TREND MICRO™

2.0 TREND MICRO™ Safe Lock™ Agent

Service Pack 1 Patch 4

Administrator's Guide

A powerful lockdown solution for fixed-function computers

Endpoint Security

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

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

© 2019 Trend Micro Incorporated. All Rights Reserved.Trend Micro, the Trend Micro t-ball logo, Trend Micro Safe Lock, Safe Lock Intelligent Manager, Trend Micro Portable Security, Trend Micro Portable Security 2, and TrendLabs are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Document Part No.: SLEM28555/181213

Release Date: January 2019

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 Policy:

https://www.trendmicro.com/en_us/about/legal/privacy-policy-product.html

Table of Contents

Preface

Chapter 1: Introduction

Chapter 2: Using the Agent Console

Chapter 3: Using the Agent Command Line Interface (CLI)

Chapter 4: Working with the Agent Configuration File

Chapter 5: Troubleshooting

Chapter 6: Technical Support

Chapter 7: Appendix: Reference

Index

Preface

This Administrator's Guide introduces Trend Micro Safe Lock and covers all aspects of product management.

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.

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

Trend Micro Safe Lock 2.0 Service Pack 1 Patch 4 includes the following new features and enhancements.

TABLE 1-1. What's New in Trend Micro Safe Lock 2.0 Service Pack 1 Patch 4

FEATURE	DESCRIPTION
Windows 10 October 2018 Update support	Safe Lock adds support for Windows 10 October 2018 Update
Performance enhancements on hash checking	Safe Lock includes additional enhancements to the DLL/Driver Lockdown feature to improve the performance of hash checks done on the Approved List.
Approved List event handling enhancements	Safe Lock improves event handling for situations when the Approve List is not yet initialized.
Exclusion settings for Approved List initialization	Safe Lock adds the option to exclude a folder path or file extension from automatic file enumeration during Approved List initialization.

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

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

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

  Note

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

- Windows Vista No-SP/SP1/SP2 (32-bit) (except Starter and Home editions)
- Windows 7 No-SP/SP1 (32-bit and 64-bit) (except Starter and Home editions)
- Windows 8 No-SP (32-bit and 64-bit)
- Windows 8 No-SP (Professional/Enterprise) (32-bit and 64-bit)
- Windows 8.1 No-SP (Professional/Enterprise with Bing) (32-bit and 64-bit)
- Windows 8.1 No-SP (32-bit and 64-bit)
- Windows 10 (Professional/Enterprise/IoT Enterprise) (32-bit and 64-bit)

  - Anniversary Update (Redstone 1)

  - Creators Update (Redstone 2)

  - Fall Creators Update (Redstone 3)

  - April 2018 Update (Redstone 4)

- October 2018 Update (Redstone 5)

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

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

Note

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

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

Note

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

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

Windows Embedded Standard:

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

Note

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

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

Windows Embedded POSReady:

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

Windows Embedded Enterprise:

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

Note

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

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

Windows Embedded Server:

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

Note

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

- Windows Embedded Server 2003 R2 (32-bit)

Note

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

- Windows Embedded Server 2008 (32-bit and 64-bit)
- Windows Embedded Server 2008 R2 (64-bit)
- Windows Embedded Server 2012 (64-bit)
- Windows Embedded Server 2012 R2 (64-bit)

Windows Storage Server

- Windows Storage Server 2016

Agent Upgrade Preparation

WARNING!

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

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

TABLE 1-3. 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

Installation Method	Installed Agent Version	Required Action	Settings Retained
Local installation using Command Line Interface Installer	1.0	Manually uninstall	No settings retained
	1.1	No preparation needed	Compatible settings retained
	2.0 or later	Manually uninstall	No settings retained
Remote 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:

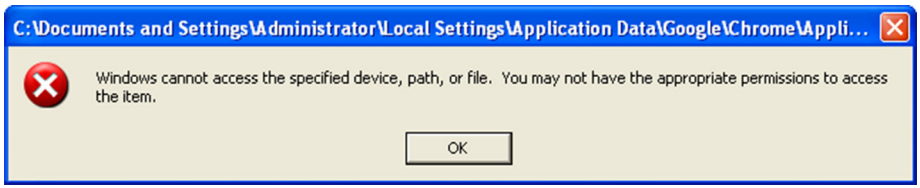


FIGURE 1-1. Trend Micro Safe Lock blocking message

Chapter 2

Using the Agent Console

This chapter describes how to configure Trend Micro Safe Lock using the agent console on the endpoint.

Topics in this chapter include:

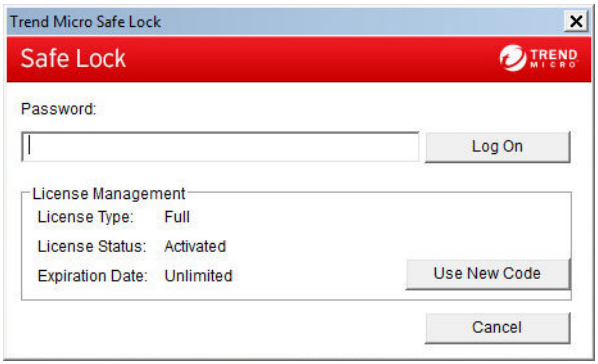
Setting Up the Approved List

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

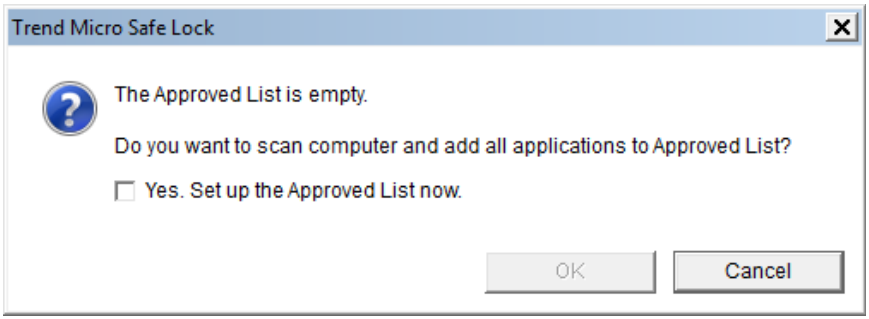
1. Open the Safe Lock console.

   The Safe Lock log on screen appears.



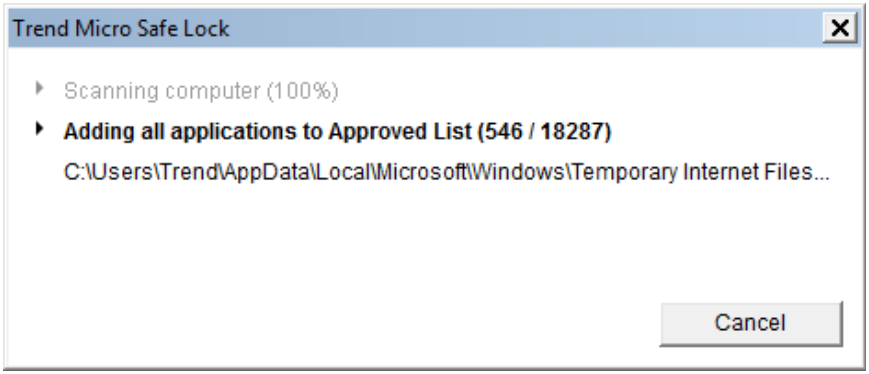
2. Provide the password and click **Login**.

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

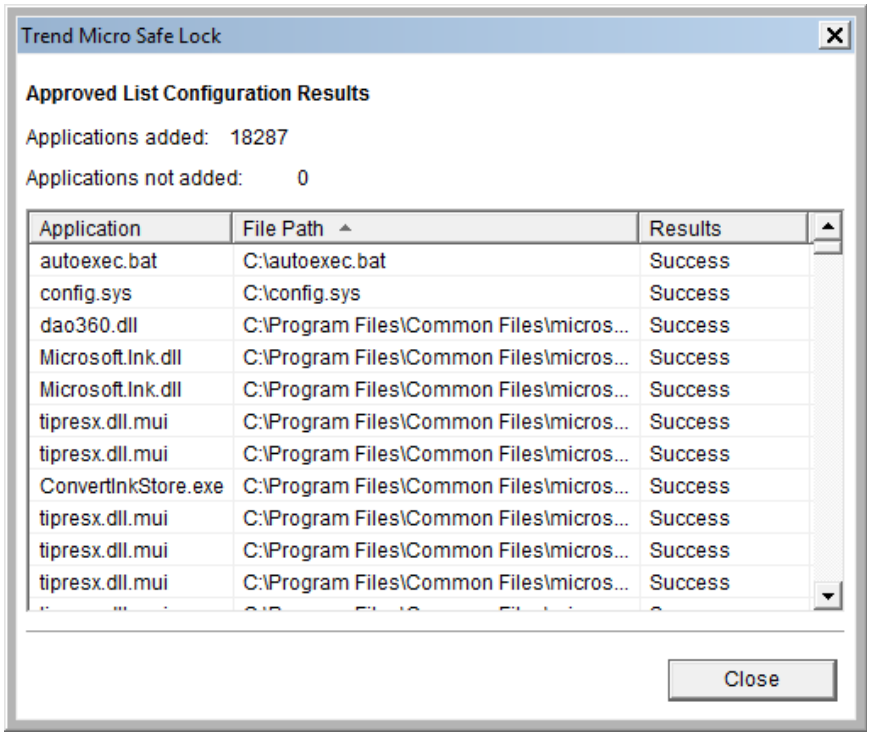


3. At the notification window, select **Yes. Set up the Approved List now** and click **OK**.

   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**.

Configuring Pop-up Notifications for Blocked Files

The administrator can set up a notification that displays on managed endpoints when Safe Lock blocks and prevents unapproved files from running or making changes to managed endpoints. This notification alerts the administrator of any blocking event and provides details about the blocked file.

Note

- This feature is disabled by default.
- Safe Lock only supports feature customization using the agent Setup.ini file and requires re-deployment to apply the customization.

TABLE 2-1. Configuring Pop-up Notifications for Blocked Files

SETTING	DEFAULT	WHERE TO ACCESS THE SETTING	
		BEFORE AGENT DEPLOYMENT	AFTER AGENT DEPLOYMENT
Enable the notification	Disabled	Customize the `BlockNotification` section of the agent Setup.ini file.	Use agent Command Line Interface to issue a `blockedfilenotification` command.
Request for administrator password when closing the notification	Enabled (if the notification feature is enabled)		Not supported
Display event details (file name, file path, and event time)			Not supported
Customize the notification title and message	• Title: Application Blocked • Message: A program has been blocked by Trend Micro Safe Lock. Please contact your help desk or administrator.		Not supported

About the Agent Console

The agent console provides easy access to commonly used features in Trend Micro Safe Lock.

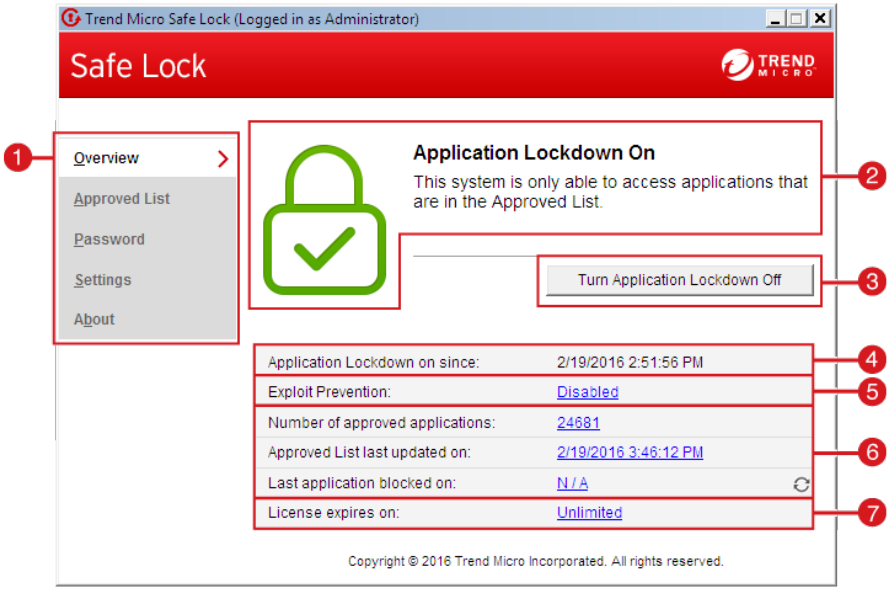


FIGURE 2-1. The Safe Lock console

The following table describes the features available on the console:

TABLE 2-2. Console Feature Descriptions

#	ITEM	DESCRIPTION
1	**Overview**	Display the software status
	Approved List	Display applications allowed to run and let users manage the list
	Password	Change the Safe Lock administrator or Restricted User passwords (only available to administrators)
	Settings	Enable or disable vulnerability protection settings and export or import the system configuration
	About	Display the product and component version numbers

#	ITEM	DESCRIPTION
2	Status information	The current status of the software
3	**Turn Application Lockdown On**	Lock down the system, blocking applications not on the Approved List from running
	Turn Application Lockdown Off	Release the system from lock down, allowing applications not on the Approved List to run **Note** After disabling Lockdown mode, Safe Lock switches to a “monitor” mode. Safe Lock does not block any applications from running, but logs when applications that are not in the Approved List run. You can use these logs to assess if the Approved List contains all the applications required on the endpoint.
4	**Application Lockdown on since**	The date and time that Application Lockdown was last turned on
	Application Lockdown off since	The date and time that Application Lockdown was last turned off
5	**Exploit Prevention**	**Enabled**: All Exploit Prevention features are enabled Click the status to open the settings screen.
		Enabled (Partly): Some Exploit Prevention features are enabled Click the status to open the settings screen.
		Disabled: No Exploit Prevention features are enabled Click the status to open the settings screen.
6	Approved List status	Click the number of Approved List items or last updated date to open the Approved List. Click the last application blocked date to open the Blocked Application Event Log.

#	ITEM	DESCRIPTION
7	**License expires on**	The time and date that the software expires Click the date to provide a new Activation Code.

Viewing Safe Lock Statuses

You can view your Safe Lock statuses as indicated by the system tray icons.

Note

System Tray icons display if they were enabled during installation.

TABLE 2-3. Status Icon Descriptions

CONSOLE ICON	SYSTEM TRAY ICON	STATUS	DESCRIPTION
		Locked	The Approved List is being enforced. Unauthorized applications cannot be run.
		Unlocked	The Approved List is not being enforced. Unauthorized applications can be run.
N/A		Expired	The Safe Lock license has expired, and the system cannot be locked. Update the Activation Code by clicking on the expiration date.

Console Icon	System Tray Icon	Status	Description
N/A		Blocked	The Safe Lock has blocked and prevented an unapproved application not from running or making changes to the managed endpoint.

About the Approved List

Use the Approved List to display the files that Safe Lock allows to run or make changes to the endpoint.

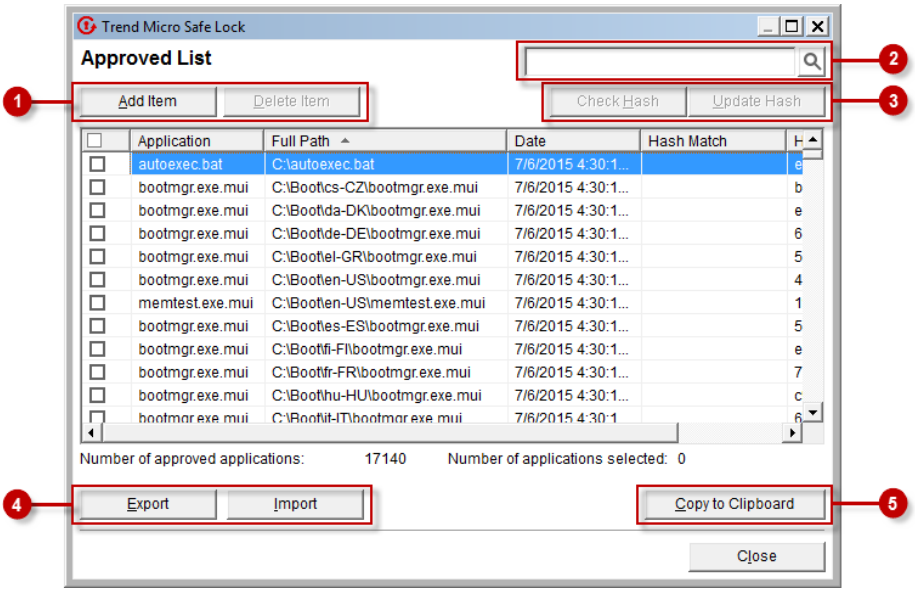


Figure 2-2. The Safe Lock Approved List

The following table describes the features available on the **Approved List**.

TABLE 2-4. Approved List Item Descriptions

#	ITEM	DESCRIPTION
1	**Add Item/Delete Item**	Adds or removes selected items to or from the Approved List.
2	Search bar	Searches the **Application** and **File Path** columns.
3	**Check Hash/Update Hash**	Checks or updates the hash values for applications in the Approved List.
4	**Export/Import**	Exports or imports the Approved List using a SQL database (`.db`) file.
5	**Copy to Clipboard**	Copies the Approved List to the clipboard in the comma separated values (CSV) format for easy review or reporting.

About Hashes

Safe Lock calculates a unique hash value for each file in the Approved List. This value can be used to detect any changes made to a file, since any change results in a different hash value. Comparing current hash values to previous values can help detect file changes.

The following table describes the hash check status icons.

TABLE 2-5. Hash Check Status Icons

ICON	DESCRIPTION
	The calculated hash value matches the stored value.
	The calculated hash value does not match the stored value.
	There was an error calculating the hash value.

Moving or overwriting files manually (without using the Trusted Updater) can result in the hash values not matching, but the mismatch could result from other applications (including malware) altering or overwriting existing files. If unsure why a hash value

mismatch has occurred, scan the endpoint for threats with Trend Micro Portable Security.

Checking or Updating Hashes

Checking the hash value of files in the Approved List can help verify the integrity of files currently permitted to run.

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 **Approved List** menu item to open the list.

   To check the file hash values:

   a. Select the files to check. To check all files, select the check box at the top of the Approved List.

   b. Click **Check Hash**.

   To update the file hash values:

   a. Select the files to update.

   b. Click **Update Hash**.

   Important

   If unsure why a hash value mismatch has occurred, scan the endpoint for threats.

Configuring the Approved List

After setting up the Approved List, users can add new programs by clicking **Add Item**, which displays the options in the following table.

TABLE 2-6. Methods for Adding Applications to the Approved List

OPTION	WHEN TO USE
Manually browse and select files	Choose this option when the software already exists on the endpoint and is up-to-date. Adding a file grants permission to run the file, but does not alter the file or the system. For example, if Windows Media Player (`wmplayer.exe`) is not in the Approved List after initial setup, users can add it to the list using the console.
Automatically add files created or modified by the selected application installer (Trusted Updater)	Choose this option when you need to update or install new applications to your managed endpoint without having to unlock Trend Micro Safe Lock. Trend Micro Safe Lock will add any new or modified files to the Approved List. For example, if Mozilla Firefox needs to be installed or updated, select this option to allow the installation or update, and also add any files created or modified in the process to the Approved List.

Adding or Removing Files

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 **Approved List** menu item to open the list.

   To add an item:

   a. Click **Add Item**, select **Manually browse and select files**, and click **Next**.

   b. In the window that opens, choose **Specific applications**, **All applications in selected folders**, or **All applications in a specified path** from the drop-down list.

      A selection window appears.

c. Select the desired application or folder to add, and click **Open** or **OK**.

d. Click **OK**. Confirm the items to be added, and click **Approve**.

e. After adding the desired items to the Approved List, click **Close**.

To remove an item:

a. Search the Approved List for the application to remove.

b. Select the check box next to the file name to be removed, and click **Delete Item**.

c. When asked to remove the item, click **OK**.

d. Click **OK** again to close the confirmation window.

Updating or Installing Using the Trusted Updater

Trend Micro Safe Lock automatically adds applications to the Approved List after the Trusted Updater adds or modifies the program files.

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 **Approved List** menu item to open the list.
4. To install or update an application, select the installer that the Trusted Updater should temporarily allow to run:

   a. Click **Add Item**, select **Automatically add files created or modified by the selected application installer**, and click **Next**.

   b. In the window that opens, choose **Specific installers**, **All installers in folders and subfolders**, or **All installers in a folder** from the drop-down list.

c. Select the desired installation package or folder to add, and click **Open**.

Note

Only existing `EXE`, `MSI`, `BAT`, and `CMD` files can be added to the Trusted Updater.

d. Check that the correct items appear on the list, and click **Start**.

The **Safe Lock Trusted Updater** window displays.

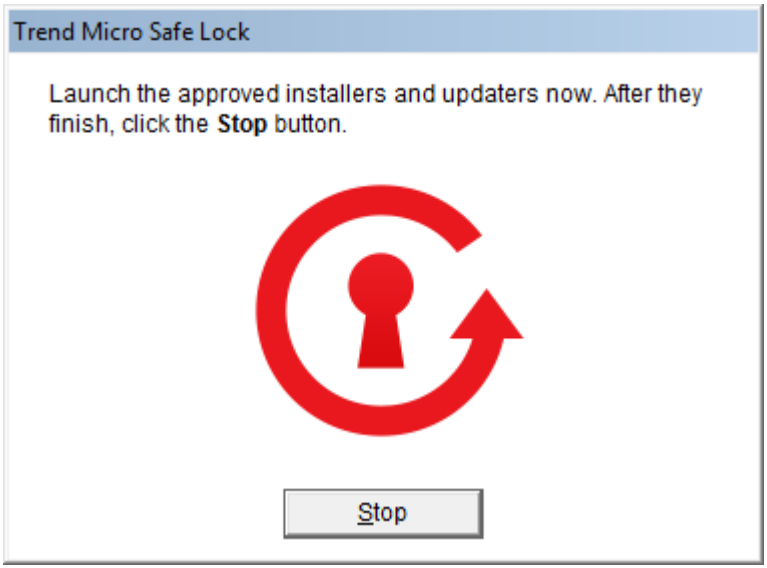


FIGURE 2-3. The Safe Lock Trusted Updater

5. Install or update the program as usual. When finished, click **Stop** on the Trusted Updater.

6. Check that the correct items appear on the Approved List, and click **Approve**, and then click **Close**.

Exporting or Importing the Approved List

Users can export or import the as a database (`.db`) file for reuse in mass deployment situations. **Copy to Clipboard** creates a CSV version of the list on the Windows clipboard.

WARNING!

The operating system files used by the exporting and importing endpoints must match exactly. Any difference between the operating system files on the endpoints can lead to operating system malfunctions or system lock-out after importing.

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 **Approved List** menu item to open the list.

   To export the Approved List:

   a. Click **Export**, and choose where to save the file.

   b. Provide a filename, and click **Save**.

   To import an Approved List:

   a. Click **Import**, and locate the database file.

   b. Select the file, and click **Open**.

Account Types

Trend Micro Safe Lock provides role-based administration, allowing administrators to grant users access to certain features on the main console. Through the configuration file, Safe Lock administrators can specify the features available to the Restricted Users account.

TABLE 2-7. Safe Lock Accounts

ACCOUNT	DETAILS
Administrator	• Default account • Full access to Safe Lock functions • Can use both the console and command line interface (CLI)
Restricted User	• Secondary maintenance account • Limited access to Safe Lock functions • Can only use the console

To enable the Restricted User account, see *Configuring Passwords on page 2-17*. To sign in with a specific account, specify the password for that account.

Configuring Passwords

While the Safe Lock administrator and Restricted User passwords can be changed from the console, only the administrator can change passwords. To log on the console as the administrator account, provide the administrator password when launching the console.

Important

The Safe Lock administrator and Restricted User passwords cannot be the same.

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 Safe Lock administrator password and click **Login**.
3. Click the **Password** menu item to display the administrator password page.

   To change the Safe Lock administrator password:

   a. Provide the current password, specify and confirm the new password, and click **Save**.

WARNING!

The only way to recover after losing the Safe Lock administrator password is by reinstalling the operating system.

To create a Restricted User password:

a. Click **Restricted User** at the top of the console.

b. Select the **Enable Restricted User** check box.

c. Specify and confirm the password, and click **Save**.

To change an existing Restricted User password:

a. Specify and confirm the new password, and click **Save**.

About Feature Settings

Safe Lock offers the following protection features.

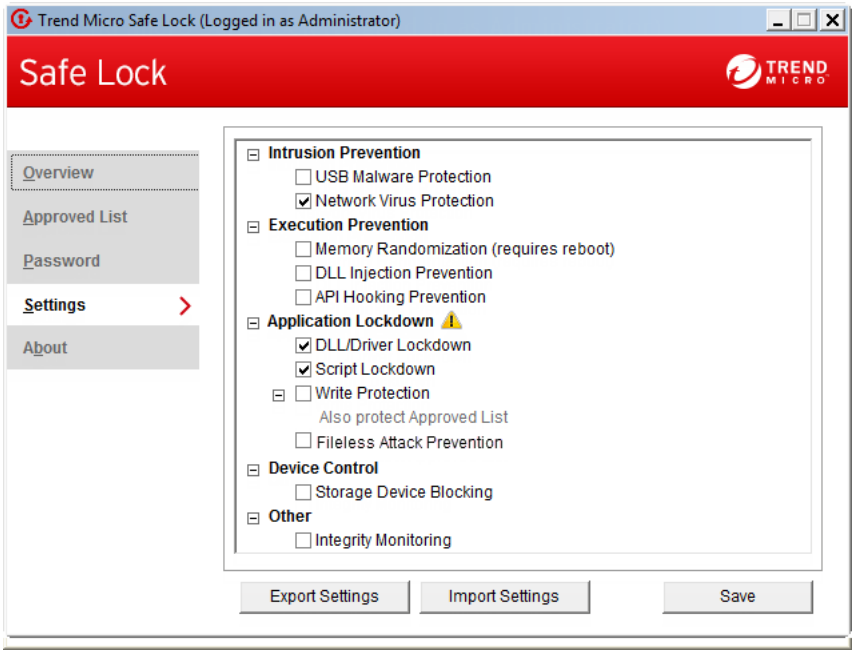


FIGURE 2-4. Safe Lock settings screen

TABLE 2-8. Intrusion Prevention

SETTING	DESCRIPTION
USB Malware Protection	USB Malware Protection prevents automated threats on USB or remote drives from infecting the endpoint. Just viewing the contents of the drive may be enough to pass along an infection. Enable this feature to prevent files on USB devices from automatically infecting the endpoint.
Network Virus Protection	Network Virus Protection scans incoming and outgoing network traffic, blocking threats from infected computers or other devices on the network. Enable this feature to prevent threats on the network from infecting the endpoint.

TABLE 2-9. Execution Prevention

SETTING	DESCRIPTION
Memory Randomization	Address Space Layout Randomization helps prevent shellcode injection by randomly assigning memory locations for important functions, forcing an attacker to guess the memory location of specific processes. Enable this feature on older operating systems such as Windows XP or Windows Server 2003, which may lack or offer limited Address Space Layout Randomization (ASLR) support. **Note** The endpoint must be restarted to enable or disable Memory Randomization.
DLL Injection Prevention	DLL Injection Prevention detects and blocks API call behaviors used by malicious software. Blocking these threats helps prevent malicious processes from running. Never disable this feature except in troubleshooting situations since it protects the system from a wide variety of serious threats.
API Hooking Prevention	API Hooking Prevention detects and blocks malicious software that tries to intercept and alter messages used in critical processes within the operating system. Never disable this feature except in troubleshooting situations since it protects the system from a wide variety of serious threats.

TABLE 2-10. Application Lockdown

SETTING	DESCRIPTION	
DLL/Driver Lockdown	DLL/Driver Lockdown prevents unapproved DLLs or drivers from being loaded into the memory of protected endpoints.	**Important** To enable DLL/Driver Lockdown, Script Lockdown, Write Protection, or Fileless Attack Prevention, ensure that Application Lockdown is also enabled on the managed endpoint.
Script Lockdown	Script Lockdown prevents unapproved script files from being run on protected endpoints.	
Write Protection	Write Protection prevents write access to objects (files, folders, and registry entries) in the Write Protection List and optionally prevents write access to files in the Approved List.	
Fileless Attack Prevention	Fileless Attack Prevention detects and blocks unapproved process chains and arguments that may lead to a fileless attack event.	

TABLE 2-11. Device Control

SETTING	DESCRIPTION
Storage Device Blocking	Blocks storage devices, including USB drives, CD/DVD drives, floppy disks, and network drives from accessing the managed endpoint.

TABLE 2-12. Other

SETTING	DESCRIPTION
Integrity Monitoring	Integrity Monitoring logs events related to changes for files, folders, and the registry on the managed endpoint. **Note** To view Integrity Monitoring logs on the managed endpoint, go to **Start** > **Control Panel** > **Administrative Tools** and access Event Viewer.

Enabling or Disabling Feature Settings

Note

By default, Trend Micro Safe Lock enables the **DLL/Driver Lockdown** and **Script Lockdown** features of the Exploit Prevention settings. If Network Virus Protection was not included in the initial installation, it cannot be selected. Reinstall Trend Micro Safe Lock if Network Virus Protection is not available.Trend Micro

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 configure Exploit Prevention settings.
4. Enable or disable the desired features.
5. Click **Save**.

Chapter 3

Using the Agent Command Line Interface (CLI)

This chapter describes how to configure and use Trend Micro Safe Lock using the command line interface (CLI).

Topics in this chapter include:

Using SLCmd at the Command Line Interface (CLI)

Administrators can work with Trend Micro Safe Lock directly from the command line interface (CLI) using the **SLCmd.exe** program.

Procedure

1. Open a command prompt window with Windows administrator privileges.
2. Navigate to the Trend Micro Safe Lock installation folder using the **cd** command.

   For example, type the following command to reach the default location:

   ```
   cd /d "c:\Program Files\Trend Micro\Trend Micro Safe Lock\"
   ```

3. Type **SLCmd.exe**.

SLCmd Program and Console Function Comparison

The following table lists the Trend Micro Safe Lock features available in SLCmd program and the Safe Lock console program..

TABLE 3-1. SLCmd Program at the Command Line Interface (CLI) and Console Function Comparison

FUNCTION	SLCMD PROGRAM AT THE COMMAND LINE INTERFACE (CLI)	CONSOLE
Account Management	Yes	Yes
Approved List Management	Yes	Yes
Decrypt/Encrypt configuration file	Yes	No
Display the blocked log	Yes	Yes
Export/Import Approved List	Yes	Yes

Function	SLCmd Program at the Command Line Interface (CLI)	Console
Export/Import configuration	Yes	Yes
Install	Yes	Yes
Windows Update Support	Yes	No
Application Lockdown	Yes	Yes
Write Protection	Yes	Yes
Write Protection Exceptions	Yes	No
Integrity Monitoring	Yes	Yes
Exception Paths	Yes	No
License Management	Yes	Yes
Administrator password	Yes	Yes
Turn on/off Application Lockdown	Yes	Yes
Enable/disable pop-up notifications for blocked files	Yes	No
Start/Stop Trusted Updater	Yes	Yes
Trusted Hash List	Yes	No
Start/Stop the service	Yes	No
Uninstall	No	No
Storage Device Control	Yes	Yes
Fileless Attack Prevention	Yes	Yes

Not all settings are available through the command line interface (CLI) or console. See *Working with the Agent Configuration File on page 4-2* for information about modifying the system configuration.

SLCmd Program Commands

The following tables list a summary commands available using the **SLCmd** program at the command line interface (CLI). To use the program, type **SLCmd** and the desired command. Type **SLCmd** and press ENTER to display the list of available commands.

Note

Only a Safe Lock administrator with Windows administrator privileges can use **SLCmd** at the command line interface (CLI). **SLCmd** will prompt for the administrator password before running certain commands.

The following is a full list of commands available using the **SLCmd** program.

General Commands

Perform general actions using the Command Line Interface.

The following table lists the available abbreviated forms of parameters.

TABLE 3-2. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
`adminpassword`	`ap`	Manage the Safe Lock admistrator password
`lock`	`lo`	Manage Application Lockdown status
`blockedlog`	`bl`	Manage the applications blocked by Safe Lock
`license`	`lc`	Manage the Safe Lock license
`settings`	`set`	Manage the Safe Lock settings
`service`	`srv`	Manage the Safe Lock service

The following table lists the commands, parameters, and values available.

TABLE 3-3. General Commands

COMMAND	PARAMETER	DESCRIPTION
help		Display a list of Safe Lock commands For example, type: **SLCmd.exe help**
activate	<activation_code>	Activate the Safe Lock program using the specified Activation Code For example, type: **SLCmd.exe activate XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX**
set adminpassword		Prompt the currently logged on administrator to specify a new password For example, type: **SLCmd.exe -p <admin_password> set adminpassword**
	<new_password>	Change the currently logged on administrator password to the newly specified password For example, type: **SLCmd.exe -p <admin_password> set adminpassword P@ssW0Rd**
set lock		Display the current Safe Lock Application Lockdown status For example, type: **SLCmd.exe -p <admin_password> set lock** **Note** The default status is `disable`.
	`enable`	Turn on Application Lockdown For example, type:

COMMAND	PARAMETER	DESCRIPTION
		SLCmd.exe -p <admin_password> set lock enable
	disable	Turn off Application Lockdown For example, type: **SLCmd.exe -p <admin_password> set lock disable**
set blockedfilenotification		Display the current notification setting For example, type: **SLCmd.exe -p <admin_password> set blockedfilenotification** **Note** The default setting is disable.
	enable	Display a notification on the managed endpoint when Safe Lock blocks a file. For example, type: **SLCmd.exe -p <admin_password> set blockedfilenotification enable**
	disable	Do not display any notification when Safe Lock blocks a file. For example, type: **SLCmd.exe -p <admin_password> set blockedfilenotification disable**
show blockedlog		Display a list of applications blocked by Safe Lock For example, type: **SLCmd.exe -p <admin_password> show blockedlog**

COMMAND	PARAMETER	DESCRIPTION
show license		Display the current Safe Lock license information For example, type: **SLCmd.exe show license**
show settings		Display the current status of the vulnerability attack prevention features For example, type: **SLCmd.exe -p <admin_password> show settings**
start service		Start the Safe Lock service For example, type: **SLCmd.exe start service**
status		Display the current status of Application Lockdown and the auto update function of the Approved List For example, type: **SLCmd.exe -p <admin_password> status**
stop service		Stop the Safe Lock service For example, type: **SLCmd.exe -p <admin_password> stop service**
version		Display the current versions of Safe Lock components For example, type: **SLCmd.exe -p <admin_password> version**

Central Management Commands

Configure central management features using the Command Line Interface by typing your command in the following format:

SLCmd.exe -p <admin_password> **<command>** <parameter> <value>

The following table lists the available abbreviated forms of parameters.

TABLE 3-4. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
managedmodeconfiguration	mmc	Manage the configuration file
servercertification	sc	Manage server certificate files
managedmode	mm	Manage agent "Managed Mode"

The following table lists the commands, parameters, and values available.

TABLE 3-5. Central Management Commands

COMMAND	PARAMETER	DESCRIPTION
decrypt managedmodeconfiguration	<path_of_encrypted_file> <path_of_decrypted_output_file>	Decrypt the configuration file used by Managed Mode
encrypt managedmodeconfiguration	<path_of_file> <path_of_encrypted_output_file>	Encrypt the configuration file used by Managed Mode
export managedmodeconfiguration	<path_of_encrypted_output>	Export the encrypted configuration file used by Managed Mode
export servercertification	<path_of_certification_file>	Export the encrypted Safe Lock Intelligent Manager SSL communication certificate file

COMMAND	PARAMETER	DESCRIPTION
import managedmodeconfiguration	<path_of_encrypted_input>	Import the encrypted configuration file used by Managed Mode
import servercertification	<path_of_certification_file>	Import the encrypted Safe Lock Intelligent Manager SSL communication certificate file
set managedmode	enable [-cfg <path_of_encrypted_file>] [-sc <path_of_certification_file]	Enable Managed Mode **Note** The default setting is disable. The following optional parameters are available: • -cfg <path_of_encrypted_file> Use -cfg value to specify the path of the configuration file • -sc <path_of_certification_file Use -sc value to specify the path of the certificate file
set managedmode		Display the current Managed Mode status
show managedmodeconfiguration		Display the configuration used by Managed Mode
test managedmode		Connect a test Managed Mode session with Safe Lock Intelligent Manager

Optional Feature Commands

Configure optional security features using the Command Line Interface by typing your command in the following format:

SLCmd.exe -p <admin_password> **<command>** <parameter> <value>

The following table lists the available abbreviated forms of parameters.

TABLE 3-6. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
apihookingprevention	api	Manage API Hooking Prevention
customaction	ca	Manage actions taken when Safe Lock blocks specific types of events
dlldriverlockdown	dd	Manage DLL/Driver Lockdown
dllinjectionprevention	dll	Manage DLL Injection Prevention
exceptionpath	ep	Manage exceptions to Application Lockdown
integritymonitoring	in	Manage Integrity Monitoring
memoryrandomization	mr	Manage Memory Randomization
networkvirusprotection	net	Manage Network Virus Protection
script	scr	Manage Script Lockdown
storagedeviceblocking	sto	Allows or blocks storage devices (CD/DVD drives, floppy disks, and network drives) from accessing the managed endpoint.

PARAMETER	ABBREVIATION	USE
usbmalwareprotection	usb	Manage USB Malware Protection
writeprotection	wp	Manage Write Protection
writeprotection-includes-approvedlist	wpal	Manage Write Protection includes Approved List

The following table lists the commands, parameters, and values available.

TABLE 3-7. Optional Feature Commands

COMMAND	PARAMETER	DESCRIPTION
set apihookingprevention	enable	Enable API Hooking Prevention For example, type: **SLCmd.exe -p <admin_password> set apihookingprevention enable** **Note** The default status is Disabled.
	disable	Disable API Hooking Prevention For example, type: **SLCmd.exe -p <admin_password> set apihookingprevention disable**
		Display the current status of API Hooking Prevention For example, type: **SLCmd.exe -p <admin_password> set apihookingprevention**

COMMAND	PARAMETER	DESCRIPTION
set customaction		Display the current setting for actions taken when Safe Lock blocks specific types of events **Note** The default setting is `Ask`.
	`ignore`	Ignore blocked files or processes when Application Lockdown blocks any of the following events: • Process launch • DLL loading • Script file access For example, type: **`SLCmd.exe -p <admin_password> set customaction ignore`**
	`quarantine`	Quarantine blocked files or processes when Application Lockdown blocks any of the following events: • Process launch • DLL loading • Script file access For example, type: **`SLCmd.exe -p <admin_password> set customaction qurantine`**

COMMAND	PARAMETER	DESCRIPTION
		Note Safe Lock does not support a custom action of “quarantine” on Windows XP or Windows 2003.
	`ask`	Ask what to do for blocked files or processes when Application Lockdown blocks any of the following events: • Process launch • DLL loading • Script file access For example, type: **`SLCmd.exe -p <admin_password> set customaction ask`**
`set` `dlldriverlockdown`		Display the current status of DLL/ Driver Lockdown For example, type: **`SLCmd.exe -p <admin_password> set dlldriverlockdown`** **Note** The default status is `Enabled`.
	`enable`	Enable DLL/Driver Lockdown For example, type: **`SLCmd.exe -p <admin_password> set dlldriverlockdown enable`**
	`disable`	Disable DLL/Driver Lockdown For example, type:

COMMAND	PARAMETER	DESCRIPTION
		SLCmd.exe -p <admin_password> set dlldriverlockdown disable
set dllinjectionprevention		Display the current status of DLL Injection Prevention For example, type: **SLCmd.exe -p <admin_password> set dllinjectionprevention** **Note** The default status is Disabled.
	enable	Enable DLL Injection Prevention For example, type: **SLCmd.exe -p <admin_password> set dllinjectionprevention enable**
	disable	Disable DLL Injection Prevention For example, type: **SLCmd.exe -p <admin_password> set dllinjectionprevention disable**
set exceptionpath		Display current setting for using exceptions to Application Lockdown For example, type: **SLCmd.exe -p <admin_password> set exceptionpath** **Note** The default setting is Disabled.

COMMAND	PARAMETER	DESCRIPTION
	`enable`	Enable exceptions to Application Lockdown For example, type: **`SLCmd.exe -p <admin_password> set exceptionpath enable`**
	`disable`	Disable exceptions to Application Lockdown For example, type: **`SLCmd.exe -p <admin_password> set exceptionpath disable`**
`set` `integritymonitoring`		Display the current status of Integrity Monitoring For example, type: **`SLCmd.exe -p <admin_password> set integritymonitoring`** **Note** The default status is `Disabled`.
	`enable`	Enable Integrity Monitoring For example, type: **`SLCmd.exe -p <admin_password> set integritymonitoring enable`**
	`disable`	Disable Integrity Monitoring For example, type: **`SLCmd.exe -p <admin_password> set integritymonitoring disable`**

COMMAND	PARAMETER	DESCRIPTION
set memoryrandomization		Display the current status of Memory Randomization For example, type: **SLCmd.exe -p <admin_password> set memoryrandomization** **Note** The default status is Disabled.
	enable	Enable Memory Randomization For example, type: **SLCmd.exe -p <admin_password> set memoryrandomization enable**
	disable	Disable Memory Randomization For example, type: **SLCmd.exe -p <admin_password> set memoryrandomization disable**
set networkvirusprotection		Display the current status of Network Virus Protection For example, type: **SLCmd.exe -p <admin_password> set networkvirusprotection** **Note** The default status is Enabled.
	enable	Enable Network Virus Protection For example, type:

COMMAND	PARAMETER	DESCRIPTION
		SLCmd.exe -p <admin_password> set networkvirusprotection enable
	disable	Disable Network Virus Protection For example, type: **SLCmd.exe -p <admin_password> set networkvirusprotection disable**
set script		Display the current status of Script Lockdown For example, type: **SLCmd.exe -p <admin_password> set script** **Note** The default status is Enabled.
	enable	Enable Script Lockdown For example, type: **SLCmd.exe -p <admin_password> set script enable**
	disable	Disable Script Lockdown For example, type: **SLCmd.exe -p <admin_password> set script disable**
set storagedeviceblocking		Display the current status of Storage Device Blocking For example, type: **SLCmd.exe -p <admin_password> set storagedeviceblocking**

COMMAND	PARAMETER	DESCRIPTION
		Note The default status is `Disabled`.
	`enable`	Enable Storage Device Blocking For example, type: **`SLCmd.exe -p <admin_password> set storagedeviceblocking enable`**
	`disable`	Disable Storage Device Blocking For example, type: **`SLCmd.exe -p <admin_password> set storagedeviceblocking disable`**
`set` `usbmalwareprotection`		Display the current status of USB Malware Protection For example, type: **`SLCmd.exe -p <admin_password> set usbmalwareprotection`** **Note** The default status is `Disabled`.
	`enable`	Enable USB Malware Protection For example, type: **`SLCmd.exe -p <admin_password> set usbmalwareprotection enable`**
	`disable`	Disable USB Malware Protection For example, type:

COMMAND	PARAMETER	DESCRIPTION
		SLCmd.exe -p <admin_password> set usbmalwareprotection disable
set writeprotection		Display the current status of Write Protection For example, type: **SLCmd.exe -p <admin_password> set writeprotection** **Note** The default status is Disabled.
	enable	Enable Write Protection For example, type: **SLCmd.exe -p <admin_password> set writeprotection enable**
	disable	Disable Write Protection For example, type: **SLCmd.exe -p <admin_password> set writeprotection disable**
set writeprotection-includes-approvedlist		Display the current status of Write Protection includes Approved List For example, type: **SLCmd.exe -p <admin_password> set writeprotection-includes-approvedlist**

COMMAND	PARAMETER	DESCRIPTION
		Note The default status is `Disabled`. However, the status changes to `Enabled` if Write Protection is enabled.
	`enable`	Enable protection of the Approved List (in addition to the Write Protection List) when Write Protection is enabled For example, type: **`SLCmd.exe -p <admin_password> set writeprotection-includes-approvedlist enable`**
	`disable`	Disable protection of the Approved List (in addition to the Write Protection List) when Write Protection is enabled For example, type: **`SLCmd.exe -p <admin_password> set writeprotection-includes-approvedlist disable`**

Restricted User Account Commands

Configure the Restricted User Account using the Command Line Interface by typing your command in the following format:

`SLCmd.exe` -p <admin_password> **`<command>`** `<parameter>` <value>

The following table lists the available abbreviated forms of parameters.

TABLE 3-8. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
`user`	`us`	Manage the Restricted User account
`userpassword`	`up`	Manage the Restricted User password

The following table lists the commands, parameters, and values available.

TABLE 3-9. Restricted User Account Commands

COMMAND	PARAMETER	DESCRIPTION
set `user`		Display the the Restricted User account status For example, type: **`SLCmd.exe -p <admin_password> set user`** **Note** The default status is `Disabled`.
	`enable`	Enable the Restricted User account For example, type: **`SLCmd.exe -p <admin_password> set user enable`**
	`disable`	Disable the Restricted User account For example, type: **`SLCmd.exe -p <admin_password> set user disable`**
set `userpassword`		Prompt the currently logged on administrator to specify a new Restricted User account password For example, type:

COMMAND	PARAMETER	DESCRIPTION
		SLCmd.exe -p <admin_password> set userpassword
	<new_password>	Change the Restricted User account password to the newly specified password For example, type: **SLCmd.exe -p <admin_password> set userpassword P@ssW0Rd**

Script Commands

Deploy scripts using the Command Line Interface by typing your command in the following format:

SLCmd.exe -p <admin_password> **<command>** <parameter> <value>

The following table lists the available abbreviated forms of parameters.

TABLE 3-10. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
script	scr	Manage script commands

The following table lists the commands, parameters, and values available.

TABLE 3-11. Script Commands

COMMAND	PARAMETER	DESCRIPTION
add script	<extension> <interpreter1> [interpreter2] ...	Add the specified script extension and the interpreter(s) required to execute the script For example, to add the script extension JSP with the interpreter file jscript.js, type: **SLCmd.exe -p <admin_password> add script jsp C:\Scripts\jscript.js**

COMMAND	PARAMETER	DESCRIPTION
remove script	<extension> [interpreter1] [interpreter2] ...	Remove the specified script extension and the interpreter(s) required to execute the script For example, to remove the script extension JSP with the interpreter file jscript.js, type: **SLCmd.exe -p <admin_password> remove script jsp C:\Scripts\jscript.js** **Note** If you do not specify any interpreter, the command removes all interpreters related to the script extension. If you specify interpreters, the command only removes the interpreters specified from the script extension rule.
show script		Display all script rules For example, type: **SLCmd.exe -p <admin_password> show script**

Note

Safe Lock uses the following default script rules:

- bat <cmd.exe>
- cmd <cmd.exe>
- com <ntvdm.exe>
- dll <ntvdm.exe>
- drv <ntvdm.exe>
- exe <ntvdm.exe>
- js <cscript.exe>,<wscript.exe>
- msi <msiexec.exe>
- pif <ntvdm.exe>
- ps1 <powershell.exe>
- sys <ntvdm.exe>
- vbe <cscript.exe>,<wscript.exe>
- vbs <cscript.exe>,<wscript.exe>

Approved List Commands

Configure the Approved List using the Command Line Interface by typing your command in the following format:

SLCmd.exe -p <admin_password> **<command>** `<parameter>` <value>

The following table lists the available abbreviated forms of parameters.

TABLE 3-12. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
`approvedlist`	`al`	Manage files in the Approved List

PARAMETER	ABBREVIATION	USE
`list`	`li`	Manage the Approved List import and export functions

The following table lists the commands, parameters, and values available.

TABLE 3-13. Approved List Commands

COMMAND	PARAMETER	DESCRIPTION
add approvedlist	[-r] <file_or_folder_path>	Add the specified file to the Approved List For example, to add all Microsoft Office files to the Approved List, type: **SLCmd.exe -p <admin_password> add approvedlist -r "C:\Program Files \Microsoft Office"** **Note** Using the optional `-r` value includes the specified folder and related subfolders.
remove approvedlist	<file_path>	Remove the specified file from the Approved List For example, to remove `notepad.exe` from the Approved List, type: **SLCmd.exe -p <admin_password> remove approvedlist C:\Windows\notepad.exe**
show approvedlist		Display the files in the Approved List For example, type: **SLCmd.exe -p <admin_password> show approvedlist**
check approvedlist	`-f`	Update the hash values in the Approved List and displays detailed results For example, type:

COMMAND	PARAMETER	DESCRIPTION
		SLCmd.exe -p <admin_password> check approvedlist -f
	-q	Update the hash values in the Approved List and displays summarized results For example, type: **SLCmd.exe -p <admin_password> check approvedlist -q**
	-v	Compare the hash values in the Approved List with the hash values calculated from the actual files and prompts the user after detecting mismatched values For example, type: **SLCmd.exe -p <admin_password> check approvedlist -v**
export list	<output_file>	Export the Approved List to the file path and file name specified For example, type: **SLCmd.exe -p <admin_password> export list c:\approvedlist\ap.db** **Note** The output file type must be DB format.
import list	[-o] <input_file>	Import an Approved List from the file path and file name specified For example, type: **SLCmd.exe -p <admin_password> import list c:\approvedlist\ap.db**

COMMAND	PARAMETER	DESCRIPTION
		Note The input file type must be `DB` format. Using the optional `-o` value overwrites the existing list.

Application Lockdown Commands

Perform actions related to Application Lockdown using the Command Line Interface by typing your command in the following format:

`SLCmd.exe` `-p` <admin_password> **`<command>`** `<parameter>` <value>

The following table lists the available abbreviated forms of parameters.

TABLE 3-14. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
`quarantinedfile`	`qf`	Manage quarantined files
`exceptionpath`	`ep`	Manage exceptions to Application Lockdown

The following table lists the commands, parameters, and values available.

TABLE 3-15. Application Lockdown Commands

COMMAND	PARAMETER	DESCRIPTION
`show` `quarantinedfile`		Display a list of quarantined files
`restore` `quarantinedfile`	<id> [`-al`] [`-f`]	Restore the specified file from quarantine Using the optional `-al` value also adds the restored file to Approved List. Using the optional `-f` value forces the restore.

COMMAND	PARAMETER	DESCRIPTION
remove quarantinedfile	<id>	Delete the specified file
show exceptionpath		Display current exceptions to Application Lockdown For example, type: `SLCmd.exe -p <admin_password> show exceptionpath`
add exceptionpath	`-e` <file_path> `-t file`	Add an exception for the specified file For example, type: `SLCmd.exe -p <admin_password> add exceptionpath -e c:\sample.bat -t file`
	`-e` <folder_path> `-t folder`	Add an exception for the specified folder For example, type: `SLCmd.exe -p <admin_password> add exceptionpath -e c:\folder -t folder`
	`-e` <folder_path> `-t folderandsub`	Add an exception for the specified folder and related subfolders For example, type: `SLCmd.exe -p <admin_password> add exceptionpath -e c:\folder -t folderandsub`
	`-e` <regular_expression> `-t regexp`	Add an exception using the regular expression. For example, type: • `SLCmd.exe -p <admin_password> add exceptionpath -e c:\\folder\\.* -t regexp` • `SLCmd.exe -p <admin_password> add exceptionpath -e \\\\computer\\folder\\.*\\file\.exe -t regexp`

COMMAND	PARAMETER	DESCRIPTION
remove exceptionpath	-e <file_path> -t file	Remove an exception for the specified file For example, type: SLCmd.exe -p <admin_password> remove exceptionpath -e c:\sample.bat -t file **Note** Specify the exact <file_path> originally specified in the corresponding add command.
	-e <folder_path> -t folder	Remove an exception for the specified folder For example, type: SLCmd.exe -p <admin_password> remove exceptionpath -e c:\folder -t folder **Note** Specify the exact <folder_path> originally specified in the corresponding add command.
	-e <folder_path> -t folderandsub	Remove an exception for the specified folder and related subfolders For example, type: SLCmd.exe -p <admin_password> remove exceptionpath -e c:\folder -t folderandsub **Note** Specify the exact <folder_path> originally specified in the corresponding add command.

COMMAND	PARAMETER	DESCRIPTION
	`-e` <regular_expression> `-t regexp`	Remove an exception using the regular expression. For example, type: `SLCmd.exe -p <admin_password> remove exceptionpath -e c:\\test\\.* -t regexp` **Note** Specify the exact <regular_expression> originally specified in the corresponding add command.
`test` `exceptionpath`	<regular_expression> <string> `-t regexp`	Check if the regular expression matches the string. For example, type: `SLCmd.exe -p <admin_password> test exceptionpath C:\\test\\.* C:\test\sample.exe -t regexp`

Write Protection Commands

Configure Write Protection List and Write Protection Exception List using the Command Line Interface by typing your command in the following format:

`SLCmd.exe` -p <admin_password> **<command>** <parameter> <value>

The following table lists the available abbreviated forms of parameters.

TABLE 3-16. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
`writeprotection`	`wp`	Manage the Write Protection feature

PARAMETER	ABBREVIATION	USE
writeprotection-file	wpfi	Manage files in the Write Protection List
writeprotection-folder	wpfo	Manage folders in the Write Protection List
writeprotection-regvalue	wprv	Manage registry values and associated registry keys in the Write Protection List
writeprotection-regkey	wprk	Manage registry keys in the Write Protection List
writeprotection-file-exception	wpfie	Manage files in the Write Protection Exception List
writeprotection-folder-exception	wpfoe	Manage folders in the Write Protection Exception List
writeprotection-regvalue-exception	wprve	Manage registry values and associated registry keys in the Write Protection Exception List
writeprotection-regkey-exception	wprke	Manage registry keys in the Write Protection Exception List

The following tables list the commands, parameters, and values available.

TABLE 3-17. Write Protection List "File" Commands

COMMAND	PARAMETER	VALUE	DESCRIPTION
show	writeprotection		Display the entire Write Protection List
	writeprotection-file		Display the files in the Write Protection List For example, type: **SLCmd.exe -p <admin_password> show writeprotection-file**

COMMAND	PARAMETER	VALUE	DESCRIPTION
	writeprotection-file-exception		Display the files in the Write Protection Exception List For example, type: **SLCmd.exe -p <admin_password> show writeprotection-file-exception**
	writeprotection-folder		Display the folders in the Write Protection List For example, type: **SLCmd.exe -p <admin_password> show writeprotection-folder**
	writeprotection-folder-exception		Display the folders in the Write Protection Exception List For example, type: **SLCmd.exe -p <admin_password> show writeprotection-folder-exception**
add	writeprotection-file	<file_path>	Add the specified file to the Write Protection List For example, type: **SLCmd.exe -p <admin_password> add writeprotection-file archive.txt**

COMMAND	PARAMETER	VALUE	DESCRIPTION
			Note The <file_path> value pattern matches from the end of the path toward the beginning of the path. For example, specifying `userfile.txt` matches `c:\Windows\userfile.txt` and `c:\Temp\userfile.txt`.
	`writeprotection-file-exception`	`-t` <file_path> `-p` <process_path>	Add the specified file and a specific process path for that file to the Write Protection Exception List For example, to add write access by a process named `notepad.exe` to a file named `userfile.txt`, type: **`SLCmd.exe -p <admin_password> add writeprotection-file-exception -t userfile.txt -p notepad.exe`**

COMMAND	PARAMETER	VALUE	DESCRIPTION
			Note The `-p` and `-t` values pattern match from the end of the path toward the beginning of the path. For example, specifying `userfile.txt` matches `c:\Windows\userfile.txt` and `c:\Temp\userfile.txt`.
		`-t` <file_path>	Add the specified file to the Write Protection Exception List For example, to add write access by any process to a file named `userfile.txt`, type: **`SLCmd.exe -p <admin_password> add writeprotection-file-exception -t userfile.txt`**

COMMAND	PARAMETER	VALUE	DESCRIPTION
			Note The `-t` value pattern matches from the end of the path toward the beginning of the path. For example, specifying `userfile.txt` matches `c:\Windows\userfile.txt` and `c:\Temp\userfile.txt`.
		`-p` <process_path>	Add the specified process path to the Write Protection Exception List For example, to add write access by a process named `notepad.exe` to any files, type: **`SLCmd.exe -p <admin_password> add writeprotection-file-exception -p notepad.exe`**

COMMAND	PARAMETER	VALUE	DESCRIPTION
			Note The `-p` value pattern matches from the end of the process path toward the beginning of the path. For example, specifying `notepad.exe` matches `c:\Windows\notepad.exe` and `c:\Temp\notepad.exe`.
	`writeprotection-folder`	[`-r`] <folder_path>	Add the specified folder(s) to the Write Protection List For example, type: **`SLCmd.exe -p <admin_password> add writeprotection-folder -r userfolder`**

COMMAND	PARAMETER	VALUE	DESCRIPTION
			Note Using the optional `-r` value includes the specified folder and related subfolders. The <folder_path> value pattern matches from the end of the path toward the beginning of the path. For example, specifying `userfile.txt` matches `c:\Windows\userfolder` and `c:\Temp\userfolder`.
	`writeprotection-folder-exception`	[`-r`] `-t` <folder_path> `-p` <process_path>	Add the specified folder and processes run from the specified path to the Write Protection Exception List For example, to add write access by a process named `notepad.exe` to a folder and related subfolders at `c:\Windows\System32\Temp`, type: **`SLCmd.exe -p <admin_password> add writeprotection-folder-exception -r -t c:\Windows\System32\Temp -p notepad.exe`**

COMMAND	PARAMETER	VALUE	DESCRIPTION
			Note Using the optional `-r` value includes the specified folder and related subfolders. The `-p` and `-t` values pattern match from the end of the path toward the beginning of the path. For example, specifying `userfile.txt` matches `c:\Windows\userfile.txt` and `c:\Temp\userfile.txt`.
		[`-r`] `-t` <folder_path>	Add the specified folder(s) to the Write Protection Exception List For example, to add write access by any process to a folder at `userfolder`, type: **`SLCmd.exe -p <admin_password> add writeprotection-folder-exception -r -t userfolder`**

COMMAND	PARAMETER	VALUE	DESCRIPTION
			Note Using the optional `-r` value includes the specified folder and related subfolders. The `-t` value pattern matches from the last part of the folder path toward the beginning of the path. For example, specifying `userfolder` matches `c:\Windows\userfolder` and `c:\Temp\userfolder`.
		`-p <process_path>`	Add processes run from the specified paths to the Write Protection Exception List For example, to add write access by a process named `notepad.exe` to any folder, type: **`SLCmd.exe -p <admin_password> add writeprotection-folder-exception -p c:\Windows\notepad.exe`**

COMMAND	PARAMETER	VALUE	DESCRIPTION
			Note The `-p` value pattern matches from the end of the process path toward the beginning of the path. For example, specifying `notepad.exe` matches `c:\Windows\notepad.exe` and `c:\Temp\notepad.exe`.
remove	`writeprotection-file`	<file_path>	Remove the specified file from the Write Protection List For example, type: **`SLCmd.exe -p <admin_password> remove writeprotection-file archive.txt`** **Note** Specify the exact <file_path> originally specified in the corresponding add command.
	`writeprotection-file-exception`	`-t` <file_path> `-p` <process_path>	Remove the specified file and process path from the Write Protection Exception List For example, type:

COMMAND	PARAMETER	VALUE	DESCRIPTION
			`SLCmd.exe -p <admin_password> remove writeprotection-file-exception -t userfile.txt -p notepad.exe` **Note** Specify the exact <file_path> and <process_path> originally specified in the corresponding add command.
		`-t` <file_path>	Remove the specified file from the Write Protection Exception List For example, type: `SLCmd.exe -p <admin_password> remove writeprotection-file-exception -t userfile.txt`

COMMAND	PARAMETER	VALUE	DESCRIPTION
			Note The `-t` value pattern matches from the end of the path toward the beginning of the path. For example, specifying `userfile.txt` matches `c:\Windows\userfile.txt` and `c:\Temp\userfile.txt`.
		`-p <process_path>`	Remove the specified process path from the Write Protection Exception List For example, type: **`SLCmd.exe -p <admin_password> remove writeprotection-file-exception -p notepad.exe`** **Note** The `-p` value pattern matches from the end of the process path toward the beginning of the path. For example, specifying `notepad.exe` matches `c:\Windows\notepad.exe` and `c:\Temp\notepad.exe`.

COMMAND	PARAMETER	VALUE	DESCRIPTION
	`writeprotection-folder`	[`-r`] <folder_path>	Remove the specified folder(s) from the Write Protection List For example, type: **`SLCmd.exe -p <admin_password> remove writeprotection-folder -r c:\Windows`** **Note** Using the optional `-r` value includes the specified folder and related subfolders. Specify the exact <folder_path> and `-r` value originally specified in the corresponding add command.
	`writeprotection-folder-exception`	[`-r`] `-t` <folder_path> `-p` <process_path>	Remove the specified folder and process path from the Write Protection Exception List For example, type: **`SLCmd.exe -p <admin_password> remove writeprotection-folder-exception -r -t c:\Windows\System32\Temp -p c:\Windows\notepad.exe`**

COMMAND	PARAMETER	VALUE	DESCRIPTION
			Note Using the optional `-r` value includes the specified folder and related subfolders. Specify the exact <folder_path>, <process_path>, and `-r` value originally specified in the corresponding add command.
		[`-r`] `-t` <folder_path>	Remove the specified folder(s) from the Write Protection Exception List For example, type: **`SLCmd.exe -p <admin_password> remove writeprotection-folder-exception -r -t userfolder`**

COMMAND	PARAMETER	VALUE	DESCRIPTION
			Note Using the optional `-r` value includes the specified folder and related subfolders. The `-t` value pattern matches from the last part of the folder path toward the beginning of the path. For example, specifying `userfolder` matches `c:\Windows\userfolder` and `c:\Temp\userfolder`.
		`-p` <process_path>	Remove the specified process path from the Write Protection Exception List For example, type: **`SLCmd.exe -p <admin_password> remove writeprotection-folder-exception -p c:\Windows\System32`**

COMMAND	PARAMETER	VALUE	DESCRIPTION
			Note The `-p` value pattern matches from the end of the process path toward the beginning of the path. For example, specifying `notepad.exe` matches `c:\Windows\notepad.exe` and `c:\Temp\notepad.exe`.

TABLE 3-18. Write Protection List "Registry" Commands

COMMAND	PARAMETER	VALUE	DESCRIPTION
show	`writeprotection`		Display the entire Write Protection List
	`writeprotection-regvalue`		Display the registry values in the Write Protection List
	`writeprotection-regvalue-exception`		Display the registry values in the Write Protection Exception List
	`writeprotection-regkey`		Display the registry keys in the Write Protection List
	`writeprotection-regkey-exception`		Display the registry keys in the Write Protection Exception List
add	`writeprotection-regvalue`	<path_of_registry_key> <registry_value>	Add the specified registry value and its related registry key to the Write Protection List For example, to add the registry value of "testvalue" in the "HKEY\test" registry key to the Write Protection List, type:

COMMAND	PARAMETER	VALUE	DESCRIPTION
			SLCmd.exe -p <admin_password> add writeprotection-regvalue HKEY\test testvalue
	writeprotection-regvalue-exception	-t <path_of_registry_key> <registry_value> -p <process_path>	Add the specified registry value and its related registry key and a specific process path for that value to the Write Protection Exception List **Note** This command allows write access by the specified process to the specified registry values. The -p value pattern matches from the end of the path toward the beginning of the path.
		-t <path_of_registry_key> <registry_value>	Add the specified registry value and its related registry key to the Write Protection Exception List **Note** This command allows write access by any process to the specified registry value.
		-p <process_path>	Add the specified process to the Write Protection Exception List

COMMAND	PARAMETER	VALUE	DESCRIPTION
			Note This command allows write access by the specified process to any registry values. The `-p` value pattern matches from the end of the process path toward the beginning of the path.
	`writeprotection-regkey`	[`-r`] <path_of_registry_key>	Add the specified registry key to the Write Protection List **Note** Using the optional `-r` value includes the specified registry key and related subkeys.
	`writeprotection-regkey-exception`	[`-r`] `-t` <path_of_registry_key> `-p` <process_path>	Add the specified registry key and processes run from the specified path to the Write Protection Exception List

COMMAND	PARAMETER	VALUE	DESCRIPTION
			Note This command allows write access by the specified process to the specified registry keys. Using the optional `-r` value includes the specified registry key and related subkeys. The `-p` value pattern matches from the end of the process path toward the beginning of the path.
		[`-r`] `-t` <path_of_registry_key>	Add the specified registry key to the Write Protection Exception List **Note** This command allows write access by any process to the specified registry keys. Using the optional `-r` value includes the specified registry key and related subkeys.
		`-p` <process_path>	Add processes run from the specified paths to the Write Protection Exception List

COMMAND	PARAMETER	VALUE	DESCRIPTION
			Note This command allows write access by the specified process to any registry keys. The `-p` value pattern matches from the end of the process path toward the beginning of the path.
remove	`writeprotection-regvalue`	<path_of_registry_key> <registry_value>	Remove the specified registry value from the Write Protection List **Note** Specify the exact <path_of_registry_key> and <registry_value> originally specified in the corresponding add command.
	`writeprotection-regvalue-exception`	`-t` <path_of_registry_key> <registry_value> `-p` <process_path>	Remove the specified registry value and process path from the Write Protection Exception List

COMMAND	PARAMETER	VALUE	DESCRIPTION
			Note Specify the exact <path_of_registry_key>, <registry_value>, and <process_path> originally specified in the corresponding add command. The `-p` value pattern matches from the end of the path toward the beginning of the path.
		`-t` <path_of_registry_key> <registry_value>	Remove the specified registry value from the Write Protection Exception List
		`-p` <process_path>	Remove the specified process path from the Write Protection Exception List **Note** The `-p` value pattern matches from the end of the path toward the beginning of the path.
	`writeprotection-regkey`	[`-r`] <path_of_registry_key>	Remove the specified registry key from the Write Protection List

COMMAND	PARAMETER	VALUE	DESCRIPTION
			Note Specify the exact <path_of_registry_key> and `-r` value originally specified in the corresponding add command. Using the optional `-r` value includes the specified registry key and related subkeys.
	`writeprotection-regkey-exception`	[`-r`] `-t` <path_of_registry_key> `-p` <process_path>	Remove the specified registry key and process path from the Write Protection Exception List **Note** Specify the exact <path_of_registry_key>, <process_path>, and `-r` value originally specified in the corresponding add command. Using the optional `-r` value includes the specified registry key and related subkeys. The `-p` value pattern matches from the end of the path toward the beginning of the path.
		[`-r`] `-t` <path_of_registry_key>	Remove the specified registry key from the Write Protection Exception List

COMMAND	PARAMETER	VALUE	DESCRIPTION
			Note Using the optional `-r` value includes the specified registry key and related subkeys.
		`-p` <process_path>	Remove the specified process path from the Write Protection Exception List **Note** The `-p` value pattern matches from the end of the path toward the beginning of the path.

Trusted Certification Commands

Configure Trusted Certificates using the Command Line Interface by typing your command in the following format:

`SLCmd.exe` `-p` <admin_password> **`<command>`** `<parameter>` <value>

The following table lists the available abbreviated forms of parameters.

TABLE 3-19. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
`trustedcertification`	`tc`	Manage Trusted Certifications

The following table lists the commands, parameters, and values available.

TABLE 3-20. Trusted Certificate Commands

COMMAND	PARAMETER	DESCRIPTION
set trustedcertification		Display current setting for using Trusted Certifications **Note** The default setting is `Enabled`.
	`enable`	Enable using Trusted Certifications
	`disable`	Disable using Trusted Certifications
show trustedcertification	[`-v`]	Display the certificate files in the Trusted Certifications List Using the optional `-v` value displays detailed information.
add trustedcertification	`-c` <file_path> [`-l` <label>] [`-u`]	Add the specified certificate file to the Trusted Certifications List Using the optional `-l` value specifies the unique label for this certificate file. Using the optional `-u` value treats the file signed by this certificate file as a Trusted Updater.
remove trustedcertification	`-l` <label>	Remove a certificate file from the Trusted Certifications List by specifying its label

Trusted Hash List Commands

Configure trusted hash values using the Command Line Interface by typing your command in the following format:

`SLCmd.exe` `-p` <admin_password> **`<command>`** `<parameter>` <value>

The following table lists the available abbreviated forms of parameters.

TABLE 3-21. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
`trustedhash`	`th`	Manage trusted hash values (files) added by the Safe Lock administrator.

The following table lists the commands, parameters, and values available.

TABLE 3-22. Trusted Hash List Commands

COMMAND	PARAMETER	DESCRIPTION
`set` `trustedhash`		Display current setting for using Trusted Hash List **Note** The default setting is `Disabled`.
	`enable`	Enable using Trusted Hash List
	`disable`	Disable using Trusted Hash List
`show` `trustedhash`		Display the hash values in the Trusted Hash List For example, type: **`SLCmd.exe -p <admin_password> show trustedhash`**
`add` `trustedhash`	`-v` <hash> [`-l` <label>] [`-u`][`-al`] [`-t`<file_path>][`-n`<note>]	Add the specified hash value to the Trusted Hash List For example, to add a trusted file with a hash value `xxx` to the Trusted Hash List, type: **`SLCmd.exe -p <admin_password> add trustedhash -v xxx`** Using the optional `-l` value specifies the unique label for this hash value. Using the optional `-u` value treats the file of the specified hash value as a Trusted Updater.

COMMAND	PARAMETER	DESCRIPTION
		Note The `-u` value requires the Predefined Trusted Updater List enabled. Using the optional `-al` value adds the file of the specified hash value to Approved List. Using the optional `-t` value specifies a file path to check for the hash value **Note** The `-t` value pattern matches from the end of the path toward the beginning of the path. For example, specifying `userfile.txt` matches `c:\Windows\userfile.txt` and `c:\Temp\userfile.txt`. Using the optional `-n` value adds a note for the file hash
`remove` `trustedhash`	`-l` <label>	Remove a file from the Trusted Hash List by specifying its label
`remove` `trustedhash`	`-a`	Remove all the hash values in the Trusted Hash List

Trusted Updater Commands

To execute installers or files not specified in agent Approved Lists, configure Trusted Updater by typing your command in the following format:

`SLCmd.exe` `-p` <admin_password> **`<command>`** `<parameter>` <value>

The following table lists the available abbreviated forms of parameters.

TABLE 3-23. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
`trustedupdater`	`tu`	Manage the Predefined Trusted Updater tool process

The following table lists the commands, parameters, and values available.

TABLE 3-24. Trusted Updater Commands

COMMAND	PARAMETER	DESCRIPTION
`start` `trustedupdater`	[`-r`] <path_of_installer>	Start Trusted Updater to add installer files (`EXE` and `MSI` file types) to the specified folder of the Approved List. **Note** Using the optional `-r` value includes the specified folder and related subfolders. For example, to include all installation packages in the `C:\Installers` folder and all sub-folders, type: **`SLCmd.exe -p <admin_password> start trustedupdater -r C:\Installers`**
`stop` `trustedupdater`	[`-f`]	Disable Trusted Updater to stop adding new or updated files to the Approved List. **Note** Using the optional `-f` value specifies that the Trusted Updater does not prompt the administrator before committing a file to the Approved List. For example, to stop the Trusted Updater and commit all identified installers (indentified before receiving the stop command) to the Approved List after receiving a prompt, type:

COMMAND	PARAMETER	DESCRIPTION
		SLCmd.exe -p <admin_password> stop trustedupdater -f

Predefined Trusted Updater Commands

Important

The `add` command for adding files to the Predefined Trusted Updater List follows a different format than the general commands specified in the Predefined Trusted Updater Commands table. For details on adding files to the Predefined Trusted Updater List, see *Predefined Trusted Updater "Add" Command on page 3-62*.

Configure Predefined Trusted Updater using the Command Line Interface by typing your command in the following format:

SLCmd.exe -p <admin_password> **<command>** <parameter> <value>

The following table lists the available abbreviated forms of parameters.

TABLE 3-25. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
predefinedtrustedupdater	ptu	Manage files in the Predefined Trusted Updater Lists

The following table lists the commands, parameters, and values available.

TABLE 3-26. Predefined Trusted Updater Commands

COMMAND	PARAMETER	DESCRIPTION
add predefinedtrustedupdater	-e <folder_or_file_exception>	Add the specified file or folder to the Predefined Trusted Updater Exception List

COMMAND	PARAMETER	DESCRIPTION
		Important The **add** command for adding files to the Predefined Trusted Updater List follows a different format than the other commands specified in the this list. For details on adding files to the Predefined Trusted Updater List (not the Predefined Trusted Updater Exception List), see *Predefined Trusted Updater "Add" Command on page 3-62*. For example, to add `notepad.exe` to the Predefined Trusted Updater Exception List, type: **SLCmd.exe -p <admin_password> add predefinedtrustedupdater -e C:\Windows\notepad.exe**
decrypt `predefinedtrustedupdater`	<path_of_encrypted_file> <path_of_decrypted_output_file>	Decrypt a file to the specified location For example, to decrypt `C:\Notepad.xen` to `C:\Editors\notepad.xml`, type: **SLCmd.exe -p <admin_password> decrypt predefinedtrustedupdater C:\Notepad.xen C:\Editors\notepad.xml**

COMMAND	PARAMETER	DESCRIPTION
encrypt predefinedtrustedupdater	<path_of_file> <path_of_encrypted_output_file>	Encrypt a file to the specified location For example, to encrypt `C:\notepad.xml` to `C:\Editors\Notepad.xen`, type: **SLCmd.exe -p <admin_password> encrypt predefinedtrustedupdater C:\Editors\notepad.xml C:\Notepad.xen**
export predefinedtrustedupdater	<path_of_encrypted_output>	Export the Predefined Trusted Updater List to the specified encrypted file For example, type: **SLCmd.exe -p <admin_password> export predefinedtrustedupdater C:\Lists\ptu_list.xen**
import predefinedtrustedupdater	<path_of_encrypted_input>	Import a Predefined Trusted Updater List from the specified encrypted file For example, type: **SLCmd.exe -p <admin_password> import predefinedtrustedupdater C:\Lists\ptu_list.xen**
remove predefinedtrustedupdater	`-l` <label_name>	Remove the specified labeled rule from the Predefined Trusted Updater List For example, to remove the "Notepad" rule, type: **SLCmd.exe -p <admin_password> remove**

COMMAND	PARAMETER	DESCRIPTION
		predefinedtrustedupdater -l Notepad
	-e <folder_or_file_exception>	Remove the specified exception from the Predefined Trusted Updater Exception List For example, to remove the notepad.exe exception, type: **SLCmd.exe -p <admin_password> remove predefinedtrustedupdater -e C:\Windows\notepad.exe**
set predefinedtrustedupdater		Display the status of the Predefined Trusted Updater List **Note** The default status is Disabled.
	enable	Enable the Predefined Trusted Updater List
	disable	Disable the Predefined Trusted Updater List
show predefinedtrustedupdater		Display the files in the Predefined Trusted Updater List For example, type: **SLCmd.exe -p <admin_password> show predefinedtrustedupdater**
	-e	Display the files in the Predefined Trusted Updater Exception List For example, type:

COMMAND	PARAMETER	DESCRIPTION
		SLCmd.exe -p <admin_password> show predefinedtrustedupdater -e

Predefined Trusted Updater "Add" Command

Add processes, files, or folders to the Predefined Trusted Updater List using the Command Line Interface by typing your command in the following format:

SLCmd.exe -p <admin_password> **add** predefinedtrustedupdater -u <folder_or_file> -t <type_of_object> [<optional_values>]

The following table lists the command, parameter, and base value.

TABLE 3-27. Predefined Trusted Updater "Add" Command

COMMAND	PARAMETER	VALUE	DESCRIPTION
add	predefinedtrustedupdater	<folder_or_file>	Add a specified file or folder to the Predefined Trusted Updater List For example, to add notepad.exe to the Predefined Trusted Updater List, type: **SLCmd.exe -p <admin_password> add predefinedtrustedupdater C:\Windows\notepad.exe**

Append the following additional values at the end of the command:

TABLE 3-28. Predefined Trusted Updater "Add" Additional Values

VALUE	REQUIRED / OPTIONAL	DESCRIPTION	EXAMPLE
`-u` <folder_or_file>	Required	Add the specified file or folder to the Predefined Trusted Updater List	N/A **Note** This parameter requires the use of the `-t` <type_of_object> value.
`-t` <type_of_object>	Required	Specify the type of object to add to the Predefined Trusted Updater List located in `-u` <folder_or_file> Available objects types are as follows: process — Indicates only `EXE` file types file — Indicates only `MSI` and `BAT` file types folder — Indicates all `EXE`, `MSI`, and `BAT` files in the specified folder folderandsub — Indicates all `EXE`, `MSI`, and `BAT` files in the specified folder and related subfolders	**`SLCmd.exe -p <admin_password> add predefinedtrustedupdater -u C:\Windows\notepad.exe -t process`**
`-p` <parent_process>	Optional	Add the full file path to the specified parent process used to invoke the	**`SLCmd.exe -p <admin_password> add predefinedtrust`**

VALUE	REQUIRED / OPTIONAL	DESCRIPTION	EXAMPLE
		file(s) specified in `-u` <folder_or_file>	`edupdater -u C:\Windows\notepad.exe -t process -p C:\batch files\note.bat`
`-l` <label_name>	Optional	Specify a label name for the file(s) specified in `-u` <folder_or_file> **Note** When left blank, Safe Lock assigns an arbitrary label name.	`SLCmd.exe -p <admin_password> add predefinedtrust edupdater -u C:\Windows\notepad.exe -t process -l EDITOR`
`-al enable`	Optional	Compare the hash values in the Approved List with the hash values calculated from the actual files **Note** Enabled by default even when `-al` is not specified.	`SLCmd.exe -p <admin_password> add predefinedtrust edupdater -u C:\Windows\notepad.exe -t process -al enable`
`-al disable`	Optional	Do not compare the hash values in the Approved List with the hash values calculated from the actual files	`SLCmd.exe -p <admin_password> add predefinedtrust edupdater -u C:\Windows\notepad.exe -t process -al disable`

Windows Update Support

Configure Windows Update Support using the Command Line Interface by typing your command in the following format:

SLCmd.exe -p <admin_password> **<command>** <parameter> <value>

The following table lists the available abbreviated forms of parameters.

TABLE 3-29. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
windowsupdatesupport	wus	Allow Windows Update to run on the agent with the Application Lockdown on.

The following table lists the commands, parameters, and values available.

TABLE 3-30. Windows Update Support Commands

COMMAND	PARAMETER	DESCRIPTION
set windowsupdatesupport		Display current setting for Windows Update Support **Note** The default setting is Disabled.
	enable	Enable Windows Update Support
	disable	Disable Windows Update Support

Blocked File Notification Commands

Enable or disable notifications for file blocking using the Command Line Interface by typing your command in the following format:

SLCmd.exe -p <admin_password> **<command>** <parameter> <value>

The following table lists the available abbreviated forms of parameters.

TABLE 3-31. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
`blockedfilenotification`	`bfn`	Display notifications on the managed endpoint when Safe Lock blocks and prevents an application from running or making changes to the endpoint.

The following table lists the commands, parameters, and values available.

TABLE 3-32. Blocked File Notification Commands

COMMAND	PARAMETER	DESCRIPTION
`set` `blockedfilenotification`		Display the current setting. **Note** The default setting is `Disabled`.
	`enable`	Enable pop-up notifications.
	`disable`	Disable pop-up notifications.

Configuration File Commands

Perform actions on the configuration file using the Command Line Interface by typing your command in the following format:

`SLCmd.exe` `-p` <admin_password> **`<command>`** `<parameter>` <value>

The following table lists the available abbreviated forms of parameters.

TABLE 3-33. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
`configuration`	`con`	Manage the configuration file

The following table lists the commands, parameters, and values available.

TABLE 3-34. Configuration File Commands

COMMAND	PARAMETER	DESCRIPTION
decrypt configuration	<path_of_encrypted_file> <path_of_decrypted_output_file>	Decrypts a configuration file to the specified location For example, to decrypt `C:\config.xen` to `C:\config.xml`, type: **SLCmd.exe -p <admin_password> decrypt configuration C:\config.xen C:\config.xml**
encrypt configuration	<path_of_file> <path_of_encrypted_output_file>	Encrypts a configuration file to the specified location For example, to encrypt `C:\config.xml` to `C:\config.xen`, type: **SLCmd.exe -p <admin_password> encrypt configuration C:\config.xml C:\config.xen**
export configuration	<path_of_encrypted_output>	Export the configuration file to the specified location For example, type: **SLCmd.exe -p <admin_password> export configuration C:\config.xen**
import configuration	<path_of_encrypted_input>	Import a configuration file from the specified location For example, type: **SLCmd.exe -p <admin_password> import configuration C:\config.xen**

Fileless Attack Prevention Commands

Configure Fileless Attack Prevention features using the Command Line Interface by typing your command in the following format:

SLCmd.exe -p <admin_password> **<command>** <parameter> <value>

The following table lists the available abbreviated forms of parameters.

TABLE 3-35. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
filelessattackprevention	flp	Manage Fileless Attack Prevention
filelessattackprevention-process	flpp	Manage Fileless Attack Prevention processes
filelessattackprevention-exception	flpe	Manage Fileless Attack Prevention exceptions

The following table lists the commands, parameters, and values available.

TABLE 3-36. Fileless Attack Prevention Commands

COMMAND	PARAMETER	DESCRIPTION
set filelessattackprevention		Display the current Fileless Attack Prevention status For example, type: SLCmd.exe -p <admin_password> set filelessattackprevention
	enable	Enable Fileless Attack Prevention For example, type: SLCmd.exe -p <admin_password> set filelessattackprevention enable
	disable	Disable Fileless Attack Prevention For example, type: SLCmd.exe -p <admin_password> set filelessattackprevention disable

COMMAND	PARAMETER	DESCRIPTION
show filelessattackprevention-process		Display the list of monitored processes For example, type: `SLCmd.exe -p <admin_password> show filelessattackprevention-process`
add filelessattackprevention-exception	`<monitored_process> <Parentprocess1> <Parentprocess2> <Parentprocess3> <Parentprocess4> -a <arguments> -regex -l <label>`	Add a Fileless Attack Prevention exception For example, given the following exception: • Monitored Process: `cscript.exe` • Parentprocess1: `a.exe` • Parentprocess2: • Parentprocess3: `c.exe` • Parentprocess4: • Arguments: `-abc -def` • Use regular expression for arguments: `No` To add the exception, type: `SLCmd.exe -p <admin_password> add flpe cscript.exe a.exe "" c.exe "" -a "-abc -def"`
remove filelessattackprevention-exception	`-l <label>`	Remove a Fileless Attack Prevention exception For example, type: `SLCmd.exe -p <admin_password> remove filelessattackprevention-exception -l <label>`

Note

- If a monitored process is launched before SafeLock is started, SafeLock is unable to detect and block the monitored process.
- In systems running Windows Vista x86 (no service pack installed), the Fileless Attack Prevention feature can run the process chain check without issues, but is unable to perform the command line argument check. If a process passes the process chain check on these systems, the command line argument check is skipped completely.

Chapter 4

Working with the Agent Configuration File

This chapter describes how to configure Trend Micro Safe Lock using the configuration file.

Topics in this chapter include:

Working with the Agent Configuration File

The configuration file allows administrators to create and deploy a single configuration across multiple machines.

See *Exporting or Importing a Configuration File on page 4-3* for more information.

Changing Advanced Settings

Some settings can only be changed though the configuration file using the command line interface (CLI). See *Using SLCmd at the Command Line Interface (CLI) on page 3-2* for more information.

Procedure

1. Export the configuration file.
2. Decrypt the configuration file.
3. Edit the configuration file with Windows Notepad or another text editor.

Important

Safe Lock only supports configuration files in the UTF-8 file format.

Tip

To update multiple agents with shared settings, you may choose to only import the modified settings.

4. Encrypt the edited configuration file.
5. Import the edited 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.

Configuration File Syntax

The configuration file uses the XML format to specify parameters used by Safe Lock.

Important

Safe Lock only supports configuration files in the UTF-8 file format.

Refer to the following example of the configuration file:

```
<?xml version="1.0" encoding="UTF-8"?>
<Configurations version="1.00.000" xmlns:xsi="http://www.w3.org/2001/XMLSchema-i
    <Configuration>
        <AccountGroup>
            <Account Id="{24335D7C-1204-43d1-9CBB-332D688C85B6}" Enable="no">
                <Password/>
            </Account>
        </AccountGroup>
        <UI>
            <SystemTaskTrayIcon Enable="yes">
                <BlockNotification Enable="no" AlwaysOnTop="yes" ShowDetails="ye
                    <Title/>
                    <Message/>
                </BlockNotification>
            </SystemTaskTrayIcon>
        </UI>
        <Feature>
            <ApplicationLockDown LockDownMode="2">
                <WhiteList RecentHistoryUnapprovedFilesLimit="50">
                            <ExclusionList>
                                  <Folder>C:\EXCLUDED_FOLDER\DLL\</Folder>
                                  <Folder>C:\EXCLUDED_FOLDER\EXE\</Folder>
                                  <Folder>C:\EXCLUDED_FOLDER\SCRIPT\</Folder>
                                  <Extension>png</Extension>
                                  <Extension>bmp</Extension>
                               </ExclusionList>
                            </WhiteList>
                <ScriptLockdown Enable="yes">
                    <Extension Id="bat">
                        <Interpreter>cmd.exe</Interpreter>
                    </Extension>
                    <Extension Id="cmd">
                        <Interpreter>cmd.exe</Interpreter>
                    </Extension>
                    <Extension Id="com">
                        <Interpreter>ntvdm.exe</Interpreter>
```

```
                    </Extension>
                    <Extension Id="dll">
                        <Interpreter>ntvdm.exe</Interpreter>
                    </Extension>
                    <Extension Id="drv">
                        <Interpreter>ntvdm.exe</Interpreter>
                    </Extension>
                    <Extension Id="exe">
                        <Interpreter>ntvdm.exe</Interpreter>
                    </Extension>
                    <Extension Id="js">
                        <Interpreter>cscript.exe</Interpreter>
                        <Interpreter>wscript.exe</Interpreter>
                    </Extension>
                    <Extension Id="msi">
                        <Interpreter>msiexec.exe</Interpreter>
                    </Extension>
                    <Extension Id="pif">
                        <Interpreter>ntvdm.exe</Interpreter>
                    </Extension>
                    <Extension Id="ps1">
                        <Interpreter>powershell.exe</Interpreter>
                    </Extension>
                    <Extension Id="sys">
                        <Interpreter>ntvdm.exe</Interpreter>
                    </Extension>
                    <Extension Id="vbe">
                        <Interpreter>cscript.exe</Interpreter>
                        <Interpreter>wscript.exe</Interpreter>
                    </Extension>
                    <Extension Id="vbs">
                        <Interpreter>cscript.exe</Interpreter>
                        <Interpreter>wscript.exe</Interpreter>
                    </Extension>
                </ScriptLockdown>
                <TrustedUpdater>
                    <PredefinedTrustedUpdater Enable="no">
                        <RuleSet/>
                    </PredefinedTrustedUpdater>
                    <WindowsUpdateSupport Enable="no"/>
                </TrustedUpdater>
                <DllDriverLockDown Enable="yes"/>
```

```
                <ExceptionPath Enable="no">
                    <ExceptionPathList/>
                </ExceptionPath>
                <TrustedCertification Enable="yes"/>
                <TrustedHash Enable="no"/>
                <WriteProtection Enable="no" ActionMode="1" ProtectApprovedList=
                <CustomAction ActionMode="0"/>
                <FilelessAttackPrevention Enable="no">
                    <ExceptionList/>
                </FilelessAttackPrevention>
            </ApplicationLockDown>
            <UsbMalwareProtection Enable="no" ActionMode="1"/>
            <NetworkVirusProtection Enable="yes" ActionMode="1"/>
            <IntegrityMonitoring Enable="no"/>
            <StorageDeviceBlocking Enable="no" ActionMode="1"/>
            <Log>
                <EventLog Enable="yes">
                    <Level>
                        <WarningLog Enable="yes"/>
                        <InformationLog Enable="no"/>
                    </Level>
                    <BlockedAccessLog Enable="yes"/>
                    <ApprovedAccessLog Enable="yes">
                        <TrustedUpdaterLog Enable="yes"/>
                        <DllDriverLog Enable="no"/>
                        <ExceptionPathLog Enable="yes"/>
                        <TrustedCertLog Enable="yes"/>
                        <TrustedHashLog Enable="yes"/>
                        <WriteProtectionLog Enable="yes"/>
                    </ApprovedAccessLog>
                    <SystemEventLog Enable="yes">
                        <ExceptionPathLog Enable="yes"/>
                        <WriteProtectionLog Enable="yes"/>
                    </SystemEventLog>
                    <ListLog Enable="yes"/>
                    <UsbMalwareProtectionLog Enable="yes"/>
                    <ExecutionPreventionLog Enable="yes"/>
                    <NetworkVirusProtectionLog Enable="yes"/>
                    <IntegrityMonitoringLog>
                        <FileCreatedLog Enable="yes"/>
                        <FileModifiedLog Enable="yes"/>
                        <FileDeletedLog Enable="yes"/>
```

```
                        <FileRenamedLog Enable="yes"/>
                        <RegValueModifiedLog Enable="yes"/>
                        <RegValueDeletedLog Enable="yes"/>
                        <RegKeyCreatedLog Enable="yes"/>
                        <RegKeyDeletedLog Enable="yes"/>
                        <RegKeyRenamedLog Enable="yes"/>
                    </IntegrityMonitoringLog>
                    <DeviceControlLog Enable="yes"/>
                </EventLog>
                <DebugLog Enable="no"/>
            </Log>
        </Feature>
        <ManagedMode Enable="no">
            <Agent>
                <Port/>
                <SslAllowBeast>1</SslAllowBeast>
                <PollServer>0</PollServer>
                <PollServerInterval>10</PollServerInterval>
            </Agent>
            <Server>
                <HostName/>
                <FastPort/>
                <SlowPort/>
                <ApiKey/>
            </Server>
            <Message InitialRetryInterval="120" MaxRetryInterval="7680">
                <Register Trigger="1"/>
                <Unregister Trigger="1"/>
                <UpdateStatus Trigger="1"/>
                <UploadBlockedEvent Trigger="1"/>
                <CheckFileHash Trigger="1"/>
                <QuickScanFile Trigger="1"/>
            </Message>
            <MessageRandomization TotalGroupNum="1" OwnGroupIndex="0" Tim
            <Proxy Mode="0">
                <HostName/>
                <Port/>
                <UserName/>
                <Password/>
            </Proxy>
        </ManagedMode>
    </Configuration>
```

```
    <Permission>
        <AccountRef Id="{24335D7C-1204-43d1-9CBB-332D688C85B6}">
            <UIControl Id="DetailSetting" State="no"/>
            <UIControl Id="LockUnlock" State="yes"/>
            <UIControl Id="LaunchUpdater" State="yes"/>
            <UIControl Id="RecentHistoryUnapprovedFiles" State="yes"/>
            <UIControl Id="ImportExportList" State="yes"/>
            <UIControl Id="ListManagement" State="yes"/>
            <UIControl Id="SupportToolUninstall" State="no"/>
        </AccountRef>
    </Permission>
</Configurations>
```

Configuration File Parameters

The configuration file contains sections that specify parameters used by Safe Lock.

TABLE 4-1. Configuration File Sections and Descriptions

SECTION		DESCRIPTION	ADDITIONAL INFORMATION
`Configuration`		Container for the Configuration section	
	`AccountGroup`	Parameters to configure the Restricted User account	See *AccountGroup Section on page 4-10*. See *Account Types on page 2-16*.
	`UI`	Parameters to configure the display of the system tray icon	See *UI Section on page 4-10*.
	`Feature`	Container for the Feature section	

SECTION			DESCRIPTION	ADDITIONAL INFORMATION
		ApplicationLockDown	Parameters to configure Safe Lock features and functions	See *Feature Section on page 4-13*.
		UsbMalwareProtection		
		DllInjectionPrevention		
		ApiHookingPrevention		
		MemoryRandomization		
		NetworkVirusProtection		
		IntegrityMonitoring		
		StorageDeviceBlocking	A parameter to control storage device access to managed endpoints	
		Log	Parameters to configure individual log types	See *Log Section on page 4-26*. See *Agent Event Log Descriptions on page 7-4*.
	ManagedMode		Parameters to configure Centralized Management functions	See *ManagedMode Section on page 4-31*.
Permission			Container for the Permission section	
	AccountRef		Parameters to configure the Safe Lock console controls available to the Restricted User account	See *AccountRef Section on page 4-35*. See *Account Types on page 2-16*.

AccountGroup Section

Parameters to configure the Restricted User account

See *Account Types on page 2-16*.

TABLE 4-2. Configuration File `AccountGroup` Section Parameters

PARAMETER	SETTING	VALUE	DESCRIPTION
`Configuration`			Container for the Configuration section
`AccountGroup`			Container for the AccountGroup section
`Account`	`ID`	<GUID>	Restricted User account GUID
	`Enable`	`yes`	Enable the Restricted User account
		`no`	Disable the Restricted User account
	`Password`	<Safe_Lock_password>	Password for the Restricted User account to access the Safe Lock console **Note** The Safe Lock administrator and Restricted User passwords cannot be the same.

UI Section

Parameters to configure the display of the system tray icon

TABLE 4-3. Configuration File `UI` Section Parameters

PARAMETER	SETTING	VALUE	DESCRIPTION
`Configuration`			Container for the Configuration section

Parameter				Setting	Value	Description
UI						Container for the UI section
	SystemTrayIcon			Enable	yes	Display the system tray icon and Windows notifications
					no	Hide the system tray icon and Windows notifications
		BlockNotification		Enable	yes	Display a notification on the managed endpoint when a file not specified in the agent Approved List is blocked.
					no	Do not display any notifications on the managed endpoint when files not specified in the agent Approved List are blocked.
				Authenticate	yes	Prompt for the administrator password when the user attempts to close the notification.
					no	Password is not required to close the notification.
				ShowDetails	yes	Show file path of the blocked file and the event time.
					no	Do not show event details.
				AlwaysOnTop	yes	Keep the notification on top of any other screen.
					no	Allow other screens to cover the notification.
				Title	<Title>	Specify the title for the notification.
				Message	<Message>	Specify the message for the notification.

Feature Section

Parameters to configure Safe Lock features and functions

See *About Feature Settings on page 2-18*.

TABLE 4-4. Configuration File `Feature` Section Parameters

PARAMETER	SETTING	VALUE	DESCRIPTION
`Configuration`			Container for the Configuration section
`Feature`			Container for the Feature section
`ApplicationLockDown`	`LockDownMode`	`1`	Turn on Application Lockdown
		`2`	Turn off Application Lockdown
`WhiteList`	`RecentHistoryUnapprovedFilesLimit`	`0 - 65535`	Maximum number of entries in the Blocked Files log
ExclusionList			Container for the Exclusion for Approved List initialization section
	Folder	<folder_path>	Exclusion folder path
	Extension	<file_extension>	Exclusion file extension
`ScriptLockDown`	`Enable`	`yes`	Enable Script Lockdown
		`no`	Disable Script Lockdown

Parameter	Setting	Value	Description
Extension	ID	<file_extension>	File extension for Script Lockdown to block For example, specify a value of `MSI` to block `.msi` files.
Interpreter		<file_name>	Interpreter for the specified file extension For example, specify **`msiexec.exe`** as the interpreter for `.msi` files.
TrustedUpdater			Container for the TrustedUpdater section
PredefinedTrustedUpdater	Enable	yes	Enable Trusted Updater
		no	Disable Trusted Updater
RuleSet			Container for RuleSet conditions
Condition	ID	<unique_ruleset_name>	Unique name for the set of rules
ApprovedListCheck	Enable	yes	Enable hash checks for programs executed using the Trusted Updater
		no	Disable hash checks for programs executed using the Trusted Updater

PARAMETER								SETTING	VALUE	DESCRIPTION
							ParentProcess	Path	<process_path>	Path of the parent process to add to the Trusted Updater List
						Exception		Path	<process_path>	Path to exclude from the Trusted Updater List
						Rule		Label	<unique_rule_name>	Unique name for this rule
							Updater	Type	process	Use the specified EXE file
									file	Use the specified MSI or BAT file
									folder	Use the EXE, MSI or BAT files in the specified folder
									folderandsub	Use the EXE, MSI or BAT files in the specified folder and its subfolders
								Path	<updater_path>	Trusted Update path
								ConditionRef	<condition_ID>	Condition ID to provide a more detailed rule for the Trusted Updater
						WindowsUpdateSupport		Enable	yes	Allow Windows Update to run on the managed endpoint when it is locked down.
									no	Block Windows Update on the managed

Parameter	Setting	Value	Description
			endpoint when it is locked down.
DLLDriverLockdown	Enable	yes	Enable DLL/Driver Lockdown
		no	Disable DLL/Driver Lockdown
ExceptionPath	Enable	yes	Enable exception paths
		no	Disable exception paths
ExceptionPathList			Container for the Exception List
ExceptionPath	Path	<exception_path>	Exception path
	Type	file	Use only the specified file
		folder	Use the files in the specified folder
		folderandsub	Use the files in the specified folder and its subfolders
		regexp	Use an exception using the regular expression
TrustedCertification	Enable	yes	Enable using Trusted Certifications
		no	Disable using Trusted Certifications
PredefinedTrustedCertification	Type	updater	File signed by this certificate is treated as a Trusted Update

Parameter	Setting	Value	Description
		lockdown	File signed by this certificate is not treated as a Trusted Update
	Hash	<SHA-1_hash_value>	SHA1-hash value of this certificate
	Label	<label>	Description of this certificate
	Subject	<subject>	Subject of this certificate
	Issuer	<issuer>	Issuer of this certificate
TrustedHash	Enable	yes	Enable using the Trusted Hash List
		no	Disable using the Trusted Hash List
PredefinedTrustedHash	Type	updater	File matched by this hash value is treated as a Trusted Update
		lockdown	File matched by this hash value is not treated as a Trusted Update
	Hash	<SHA-1_hash_value>	SHA-1 hash value of this file
	Label	<label>	Description of this file
	AddToApprovedList	yes	Add the file matched by this hash value to the Approved List when it is accessed for the first time

Parameter	Setting	Value	Description
		no	Do not add the file matched by this hash value to the Approved List
	Path	<file_path>	File path
	Note	<note>	Add a note for the file matched by this hash value
WriteProtection	Enable	yes	Enable Write Protection
		no	Disable Write Protection
	ActionMode	0	Allow actions such as edit, rename, and delete
		1	Block actions such as edit, rename, and delete
	ProtectApprovedList	yes	Enable protection of the Approved List (in addition to the Write Protection List) when Write Protection is enabled
		no	Disable protection of the Approved List (in addition to the Write Protection List) when Write Protection is enabled
List			Container for the Write Protection List

Parameter	Setting	Value	Description
File	Path	<file_path>	File path
Folder	Path	<folder_path>	Folder path
	IncludeSubfolder	yes	Use the files in the specified folder and its subfolders
		no	Use the files in the specified folder
RegistryKey	Key	<reg_key>	Registry key <reg_key> can be abbreviated or expanded as shown below: • HKEY_LOCAL_MACHINE\test HKLM\test • HKEY_CURRENT_CONFIG\test HKCC\test • HKEY_CLASSES_ROOT\test HKCR\test • HKEY_CURRENT_USER\test HKCU\test • HKEY_USERS\test HKU\test
	IncludeSubkey	yes	Include any subkeys

PARAMETER			SETTING	VALUE	DESCRIPTION
				no	Do not include any subkeys
		RegistryValue	Key	<reg_key>	Registry key <reg_key> can be abbreviated or expanded as shown below: • HKEY_LOCAL_MACHINE\test HKLM\test • HKEY_CURRENT_CONFIG\test HKCC\test • HKEY_CLASSES_ROOT\test HKCR\test • HKEY_CURRENT_USER\test HKCU\test • HKEY_USERS\test HKU\test
			Name	<reg_value_name>	Registry value name
	ExceptionList				Container for the Write Protection Exception List
		Process	Path	<process_path>	Path of the process

PARAMETER						SETTING	VALUE	DESCRIPTION
					File	Path	<file_path>	File path
					Folder	Path	<folder_path>	Folder path
						IncludeSubfolder	yes	Use the files in the specified folder and its subfolders
							no	Use the files in the specified folder
					RegistryKey	Key	<reg_key>	Registry key <reg_key> can be abbreviated or expanded as shown below: • HKEY_LOCAL_MACHINE\test HKLM\test • HKEY_CURRENT_CONFIG\test HKCC\test • HKEY_CLASSES_ROOT\test HKCR\test • HKEY_CURRENT_USER\test HKCU\test • HKEY_USERS\test HKU\test
						IncludeSubkey	yes	Include any subkeys

Parameter				Setting	Value	Description
					no	Do not include any subkeys
			RegistryValue	Key	<reg_key>	Registry key <reg_key> can be abbreviated or expanded as shown below: • HKEY_LOCAL_MACHINE\test HKLM\test • HKEY_CURRENT_CONFIG\test HKCC\test • HKEY_CLASSES_ROOT\test HKCR\test • HKEY_CURRENT_USER\test HKCU\test • HKEY_USERS\test HKU\test
				Name	<reg_value_name>	Registry value name
		CustomAction		ActionMode	0	Ignore blocked files or processes when Application Lockdown blocks any of the following events: • Process launch

Parameter	Setting	Value	Description
			• DLL loading • Script file access
		1	Quarantine blocked files or processes when Application Lockdown blocks any of the following events: • Process launch • DLL loading • Script file access
		2	Ask what to do for blocked files or processes when Application Lockdown blocks any of the following events: • Process launch • DLL loading • Script file access
UsbMalwareProtection	Enable	yes	Enable USB Malware Protection
		no	Disable USB Malware Protection
	ActionMode	0	Allow action by detected malware
		1	Block action by detected malware
DllInjectionPrevention	Enable	yes	Enable DLL Injection Prevention
		no	Disable DLL Injection Prevention

Parameter	Setting	Value	Description
	ActionMode	0	Allows DLL injections
		1	Blocks DLL injections
ApiHookingPrevention	Enable	yes	Enable API Hooking Prevention
		no	Disable API Hooking Prevention
	ActionMode	0	Allow API hooking
		1	Block API hooking
MemoryRandomization	Enable	yes	Enable Memory Randomization
		no	Disable Memory Randomization
NetworkVirusProtection	Enable	yes	Enable Network Virus Protection
		no	Disable Network Virus Protection
	ActionMode	0	Allow action by detected network viruses
		1	Block action by detected network viruses
IntegrityMonitoring	Enable	yes	Enable Integrity Monitoring
		no	Disable Integrity Monitoring
StorageDeviceBlocking	Enable	yes	Blocks access of storage devices (CD/DVD drives, floppy disks, and network

PARAMETER	SETTING	VALUE	DESCRIPTION
			drives) to managed endpoints
	Disable	no	Allows access of storage devices (CD/DVD drives, floppy disks, and network drives) to managed endpoints
	ActionMode	0	Allow actions such as edit, rename, and delete
		1	Block actions such as edit, rename, and delete
	Log		Container for configuring logs See *Log Section on page 4-26*.
FilelessAttackPrevention	Enable	yes	Enable Fileless Attack Prevention
		no	Disable Fileless Attack Prevention
ExceptionList			Container for the Fileless Attack Prevention Exception List
Exception	Target	<monitored process>	Specify `powershell.exe`, `wscript.exe`, `CScript.exe`, or `mshta.exe`
	Label	<label>	Unique name of this exception

PARAMETER	SETTING	VALUE	DESCRIPTION
Arguments		<arguments>	Arguments to be approved
	Regex	yes	Specify yes if argument includes a regular exception
		no	Specify no if argument does not include a regular exception
Parent1		<parent process>	Parent process of the monitored process
Parent2		<grandparent process>	Grandparent process of the monitored process
Parent3		<great grandparent process>	Great grandparent process of the monitored process
Parent4		<great great grandparent process>	Great great grandparent process of the monitored process

Log Section

Parameters to configure individual log types

See *Agent Event Log Descriptions on page 7-4*.

TABLE 4-5. Configuration File `Log` Section Parameters

PARAMETER	SETTING	VALUE	DESCRIPTION
`Configuration`			Container for the Configuration section
`Feature`			Container for the Feature section
`Log`			Container for configuring logs
`EventLog`	`Enable`	`yes`	Log the Safe Lock events specified in the following elements
		`no`	Do not log the Safe Lock events specified in the following elements
`Level`			Container for configuring log levels
`WarningLog`	`Enable`	`yes`	Log “Warning” level events related to Safe Lock
		`no`	Do not log “Warning” level events related to Safe Lock
`InformationLog`	`Enable`	`yes`	Log “Information” level events related to Safe Lock
		`no`	Do not log “Information” level events related to Safe Lock
`BlockedAccessLog`	`Enable`	`yes`	Log files blocked by Safe Lock
		`no`	Do not log files blocked by Safe Lock
`ApprovedAccessLog`	`Enable`	`yes`	Log files approved by Safe Lock
		`no`	Do not log files approved by Safe Lock

Parameter	Setting	Value	Description
TrustedUpdaterLog	Enable	yes	Log Trusted Updater approved access
		no	Do not log Trusted Updater approved access
DLLDriverLog	Enable	yes	Log DLL/Driver approved access
		no	Do not log DLL/Driver approved access
ExceptionPathLog	Enable	yes	Log Application Lockdown exception path approved access
		no	Do not log Application Lockdown exception path approved access
TrustedCertLog	Enable	yes	Log Trusted Certifications approved access
		no	Do not log Trusted Certifications approved access
WriteProtectionLog	Enable	yes	Log Write Protection approved access
		no	Do not log Write Protection approved access
SystemEventLog	Enable	yes	Log events related to the system
		no	Do not log events related to the system
ExceptionPathLog	Enable	yes	Log exceptions to Application Lockdown
		no	Do not log exceptions to Application Lockdown

PARAMETER	SETTING	VALUE	DESCRIPTION
WriteProtectionLog	Enable	yes	Log Write Protection events
		no	Do not log Write Protection events
ListLog	Enable	yes	Log events related to the Approved list
		no	Do not log events related to the Approved list
USBMalwareProtectionLog	Enable	yes	Log events that trigger USB Malware Protection
		no	Do not log events that trigger USB Malware Protection
ExecutionPreventionLog	Enable	yes	Log events that trigger Execution Prevention
		no	Do not log events that trigger Execution Prevention
NetworkVirusProtectionLog	Enable	yes	Log events that trigger Network Virus Protection
		no	Do not log events that trigger Network Virus Protection
IntegrityMonitoringLog			Container for configuring Integrity Monitoring logs
FileCreatedLog	Enable	yes	Log file and folder created events
		no	Do not log file and folder created events
FileModifiedLog	Enable	yes	Log file modified events
		no	Do not log file modified events
FileDeletedLog	Enable	yes	Log file and folder deleted events

Parameter	Setting	Value	Description
		no	Do not log file and folder deleted events
FileRenamedLog	Enable	yes	Log file and folder renamed events
		no	Do not log file and folder renamed events
RegValueModifiedLog	Enable	yes	Log registry value modified events
		no	Do not log registry value modified events
RegValueDeletedLog	Enable	yes	Log registry value deleted events
		no	Do not log registry value deleted events
RegKeyCreatedLog	Enable	yes	Log registry key created events
		no	Do not log registry key created events
RegKeyDeletedLog	Enable	yes	Log registry key deleted events
		no	Do not log registry key deleted events
RegKeyRenamedLog	Enable	yes	Log registry key renamed events
		no	Do not log registry key renamed events
DeviceControlLog	Enable	yes	Log storage device control events.
		no	Do not log storage device control events.
DebugLog	Enable	yes	Log debugging information

PARAMETER	SETTING	VALUE	DESCRIPTION
		no	Do not log debugging information

ManagedMode Section

Parameters to configure Centralized Management functions

TABLE 4-6. Configuration File `ManagedMode` Section Parameters

PARAMETER	SETTING	VALUE	DESCRIPTION
Configuration			Container for the Configuration section
ManagedMode	Enable	yes	Enable managed mode
		no	Disable managed mode
Agent			Container for configuring Safe Lock agents
Port		<server_messages_port>	Specify the secure port for server communications (formerly the agent listening port)
SslAllowBeast		0	Allow upload of large files (>10MB) on Windows Server 2008 platforms
		1	Prevent the unsuccessful upload of large files (>10MB) on Windows Server 2008 platforms (default value)
PollServer		0	Identify the agent as a non-NAT agent

PARAMETER	SETTING	VALUE	DESCRIPTION
		1	Identify the agent as a NAT agent.
PollServerInterval		<interval_period>	Specify a NAT connection frequency from 1 to 64800 minutes (connect to the Safe Lock server every 1-64800 minutes)
Server			Container for configuring Safe Lock Intelligent Manager
HostName		<hostname>	Specify the host name of the Intelligent Manager server
FastPort		<logs_port>	Specify secure port for collecting logs and status (formerly Fast Lane)
SlowPort		<files_port>	Specify secure port for collecting files for scanning (formerly Slow Lane)
ApiKey		<API_key>	Specify API key
Message			Container for configuring automated messages to Safe Lock Intelligent Manager
Register	Trigger	1	Send as soon as possible after the event occurs
		2	Do not send unless requested to by Intelligent Manager

PARAMETER	SETTING	VALUE	DESCRIPTION
Unregister	Trigger	1	Send as soon as possible after the event occurs
		2	Do not send unless requested to by Intelligent Manager
UpdateStatus	Trigger	1	Send as soon as possible after the event occurs
		2	Do not send unless requested to by Intelligent Manager
UploadBlockedEvent	Trigger	1	Send as soon as possible after the event occurs
		2	Do not send unless requested to by Intelligent Manager
CheckFileHash	Trigger	1	Send as soon as possible after the event occurs
		2	Do not send unless requested to by Intelligent Manager
QuickScanFile	Trigger	1	Send as soon as possible after the event occurs
		2	Do not send unless requested to by Intelligent Manager
MessageRandomization			

PARAMETER	SETTING	VALUE	DESCRIPTION
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.			
	`TotalGroupNum`	Positive Integer (>= `1`)	Specify the total number of message time groups
	`OwnGroupIndex`	Zero or Positive Integer, < `TotalGroupNum`	Specify the message time group ID number of this Safe Lock agent
	`TimePeriod`	Zero or Positive Integer	Specify the duration of time in whole seconds that this message time group ID number will send automated messages to Intelligent Manager when this group's message-sending cycle is active **Note** Message time groups do not become active if their duration is set to zero (0).
`Proxy`	`Mode`	`0`	Do not use a proxy (direct access)
		`1`	Use a proxy (manual setting)
		`2`	Synchronize proxy settings with Internet Explorer

PARAMETER	SETTING	VALUE	DESCRIPTION
HostName		<proxy_hostname>	Specify the proxy host name
Port		<proxy_port>	Specify the proxy port number
UserName		<proxy_user_name>	Specify the proxy user name
Password		<proxy_password>	Specify the proxy password

AccountRef Section

Parameters to configure the Safe Lock console controls available to the Restricted User account

See *Account Types on page 2-16*.

TABLE 4-7. Configuration File `AccountRef` Section Parameters

PARAMETER	SETTING	VALUE	DESCRIPTION
Configuration			Container for the Configuration section
Permission			Container for the Permission section
AccountRef			Container for the AccountRef section
UIControl	ID	DetailSetting	Access the features and functions on the Safe Lock console **Settings** page

PARAMETER	SETTING	VALUE	DESCRIPTION
			Note The **Password** page is not available to the Restricted User account.
		`LockUnlock`	Access the Application Lockdown setting on the **Overview** screen
		`LaunchUpdater`	Access the **Automatically add files created or modified by the selected application installer** option when a Restricted User clicks **Add Item** on the **Approved List** screen
		`RecentHistoryUnapprovedFIles`	Access the Block logs if a Restricted User clicks **Last application blocked** on the **Overview**screen
		`ImportExportList`	Access the **Import List** and **Export List** buttons
		`ListManagement`	Access the following items on the **Approved List** screen: • The **Delete Item** button • The **Update Hash** button • The **Add Item** > **Add Files/ Folders** menu
	`State`	`yes`	Enable the permission specified by `ID`
		`no`	Disable the permission specified by `ID`

Chapter 5

Troubleshooting

This chapter describes troubleshooting techniques and frequently asked questions about Trend Micro Safe Lock .

Topics in this chapter include:

Frequently Asked Questions (FAQ)

What if the endpoint becomes infected by a threat?

Use Trend Micro Portable Security to remove the threat without having to update the Approved List or turn off Application Lockdown at the endpoint.

What if the endpoint uses SHA1 certificates that have reached end-of-support?

Endpoints running Windows Vista or earlier may be set up with SHA1 certificates that have expired past their EOS (end-of-support) date. This may cause issues when running Trend Micro Portable Security or Trend Micro USB Security on endpoints where Trend Micro Safe Lock is installed. To ensure that Trend Micro Portable Security or Trend Micro USB Security run without issues, perform the following:

Procedure

1. On the agent, launch the Trend Micro Safe Lock settings screen.

   For details, see *Enabling or Disabling Feature Settings on page 2-22*.

2. Under **Intrusion Prevention**, disable **USB Malware Protection**.

3. Click the **Approved List** menu item.

4. Add all the modules required for each product to the Approved List:

   - Add Trend Micro Portable Security modules to the Approved List
   - Add Trend Micro USB Security modules to the Approved List

   For details, see *Adding or Removing Files on page 2-13*.

Note

To determine the required modules, contact Trend Micro support.

5. Launch Trend Micro Portable Security or Trend Micro USB Security.

   Trend Micro Portable Security or Trend Micro USB Security should run without issues.

Where can I get more help with Trend Micro Safe Lock ?

Get the most up-to-date information and support from the Trend Micro support website at:

http://esupport.trendmicro.com/en-us/business/

Troubleshooting Safe Lock

The Trend Micro Safe Lock Diagnostic Toolkit offers administrators the ability to perform a number of diagnostic functions, including:

- Create, collect, and delete debugging logs
- Enable or disable Self Protection

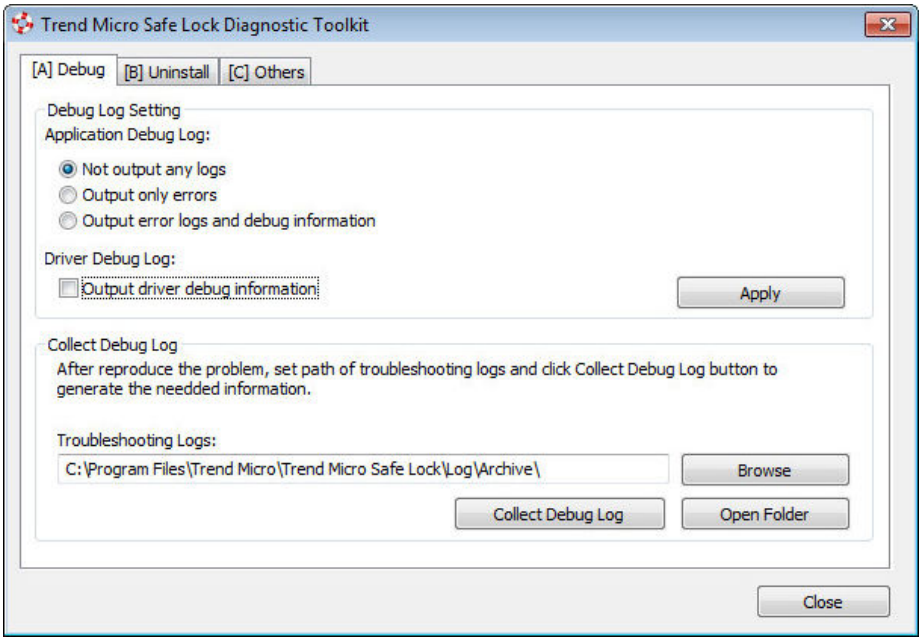


FIGURE 5-1. The Trend Micro Safe Lock Diagnostic Toolkit Debug Tab

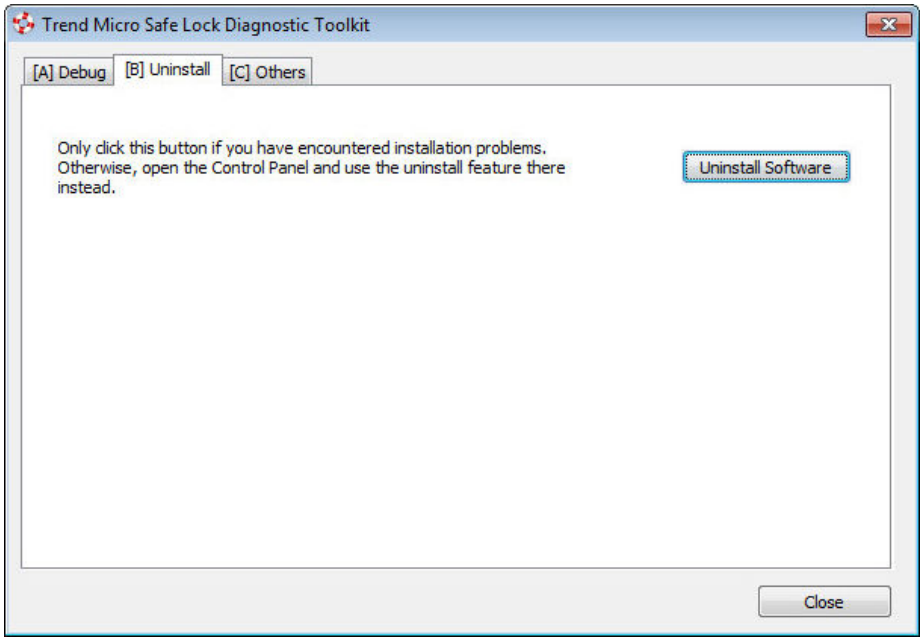


FIGURE 5-2. The Trend Micro Safe Lock Diagnostic Uninstall Tab

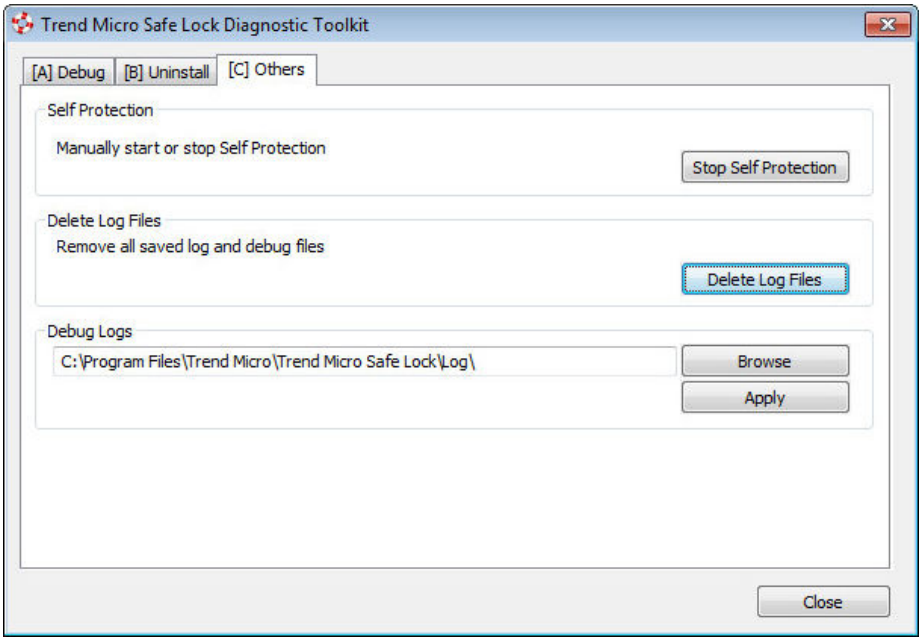


FIGURE 5-3. The Trend Micro Safe Lock Diagnostic Toolkit Others Tab

Using the Diagnostic Toolkit

If Trend Micro Safe Lock experiences problems, generate a complete set of application and driver diagnostic logs for analysis, or send them to to Trend Micro Technical Support. Both the Trend Micro administrator and Restricted User accounts can collect the logs.

Procedure

1. Open the Diagnostic Toolkit and enable full logging:

   a. Open the Trend Micro Safe Lock installation folder and run `WKSupportTool.exe`.

Note

The default installation location is `c:\Program Files\Trend Micro \Safe Lock\`.

b. Provide the Trend Micro administrator or Restricted User password and click **OK**.

c. On the **[A] Debug** tab, select **Output error logs and debug information** and **Output driver debug information**, and click **Apply**.

2. Reproduce the problem.

3. Collect the diagnostic logs:

a. Reopen the Diagnostic Toolkit.

b. On the **[A] Debug** tab, click **Browse** to choose the location where Trend Micro Safe Lock saves the logs.

Note

The default location for saved logs is: `c:\Program Files\Trend Micro \Safe Lock\Log\Archive\`.

c. Click **OK** when finished.

d. Click **Collect Debug Log**.

e. Once the Debug Logs have been collected, click **Open Folder** to access the zipped log files for review, or to send them to Trend Micro Technical Support.

Diagnostic Toolkit Commands

The following table lists the commands available using the Diagnostic Toolkit, `WKSupportTool.exe`.

Note

Only the Safe Lock administrator can use the Diagnostic Toolkit, and `WKSupportTool.exe` will prompt for the administrator password before running a command.

TABLE 5-1. Diagnostic Toolkit Commands

COMMAND	DESCRIPTION
`-p <password>`	Authenticates the user, allowing the command to run.
`debug [on|off] [verbose|normal] [-drv on] [-drv off]`	Turns the debug logs on or off, specifies the log detail level, and if driver logs are included.
`collect [path]`	Collects debugging information and creates a zip file to the specified path. If no path is specified, the default log location `<installation directory>\Log\Archive` is used.
`selfprotection [on|off]`	Turns on or off Safe Lock self protection.
`deletelogs`	Deletes all Safe Lock logs.
`uninstall`	Uninstalls Trend Micro Safe Lock .
`changelogpath [path]`	Change debug log output folder.
`EncryptSetupIni Setup.ini Setup.bin`	Encrypt the Setup.ini file.

Chapter 6

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

Chapter 7

Appendix: Reference

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

Topics in this chapter include:

Enabling Local Administrator Accounts

Windows NT Version 6.x (Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows Server 2008 and Windows Server 2012) and Windows NT 10.x (Windows 10 and Windows Server 2016) require special steps to allow you to use local Windows administrator accounts.

Procedure

1. Open **Computer Management**.
   a. Open the **Start** menu.
   b. Right-click **Computer**.
   c. Go to **Manage**.

      The **Computer Management** window appears.
2. In the list on the left, go to **Computer Management** > **System Tools** > **Local Users and Groups** > **Users**.

   The list of local Windows user accounts displays.
3. In the list of user accounts, right-click **Administrator**, then go to **Properties**.

   The **Administrator Properties** window appears.
4. In the **General** tab, clear **Account is disabled**.
5. Click **OK**.

   The **Computer Management** window reappears, displaying the list of local Windows user accounts.
6. Right-click **Administrator**, then go to **Set Password...**.

   A message displays instructions for setting the password.
7. Set the password.
8. Exit **Computer Management**.

Enabling Local Accounts for Default Shares

Windows NT Version 6.x, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2008, and Windows Server 2012 require special steps to allow local Windows administrator accounts to access default shares, for example the default share `admin$`.

Tip

Steps vary depending on your Windows version. For specific instructions and help for your Windows version, refer to the Microsoft Knowledgebase at http://msdn.microsoft.com.

Procedure

1. Open **Registry Editor** (`regedit.exe`).
   a. Go to **Start** > **Run**
   b. Type **`regedit`**, then press ENTER.
2. Locate and click the following registry subkey:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
   \CurrentVersion\Policies\System
   ```

3. Locate the `LocalAccountTokenFilterPolicy` registry entry.

   If the registry entry does not exist, follow these steps:

   a. Go to **Edit** > **New**.
   b. Select `DWORD Value`.
   c. Type `LocalAccountTokenFilterPolicy`, then press ENTER.
4. Right-click `LocalAccountTokenFilterPolicy`, then go to **Modify**.
5. In the **Value**field, type `1`.
6. Click **OK**.

7. Exit **Registry Editor**.

Agent Event Log Descriptions

Trend Micro Safe Lock leverages the Windows™ Event Viewer to display the Safe Lock event log. Access the Event Viewer at **Start** > **Control Panel** > **Administrative Tools**.

Tip

Safe Lock event logging can be customized by doing the following:

- Before installation, modify the Setup.ini file. See *Setup.ini File Arguments* > *EventLog Section* in the Safe Lock Installation Guide.
- After installation, modify the configuration file. See *Configuration File Parameters* > *Log Section on page 4-26*.

TABLE 7-1. Windows Event Log Descriptions

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
1000	System	Information	Service started.
1001	System	Warning	Service stopped.
1002	System	Information	Application Lockdown Turned On.
1003	System	Warning	Application Lockdown Turned Off.
1004	System	Information	Disabled.
1005	System	Information	Administrator password changed.
1006	System	Information	Restricted User password changed.
1007	System	Information	Restricted User account enabled.
1008	System	Information	Restricted User account disabled.

Event ID	Task Category	Level	Log Description
1009	System	Information	Product activated.
1010	System	Information	Product deactivated.
1011	System	Warning	License Expired. Grace period enabled.
1012	System	Warning	License Expired. Grace period ended.
1013	System	Information	Product configuration import started: %path%
1014	System	Information	Product configuration import complete: %path%
1015	System	Information	Product configuration exported to: %path %
1016	System	Information	USB Malware Protection set to Allow.
1017	System	Information	USB Malware Protection set to Block.
1018	System	Information	USB Malware Protection enabled.
1019	System	Warning	USB Malware Protection disabled.
1020	System	Information	Network Virus Protection set to Allow.
1021	System	Information	Network Virus Protection set to Block.
1022	System	Information	Network Virus Protection enabled.
1023	System	Warning	Network Virus Protection disabled.
1025	System	Information	Memory Randomization enabled.
1026	System	Warning	Memory Randomization disabled.
1027	System	Information	API Hooking Prevention set to Allow.
1028	System	Information	API Hooking Prevention set to Block.
1029	System	Information	API Hooking Prevention enabled.
1030	System	Warning	API Hooking Prevention disabled.

Event ID	Task Category	Level	Log Description
1031	System	Information	DLL Injection Prevention set to Allow.
1032	System	Information	DLL Injection Prevention set to Block.
1033	System	Information	DLL Injection Prevention enabled.
1034	System	Warning	DLL Injection Prevention disabled.
1035	System	Information	Pre-defined Trusted Update enabled.
1036	System	Information	Pre-defined Trusted Update disabled.
1037	System	Information	DLL/Driver Lockdown enabled.
1038	System	Warning	DLL/Driver Lockdown disabled.
1039	System	Information	Script Lockdown enabled.
1040	System	Warning	Script Lockdown disabled.
1041	System	Information	Script added. [Details] File extension: %extension% Interpreter: %interpreter%
1042	System	Information	Script removed. [Details] File extension: %extension% Interpreter: %interpreter%
1044	System	Information	Exception path enabled.
1045	System	Information	Exception path disabled.
1047	System	Information	Trusted certification enabled.
1048	System	Information	Trusted certification disabled.

Event ID	Task Category	Level	Log Description
1049	System	Information	Write Protection enabled.
1050	System	Warning	Write Protection disabled.
1051	System	Information	Write Protection set to Allow.
1052	System	Information	Write Protection set to Block.
1055	System	Information	Added file to Write Protection List. Path: %path%
1056	System	Information	Removed file from Write Protection List. Path: %path%
1057	System	Information	Added file to Write Protection Exception List. Path: %path% Process: %process%
1058	System	Information	Removed file from Write Protection Exception List. Path: %path% Process: %process%
1059	System	Information	Added folder to Write Protection List. Path: %path% Scope: %scope%
1060	System	Information	Removed folder from Write Protection List. Path: %path% Scope: %scope%

Event ID	Task Category	Level	Log Description
1061	System	Information	Added folder to Write Protection Exception List. Path: %path% Scope: %scope% Process: %process%
1062	System	Information	Removed folder from Write Protection Exception List. Path: %path% Scope: %scope% Process: %process%
1063	System	Information	Added registry value to Write Protection List. Registry Key: %regkey% Registry Value Name: %regvalue%
1064	System	Information	Removed registry value from Write Protection List. Registry Key: %regkey% Registry Value Name: %regvalue%
1065	System	Information	Added registry value to Write Protection Exception List. Registry Key: %regkey% Registry Value Name: %regvalue% Process: %process%

Event ID	Task Category	Level	Log Description
1066	System	Information	Removed registry value from Write Protection Exception List. Registry Key: %regkey% Registry Value Name: %regvalue% Process: %process%
1067	System	Information	Added registry key to Write Protection List. Path: %regkey% Scope: %scope%
1068	System	Information	Removed registry key from Write Protection List. Path: %regkey% Scope: %scope%
1069	System	Information	Added registry key to Write Protection Exception List. Path: %regkey% Scope: %scope% Process: %process%
1070	System	Information	Removed registry key from Write Protection Exception List. Path: %regkey% Scope: %scope% Process: %process%
1071	System	Information	Custom Action set to Ignore.
1072	System	Information	Custom Action set to Quarantine.

Event ID	Task Category	Level	Log Description
1073	System	Information	Custom Action set to Ask Intelligent Manager
1074	System	Information	Quarantined file is restored. [Details] Original Location: %path% Source: %source%
1075	System	Information	Quarantined file is deleted. [Details] Original Location: %path% Source: %source%
1076	System	Information	Integrity Monitoring enabled.
1077	System	Information	Integrity Monitoring disabled.
1078	System	Information	Root cause analysis report unsuccessful. [Details] Access Image Path: %path%
1079	System	Information	Server certification imported: %path%
1080	System	Information	Server certification exported to: %path%
1081	System	Information	Managed mode configuration imported: %path%
1082	System	Information	Managed mode configuration exported to: %path%
1083	System	Information	Managed mode enabled.
1084	System	Information	Managed mode disabled.

Event ID	Task Category	Level	Log Description
1085	System	Information	Protection applied to Write Protection List and Approved List while Write Protection is enabled
1086	System	Warning	Protection applied to Write Protection List while Write Protection is enabled.
1088	System	Information	Windows Update Support enabled.
1089	System	Information	Windows Update Support disabled.
1094	System	Information	Trend Micro Safe Lock updated. File applied: %file_name%
1096	System	Information	Trusted Hash List enabled.
1097	System	Information	Trusted Hash List disabled.
1099	System	Information	Storage device access set to Allow
1100	System	Information	Storage device access set to Block
1101	System	Information	Storage device control enabled
1102	System	Warning	Storage device control disabled

Event ID	Task Category	Level	Log Description
1103	System	Information	Event Log settings changed. [Details] Windows Event Log: %ON|off% Level: Warning Log: %ON|off% Information Log: %ON|off% System Log: %ON|off% Exception Path Log: %ON|off% Write Protection Log: %ON|off% List Log: %ON|off% Approved Access Log: DllDriver Log: %ON|off% Trusted Updater Log: %ON|off% Exception Path Log: %ON|off% Trusted Certification Log: %ON|off% Trusted Hash Log: %ON|off% Write Protection Log: %ON|off% Blocked Access Log: %ON|off% USB Malware Protection Log: %ON|off% Execution Prevention Log: %ON|off% Network Virus Protection Log: %ON|off%

Event ID	Task Category	Level	Log Description
			Integrity Monitoring Log File Created Log: %ON|off% File Modified Log: %ON|off% File Deleted Log: %ON|off% File Renamed Log: %ON|off% RegValue Modified Log: %ON|off% RegValue Deleted Log: %ON|off% RegKey Created Log: %ON|off% RegKey Deleted Log: %ON|off% RegKey Renamed Log: %ON|off% Device Control Log: %ON|off% Debug Log: %ON|off%
1104	System	Warning	Memory Randomization is not available in this version of Windows.
1105	System	Information	Blocked File Notification enabled.
1106	System	Information	Blocked File Notification disabled.
1107	System	Information	Administrator password changed remotely.
1111	System	Information	Fileless Attack Prevention enabled.
1112	System	Warning	Fileless Attack Prevention disabled.
1500	List	Information	Trusted Update started.
1501	List	Information	Trusted Update stopped.
1502	List	Information	Approved List import started: %path%
1503	List	Information	Approved List import complete: %path%

Event ID	Task Category	Level	Log Description
1504	List	Information	Approved List exported to: %path%
1505	List	Information	Added to Approved List: %path%
1506	List	Information	Added to Trusted Updater List: %path%
1507	List	Information	Removed from Approved List: %path%
1508	List	Information	Removed from Trusted Updater List: %path%
1509	List	Information	Approved List updated: %path%
1510	List	Information	Trusted Updater List updated: %path%
1511	List	Warning	Unable to add to or update Approved List: %path%
1512	List	Warning	Unable to add to or update Trusted Updater List: %path%
1513	System	Information	Added to Exception Path List. [Details] Type: %exceptionpathtype% Path: %exceptionpath%
1514	System	Information	Removed from Exception Path List. [Details] Type: %exceptionpathtype% Path: %exceptionpath%

Event ID	Task Category	Level	Log Description
1515	System	Information	Added to Trusted Certification List. [Details] Label: %label% Hash: %hashvalue% Type: %type% Subject: %subject% Issuer: %issuer%
1516	System	Information	Removed from Trusted Certification List. [Details] Label: %label% Hash: %hashvalue% Type: %type% Subject: %subject% Issuer: %issuer%
1517	System	Information	Added to the Trusted Hash List.%n [Details] Label : %label% Hash : %hashvalue% Type : %type% Add to Approved List: %yes|no% Path : %path% Note: %note%

Event ID	Task Category	Level	Log Description
1518	System	Information	Removed from the Trusted Hash List.%n [Details] Label : %label% Hash : %hashvalue% Type : %type% Add to Approved List: %yes|no% Path : %path% Note: %note%
1519	List	Information	Removed from Approved List remotely: %path%
1520	List	Warning	Unable to create Approved List because an unexpected error occurred during enumeration of the files in %1 %n Error Code: %2 %n
1521	System	Information	Added Fileless Attack Prevention exception. [Details] Label : %label% Target Process: %process_name% Arguments: %arguments% %regex_flag% Parent Process 1 Image Path: %path% Parent Process 2 Image Path: %path% Parent Process 3 Image Path: %path% Parent Process 4 Image Path: %path%

Event Id	Task Category	Level	Log Description
1522	System	Information	Removed Fileless Attack Prevention exception. [Details] Label : %label% Target Process: %process_name% Arguments: %arguments% %regex_flag% Parent Process 1 Image Path: %path% Parent Process 2 Image Path: %path% Parent Process 3 Image Path: %path% Parent Process 4 Image Path: %path%
2000	Access Approved	Information	File access allowed: %path% [Details] Access Image Path: %path% Access User: %username% Mode: %mode% List: %list%
2001	Access Approved	Warning	File access allowed: %path% [Details] Access Image Path: %path% Access User: %username% Mode: %mode% File Hash allowed: %hash%

Event ID	Task Category	Level	Log Description
2002	Access Approved	Warning	File access allowed: %path% Unable to get the file path while checking the Approved List. [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2003	Access Approved	Warning	File access allowed: %path% Unable to calculate hash while checking the Approved List. [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2004	Access Approved	Warning	File access allowed: %path% Unable to get notifications to monitor process.
2005	Access Approved	Warning	File access allowed:%path% Unable to add process to non exception list.

Event ID	Task Category	Level	Log Description
2006	Access Approved	Information	File access allowed: %path% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2007	Access Approved	Warning	File access allowed: %path% An error occurred while checking the Exception Path List. [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2008	Access Approved	Warning	File access allowed: %path% An error occurred while checking the Trusted Certification List. [Details] Access Image Path: %path% Access User: %username% Mode: %mode%

Event ID	Task Category	Level	Log Description
2011	Access Approved	Information	Registry access allowed. Registry Key: %regkey% Registry Value Name: %regvalue% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2012	Access Approved	Information	Registry access allowed. Registry Key: %regkey% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2013	Access Approved	Information	Change of File/Folder allowed by Exception List: %path% [Details] Access Image Path: Access User: %username% Mode: %mode%

Event ID	Task Category	Level	Log Description
2015	Access Approved	Information	Change of Registry Value allowed by Exception List. Registry Key: %regkey% Registry Value Name: %regvalue% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2016	Access Approved	Information	Change of Registry Key allowed by Exception List. Registry Key: %regkey% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2017	Access Approved	Warning	Change of File/Folder allowed: %path% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%

Event ID	Task Category	Level	Log Description
2019	Access Approved	Warning	Change of Registry Value allowed. Registry Key: %regkey% Registry Value Name: %regvalue% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2020	Access Approved	Warning	Change of Registry Key allowed. Registry Key: %regkey% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2021	Access Approved	Warning	File access allowed: %path% An error occurred while checking the Trusted Hash List. [Details] Access Image Path: %path% Access User: %username% Mode: %mode%

Event ID	Task Category	Level	Log Description
2022	Access Approved	Warning	Process allowed by Fileless Attack Prevention: %path% %argument% [Details] Access User: %username% Parent Process 1 Image Path: %path% Parent Process 2 Image Path: %path% Parent Process 3 Image Path: %path% Parent Process 4 Image Path: %path% Mode: Unlocked Reason: %reason%
2503	Access Blocked	Warning	Change of File/Folder blocked: %path% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2505	Access Blocked	Warning	Change of Registry Value blocked. Registry Key: %regkey% Registry Value Name: %regvalue% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%

Event ID	Task Category	Level	Log Description
2506	Access Blocked	Warning	Change of Registry Key blocked. Registry Key: %regkey% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2507	Access Blocked	Information	Action completed successfully: %path% [Details] Action: %action% Source: %source%
2508	Access Blocked	Warning	Unable to take specified action: %path% [Details] Action: %action% Source: %source%
2509	Access Blocked	Warning	File access blocked: %path% [Details] Access Image Path: %path% Access User: %username% Mode: %mode% Reason: Not in Approved List File Hash blocked: %hash%

Event ID	Task Category	Level	Log Description
2510	Access Blocked	Warning	File access blocked: %path% [Details] Access Image Path: %path% Access User: %username% Mode: %mode% Reason: Hash does not match expected value File Hash blocked: %hash%
2511	Access Blocked	Information	Change of File/Folder blocked: %path% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2512	Access Blocked	Warning	Change of Registry Value blocked. Registry Key: %regkey% Registry Value Name: %regvalue% [Details] Access Image Path: %path% Access User: %username% **Note** Enabling the Service Creation Prevention feature triggers Event ID 2512.

Event ID	Task Category	Level	Log Description
2513	Access Blocked	Warning	Process blocked by Fileless Attack Prevention: %path% %argument% [Details] Access User: %username% Parent Process 1 Image Path: %path% Parent Process 2 Image Path: %path% Parent Process 3 Image Path: %path% Parent Process 4 Image Path: %path% Mode: locked Reason: %reason%
2514	Access Blocked	Warning	File access blocked : %BLOCKED_FILE_PATH% [Details] Access Image Path: %PARENT_PROCESS_PATH% Access User: %USER_NAME% Reason: Blocked file is in a folder that has the case sensitive attribute enabled.
3000	USB Malware Protection	Warning	Device access allowed: %path% [Details] Access Image Path: %path% Access User: %username% Device Type: %type%

Event ID	Task Category	Level	Log Description
3001	USB Malware Protection	Warning	Device access blocked: %path% [Details] Access Image Path: %path% Access User: %username% Device Type: %type%
3500	Network Virus Protection	Warning	Network virus allowed: %name% [Details] Protocol: TCP Source IP Address: %ip_address% Source Port: %port% Destination IP Address: %ip_address% Destination Port: 80
3501	Network Virus Protection	Warning	Network virus blocked: %name% [Details] Protocol: TCP Source IP Address: %ip_address% Source Port: %port% Destination IP Address: %ip_address% Destination Port: 80

Event ID	Task Category	Level	Log Description
4000	Process Protection Event	Warning	API Hooking/DLL Injection allowed: %path% [Details] Threat Image Path: %path% Threat User: %username%
4001	Process Protection Event	Warning	API Hooking/DLL Injection blocked: %path% [Details] Threat Image Path: %path% Threat User: %username%
4002	Process Protection Event	Warning	API Hooking allowed: %path% [Details] Threat Image Path: %path% Threat User: %username%
4003	Process Protection Event	Warning	API Hooking blocked: %path% [Details] Threat Image Path: %path% Threat User: %username%
4004	Process Protection Event	Warning	DLL Injection allowed: %path% [Details] Threat Image Path: %path% Threat User: %username%

Event ID	Task Category	Level	Log Description
4005	Process Protection Event	Warning	DLL Injection blocked: %path% [Details] Threat Image Path: %path% Threat User: %username%
4500	Changes in System	Information	File/Folder created: %path% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4501	Changes in System	Information	File modified: %path% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4502	Changes in System	Information	File/Folder deleted: %path% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%

Event ID	Task Category	Level	Log Description
4503	Changes in System	Information	File/Folder renamed: %path% New Path: %path% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4504	Changes in System	Information	Registry Value modified. Registry Key: %regkey% Registry Value Name: %regvalue% Registry Value Type: %regvaluetype% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4505	Changes in System	Information	Registry Value deleted. Registry Key: %regkey% Registry Value Name: %regvalue% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%

Event ID	Task Category	Level	Log Description
4506	Changes in System	Information	Registry Key created. Registry Key: %regkey% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4507	Changes in System	Information	Registry Key deleted. Registry Key: %regkey% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4508	Changes in System	Information	Registry Key renamed. Registry Key: %regkey% New Registry Key: %regkey% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%

Agent Error Code Descriptions

This list describes the various error codes used in Trend Micro Safe Lock.

TABLE 7-2. Trend Micro Safe Lock Error Code Descriptions

CODE	DESCRIPTION
0x00040200	Operation successful.
0x80040201	Operation unsuccessful.
0x80040202	Operation unsuccessful.
0x00040202	Operation partially successful.
0x00040203	Requested function not installed.
0x80040203	Requested function not supported.
0x80040204	Invalid argument.
0x80040205	Invalid status.
0x80040206	Out of memory.
0x80040207	Busy. Request ignored.
0x00040208	Retry. (Usually the result of a task taking too long)
0x80040208	System Reserved. (Not used)
0x80040209	The file path is too long.
0x0004020a	System Reserved. (Not used)
0x8004020b	System Reserved. (Not used)
0x0004020c	System Reserved. (Not used)
0x0004020d	System Reserved. (Not used)
0x8004020d	System Reserved. (Not used)
0x0004020e	Reboot required.
0x8004020e	Reboot required for unexpected reason.
0x0004020f	Allowed to perform task.
0x8004020f	Permission denied.

Code	Description
0x00040210	System Reserved. (Not used)
0x80040210	Invalid or unexpected service mode.
0x00040211	System Reserved. (Not used)
0x80040211	Requested task not permitted in current status. Check license.
0x00040212	System Reserved. (Not used)
0x00040213	System Reserved. (Not used)
0x80040213	Passwords do not match.
0x00040214	System Reserved. (Not used)
0x80040214	System Reserved. (Not used)
0x00040215	Not found.
0x80040215	"Expected, but not found."
0x80040216	Authentication is locked.
0x80040217	Invalid password length.
0x80040218	Invalid characters in password.
0x00040219	Duplicate password. Administrator and Restricted User passwords cannot match.
0x80040220	System Reserved. (Not used)
0x80040221	System Reserved. (Not used)
0x80040222	System Reserved. (Not used)
0x80040223	File not found (as expected, and not an error).
0x80040224	System Reserved. (Not used)
0x80040225	System Reserved. (Not used)
0x80040240	Library not found.

CODE	DESCRIPTION
0x80040241	Invalid library status or unexpected error in library function.
0x80040260	System Reserved. (Not used)
0x80040261	System Reserved. (Not used)
0x80040262	System Reserved. (Not used)
0x80040263	System Reserved. (Not used)
0x80040264	System Reserved. (Not used)
0x00040265	System Reserved. (Not used)
0x80040265	System Reserved. (Not used)
0x80040270	System Reserved. (Not used)
0x80040271	System Reserved. (Not used)
0x80040272	System Reserved. (Not used)
0x80040273	System Reserved. (Not used)
0x80040274	System Reserved. (Not used)
0x80040275	System Reserved. (Not used)
0x80040280	Invalid Activation Code.
0x80040281	Incorrect Activation Code format.

Index

S

T

U

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: SLEM28555/181213