



1.1

Trend Micro Safe Lock™ Agent

Installation Guide

A powerful lockdown solution for fixed-function computers

TXOne Edition



Endpoint Security

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

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

© 2020 Trend Micro Incorporated. All Rights Reserved. Trend Micro, the Trend Micro t-ball logo, Trend Micro Safe Lock, Safe Lock Intelligent Manager, 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.: SLEM18967/200414

Release Date: April 2020

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

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

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

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

Evaluate this documentation on the following site:

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

Privacy and Personal Data Collection Disclosure

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

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

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

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

<https://www.trendmicro.com/privacy>

Table of Contents

Preface

Preface	iii
About the Documentation	iii
Audience	iv
Document Conventions	iv

Chapter 1: Introduction

About Trend Micro Safe Lock	1-2
What's New	1-2
Agent Features and Benefits	1-3
Safe Lock Requirements	1-5
Agent Use Overview	1-13

Chapter 2: Local Agent Installation

Local Installation Overview	2-2
Installing from Windows	2-3
Setting Up the Approved List	2-11
Installation Using the Command Line	2-13
Installer Command Line Interface Parameters	2-14
Customizing Installation Parameters	2-17
Setup.ini File Arguments	2-18

Chapter 3: Agent Configuration File Deployment

Deployment for Standalone Agents	3-2
Exporting or Importing a Configuration File	3-2
Deployment using Intelligent Manager	3-3
Remotely Exporting Agent Settings	3-3
Remotely Importing Agent Settings	3-4

Chapter 4: Local Agent Uninstallation

Uninstalling Agents from Windows	4-2
--	-----

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 and guides administrators through installation and deployment.

Topics in this chapter include:

- *About the Documentation on page iii*
- *Audience on page iv*
- *Document Conventions on page iv*

About the Documentation

Trend Micro Safe Lock documentation includes the following:

TABLE 1. Trend Micro Safe Lock Documentation

DOCUMENTATION	DESCRIPTION
Installation Guide	A PDF document that discusses requirements and procedures for installing Safe Lock .
Administrator's Guide	A PDF document that discusses getting started information and Safe Lock usage and management.
Readme file	Contains a list of known issues. It may also contain late-breaking product information not found in the printed documentation.
Knowledge Base	An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following website: http://esupport.trendmicro.com

Download the latest version of the PDF documents and Readme at:

<http://docs.trendmicro.com>




Audience


Trend Micro Safe Lock documentation is intended for administrators responsible for Safe Lock 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 documentation:

TABLE 2. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
<i>Italics</i>	References to other documents
Monospace	Sample command lines, program code, web URLs, file names, and program output
Navigation > Path	The navigation path to reach a particular screen For example, File > Save means, click File and then click Save on the interface
 Note	Configuration notes
 Tip	Recommendations or suggestions
 Important	Information regarding required or default configuration settings and product limitations

CONVENTION	DESCRIPTION
 WARNING!	Critical actions and configuration options

Chapter 1

Introduction

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

Topics in this chapter include:

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

About Trend Micro Safe Lock

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

What's New

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

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

FEATURE	DESCRIPTION
Enhanced agent-server communication	Safe Lock agent-server communication has been enhanced to support Safe Lock agents with a fixed IP address.
New operating system support	Safe Lock agent installation supports the following operating systems: <ul data-bbox="537 909 1068 1047" style="list-style-type: none">• Microsoft Windows 10 May 2019 Update (19H1)• Microsoft Windows 10 November 2019 Update (19H2)• Microsoft Windows 10 20H1
Anti-malware scanning	Safe Lock agent provides the scan function that you can start manually on endpoints to scan for malware.
Enhanced event processing	The enhanced Safe Lock data flow and system function processing increase system operation efficiency.

Agent Features and Benefits

Trend Micro Safe Lock includes the following features and benefits.

Application Lockdown

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

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

Exploit Prevention

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

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

Approved List Management

When software needs to be installed or updated, you can use one of the following methods to make changes to the endpoint and automatically add new or modified files to the Approved List, all without having to unlock Trend Micro Safe Lock:

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

- Trusted hash
- Trusted certifications

Small Footprint

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

Role Based Administration

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

Graphical and Command Line Interfaces

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

Self Protection

Self Protection provides ways for Trend Micro Safe Lock to defend its processes and resources, required to function properly, from being disabled by programs or actual users.

Self Protection blocks all attempts to terminate the following services:

- Trend Micro Safe Lock Service (`WkSrv.exe`)
- Trend Micro Unauthorized Change Prevention Service (`TMBMSRV.exe`)
- Trend Micro Personal Firewall (`TmPfw.exe`)

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 1-2. Required Hardware for Safe Lock

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



Important

Safe Lock cannot be installed on a system that already runs one of the following:

- Trend Micro OfficeScan
- Trend Micro Titanium
- Another Trend Micro endpoint solution

Operating Systems



Important

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

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

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

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



Note

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

Windows clients:

- Windows 2000 SP4 (32-bit)
-



Note

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

To support these features, install Filter Manager:

- For Windows 2000 Service Pack 4, apply the update KB891861 from the Microsoft Update Catalog website.
 - For Windows XP SP1, upgrade to Windows XP SP2.
-
- Windows XP SP1*/SP2/SP3 (32-bit) (except Starter and Home editions)

**Note**

- Safe Lock installed on Windows 2000 SP4 (without update rollup) or Windows XP SP1 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, Maintenance Mode, and Predefined Trusted Updater.
 - Safe Lock does not support a custom action of “quarantine” on Windows XP.
-
- Windows Vista No-SP/SP1/SP2 (32-bit) (except Starter and Home editions)
 - Windows 7 No-SP/SP1 (32-bit and 64-bit) (except Starter and Home editions)
 - Windows 8 No-SP (32-bit and 64-bit)
 - Windows 8 No-SP (Professional/Enterprise) (32-bit and 64-bit)
 - Windows 8.1 No-SP (Professional/Enterprise with Bing) (32-bit and 64-bit)
 - Windows 8.1 No-SP (32-bit and 64-bit)
 - Windows 10 (Professional/Enterprise/IoT Enterprise) (32-bit and 64-bit)
 - Anniversary Update (Redstone 1)
 - Creators Update (Redstone 2)
 - Fall Creators Update (Redstone 3)
 - April 2018 Update (Redstone 4)
 - October 2018 Update (Redstone 5)
 - May 2019 Update (19H1)
 - November 2019 Update (19H2)
 - 20H1

**Note**

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

Windows Server:

- Windows 2000 Server SP4* (32-bit)

**Note**

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

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

**Note**

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

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

**Note**

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

- Windows Server 2008 SP1/SP2 (32-bit and 64-bit)
- Windows Server 2008 R2 No-SP/SP1 (64-bit)
- Windows Server 2012 No-SP (64-bit)
- Windows Server 2012 R2 No-SP (64-bit)
- Windows Server 2016 (Standard) (64-bit)
- Windows Server 2019 (Standard) (64-bit)

Windows Embedded Standard:

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



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

- Windows Embedded Standard 2009 (32-bit)
- Windows Embedded Standard 7 (32-bit and 64-bit)
- Windows Embedded Standard 8 (32-bit and 64-bit)
- Windows Embedded 8 Standard No-SP (32-bit and 64-bit)
- Windows Embedded Standard 8.1 (32-bit and 64-bit)
- Windows Embedded 8.1 Standard (Professional/Industry Pro) (32-bit and 64-bit)

Windows Embedded POSReady:

- Windows Embedded POSReady (32-bit)
- Windows Embedded POSReady 2009 (32-bit)
- Windows Embedded POSReady 7 (32-bit and 64-bit)

Windows Embedded Enterprise:

- Windows Embedded Enterprise XP SP1*/SP2/SP3 (32-bit)

**Note**

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

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

Windows Embedded Server:

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

**Note**

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

- Windows Embedded Server 2003 R2 (32-bit)
-

**Note**

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

- Windows Embedded Server 2008 (32-bit and 64-bit)
- Windows Embedded Server 2008 R2 (64-bit)

- Windows Embedded Server 2012 (64-bit)
- Windows Embedded Server 2012 R2 (64-bit)

Windows Storage Server

- Windows Storage Server 2016

Agent Upgrade Preparation



Note

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

- Safe Lock TXOne Edition



WARNING!

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

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

TABLE 1-3. Fresh Installation of the Safe Lock agent

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



INSTALLATION METHOD	INSTALLED AGENT VERSION	REQUIRED ACTION	SETTINGS RETAINED
Remote installation <hr/>  Note Safe Lock supports remote installation using Safe Lock Intelligent Manager Remote Setup Tool (SLrst).	TXOne Edition 1.1	Manually uninstall	No settings retained

TABLE 1-4. Post-installation agent upgrade

INSTALLATION METHOD	INSTALLED AGENT VERSION	REQUIRED ACTION	SETTINGS RETAINED
Patch package For example, running <code>tmsl_txone_11_win_en.exe</code>	<ul style="list-style-type: none"> TXOne Edition 1.0 TXOne Edition 1.1 	No preparation needed	Compatible settings retained
Remote installation <hr/>  Note Safe Lock supports remote patch deployment from Safe Lock Intelligent Manager.	<ul style="list-style-type: none"> TXOne Edition 1.0 TXOne Edition 1.1 	No preparation needed	Compatible settings retained

Agent Use Overview

Trend Micro Safe Lock is a whitelist solution that locks down computers, preventing all applications not on the Approved List from running. Safe Lock can be configured and

maintained using the graphical user interface (GUI) agent console or the command line interface (CLI). System updates can be applied without turning off Application Lockdown at the endpoint through the Predefined Trusted Updater List or by using the Trusted Updater.

Consider this typical use case scenario:

1. Set up the Approved List and turn on Application Lockdown on the endpoint so that unapproved applications cannot be run.
2. Use the Trusted Updater to update or install software whose installer is not on the Predefined Trusted Updater list.
3. Configure and enable the Restricted User account for later maintenance.

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

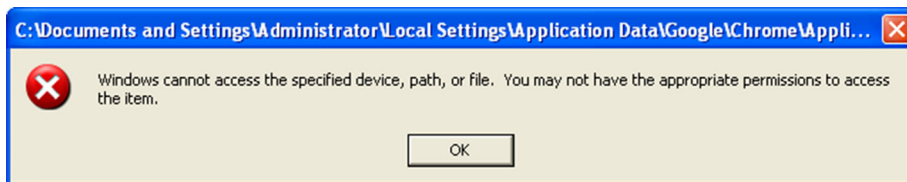


FIGURE 1-1. Trend Micro Safe Lock blocking message

Chapter 2

Local Agent Installation

This chapter describes local Trend Micro Safe Lock agent installation and setup procedures.

Topics in this chapter include:

- *Local Installation Overview on page 2-2*
- *Installing from Windows on page 2-3*
- *Setting Up the Approved List on page 2-11*
- *Installation Using the Command Line on page 2-13*
- *Customizing Installation Parameters on page 2-17*

Local Installation Overview

Procedure

1. Verify that the endpoint meets the Trend Micro Safe Lock system requirements and review any upgrade limitations.

For details, see *Safe Lock Requirements on page 1-5*.



WARNING!

Depending on the installation method selected, some Safe Lock versions may require preparation before upgrading.

For details, see *Agent Upgrade Preparation on page 1-12*.

2. Install Trend Micro Safe Lock using your preferred installation method.

Trend Micro Safe Lock can be installed using either the Windows Installer or the command line interface (CLI) installer.

TABLE 2-1. Safe Lock Local Installation Methods

INSTALLATION METHOD	BENEFITS
Windows Installer	<p>The Windows Installer provides simplified step-by-step installation wizard for first-time or single installation and is also suitable for preparing for mass deployment for cloned endpoint systems.</p> <p>For details, see <i>Installing from Windows on page 2-3</i>.</p>
Command line interface installer	<p>The command line interface (CLI) installer provides silent installation and can be integrated into a batch file for mass deployment.</p> <p>For details, see <i>Installation Using the Command Line on page 2-13</i>.</p>

**Note**

To customize installations using either the Windows Installer or the command line interface (CLI) installer, modify the `Setup.ini` file.

For details, see *Customizing Installation Parameters on page 2-17*.

3. Configure the new installation.
 - a. Open the Trend Micro Safe Lock console and set up the Approved List.

Before Trend Micro Safe Lock can protect the endpoint, it must check the endpoint for existing applications and files necessary for the system to run correctly.

For details, see *Setting Up the Approved List on page 2-11*.
 - b. Modify the Trend Micro Safe Lock settings.

**Note**

Trend Micro recommends turning **Application Lockdown** on after the Approved List has been set up.

For more information, refer to the Trend Micro Safe Lock Agent Administrator's Guide. For details on Trend Micro Safe Lock usage and management, refer to the documentation available at:

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

- c. (Optional) Deploy the updated settings to multiple agents.

To deploy settings to multiple Trend Micro Safe Lock agents, use an agent configuration file.
-

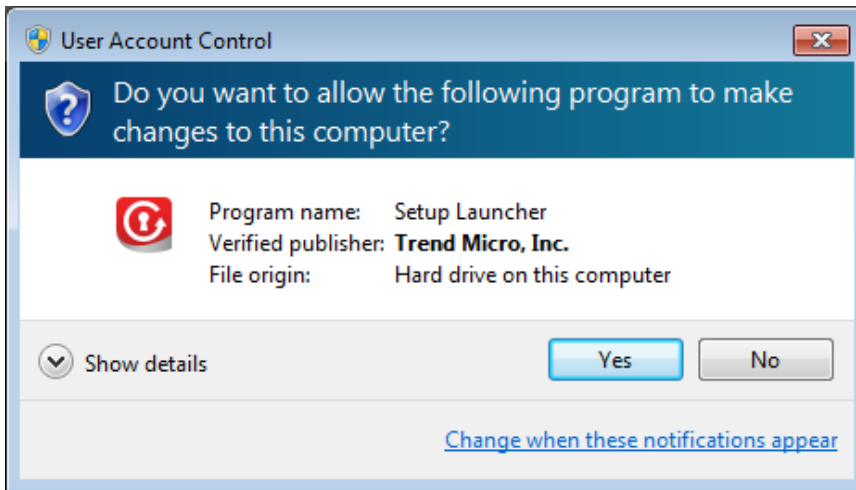
Installing from Windows

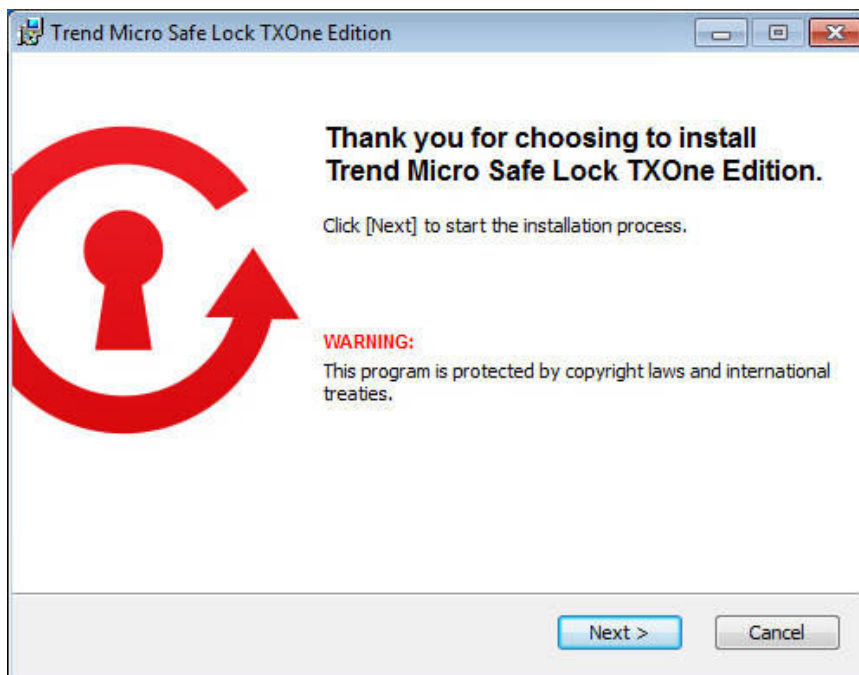
To install Trend Micro Safe Lock, you must log on using an account with administrator privileges.

Procedure

1. Double-click `SL_Install.exe`.

If a **User Account Control** warning from Windows appears, click **Yes**.





2. When the installation wizard opens, click **Next**.

**Note**

If there is another version of Safe Lock on the endpoint, the installer will remove it before installing the latest version.

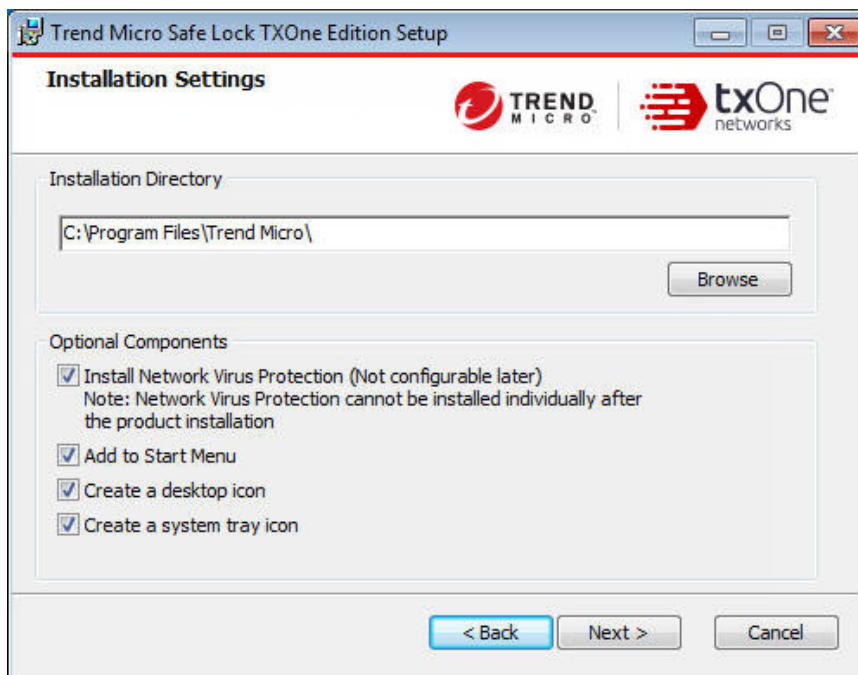
3. Read the license agreement, select **I accept the terms in the License Agreement**, and click **Next**.



4. Make any necessary changes to the installation options, and click **Next**.

**Important**

Network Virus Protection can only be installed during the initial program installation, but it can be disabled after installation, if necessary. See *Exploit Prevention Settings* in the Administrator's Guide for more information.



5. Provide the Activation Code and specify an administrator password for Trend Micro Safe Lock.

**Note**

The password must be 8 to 64 alphanumeric characters. The following characters are not supported: | > < \ " spaces. The Safe Lock administrator password is unrelated to the Windows administrator password.

Trend Micro Safe Lock TXOne Edition Setup

Product Activation Code & Create Administrator Password

TREND MICRO | txOne networks

Product Activation Code

(Format: XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX)

Administrator Password

The password must be 8 to 64 alphanumeric characters. The following characters are not supported: | > < \ ' spaces.

Password:

Confirm Password:

< Back Next > Cancel



WARNING!

Do not forget the Safe Lock administrator password. The only way to recover after losing the Safe Lock administrator password is by reinstalling the operating system.

6. Click **Next**.

A message appears asking if you would like to scan the endpoint for threats before continuing with the installation.



7. (Optional) Scan the endpoint for threats before continuing with the installation. Trend Micro recommends you perform this scan.

- To scan the endpoint for threats, click **Scan**.
 - a. The **Endpoint Prescan** window appears.
 - b. To customize the scan settings, click **Edit Scan Settings**.
 - c. Click **Scan Now**.

If Endpoint Prescan detects security risks, Trend Micro recommends canceling the installation. Remove threats from the endpoint and try again. If critical programs are detected as threats, confirm that the endpoint is secure and that the versions of the programs installed do not contain threats. Ignore detected threats only if you are absolutely certain that they are false positives.



Note

You cannot stop a scan process when you set the PRESCANCLEANUP and FORCE_PRESCAN options in the Setup.ini file.

For more information, see [Prescan Section on page 2-38](#).



Tip

Perform a manual scan to detect and remove threats on endpoints. For more information, see [Manual Scan Commands](#) in the Administrator's Guide.

- To skip scanning, click **Do Not Scan**.
-

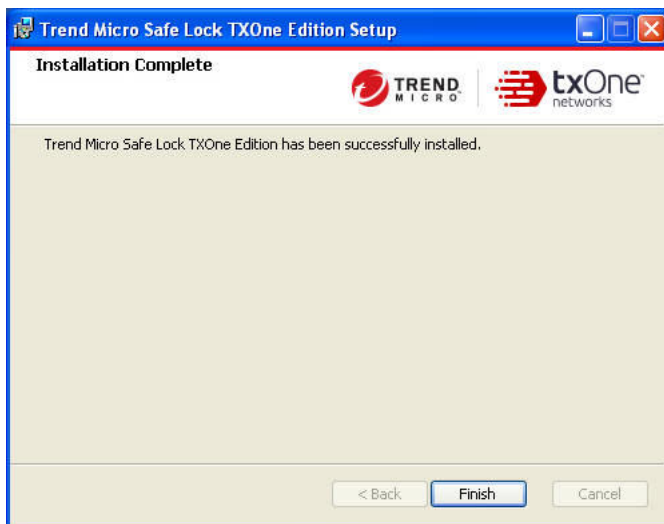


Note

The **Do Not Scan** and close buttons are not applicable when you set the PRESCANCLEANUP and FORCE_PRESCAN options in the Setup.ini file.

For more information, see [Prescan Section on page 2-38](#).

8. When the **Installation Complete** window displays, click **Finish**.



**Note**

Optionally enable memory randomization on older operating systems such as Windows XP or Windows Server 2003, which may lack or offer limited Address Space Layout Randomization (ASLR) support. See *Exploit Prevention Settings* in the Administrator's Guide for more information.

Setting Up the Approved List

Before Trend Micro Safe Lock can protect the endpoint, it must check the endpoint for existing applications and files necessary for the system to run correctly.

Procedure

1. Open the Safe Lock console.

The Safe Lock log on screen appears.

Trend Micro Safe Lock TXOne Edition

Trend Micro Safe Lock

TRTND MICRO | txOne networks

Password:

Log On

License Management

License Type: Full

License Status: Activated

Expiration Date: Unlimited

Use New Code

Cancel

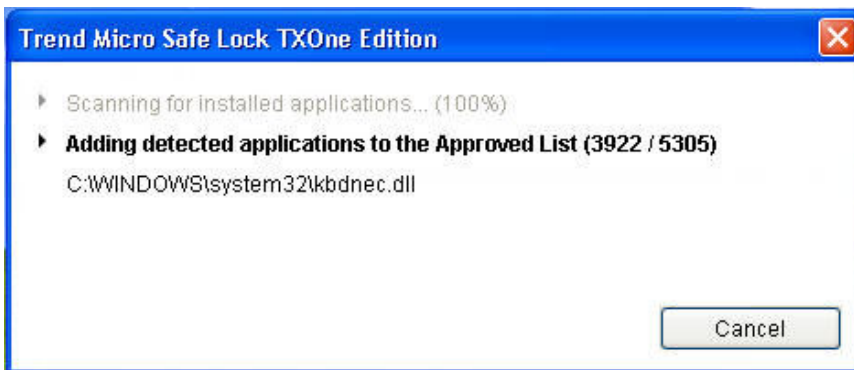
2. Provide the password and click **Login**.

Safe Lock asks if you want to set up the Approved List now.

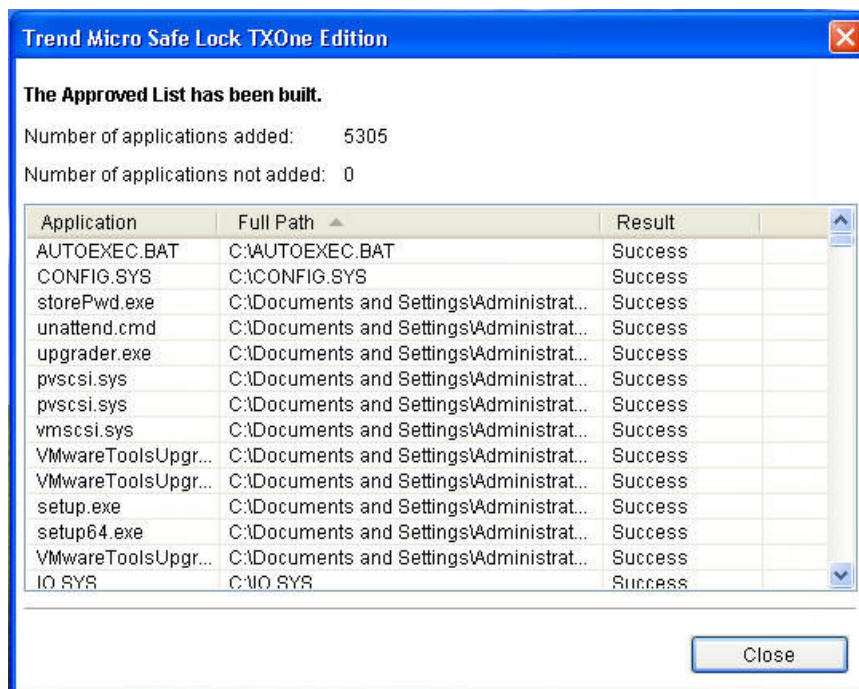


3. At the notification window, select **Yes. Set up the Approved List now** and click **OK**.

Safe Lock scans the endpoint and adds all applications to the Approved List.



Safe Lock displays the Approved List Configuration Results.



Note

When Trend Micro Safe Lock Application Lockdown is on, only applications that are in the Approved List will be able to run.

4. Click **Close**.

Installation Using the Command Line

Administrators can install Safe Lock from the command line interface (CLI) or using a batch file, allowing for silent installation and mass deployment. For mass deployment,

Trend Micro recommends first installing Safe Lock on a test endpoint since a customized installation may require a valid configuration file and Approved List. See the Trend Micro Safe Lock Administrator's Guide for more information about the Approved List and configuration file.

**WARNING!**

- Do not forget the Safe Lock administrator password. The only way to recover after losing the Safe Lock administrator password is by reinstalling the operating system.
 - Make sure to enable memory randomization on older operating systems such as Windows XP or Windows Server 2003, which may lack or offer limited Address Space Layout Randomization (ASLR) support. See *Exploit Prevention Settings* in the Administrator's Guide for more information.
-

**Important**

Network Virus Protection can only be installed during the initial program installation, but it can be disabled after installation, if necessary. See *Exploit Prevention Settings* in the Administrator's Guide for more information.



**Note**


The password must be 8 to 64 alphanumeric characters. The following characters are not supported: | > < \ " spaces. The Safe Lock administrator password is unrelated to the Windows administrator password.

Installer Command Line Interface Parameters

The following table lists the commands available for `SL_Install.exe`.

TABLE 2-2. Safe Lock Installer Command Line Options

PARAMETER	VALUE	DESCRIPTION
-q		<p>Run the installer silently</p> <hr/> <p> Note During the installation process, you can view the following log files in the folder <code>C:\windows\temp</code> to check the status of the the prescan and initial approved process:</p> <ul style="list-style-type: none"> • Prescan process: <code>YYYYMMDDHHMMSS_wk_PreScanProgress.log</code> • Initial approved process: <code>YYYYMMDDHHMMSS_wk_InitListProgress.log</code>
-p	<administrator_password>	Specify the administrator password
-d	<path>	Specify the installation path
-ac	<activation_code>	Specify the activation code
-nd		Do not create a desktop shortcut
-fw		Enable Network Virus Protection
-ns		Do not add a shortcut to the Start menu
-ni		Hide the task tray icon
-cp	<path>	<p>Specify the Safe Lock configuration file</p> <hr/> <p> Note The Safe Lock configuration file can be exported after installing Safe Lock.</p>

PARAMETER	VALUE	DESCRIPTION
-lp	<path>	Specify the Approved List  Note After installing Safe Lock and creating the Approved List, the list can be exported.
-qp	<path>	Specify the folder path for quarantined files when custom action is set to “quarantine” mode.
-nrca		Disable the Root Cause Analysis (RCA) report
-nps		Do not execute Prescan
-ips		Do not cancel installation when Prescan detects threats

An example command line interface (CLI) install would look like this:

```
SL_Install.exe -q -ac XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX -p
P@ssW0rd -nd
```



Important

An administrator password and Activation Code must be specified for the installation to continue.

Customizing Installation Parameters



Note

The installer applies the specified arguments in the following order:

- Encrypted `setup.bin`
- Command line interface (CLI)
- `setup.ini`

If `setup.bin` exists, the installer applies the configuration in `setup.bin` takes precedence and ignores settings from the CLI and `setup.ini` file.

For example, if the switch `-nd` is added to `SL_Install.exe`, and `setup.ini` contains `NO_DESKTOP=0`, the switch will take precedence, and a Safe Lock desktop shortcut will not be created.

To change the default installation parameters using a `Setup.ini` file, follow the steps below.

Procedure

1. Locate the `Setup.ini` file in the installation folder.
2. Customize the installation parameters as required.

For information on installation parameters and their possible values, see [Setup.ini File Arguments on page 2-18](#).

3. Optionally encrypt the `Setup.ini` file to prevent unauthorized access to important settings.
 - a. From the installation folder, copy the `Setup.ini` file and the `WKSsupportTool.exe` file to your desktop.
 - b. Run a command prompt window as administrator.
 - c. Navigate to the desktop and type `WKSsupportTool.exe encryptsetupini Setup.ini Setup.bin` to encrypt the `Setup.ini` file and name the encrypted file as "Setup.bin".

- d. Save the Setup.bin file in the installation folder and remove the Setup.ini file.

Setup.ini File Arguments



Note

The installer applies the specified arguments in the following order:

- Encrypted setup.bin
- Command line interface (CLI)
- setup.ini

If setup.bin exists, the installer applies the configuration in setup.bin takes precedence and ignores settings from the CLI and setup.ini file.

For example, if the switch -nd is added to SL_Install.exe, and setup.ini contains NO_DESKTOP=0, the switch will take precedence, and a Safe Lock desktop shortcut will not be created.

The following tables list the commands available for setup.ini. If no value is specified in the setup file, the default value will be used.

Property Section


The following table lists the commands available for setup.ini. If no value is specified in the setup file, the default value will be used.

TABLE 2-3. Setup.ini File [PROPERTY] Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
ACTIVATION_CODE	Activation Code	<activation_code>	<empty>	No
NO_DESKTOP	Create a shortcut on desktop	<ul style="list-style-type: none"> • 0: Create shortcut 	0	No


KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		<ul style="list-style-type: none"> 1: Do not create shortcut 		
NO_STARTMENU	Create a shortcut in the Start menu	<ul style="list-style-type: none"> 0: Create shortcut 1: Do not create shortcut 	0	No
NO_SYSTRAY	Display the system tray icon and Windows notifications	<ul style="list-style-type: none"> 0: Create system tray icon 1: Do not create system tray icon 	0	No
NO_NSC	Install firewall for network malware protection	<ul style="list-style-type: none"> 0: Create firewall 1: Do not create firewall 	0	No
CONFIG_PATH	Configuration file path	<path>	<empty>	No
LIST_PATH	Approved List path for import	<path>	<empty>	No
APPLICATION FOLDER	Installation path for agent program	<path>	<empty>	No
MANAGED_MODE	Specify if Safe Lock is managed by the Safe Lock Intelligent Manager server	<ul style="list-style-type: none"> 0: Standalone mode 1: Managed mode 	0	No
PASSWORD	Password which is used for SLcmd.exe and Safe Lock console	<password>	<empty>	No


KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
CUSTOM_ACTION	Custom action for blocked events	<ul style="list-style-type: none"> 0: Ignore 1: Quarantine 2: Ask server 	0	No
QUARANTINE_FOLDER_PATH	Quarantine path for agent program	<path>	<empty>	No
ROOT_CAUSE_ANALYSIS	Enable root cause analysis reporting	<ul style="list-style-type: none"> 0: Disable Other value: Enable 	1	No
INTEGRITY_MONITOR	Enable Integrity Monitor	<ul style="list-style-type: none"> 0: Disable 1: Enable 	0	No
PREDEFINED_TRUSTED_UPDATER	Enable Predefined Trusted Updater	<ul style="list-style-type: none"> 0: Disable 1: Enable 	0	No
WINDOWS_UPDATE_SUPPORT	Enable Window Update Support	<ul style="list-style-type: none"> 0: Disable 1: Enable 	0	No
PRESCAN	Prescan the endpoint before installing Safe Lock	<ul style="list-style-type: none"> 0: Do not prescan the endpoint 1: Prescan the endpoint 	1	No
MAX_EVENT_DATABASE_SIZE	Maximum database file size (MB)	Positive integer	1024	No
WEL_SIZE	Windows Event Log size (KB)	Positive integer	10240	No


KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		 Note Default value for new installations. Upgrading Safe Lock does not change any user-defined WEL_SIZE values set in the previous installation.		
WEL_RETENTION	Windows Event Log option when maximum event log size is reached on Windows Event Log.	For Windows XP or earlier platforms: <ul style="list-style-type: none"> • 0: Overwrite events as needed • 1 - 365: Overwrite events older than (1-365) days • -1: Do not overwrite events (Clear logs manually) For Windows Vista or later platforms: <ul style="list-style-type: none"> • 0: Overwrite events as needed (oldest events first) • 1: Archive the log when full, do 	0	No


KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		<p>not overwrite events</p> <ul style="list-style-type: none"> -1: Do not overwrite events (Clear logs manually) 		
WEL_IN_SIZE	Windows Event Log size for Integrity Monitor events (KB)	Positive integer	10240	No
WEL_IN_RETENTION	Windows Event Log option when maximum event log size for Integrity Monitor events is reached on Windows Event Log.	<p>For Windows XP or earlier platforms:</p> <ul style="list-style-type: none"> 0: Overwrite events as needed 1 - 365: Overwrite events older than (1-365) days -1: Do not overwrite events (Clear logs manually) <p>For Windows Vista or later platforms:</p> <ul style="list-style-type: none"> 0: Overwrite events as needed (oldest events first) 1: Archive the log when full, do not overwrite events 	0	No


KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		<ul style="list-style-type: none"> -1: Do not overwrite events (Clear logs manually) 		
USR_DEBUGLOG_ENABLE	Enable debug logging for user sessions	<ul style="list-style-type: none"> 0: Do not log 1: Log 	0	No
USR_DEBUGLOG_LEVEL	The number of debug log entries allowed for user sessions	<ul style="list-style-type: none"> 273 	273	No
SRV_DEBUGLOG_ENABLE	Enable debug logging for service sessions.	<ul style="list-style-type: none"> 0: Do not log 1: Log 	0	No
SRV_DEBUGLOG_LEVEL	The number of debug log entries allowed for service sessions	<ul style="list-style-type: none"> 273 	273	No
SILENT_INSTALL	Execute installation in silent mode	<ul style="list-style-type: none"> 0: Do not use silent mode 1: Use silent mode 	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
	 Important To use silent mode, you must also specify the ACTIVATION_CODE and PASSWORD keys and values. For example: <pre>[PROPERTY] ACTIVATION_CODE=XX-XXXXX-XXXXX-XXXXX-XXXXX PASSWORD=P@ssw0Rd SILENT_INSTALL=1</pre>			
STORAGE_DEVICE_BLOCKING	Blocks storage devices, including CD/DVD drives, floppy disks, and USB devices, from accessing managed endpoints.	<ul style="list-style-type: none"> 0: Allow access from storage devices 1: Block access from storage devices 	0	No
INIT_LIST	Initialize the Approved List during installation	<ul style="list-style-type: none"> 0: Do not initialize the Approved List during installation 1: Initialize the Approved List during installation 	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
	 Note LIST_PATH has priority over INIT_LIST. For example: <pre>[PROPERTY] LIST_PATH=liststore.db INIT_LIST=1</pre> In this case, liststore.db is imported and INIT_LIST is ignored.			
INIT_LIST_PATH	A folder path to be traversed for the Approved List initialization. Each local disk's root directory will be traversed if empty.	<folder path>	<empty>	No
INIT_LIST_PATH_OPTIONAL	A folder path to be traversed for the Approved List initialization. Each local disk's root directory will be traversed if empty.	<folder path>	<empty>	No
INIT_LIST_EXCLUDED_FOLDER	An absolute folder path to exclude from	<folder path>	<empty>	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
	<p>automatic file enumeration for Approved List initialization.</p> <p>The configuration applies to the Approved List first initialized and all subsequent Approved List updates.</p> <p>Specify multiple folders by creating new entries with names that start with <code>INIT_LIST_EXCLUDED_FOLDER.</code> Ensure each entry name is unique. For example:</p> <pre>INIT_LIST_EXCLUDED_FOLDER= c:\folder1 INIT_LIST_EXCLUDED_FOLDER2 =c:\folder2 INIT_LIST_EXCLUDED_FOLDER3 =c:\folder3</pre>	<p> Note</p> <ul style="list-style-type: none"> • Folder path supports a maximum length of 260 characters • Folder paths that do not exist may be specified. • The exclusion applies to subfolders 		

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
INIT_LIST_EXCLUDED_EXTENSION	<p>A file extension to exclude from automatic file enumeration for Approved List initialization.</p> <p>The configuration applies to the Approved List first initialized and all subsequent Approved List updates.</p> <p>Specify multiple extensions by creating new entries with names that start with INIT_LIST_EXCLUDED_EXTENSION. Ensure each entry name is unique. For example:</p> <p>INIT_LIST_EXCLUDED_EXTENSION=bmp</p> <p>INIT_LIST_EXCLUDED_EXTENSION2=png</p>	<p><file extension></p> <hr/> <p> Note</p> <p>Specifying file extensions of executable files (e.g. exe, dll and sys) may cause issues with Application Lockdown.</p> <hr/>	<empty>	No
LOCKDOWN	Turn Application	<ul style="list-style-type: none"> 0: Turn off Application Lockdown 	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
	Lockdown on after installation	<ul style="list-style-type: none"> 1: Turn on Application Lockdown 		
FILELESS_ATTACK_PREVENTION	Enable the Fileless Attack Prevention feature	<ul style="list-style-type: none"> 0: Disable feature 1: Enable feature 	0	No
SERVICE_CREATION_PREVENTION	Enable the Service Creation Prevention feature	<ul style="list-style-type: none"> 0: Disable feature 1: Enable feature 	0	No
	 Note Safe Lock temporarily disables the Service Creation Prevention feature under the following conditions: <ul style="list-style-type: none"> Updating or installing new applications using installers allowed by Trusted Updater. The feature is automatically re-enabled after the Trusted Updater process is complete. Enabling Windows Update Support. Disabling Windows Update Support automatically re-enables the feature. 			
USR_DEBUGLOG_ENABLE	Enable debug log in user session	<ul style="list-style-type: none"> 0: Disable debug log 1: Enable debug log 	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
USR_DEBUGLOGLEVEL	Debug level in user session	273	273	No
SRV_DEBUGLOG_ENABLE	Enable debug log in service session	<ul style="list-style-type: none"> • 0: Disable debug log • 1: Enable debug log 	0	No
SRV_DEBUGLOGLEVEL	Debug level in service session	<ul style="list-style-type: none"> • 273 	273	No
FW_USR_DEBUGLOG	Enable debug log in user session of firewall	<ul style="list-style-type: none"> • 0: Disable debug log • 1: Enable debug log 	0	No
FW_USR_DEBUGLOG_LEVEL	Debug level in user session of firewall	number	273	No
FW_SRV_DEBUGLOG_ENABLE	Enable debug log in service session of firewall	<ul style="list-style-type: none"> • 0: Disable debug log • 1: Enable debug log 	0	No
FW_SRV_DEBUGLOG_LEVEL	Debug level in service session of firewall	number	273	No
BM_SRV_DEBUGLOG_ENABLE	Enable debug log of Behavior Monitoring Core service	<ul style="list-style-type: none"> • 0: Disable debug log • 1: Enable debug log 	0	No
BM_SRV_DEBUGLOG_LEVEL	Debug level of Behavior Monitoring Core service	<ul style="list-style-type: none"> • 51 	51	No

EventLog Section

The following table lists the commands available for `setup.ini`. If no value is specified in the setup file, the default value will be used.

TABLE 2-4. Setup.ini File [EVENTLOG] Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
ENABLE	Log events related to Safe Lock	<ul style="list-style-type: none"> • 1: Log • 0: Do not log 	1	No
LEVEL_WARNINGLOG	Log "Warning" level events related to Safe Lock	<ul style="list-style-type: none"> • 1: Log • 0: Do not log 	1	No
LEVEL_INFORMATIONLOG	Log "Information" level events related to Safe Lock	<ul style="list-style-type: none"> • 1: Log • 0: Do not log 	0	No
BLOCKEDACCESSLOG	Log files blocked by Safe Lock	<ul style="list-style-type: none"> • 1: Log • 0: Do not log 	1	No
APPROVEDACCESSLOG	Log files approved by Safe Lock	<ul style="list-style-type: none"> • 1: Log • 0: Do not log 	1	No
APPROVEDACCESSLOG_TRUSTEDUPDATER	Log Trusted Updater approved access	<ul style="list-style-type: none"> • 1: Log • 0: Do not log 	1	No
APPROVEDACCESSLOG_TRUSTEDHASH	Log Trusted Hash approved access	<ul style="list-style-type: none"> • 1: Log • 0: Do not log 	1	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
APPROVEDACCESSLOG_DLLDRIVER	Log DLL/Driver approved access	<ul style="list-style-type: none"> • 1: Log • 0: Do not log 	0	No
APPROVEDACCESSLOG_EXCEPTIONPATH	Log Application Lockdown exception path approved access	<ul style="list-style-type: none"> • 1: Log • 0: Do not log 	1	No
APPROVEDACCESSLOG_TRUSTEDCERT	Log Trusted Certifications approved access	<ul style="list-style-type: none"> • 1: Log • 0: Do not log 	1	No
APPROVEDACCESSLOG_WRITEPROTECTION	Log Write Protection approved access	<ul style="list-style-type: none"> • 1: Log • 0: Do not log 	1	No
SYSTEMEVENTLOG	Log events related to the system	<ul style="list-style-type: none"> • 1: Log • 0: Do not log 	1	No
SYSTEMEVENTLOG_EXCEPTIONPATH	Log exceptions to Application Lockdown	<ul style="list-style-type: none"> • 1: Log • 0: Do not log 	1	No
SYSTEMEVENTLOG_WRITEPROTECTION	Log Write Protection events	<ul style="list-style-type: none"> • 1: Log • 0: Do not log 	1	No
LISTLOG	Log events related to the Approved list	<ul style="list-style-type: none"> • 1: Log • 0: Do not log 	1	No
USBMALWAREPROTECTIONLOG	Log events that trigger USB Malware Protection	<ul style="list-style-type: none"> • 1: Log • 0: Do not log 	1	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
EXECUTIONPREVENTIONLOG	Log events that trigger Execution Prevention	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
NETWORKVIRUSPROTECTIONLOG	Log events that trigger Network Virus Protection	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
INTEGRITYMONITORINGLOG_FILECREATED	Log file and folder created events	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
INTEGRITYMONITORINGLOG_FILEMODIFIED	Log file modified events	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
INTEGRITYMONITORINGLOG_FILEDELETED	Log file and folder deleted events	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
INTEGRITYMONITORINGLOG_FILERENAMED	Log file and folder renamed events	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
INTEGRITYMONITORINGLOG_REGVALUEMODIFIED	Log registry value modified events	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
INTEGRITYMONITORINGLOG_REGVALUEDELETED	Log registry value deleted events	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
INTEGRITYMONITORINGLOG	Log registry key created events	<ul style="list-style-type: none"> 1: Log 	1	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
_REGKEYCREATED		<ul style="list-style-type: none"> 0: Do not log 		
INTEGRITYMONITORINGLOG_REGKEYDELETED	Log registry key deleted events	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
INTEGRITYMONITORINGLOG_REGKEYRENAMED	Log registry key renamed events	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
DEVICECONTROLLOG	Log events related to device access control	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No

Server Section

The following table lists the commands available for `setup.ini`. If no value is specified in the setup file, the default value will be used.

TABLE 2-5. Setup.ini File [SERVER] Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
HOSTNAME	Server host name	<host_name>	<empty>	No
PORT_FAST	Server listen port for fast lane	1 - 65535	<empty>	No
PORT_SLOW	Server listen port for slow lane	1 - 65535	<empty>	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
CERT	Certificate file name	<certificate_file_name>	<empty>	No
API_KEY	API key	<API_key>	<empty>	No

Agent Section

The following table lists the commands available for `setup.ini`. If no value is specified in the setup file, the default value will be used.

TABLE 2-6. Setup.ini File [AGENT] Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
PORT	Agent listening port	1 - 65535	<empty>	No
SSL_ALLOW_BEAST	Handles possible security flaws in SSL3 and TLS 1.0 protocols for BEAST attacks	<ul style="list-style-type: none"> • 0: Protect against BEAST attacks • 1: Do not implement any security workarounds for BEAST vulnerabilities 	1	No
POLL_SERVER	Identify the agent as an NAT agent	<ul style="list-style-type: none"> • 0: Non-NAT agent • 1: NAT agent 	0	No
POLL_SERVER_INTERVAL	Set the NAT connection frequency	<ul style="list-style-type: none"> • 1 - 64800: Connect to the Safe Lock server every (1 - 64800) minutes 	10	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
FixedIp	Set the agent IP address to communicate with the Safe Lock server.	<ul style="list-style-type: none"> A.B.C.D/E A,B,C,D: 0~255 E: 1~32 	<empty>	No



Note

The POLL_SERVER state can also be toggled from NAT to non-NAT agent by performing one of the following:

- Running SLCmd.exe commands
- Importing another agent's configuration

Message Section

The following table lists the commands available for `setup.ini`. If no value is specified in the setup file, the default value will be used.

TABLE 2-7. Setup.ini File [MESSAGE] Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
REGISTER_TRIGGER	Register message trigger	<ul style="list-style-type: none"> 1: Immediately 2: On demand 	1	No
UNREGISTER_TRIGGER	Unregister message trigger	<ul style="list-style-type: none"> 1: Immediately 2: On demand 	1	No
UPDATESTATUS_TRIGGER	Update status message trigger	<ul style="list-style-type: none"> 1: Immediately 2: On demand 	1	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
UPLOADBLOCKED EVENT_TRIGGER	Upload blocked event message trigger	<ul style="list-style-type: none"> 1: Immediately 2: On demand 	1	No
CHECKFILEHASH_TRIGGER	Check file hash message trigger	<ul style="list-style-type: none"> 1: Immediately 2: On demand 	1	No
QUICKSCANFILE_TRIGGER	Quick scan file message trigger	<ul style="list-style-type: none"> 1: Immediately 2: On demand 	1	No
INITIAL_RETRY_INTERVAL	Starting interval, in seconds, between attempts to resend an event to Intelligent Manager. This interval doubles in size for each unsuccessful attempt, until it exceeds the MAX_RETRY_INTERVAL value.	<ul style="list-style-type: none"> 0 ~ 2147483647 	120	No
MAX_RETRY_INTERVAL	Maximum interval, in seconds, between attempts to resend events to Intelligent Manager.	<ul style="list-style-type: none"> 0 ~ 2147483647 	7680	No

MessageRandomization Section



Note

Safe Lock agents respond as soon as possible to direct requests from Safe Lock Intelligent Manager. For details, refer to Applying Message Time Groups in the Safe Lock Administrator's Guide.

The following table lists the commands available for `setup.ini`. If no value is specified in the setup file, the default value will be used.

TABLE 2-8. Setup.ini File [MESSAGERANDOMIZATION] Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
TOTAL_GROUP_NUM	Number of groups controlled by the server	0 - 2147483646	0	No
OWN_GROUP_IN_DEX	Index of group which this agent belongs to	0 - 2147483646	0	No
TIME_PERIOD	Maximum amount of time agents have to upload data (in seconds)	0 - 2147483647	0	No

Proxy Section

The following table lists the commands available for `setup.ini`. If no value is specified in the setup file, the default value will be used.

TABLE 2-9. Setup.ini File [PROXY] Section Arguments


KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
MODE	Proxy mode	<ul style="list-style-type: none"> 0: No proxy used 1: Proxy used with manual settings 2: Proxy used with settings retrieved from Internet Explorer automatically 	0	No
HOSTNAME	Proxy host name	<host_name>	<empty>	No
PORT	Proxy port	1 - 65535	<empty>	No
USERNAME	Proxy user name	<user_name>	<empty>	No
PASSWORD	Proxy password	<password>	<empty>	No

Prescan Section

The following table lists the commands available for `setup.ini`. If no value is specified in the setup file, the default value will be used.

TABLE 2-10. Setup.ini File [PRESCAN] Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
IGNORE_THREAT	Cancel installation after detecting malware threat during prescan	<ul style="list-style-type: none"> 0: Cancel 1: Continue installation after detecting malware threat during prescan 	0	No


KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		<ul style="list-style-type: none"> 2: Continue installation when no malware is detected, or after all detected malware is cleaned, deleted, or quarantined successfully without a system reboot. 		
REPORT_FOLDER	An absolute folder path where prescan result reports are saved.	<ul style="list-style-type: none"> <folder_path> <empty>: Defaults to %windir%\temp\prescan\log 	<empty>	No
SCAN_TYPE	<p>The type of scan executed during silent installation</p> <hr/>  Note The selected value is used as the default value for a UI installation.	<ul style="list-style-type: none"> Full: Scan all folders on the endpoint. Quick: Scans the following folders: <ul style="list-style-type: none"> Fixed root drives For example: c:\ d:\ System root folder For example, 	Full	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		<p>c:\Windows</p> <ul style="list-style-type: none"> • System folder <p>For example, c:\Windows\System</p> <ul style="list-style-type: none"> • System32 folder <p>For example, c:\Windows\System32</p> <ul style="list-style-type: none"> • Driver folder <p>For example, c:\Windows\System32\Drivers</p> <ul style="list-style-type: none"> • Temp folder <p>For example, c:\Users\ Trend\AppData\Local\Temp</p> <ul style="list-style-type: none"> • Desktop folder including 		

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		<p>sub folders and files</p> <p>For example, c:\Users \Trend \Desktop</p> <ul style="list-style-type: none"> Specific: Scan folders specified with SPECIFIC_FOLDER entries 		
COMPRESS_LAYER	The number of compressed layers to scan when a compressed file is scanned.	<ul style="list-style-type: none"> 0: Do not scan compressed files 1 - 20: Scan up to the specified number of layers of a compressed file 	2	No
MAX_FILE_SIZE	The largest file allowed for scan	<ul style="list-style-type: none"> 0: Scan files of any sizes 1 - 9999: Only scan files equal to or smaller than the specified size (MB) 	0	No
SCAN_REMOVABLE_DRIVE	Scan removable drives	<ul style="list-style-type: none"> 0: Do not scan removable drives 1: Scan removable drives 	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
SPECIFIC_FOLDER	An absolute folder path to scan when the scan type is [Specific]	<p><folder_path></p> <p>Multiple folders can be specified by creating new entries whose name starting with SPECIFIC_FOLDER. Every entry name needs to be unique.</p> <p>For example:</p> <p>SPECIFIC_FOLDER=c:\folder1</p> <p>SPECIFIC_FOLDER2=c:\folder2</p> <p>SPECIFIC_FOLDER3=c:\folder3</p>	<empty>	No
EXCLUDED_FILE	An absolute file path to exclude from scanning	<p><file_path></p> <p>Multiple files can be specified by creating new entries whose name starting with EXCLUDED_FILE. Every entry name needs to be unique.</p> <p>For example:</p> <p>EXCLUDED_FILE=c:\file1.exe</p> <p>EXCLUDED_FILE2=c:\file2.exe</p> <p>EXCLUDED_FILE3=c:\file3.exe</p>	<empty>	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
EXCLUDED_FOLDER	An absolute folder path to exclude from scanning	<p><folder_path></p> <p>Multiple folders can be specified by creating new entries whose name starting with EXCLUDED_FOLDER. Every entry name needs to be unique.</p> <p>For example:</p> <p>EXCLUDED_FOLDER=c:\file1</p> <p>EXCLUDED_FOLDER2=c:\file2</p> <p>EXCLUDED_FOLDER3=c:\file3</p>	<empty>	No
EXCLUDED_EXTENSION	A file extension to exclude from scanning	<p><file_extension></p> <p>Multiple extensions can be specified by creating new entries whose name starting with EXCLUDED_EXTENSION. Every entry name needs to be unique.</p> <p>For example:</p> <p>EXCLUDED_EXTENSION=bmp</p> <p>EXCLUDED_EXTENSION2=png</p>	<empty>	No
PRESCANCLEANUP	Attempt to clean detected	<ul style="list-style-type: none"> 0: No action. This is the default setting 	2	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
	<p>files during prescan</p> <hr/>  Note You must manually include this option in the Setup.ini file. Only valid during silent installations.	<p>for installations using the Windows Installer.</p> <ul style="list-style-type: none"> • 1: Clean, or delete if the clean action is unsuccessful • 2: Clean, or quarantine if the clean action is unsuccessful • 3: Clean, or ignore if the clean action is unsuccessful 		
FORCE_PRESCAN	Perform a prescan before installation	<ul style="list-style-type: none"> • 0: Disable • 1: Enable 	0	No

BlockNotification Section

The following table lists the notification commands available for `setup.ini`. If no value is specified in the setup file, the default value will be used.

See [Property Section on page 2-18](#) for more information.



Important

To enable the feature, make sure to also enable the display for system tray icons and notifications. See `NO_SYSTRAY` in this table for details.

TABLE 2-11. Setup.ini File [BlockNotification] Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
ENABLE	Display notifications on managed endpoints when Safe Lock blocks an unapproved file.	<ul style="list-style-type: none"> • 0: Disable • 1: Enable 	0	No
ALWAYS_ON_TOP	Display the file blocking notification on top of other screens.	<ul style="list-style-type: none"> • 0: Disable • 1: Enable 	1	No
SHOW_DETAILS	Display file name, file path, and event time in the notification.	<ul style="list-style-type: none"> • 0: Disable • 1: Enable 	1	No
AUTHENTICATE	Authenticate the user by requesting the administrator password when closing the notification.	<ul style="list-style-type: none"> • 0: Disable • 1: Enable 	1	No
TITLE	Notification title	<notification_title>	<empty>	No
MESSAGE	Notification content	<notification_content>	<empty>	No

Chapter 3

Agent Configuration File Deployment

This chapter describes the deployment of settings to multiple Trend Micro Safe Lock agents using an Agent Configuration File.

Deployment for Standalone Agents

Agents installed in `Standalone` mode are not managed by a Trend Micro Safe Lock Intelligent Manager server. To manually deploy a single configuration to multiple `Standalone` agents, use an agent configuration file.

Exporting or Importing a Configuration File



Note

Trend Micro Safe Lock encrypts the configuration file before export. Users must decrypt the configuration file before modifying the contents.

For details, refer to the Safe Lock Agent Administration Guide available at:

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

Procedure

1. Open the Trend Micro Safe Lock console using the desktop icon (if available) or the **Start** menu by clicking **All Programs > Trend Micro Safe Lock**.
2. Provide the password and click **Login**.
3. Click the **Settings** menu item to access the **Export/Import Configuration** section.

To export the configuration file as a database (`.xen`) file:

- a. Click **Export**, and choose the location to save the file.
- b. Provide a filename, and click **Save**.

To import the configuration file as a database (`.xen`) file:

- a. Click **Import**, and locate the database file.
- b. Select the file, and click **Open**.

Trend Micro Safe Lock overwrites the existing configuration settings with the settings in the database file.

Deployment using Intelligent Manager

Agents installed in *Managed* mode are managed by a Trend Micro Safe Lock Intelligent Manager server, which can issue remote commands to all managed agents. To deploy agent configuration settings to multiple managed agents, launch the Trend Micro Safe Lock Intelligent Manager web console and use the **Send Command** menu located on the **Agent Management** screen.

Remotely Exporting Agent Settings

You can remotely obtain agent configuration settings and Approved Lists by exporting and downloading them from the Intelligent Manager.

Procedure

1. Click **Agents** from the Intelligent Manager console.
The **Agent Management** screen appears.
2. Select a target endpoint.
3. Click **Send Command**, select **Export Settings**, and select one of the following:
 - **Approved List**
 - **Agent Configuration**

The Intelligent Manager starts issuing the command. The progress can be viewed from the pop-up **Details** window.

4. To export more settings, repeat the above steps.

When the exports are complete, you will be confirmed by this message on the top of the screen:

 One or more agent settings are exported and ready for download. [View Details](#)

5. Click **View Details** to download the exported settings.

**Note**

Intelligent Manager can keep up to 20 sets of exported settings and cleans any file from this list as soon as the file is downloaded.

Remotely Importing Agent Settings

You can remotely apply new agent settings to agents or agent groups from the Trend Micro Safe Lock Intelligent Manager web console. This feature allows you to:

- Remotely overwrite agent configurations
- Remotely overwrite Approved Lists
- Remotely add approved items to Approved Lists

Procedure

1. Prepare a customized agent configuration file or Approved List.
 - a. Export and download an agent configuration file or Approved List. For detailed steps, see [Remotely Exporting Agent Settings on page 3-3](#).
 - b. Customize the downloaded file.

**Note**

To ensure successful import, verify that the file to import meets the following requirements:

- File is in the CSV format and uses UTF-8 encoding
 - For Approved List, maximum file size supported is 20 MB
 - For agent configuration file, maximum file size supported is 1 MB
-

2. Click **Agents** from the Trend Micro Safe Lock Intelligent Manager console.

The **Agent Management** screen appears.

3. To import the customized file to one or more ungrouped agents or agents in different groups, follow the steps below.

- a. From the Endpoint column, select one or more agents.
- b. Click **Send Command**.
- c. Select **Import Settings**.
- d. Select **Approved List** or **Agent Configuration**.

The import dialog appears.

4. To import the customized file to an agent group, follow the steps below.

- a. From the left panel, right-click an agent group and go to **Send Command > Import Settings**.
- b. Select **Approved List** or **Agent Configuration**.

The import dialog appears.

5. By default, Trend Micro Safe Lock Intelligent Manager does the following:

- **Approved List:** accumulates items from the customized Approved List to the target Approved Lists. To replace the target Approved Lists with the customized Approved List, select **Overwrite the existing Approved List**.
- **Agent Configuration:** overwrites the target Approved Lists with the customized Approved List.

6. Click **Browse** to select the customized file.
 7. Click **Import and Apply**.
-

Chapter 4

Local Agent Uninstallation

This chapter describes Trend Micro Safe Lock agent uninstallation procedures.

Topics in this chapter include:

- *Uninstalling Agents from Windows on page 4-2*

Uninstalling Agents from Windows



Note

The Safe Lock administrator password is required to uninstall the software from the endpoint.

Procedure

1. On an endpoint with the Safe Lock agent installed, launch Trend Micro Safe Lock Setup.

Depending on your operating system, do one of the following:

OPTION	DESCRIPTION
<p>If you use one of the following operating systems:</p> <ul style="list-style-type: none"> • Windows 10 Enterprise • Windows 10 IoT Enterprise • Windows 10 Professional • Windows 10 Fall Creators Update (Redstone 3) • Windows 10 April 2018 Update (Redstone 4) • Windows 10 October 2018 Update (Redstone 5) 	<ol style="list-style-type: none"> a. Go to Start > Settings. b. Depending on your version of Windows 10, locate the Apps & features section under one of the following categories: <ul style="list-style-type: none"> • System • Apps c. On the left pane, click Apps & features. d. In the list, click Trend Micro Safe Lock. e. Click Uninstall.
<p>If you use one of the following operating systems:</p> <ul style="list-style-type: none"> • Windows 7 • Windows 8 • Windows Vista • Windows Server 2008 	<ol style="list-style-type: none"> a. Go to Start > Control Panel > Programs and Features. b. In the list, double-click Trend Micro Safe Lock.

OPTION	DESCRIPTION
<ul style="list-style-type: none">• Windows Server 2012• Windows Server 2016• Windows Storage Server 2016• Windows Server 2019	
If you use one of the following operating systems: <ul style="list-style-type: none">• Windows Server 2003• Windows XP• Windows 2000	<ol style="list-style-type: none">a. Go to Start > Control Panel > Add or Remove Programs.b. In the list, select Trend Micro Safe Lock.c. Click Remove.

Safe Lock Setup opens in uninstaller mode.

2. After Safe Lock Setup opens, click **Next**.
 3. Provide the Safe Lock administrator password, and click **Next**.
 4. After the software is finished uninstalling, click **Finish**.
-

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

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



Tip

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

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

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

Threat Encyclopedia

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

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

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

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

Contacting Trend Micro

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

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

- Worldwide support offices:
<http://www.trendmicro.com/us/about-us/contact/index.html>
- Trend Micro product documentation:
<http://docs.trendmicro.com>

Speeding Up the Support Call

To improve problem resolution, have the following information available:

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

Sending Suspicious Content to Trend Micro

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

Email Reputation Services

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

<https://ers.trendmicro.com/>

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

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

File Reputation Services

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

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

Record the case number for tracking purposes.

Web Reputation Services

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

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

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

Other Resources

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

Download Center

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

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

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

Documentation Feedback

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

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

Index

A

- agent configuration file
 - exporting or importing, 3-2
- agent installer
 - approved list, 2-11
 - command line interface, 2-13, 2-14
 - overview, 2-2
 - Setup.ini Agent section, 2-34
 - Setup.ini arguments, 2-18
 - Setup.ini BlockNotification section, 2-44
 - Setup.ini EventLog section, 2-30
 - Setup.ini MessageRandomization section, 2-37
 - Setup.ini Message section, 2-35
 - Setup.ini Prescan section, 2-38
 - Setup.ini Property section, 2-18
 - Setup.ini Proxy section, 2-37
 - Setup.ini Server section, 2-33
 - Setup.ini use, 2-17
 - upgrade preparation, 1-12
 - Windows Installer, 2-3
- agents, 1-2
 - accounts, 1-4
 - features and benefits, 1-3
 - operating systems, 1-6
 - system requirements, 1-5
 - uninstallation, 4-2
 - use overview, 1-13
- Application Lockdown, 1-3
- Approved List
 - setting up, 2-11

D

- documentation, iii

- documentation feedback, 5-6

E

- Exploit Prevention, 1-3

I

- installation
 - customization, 2-17
 - methods, 2-2
- installer
 - agent, 1-12

N

- Network Virus Protection, 2-6, 2-14

O

- operating systems, 1-6

R

- requirements, 1-5

S

- Safe Lock, 1-2
- Self Protection, 1-4
- support
 - resolve issues faster, 5-4
- system requirements, 1-5

U

- uninstallation, 4-2
- upgrading, 1-12

