TREND MICRO™

2.0 Trend Micro Safe Lock™

Service Pack 1 Patch 1

Installation Guide

A powerful lockdown solution for fixed-function computers

Endpoint Security

Document Part No.: SLEM27766/170331

Release Date: April 2017

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

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

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

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

Evaluate this documentation on the following site:

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

Table of Contents

Index

Preface

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

Topics in this chapter include:

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
Italics	References to other documents
`Monospace`	Sample command lines, program code, web URLs, file names, and program output
Navigation > **Path**	The navigation path to reach a particular screen For example, **File** > **Save** means, click **File** and then click **Save** on the interface
Note	Configuration notes
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 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

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

What's New in Trend Micro Safe Lock 2.0 SP 1 Patch 1

Trend Micro Safe Lock 2.0 SP1 Patch 1 includes the following new features and enhancements.

TABLE 1-1. Features

FEATURE	DESCRIPTION
Platform support	Trend Micro Safe Lock now supports Windows 10.
Protection against storage device access	You can allow or block storage device access to managed endpoints.
Application lockdown enhancement	Application lockdown is enhanced with pop-up notifications on managed endpoints to inform the latest application blocking. This notification is disabled by default. To enable the feature, use the `SLCmd.exe` program.
Enhanced security of agent settings	The agent Setup.ini file can now be encrypted to prevent unauthorized access to important settings such as the password.

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.

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

Note

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

TABLE 1-3. List of Supported Operating Systems

WINDOWS VERSION TYPE	WINDOWS VERSION NAME
Windows Clients	Windows 2000 SP4 (32-bit)

WINDOWS VERSION TYPE	WINDOWS VERSION NAME
	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 8.1 No-SP (32-bit and 64-bit)
	Windows 10 Enterprise (32-bit and 64-bit)

WINDOWS VERSION TYPE	WINDOWS VERSION NAME
	Note • Make sure to unlock the endpoint before updating your Windows 10 operating system for the Anniversary Update. • **Memory Randomization** is not supported on operating systems running Windows 10 Creators Update.
	Windows 10 IoT Enterprise (32-bit and 64-bit) **Note** • Make sure to unlock the endpoint before updating your Windows 10 operating system for the Anniversary Update. • **Memory Randomization** is not supported on operating systems running Windows 10 Creators Update.
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)

WINDOWS VERSION TYPE	WINDOWS VERSION NAME
	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 (32-bit and 64-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 Embedded Standard	Windows (Standard) XP Embedded SP1*/SP2 (32-bit)

WINDOWS VERSION TYPE	WINDOWS VERSION NAME
	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 Standard 8.1 (32-bit and 64-bit)
Windows Embedded POSReady	Windows Embedded POSReady (32-bit)
	Windows Embedded POSReady 2009 (32-bit)
	Windows Embedded POSReady 7 (32-bit and 64-bit)
Windows Embedded Enterprise	Windows Embedded Enterprise XP SP1*/SP2/SP3 (32-bit) **Note** • 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 VERSION TYPE	WINDOWS VERSION NAME
	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), 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)

Note

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

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 1-4. Upgrade Actions Required by Installation Method and Installed Agent Version

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

Installation Method	Installed Agent Version	Required Action	Settings Retained
Remote installation **Note** Safe Lock supports remote installation using Safe Lock Intelligent Manager.	1.0	Manually uninstall	No settings retained
	1.1	Manually uninstall	No settings retained
	2.0 or later	Manually uninstall	No settings retained

Agent Use Overview

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

Consider this typical use case scenario:

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

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

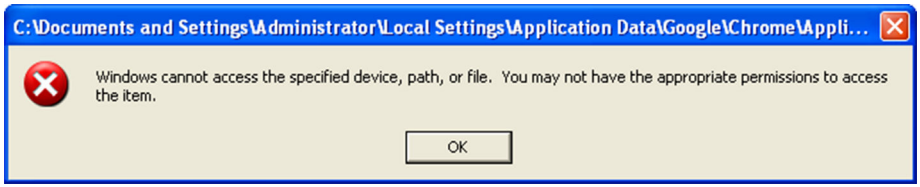


FIGURE 1-1. Trend Micro Safe Lock blocking message

Chapter 2

Local Agent Installation

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

Topics in this chapter include:

Local Installation Overview

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	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 computer systems.
Command line interface installer	The command line interface (CLI) installer provides silent installation and can be integrated into a batch file for mass deployment.

WARNING!

Depending on the installation method you select, Safe Lock versions require different preparation before upgrading. See *Agent Upgrade Preparation on page 1-11* for more information.

To customize installations using either the Windows Installer or the command line interface (CLI) installer, modify the Setup.ini file. See *Customizing Installation Parameters on page 2-14*.

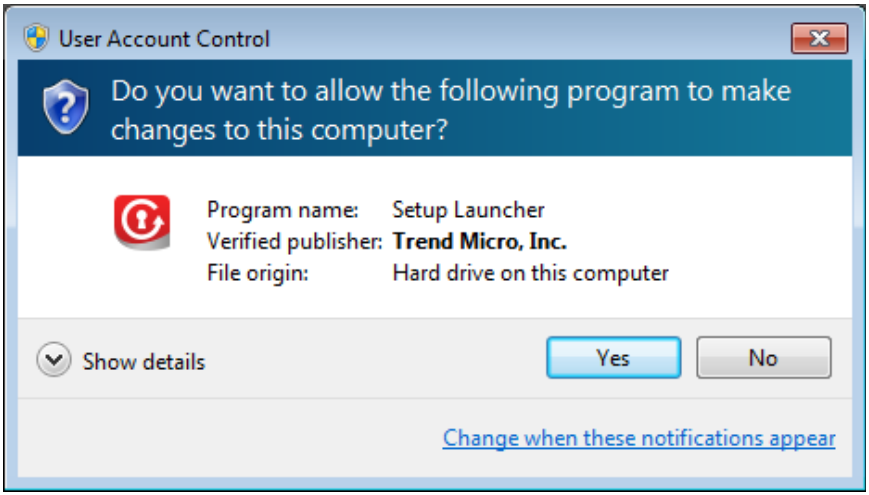
Installing from Windows

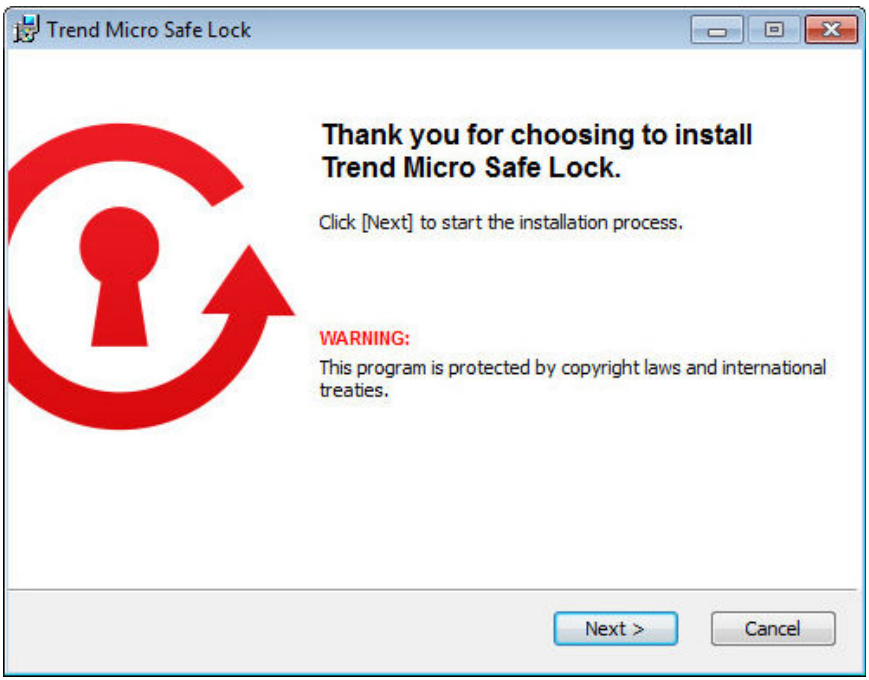
To install Trend Micro Safe Lock, you must log on using an account with administrator privileges.

Procedure

1. Double-click `SL_Install.exe`.

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


User Account Control
Do you want to allow the following program to make changes to this computer?
Program name: Setup Launcher
Verified publisher: Trend Micro, Inc.
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear

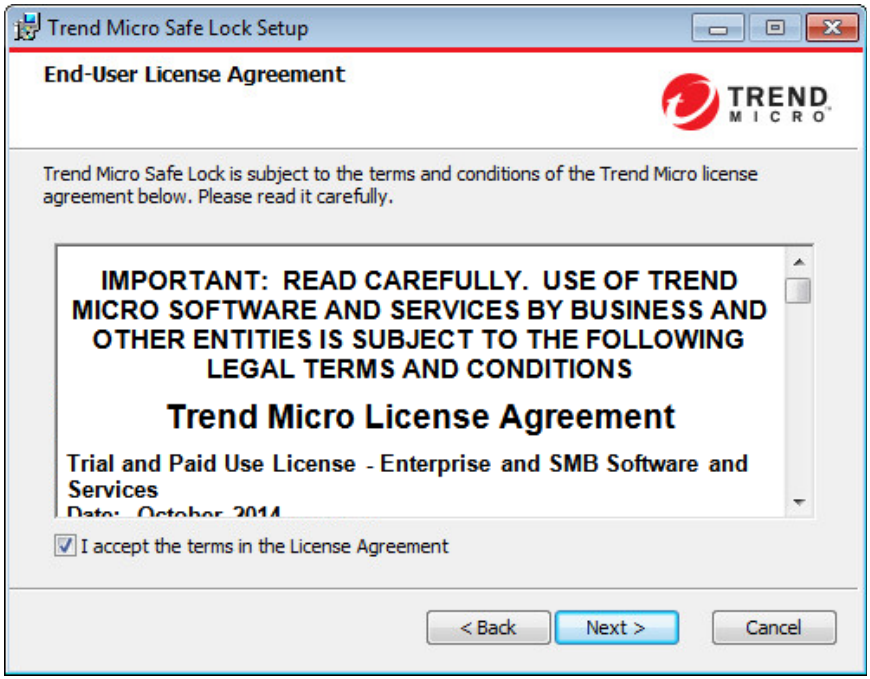

Trend Micro Safe Lock
Thank you for choosing to install Trend Micro Safe Lock.
Click [Next] to start the installation process.
WARNING:
This program is protected by copyright laws and international treaties.
Next >
Cancel

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.

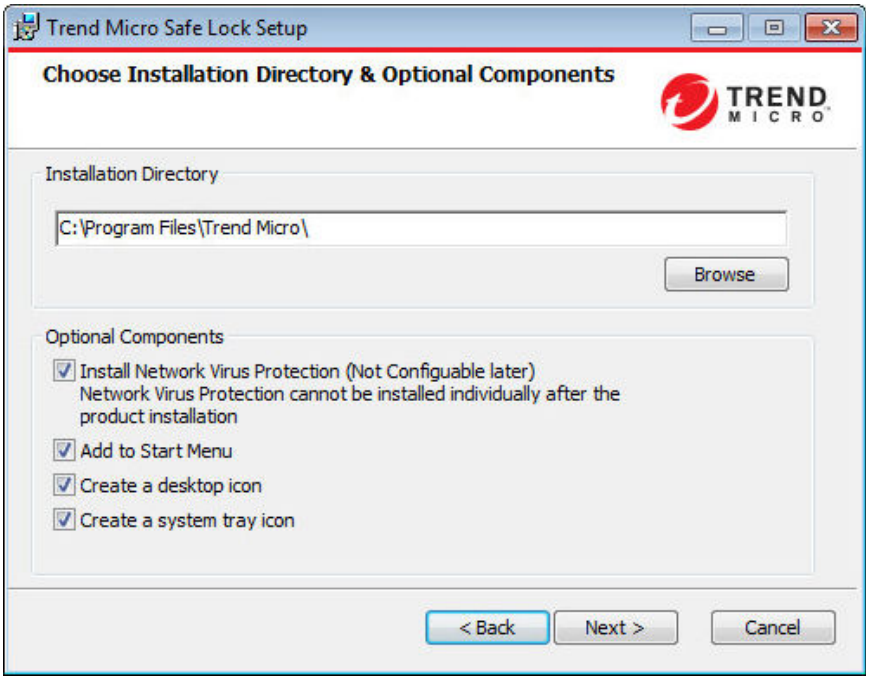
3. Read the license agreement, select **I accept the terms in the License Agreement**, and click **Next**.



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

Important

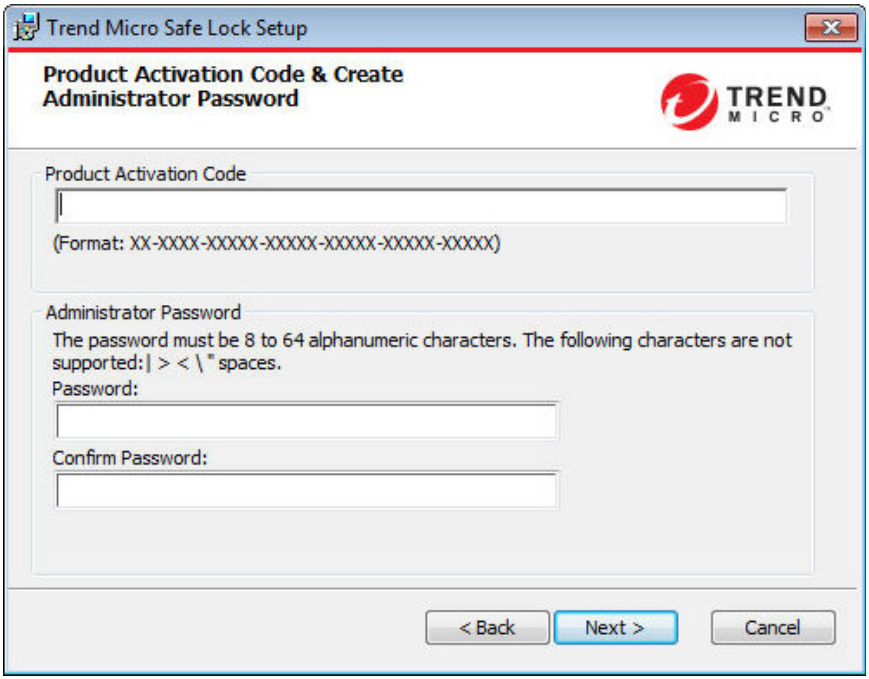
Network Virus Protection can only be installed during the initial program installation, but it can be disabled after installation, if necessary. See *Exploit Prevention Settings* in the Administrator's Guide for more information.



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.

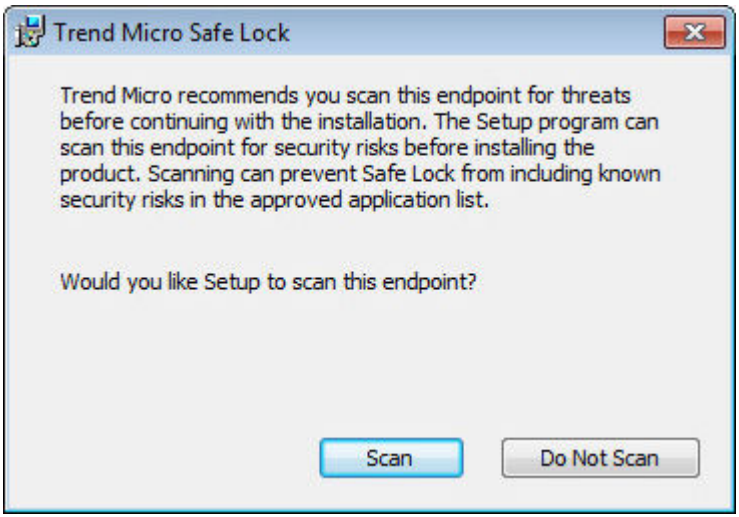


WARNING!

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. Optionally, 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**.

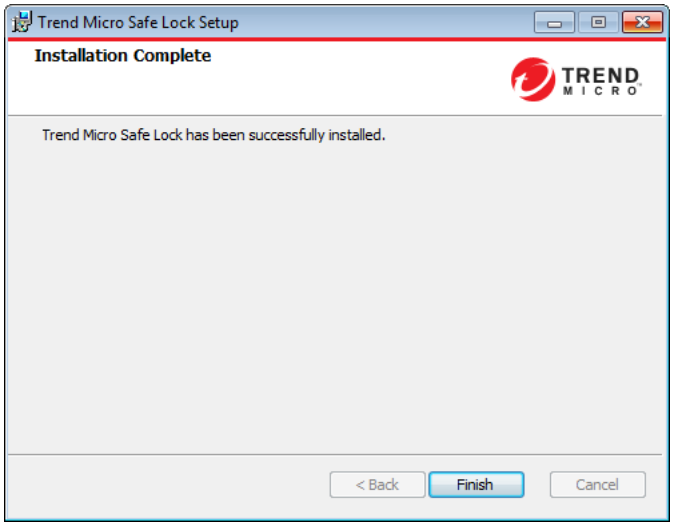
        If Endpoint Prescan detects security risks, Trend Micro recommends canceling the installation. Remove threats from the endpoint and try again. If critical programs are detected as threats, confirm that the endpoint is secure and that the versions of the programs installed do not contain threats. Ignore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

Tip

Trend Micro provides solutions for detecting and removing threats. For endpoints with limited or no network access, Trend Micro recommends using Trend Micro Portable Security. See *Trend Micro Portable Security Compatible on page 1-4*. For more information about this and other solutions from Trend Micro, go to http://trendmicro.com/.

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

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.

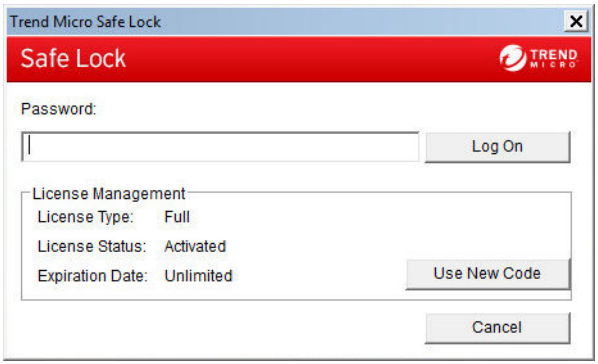
Setting Up the Approved List

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

Procedure

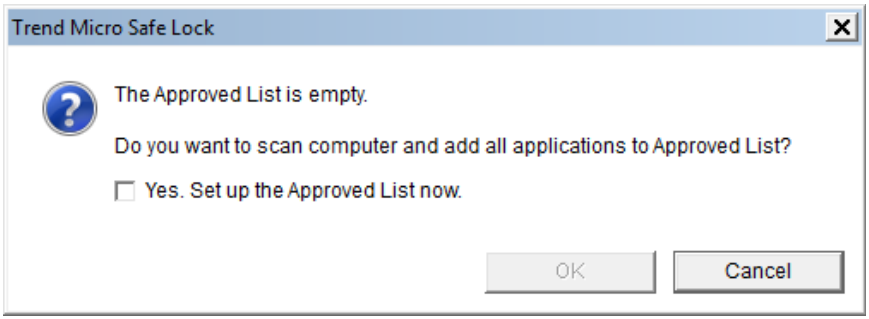
1. Open the Safe Lock console.

   The Safe Lock log on screen appears.



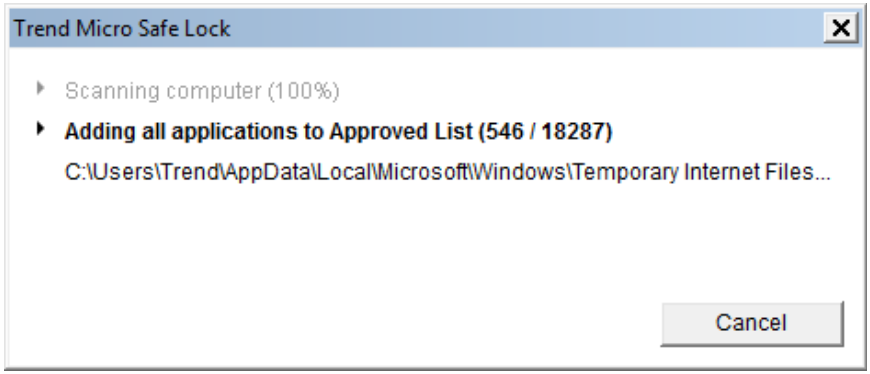
2. Provide the password and click **Login**.

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

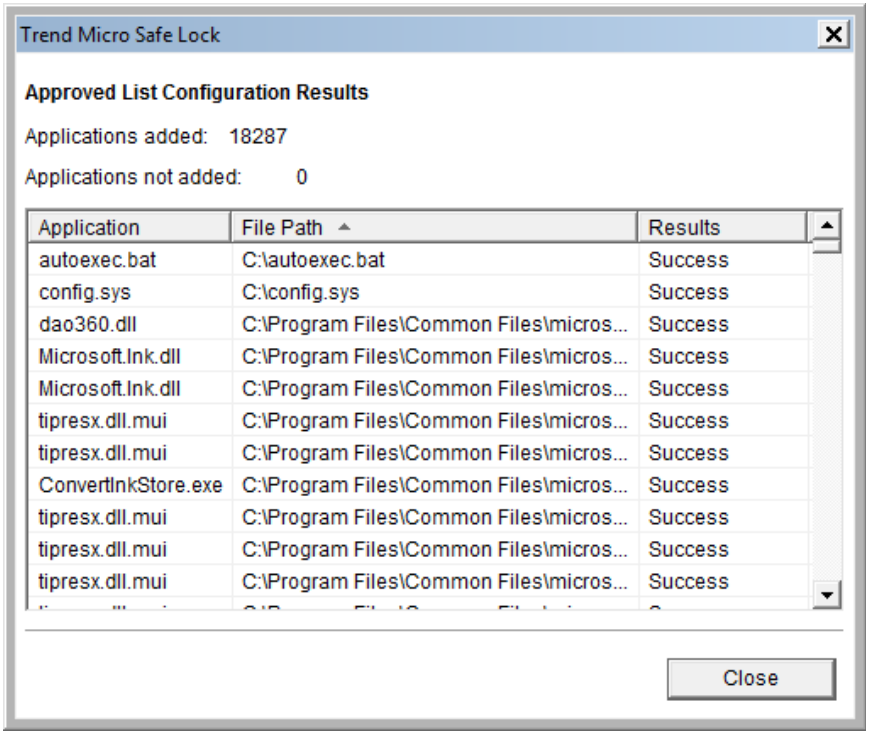


3. At the notification window, select **Yes. Set up the Approved List now** and click **OK**.

   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 computer 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`		Run the installer silently
`-p`	<administrator_password>	Specify the administrator password

PARAMETER	VALUE	DESCRIPTION
-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>	Specify the Safe Lock configuration file **Note** The Safe Lock configuration file can be exported after installing Safe Lock.
-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-XXXXX -p
P@ssW0Rd -nd
```

Important

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

Customizing Installation Parameters

Note

Arguments specified at the command line interface (CLI) take higher priority than the setup file, which takes higher priority over the default values. 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 2-15*.
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 WKSupportTool.exe file to your desktop.

   b. Run a command prompt window as administrator.

   c. Navigate to the desktop and type `WKSupportTool.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

Arguments specified at the command line interface (CLI) take higher priority than the setup file, which takes higher priority over the default values. 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	• 0: Create shortcut • 1: Do not create shortcut	0	No
NO_STARTMENU	Create a shortcut in the Start menu	• 0: Create shortcut • 1: Do not create shortcut	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
NO_SYSTRAY	Display the system tray icon and Windows notifications	• 0: Create system tray icon • 1: Do not create system tray icon	0	No
TITLE	Title content for pop-up notifications	Text up to 64 characters	Application Blocked	No
MESSAGE	Message content for pop-up notifications	Text up to 200 characters	A program has been blocked by Trend Micro Safe Lock. Please contact your help desk or administrator.	No
FILEINFO	Display the name and path of a blocked file in the pop-up notification	• 0: Disable • 1: Enable	0	No
PASSWORD	Authenticate user identity by requesting for the administrator password before closing a pop-up notification	• 0: Disable • 1: Enable	0	No
NO_NSC	Install firewall	• 0: Create firewall • 1: Do not create firewall	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
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	• 0: Standalone mode • 1: Managed mode	0	No
PASSWORD	Password which is used for **SLCmd.exe** and Safe Lock console	<password>	<empty>	No
CUSTOM_ACTION	Custom action for blocked events	• 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	• 0: Disable • Other value: Enable	1	No
INTEGRITY_MONITOR	Enable Integrity Monitor	• 0: Disable • 1: Enable	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
PREDEFINED_TRUSTED_UPDATER	Enable Predefined Trusted Updater	• 0: Disable • 1: Enable	0	No
WINDOWS_UPDATE_SUPPORT	Enable Window Update Support	• 0: Disable • 1: Enable	0	No
PRESCAN	Prescan the endpoint before installing Safe Lock	• 0: Do not prescan the endpoint • 1: Prescan the endpoint	1	No
MAX_EVENT_DB_SIZE	Maximum database file size (MB)	Positive integer	1024	No
WEL_SIZE	Windows Event Log size (KB)	Positive integer	1024	No
WEL_RETENTION	Windows Event Log option when maximum event log size is reached on Windows Event Log.	For Windows XP or earlier platforms: • 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:	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		• 0: Overwrite events as needed (oldest events first) • 1: Archive the log when full, do not overwrite events • -1: Do not overwrite events (Clear logs manually)		
WEL_IN_SIZE	Windows Event Log size for Integrity Monitor events (KB)	Positive integer	1024	No
WEL_IN_RETENTION	Windows Event Log option when maximum event log size for Integrity Monitor events is reached on Windows Event Log.	For Windows XP or earlier platforms: • 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: • 0: Overwrite events as	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		needed (oldest events first) • 1: Archive the log when full, do not overwrite events • -1: Do not overwrite events (Clear logs manually)		
USR_DEBUGLOG_ENABLE	Enable debug logging for user sessions	• 0: Log • 1: Do not log	0	No
USR_DEBUGLOGLEVEL	The number of debug log entries allowed for user sessions	• 273	273	No
SRV_DEBUGLOG_ENABLE	Enable debug logging for service sessions.	• 0: Log • 1: Do not log	0	No
SRV_DEBUGLOGLEVEL	The number of debug log entries allowed for service sessions	• 273	273	No
SILENT_INSTALL	Execute installation in silent mode	• 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:
	`[PROPERTY]`
	`ACTIVATION_CODE=XX-XXXX-XXX`
	`XX-XXXXX-XXXXX-XXXXX-XXXXX`
	`PASSWORD=P@ssW0Rd`
	`SILENT_INSTALL=1`			

`STORAGE_DEVICE_BLOCKING`	Blocks storage devices, including CD/DVD drives, floppy disks, and network drives, from accessing managed endpoints.	• `0`: Allow access from storage devices • `1`: Block access from storage devices	`0`	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	• `1`: Log • `0`: Do not log	`1`	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
LEVEL_WARNINGLOG	Log “Warning” level events related to Safe Lock	• 1: Log • 0: Do not log	1	No
LEVEL_INFORMATIONLOG	Log “Information” level events related to Safe Lock	• 1: Log • 0: Do not log	0	No
BLOCKEDACCESSLOG	Log files blocked by Safe Lock	• 1: Log • 0: Do not log	1	No
APPROVEDACCESSLOG	Log files approved by Safe Lock	• 1: Log • 0: Do not log	1	No
APPROVEDACCESSLOG_TRUSTEDUPDATER	Log Trusted Updater approved access	• 1: Log • 0: Do not log	1	No
APPROVEDACCESSLOG_DLLDRIVER	Log DLL/Driver approved access	• 1: Log • 0: Do not log	0	No
APPROVEDACCESSLOG_EXCEPTIONPATH	Log Application Lockdown exception path approved access	• 1: Log • 0: Do not log	1	No
APPROVEDACCESSLOG_TRUSTEDCERT	Log Trusted Certifications approved access	• 1: Log • 0: Do not log	1	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
APPROVEDACCESSLOG_WRITEPROTECTION	Log Write Protection approved access	• 1: Log • 0: Do not log	1	No
SYSTEMEVENTLOG	Log events related to the system	• 1: Log • 0: Do not log	1	No
SYSTEMEVENTLOG_EXCEPTIONPATH	Log exceptions to Application Lockdown	• 1: Log • 0: Do not log	1	No
SYSTEMEVENTLOG_WRITEPROTECTION	Log Write Protection events	• 1: Log • 0: Do not log	1	No
LISTLOG	Log events related to the Approved list	• 1: Log • 0: Do not log	1	No
USBMALWAREPROTECTIONLOG	Log events that trigger USB Malware Protection	• 1: Log • 0: Do not log	1	No
EXECUTIONPREVENTIONLOG	Log events that trigger Execution Prevention	• 1: Log • 0: Do not log	1	No
NETWORKVIRUSPROTECTIONLOG	Log events that trigger Network Virus Protection	• 1: Log • 0: Do not log	1	No
INTEGRITYMONITORINGLOG_FILECREATED	Log file and folder created events	• 1: Log • 0: Do not log	1	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
INTEGRITYMONITORINGLOG_FILEMODIFIED	Log file modified events	• 1: Log • 0: Do not log	1	No
INTEGRITYMONITORINGLOG_FILEDELETED	Log file and folder deleted events	• 1: Log • 0: Do not log	1	No
INTEGRITYMONITORINGLOG_FILERENAMED	Log file and folder renamed events	• 1: Log • 0: Do not log	1	No
INTEGRITYMONITORINGLOG_REGVALUEMODIFIED	Log registry value modified events	• 1: Log • 0: Do not log	1	No
INTEGRITYMONITORINGLOG_REGVALUEDELETED	Log registry value deleted events	• 1: Log • 0: Do not log	1	No
INTEGRITYMONITORINGLOG_REGKEYCREATED	Log registry key created events	• 1: Log • 0: Do not log	1	No
INTEGRITYMONITORINGLOG_REGKEYDELETED	Log registry key deleted events	• 1: Log • 0: Do not log	1	No
INTEGRITYMONITORINGLOG_REGKEYRENAMED	Log registry key renamed events	• 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
`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	• `0`: Protect against BEAST attacks	`1`	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
	TLS 1.0 protocols for BEAST attacks	• 1: Do not implement any security workarounds for BEAST vulnerabilities		
POLL_SERVER	Identify the agent as an NAT agent	• 0: Non-NAT agent • 1: NAT agent	0	No
POLL_SERVER_INTERVAL	Set the NAT connection frequency	• 1 - 64800: Connect to the Safe Lock server every (1 - 64800) minutes	10	No

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	• 1: Immediately • 2: On demand	1	No
UNREGISTER_TRIGGER	Unregister message trigger	• 1: Immediately • 2: On demand	1	No
UPDATESTATUS_TRIGGER	Update status message trigger	• 1: Immediately • 2: On demand	1	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
UPLOADBLOCKEDEVENT_TRIGGER	Upload blocked event message trigger	• 1: Immediately • 2: On demand	1	No
CHECKFILEHASH_TRIGGER	Check file hash message trigger	• 1: Immediately • 2: On demand	1	No
QUICKSCANFILE_TRIGGER	Quick scan file message trigger	• 1: Immediately • 2: On demand	1	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 - 2147483647	0	No
OWN_GROUP_INDEX	Index of group which this agent belongs to	0 - 2147483647	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
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	• 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 **Note** Only valid during silent installations.	• `0`: Cancel • `1`: Continue installation after detecting malware threat during prescan	`0`	No
`REPORT_FOLDER`	An absolute folder path where prescan result reports are saved.	• <folder_path> • <empty>: Defaults to `%windir%\temp\prescan\log`	<empty>	No

`SCAN_TYPE`	The type of scan executed during silent installation	• `Full`: Scan all folders on the endpoint.
		• `Quick`: Scans the following folders:
		  • Fixed root drives
		  For example:
			`Full`	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED

	Note
	The selected value is used as the default value for a UI installation.
		`c:\`
		`d:\`
		• System root folder
		For example, `c:\Windows`
		• System folder
		For example, `c:\Windows\System`
		• System32 folder
		For example, `c:\Windows\System32`
		• Driver folder
		For example, `c:\Windows\System32\Drivers`
		• Temp folder
		For example, `c:\Users`		

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		\Trend \AppData \Local \Temp • Desktop folder including sub folders and files For example, c:\Users \Trend \Desktop • Specific: Scan folders specified with SPECIFIC_FOLDER entries		
COMPRESS_LAYER	The number of compressed layers to scan when a compressed file is scanned.	• 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	• 0: Scan files of any sizes • 1 - 9999: Only scan files equal to or smaller than the specified size (MB)	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
SCAN_REMOVABLE_DRIVE	Scan removable drives	• 0: Do not scan removable drives • 1: Scan removable drives	0	No
SPECIFIC_FOLDER	An absolute folder path to scan when the scan type is [Specific]	<folder_path> Multiple folders can be specified by creating new entries whose name starting with SPECIFIC_FOLDER. Every entry name needs to be unique. For example: SPECIFIC_FOLDER=c:\folder1 SPECIFIC_FOLDER2=c:\folder2 SPECIFIC_FOLDER3=c:\folder3	<empty>	No
EXCLUDED_FILE	An absolute file path to exclude from scanning	<file_path> Multiple files can be specified by creating new entries whose name starting with EXCLUDED_FILE. Every entry name needs to be unique. For example: EXCLUDED_FILE=c:\file1.exe	<empty>	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		EXCLUDED_FILE2=c:\file2.exe EXCLUDED_FILE3=c:\file3.exe		
EXCLUDED_FOLDER	An absolute folder path to exclude from scanning	<folder_path> Multiple folders can be specified by creating new entries whose name starting with EXCLUDED_FOLDER. Every entry name needs to be unique. For example: EXCLUDED_FOLDER=c:\file1.exe EXCLUDED_FOLDER2=c:\file2.exe EXCLUDED_FOLDER3=c:\file3.exe	<empty>	No
EXCLUDED_EXTENSION	A file extension to exclude from scanning	<file_extension> Multiple extensions can be specified by creating new entries whose name starting with EXCLUDED_EXTENSION. Every entry name needs to be unique. For example: EXCLUDED_EXTENSION=bmp	<empty>	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		EXCLUDED_EXTENSION2=png		

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.

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 `[PRESCAN]` Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
`ENABLE`	Display notifications on managed endpoints when Safe Lock blocks an unapproved file.	• `0`: Disable • `1`: Enable	`0`	No
`ALWAYS_ON_TOP`	Display the file blocking notification on top of other screens.	• `0`: Disable • `1`: Enable	`1`	No
`SHOW_DETAILS`	Display file name, file path, and event time in the notification.	• `0`: Disable • `1`: Enable	`1`	No
`AUTHENTICATE`	Authenticate the user by requesting the administrator password when	• `0`: Disable • `1`: Enable	`1`	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
	closing the notification.			
TITLE	Notification title	<notification_title>	<empty>	No
MESSAGE	Notification content	<notification_content>	<empty>	No

Chapter 3

Local Agent Uninstallation

This chapter describes Trend Micro Safe Lock agent uninstallation procedures.

Topics in this chapter include:

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
If you use one of the following operating systems: • Windows Server 2012 • Windows Server 2008 • Windows 10 Enterprise • Windows 10 IoT Enterprise • Windows 8 • Windows 7 • Windows Vista	a. Go to **Start** > **Control Panel** > **Prorgrams and Features**. b. In the list, double-click Trend Micro Safe Lock.
If you use one of the following operating systems: • Windows Server 2003 • Windows XP • Windows 2000	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 4

Technical Support

Learn about the following topics:

Troubleshooting Resources

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

Using the Support Portal

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

Procedure

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

Tip

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

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

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

Threat Encyclopedia

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

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

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

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

Contacting Trend Micro

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

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

- Worldwide support offices:

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

- Trend Micro product documentation:

  http://docs.trendmicro.com

Speeding Up the Support Call

To improve problem resolution, have the following information available:

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

Sending Suspicious Content to Trend Micro

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

Email Reputation Services

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

https://ers.trendmicro.com/

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

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

File Reputation Services

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

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

Record the case number for tracking purposes.

Web Reputation Services

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

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

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

Other Resources

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

Download Center

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

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

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

Documentation Feedback

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

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

Index

TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: SLEM27766/170331