important

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

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

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:
Intelligent Manager Deployment Preparation

- 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
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.

---

**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.
   
   
   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 and connect it to Safe Lock Intelligent Manager.

   See *Importing a Database* on page 2-18.

### 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.

h. Click Next >.

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**.

1. 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 `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 `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 2-20.*
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 at the command prompt with Windows administrator privileges:

   ```
   <Safe_Lock_Intelligent_Manager_installation_path>\CmdTools\Installer\SLIM_Install.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 Manager program 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.
  

  • Check the required hardware and software specifications.
  
  See Safe Lock Intelligent Manager Requirements on page 1-6.

  • 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


    • 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 on page 3-2*
• *Safe Lock Intelligent Manager Server Installation on page 3-6*
• *Configuring a Failover Cluster on page 3-17*
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**

<table>
<thead>
<tr>
<th>INSTALLER SCREEN</th>
<th>NEEDED INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Installer Screen 1" /></td>
<td>None</td>
</tr>
<tr>
<td><img src="image2.png" alt="Installer Screen 2" /></td>
<td>None</td>
</tr>
</tbody>
</table>
### INSTALLER SCREEN

<table>
<thead>
<tr>
<th>Database Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the type of SQL server for the Safe Lock Intelligent Manager database.</td>
</tr>
<tr>
<td>- Use an existing Microsoft SQL server: This includes Microsoft SQL Server (recommended) or an existing SQL Express that is managing a Safe Lock Intelligent Manager database on this endpoint.</td>
</tr>
<tr>
<td>- Install Microsoft SQL Express: Installs SQL Express on this endpoint and creates a new database. Any existing SQL Express databases will be ignored. SQL Express is suitable for testing purposes, but it is not ideal for larger production environments.</td>
</tr>
</tbody>
</table>

### 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.
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
<table>
<thead>
<tr>
<th>Installer Screen</th>
<th>Needed Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Identification</strong></td>
<td>The fully qualified domain name (FQDN), host name, or IP address, which allows agents to identify the Safe Lock Intelligent Manager server. See <em>The Server Identification Screen on page 3-13.</em></td>
</tr>
<tr>
<td><strong>Network Configuration</strong></td>
<td>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 <em>The Network Configuration Screen on page 3-14.</em></td>
</tr>
<tr>
<td><strong>Port for Server Communication</strong></td>
<td>The port number, which Safe Lock Intelligent Manager uses to deploy remote agent installation packages. See <em>The Destination Folder and Port for Server Communication Screen on page 3-16.</em></td>
</tr>
</tbody>
</table>
## 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 (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.


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.

![Safe Lock Intelligent Manager Web Console](image)

**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.

![Database Configuration](image)

**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 (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:
<table>
<thead>
<tr>
<th>Selection</th>
<th>Resulting Screen</th>
<th>Information to Specify</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use an existing Microsoft SQL Server</td>
<td><img src="image" alt="Figure 3-3. Configuring the Database Server" /></td>
<td><strong>Existing SQL server location:</strong> Specify the path to the SQL server that hosts the Safe Lock Intelligent Manager database. <strong>User name</strong> and <strong>Password:</strong> Set the password that Safe Lock Intelligent Manager uses to access the database.</td>
</tr>
</tbody>
</table>
### Selection

- **Install Microsoft SQL Express**

### Resulting Screen

![Configuring the Database Server](image)

**FIGURE 3-4. Configuring the Database Server**

### Information to Specify

- **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.


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.

![Setting the Server Communication Port](image)

**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
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.


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.


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](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 on page 4-2
• Uninstalling Intelligent Manager on page 4-3
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.
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 5.3.29 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 on page 5-2
- Contacting Trend Micro on page 5-3
- Sending Suspicious Content to Trend Micro on page 5-4
- Other Resources on page 5-5
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

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:


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:

<table>
<thead>
<tr>
<th>Address</th>
<th>Trend Micro, Incorporated</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>225 E. John Carpenter Freeway, Suite 1500</td>
</tr>
<tr>
<td></td>
<td>Irving, Texas 75062 U.S.A.</td>
</tr>
<tr>
<td>Phone</td>
<td>Phone: +1 (817) 569-8900</td>
</tr>
<tr>
<td></td>
<td>Toll-free: (888) 762-8736</td>
</tr>
<tr>
<td>Website</td>
<td><a href="http://www.trendmicro.com">http://www.trendmicro.com</a></td>
</tr>
<tr>
<td>Email address</td>
<td><a href="mailto:support@trendmicro.com">support@trendmicro.com</a></td>
</tr>
</tbody>
</table>

- Worldwide support offices:
  

- 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:

File Reputation Services

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


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

A
agent installer
  upgrade preparation, 1-22
agents, 1-11
  accounts, 1-14
  features and benefits, 1-13
  operating systems, 1-16
  system requirements, 1-15
  use overview, 1-23
Application Lockdown, 1-13

D
database
  exporting, 2-16
  importing, 2-18
  migrating, 2-15
  requirements, 2-4
  use existing, 2-20
  documentation, v
  documentation feedback, 5-6

E
Exploit Prevention, 1-13

F
features, 1-2
  overview, 1-4
  features and benefits, 1-4

I
installation
  overview, 2-2
installer
  agent, 1-22

O
operating systems, 1-6, 1-16

R
requirements, 1-15

S
Safe Lock, 1-2, 1-11
Safe Lock Intelligent Manager, 1-2
server, 1-2, 3-17
  accounts, 1-9, 3-17
  features and benefits, 1-4
  migration, 2-21
  operating systems, 2-6
  passwords, 3-17
  system requirements, 1-6, 2-5, 2-6
  uninstallation, 4-2, 4-3
server database, 2-20
server installer
  checklist, 2-21
  database configuration, 3-8
  flow, 3-2
  network configuration, 3-14
  password requirements, 3-17
  ports, 3-16
  procedure, 3-6
  server clustering, 3-17
  server identification, 3-13
server preparation, 2-6
  Windows 7, 2-14
  Windows 8, 2-13
  Windows 8.1, 2-13
  Windows Server 2008, 2-11
  Windows Server 2008 R2, 2-10
  Windows Server 2012, 2-9
Windows Server 2012 R2, 2-9
support
resolve issues faster, 5-4
system requirements, 1-6, 1-15
disk space, 1-8
operating systems, 1-6
processor, 1-8
RAM, 1-8
web browsers, 1-7
with SQL Express Server
disk space, 1-9
processor, 1-8, 1-9
RAM, 1-8, 1-9

terminalogy, vii
Trend Micro Portable Security, 1-14

uninstallation, 4-3
upgrading, 1-22

what's new, 1-2