TREND MICRO™

2.0 TREND MICRO™ Safe Lock

Administrator's Guide

A powerful lockdown solution for fixed-function computers

Endpoint Security

Document Part No.: SLEM26722/141016

Release Date: December 2014

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

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

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

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

Evaluate this documentation on the following site:

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

Table of Contents

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 guides administrators through installation and deployment.

Topics in this chapter include:

About the Documentation

Trend Micro Safe Lock documentation includes the following:

TABLE 1. Trend Micro Safe Lock Documentation

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

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

http://docs.trendmicro.com

Audience

Trend Micro Safe Lock documentation is intended for administrators responsible for Safe Lock management, including agent installation.

Document Conventions

The following table provides the official terminology used throughout the Trend Micro Safe Lock documentation:

TABLE 2. Document Conventions

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

Convention	Description
 **WARNING!**	Critical actions and configuration options

Chapter 1

Introduction

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

Topics in this chapter include:

About Trend Micro Safe Lock

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

What's New in This Version

This section lists the new features and enhancements available in each release.

Trend Micro Safe Lock 2.0 Features and Enhancements

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

TABLE 1-1. New Features

FEATURE	DESCRIPTION
Write Protection	Prevents write access to all files in the Approved List and all objects (files, folders, and registry entries) in the Write Protection List
Integrity Monitoring	Monitors file change events system-wide for files, folders, and the registry
Approved List and Trusted Updater support Digital Signatures	Allow to loading or launching files that have pre-defined digital signatures, even if the files are not in the Approved List
Exception Path	Allow to loading or launching files in a pre-defined “exceptions” folder without adding them to the Approved List
Custom Action	Takes action on blocked files, for example Ignore, Quarantine, or Ask Server (requires Safe Lock Intelligent Manager)

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.

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 the processes and other resources required to function properly. Self Protection helps thwart attempts by programs or actual users to disable the software.

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 Agent Requirements

This section introduces Safe Lock system requirements and upgrade limitations.

Agent 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

Agent Operating Systems

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

Note

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

TABLE 1-3. List of Supported Operating Systems

WINDOWS VERSION TYPE	WINDOWS VERSION NAME
Windows Clients	Windows 2000 SP4* (32-bit) **Note** *Without Update Rollup, this version of Windows does not support DLL/Driver Lockdown, Integrity Monitoring, and the Predefined Trusted Updater.
	Windows XP SP1*/SP2/SP3 (32-bit) (except Starter and Home editions) **Note** *This version of Windows does not support DLL/Driver Lockdown, Integrity Monitoring, and the 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 Enterprise No-SP (32-bit and 64-bit)
	Windows 8.1 Enterprise No-SP (32-bit and 64-bit)

WINDOWS VERSION TYPE	WINDOWS VERSION NAME
Windows Server	Windows 2000 Server SP4* (32-bit) **Note** *Without Update Rollup, this version of Windows does not support DLL/Driver Lockdown, Integrity Monitoring, and the Predefined Trusted Updater.
	Windows Server 2003 SP1/SP2 (32-bit) **Note** Safe Lock does not support a custom action of “quarantine” on Windows XP or Windows 2003.
	Windows Server 2003 R2 No-SP/SP2 (32-bit) **Note** 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 VERSION TYPE	WINDOWS VERSION NAME
Windows Embedded Standard	Windows (Standard) XP Embedded SP1*/SP2 (32-bit) **Note** *This version of Windows does not support DLL/Driver Lockdown, Integrity Monitoring, and the Predefined Trusted Updater. Safe Lock does not support a custom action of "quarantine" on Windows XP or Windows 2003.
	Windows Embedded Standard 2009 (32-bit)
	Windows Embedded Standard 7 (32-bit and 64-bit)
	Windows Embedded Standard 8 (32-bit and 64-bit)
	Windows Embedded Standard 8.1 (32-bit and 64-bit)
Windows Embedded POSReady	Windows Embedded POSReady (32-bit)
	Windows Embedded POSReady 2009 (32-bit)
	Windows Embedded POSReady 7 (32-bit and 64-bit)
Windows Embedded Enterprise	Windows Embedded Enterprise XP SP1*/SP2/SP3 (32-bit) **Note** *This version of Windows does not support DLL/Driver Lockdown, Integrity Monitoring, and the 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 VERSION TYPE	WINDOWS VERSION NAME
Windows Embedded Server	Windows Embedded Server 2003 SP1/SP2 (32-bit) **Note** 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 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)

Agent Upgrade Preparation

WARNING!

Depending on the installation method you select, Safe Lock versions require different preparation before upgrading.

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

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

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

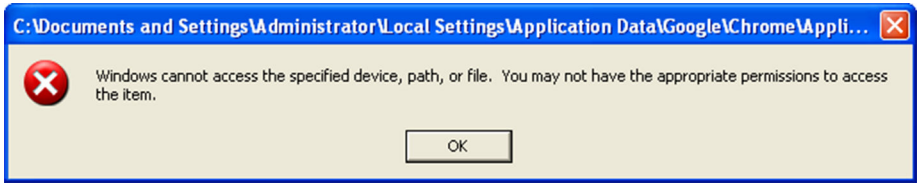


FIGURE 1-1. Trend Micro Safe Lock blocking message

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:

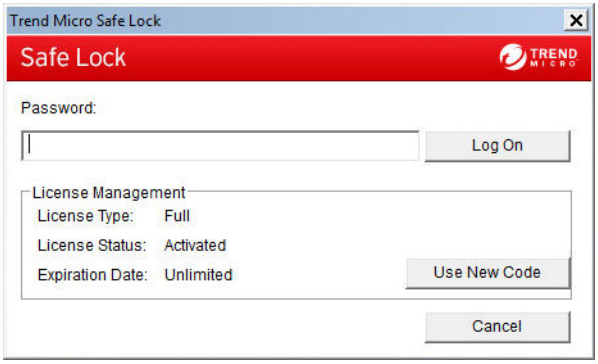
Setting Up the Approved List

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

Procedure

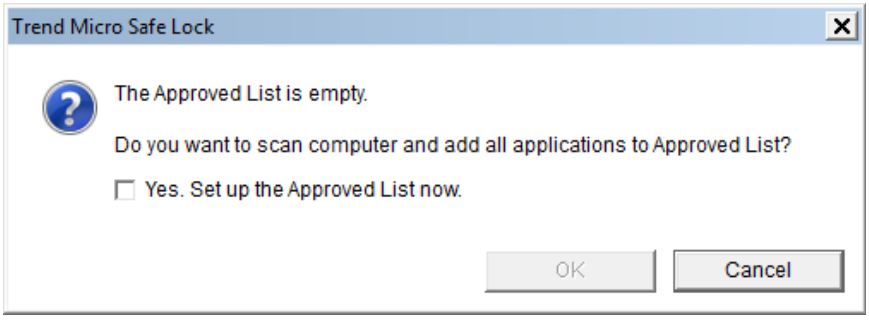
1. Open the Safe Lock console.

   The Safe Lock log on screen appears.



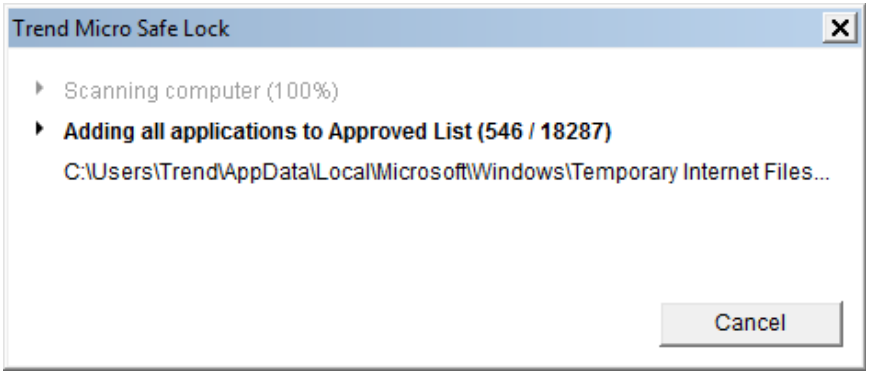
2. Provide the password and click **Login**.

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

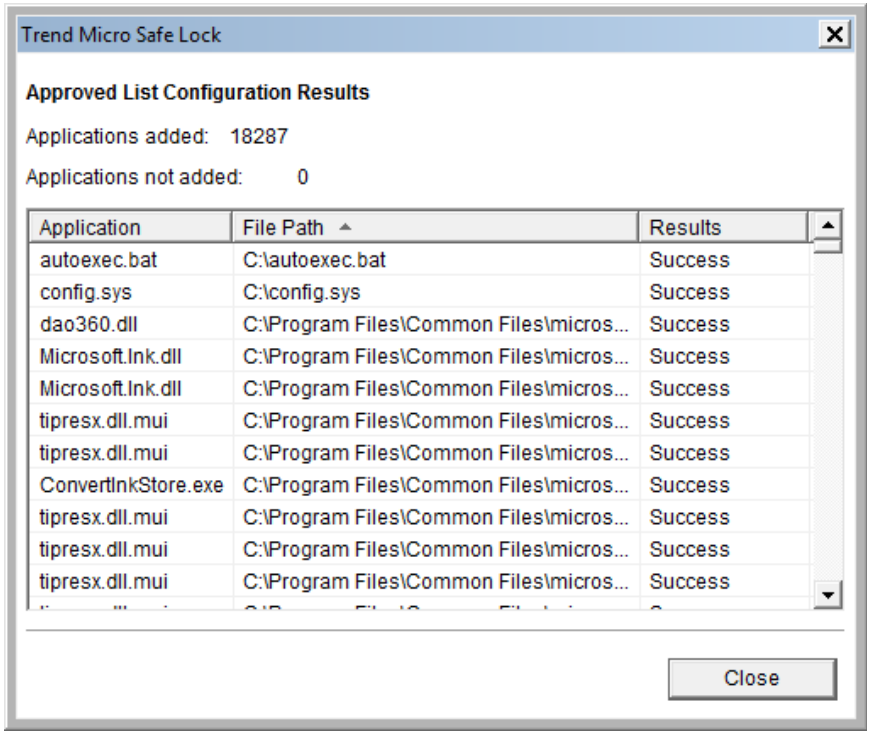


3. At the notification window, select **Yes. Set up the Approved List now** and click **OK**.

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



Safe Lock displays the Approved List Configuration Results.



Note

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

4. Click **Close**.

About the Agent Console

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

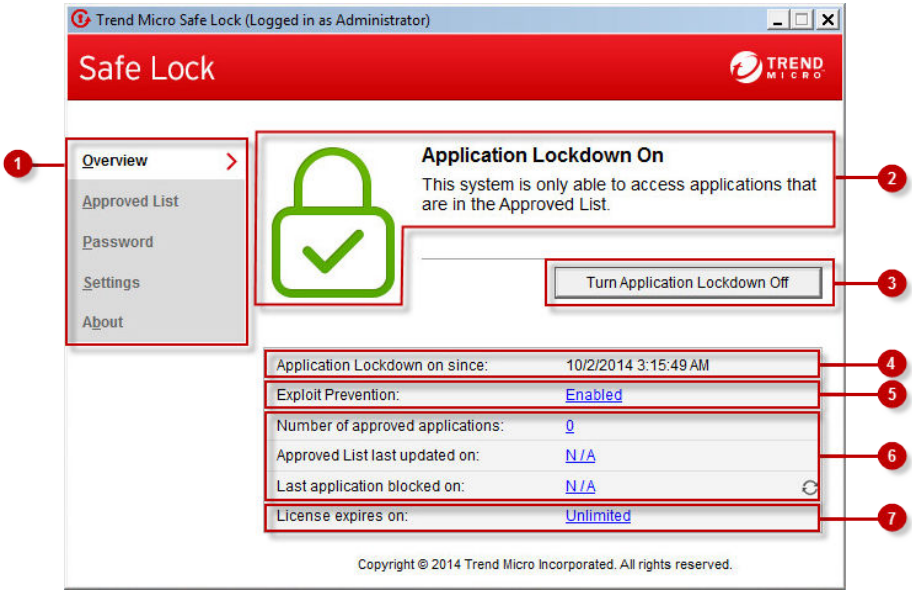


FIGURE 2-1. The Safe Lock console

The following table describes the features available on the console:

TABLE 2-1. 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
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

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

About Status Icons

Use the status icons for a visual indication of the current status of Safe Lock.

Note

System Tray icons display if they were enabled during installation.

TABLE 2-2. 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	When the Safe Lock license has expired, the system cannot be locked. Update the Activation Code by clicking on the expiration date.

About the Approved List

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

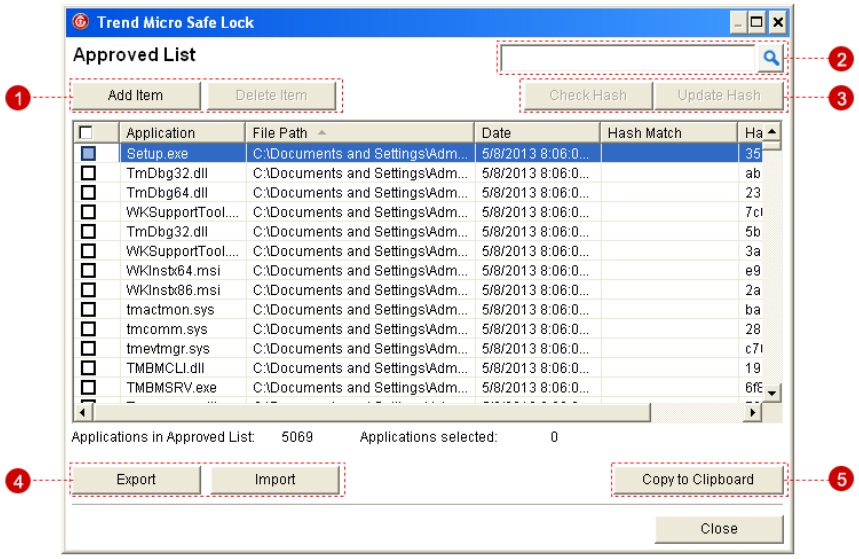


FIGURE 2-2. The Safe Lock Approved List

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

TABLE 2-3. 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.

#	ITEM	DESCRIPTION
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

Trend Micro 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 2-4. 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 2-5. 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 to open the Trusted Updater when updating the endpoint or installing new software. For example, if Mozilla Firefox needs to be installed or updated, use the Trusted Updater. Trend Micro Safe Lock adds or updates any files modified by an installer 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 folders and subfolders**, or **All applications in a folder** 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 **File**, **Folder**, or **Folder and sub folders** 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.

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 2-6. 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 2-16* . 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 **Use 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.

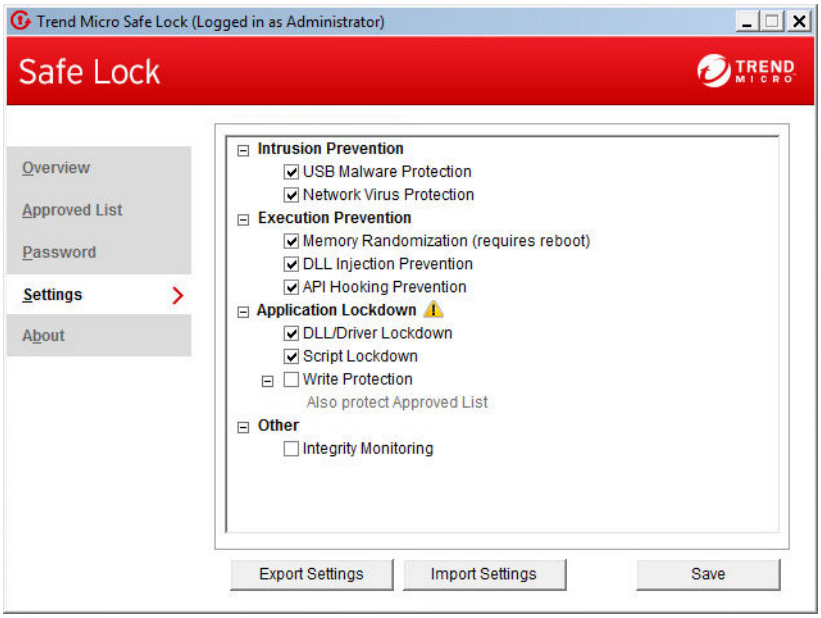


FIGURE 2-4. Safe Lock settings screen

TABLE 2-7. Intrusion Prevention

SETTING	DESCRIPTION
USB Malware Protection	USB Malware Protection prevents 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 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 2-8. 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 2-9. Application Lockdown

SETTING	DESCRIPTION
DLL/Driver Lockdown	DLL/Driver Lockdown prevents unapproved DLLs or drivers from being loaded into the memory of protected endpoints.
Script Lockdown	Script Lockdown prevents unapproved script files from being run on protected endpoints.

SETTING	DESCRIPTION
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.

TABLE 2-10. Other

SETTING	DESCRIPTION
Integrity Monitoring	Integrity Monitoring logs events related to file changes system-wide for files, folders, and the registry.

Enabling or Disabling Feature Settings

Note

By default, Trend Micro Safe Lock enables all 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.

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 at the command line.

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

FUNCTION	SLCMD PROGRAM AT THE COMMAND LINE INTERFACE (CLI)	CONSOLE
Export/Import Approved List	Yes	Yes
Export/Import configuration	Yes	Yes
Install	Yes	Yes
Lock/Unlock	Yes	Yes
License Management	Yes	Yes
Settings	Limited	Limited
Start/Stop Trusted Updater	Yes	Yes
Start/Stop the service	Yes	No
Uninstall	No	No

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	VALUE	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`**

COMMAND	PARAMETER	VALUE	DESCRIPTION
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**
			Prompt the currently logged on administrator to specify a new password For example, type: **SLCmd.exe -p <admin_password> set adminpassword**
set	lock	enable	Turn on Application Lockdown For example, type: **SLCmd.exe -p <admin_password> set lock enable**
		disable	Turn off Application Lockdown For example, type: **SLCmd.exe -p <admin_password> set lock disable**
			Display the current Safe Lock Application Lockdown status For example, type: **SLCmd.exe -p <admin_password> set lock**
show	blockedlog		Display a list of applications blocked by Safe Lock For example, type:

COMMAND	PARAMETER	VALUE	DESCRIPTION
			SLCmd.exe -p <admin_password> show blockedlog
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:

COMMAND	PARAMETER	VALUE	DESCRIPTION
			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	VALUE	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	Encrypt the configuration file used by Managed Mode

COMMAND	PARAMETER	VALUE	DESCRIPTION
		_output_file>	
export	`managedmodeconfiguration`	<path_of_encrypted_output>	Export the encrypted configuration file used by Managed Mode
	`servercertification`	<path_of_certification_file>	Export the encrypted Safe Lock Intelligent Manager SSL communication certificate file
import	`managedmodeconfiguration`	<path_of_encrypted_input>	Import the encrypted configuration file used by Managed Mode
	`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** Using the optional `-cfg` value specifies the path of the configuration file. Using the optional `-sc` value specifies 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
usbmalwareprotection	usb	Manage USB Malware Protection
networkvirusprotection	net	Manage Network Virus Protection
memoryrandomization	mr	Manage Memory Randomization
dllinjectionprevention	dll	Manage DLL Injection Prevention
apihookingprevention	api	Manage API Hooking Prevention
dlldriverlockdown	dd	Manage DLL/Driver Lockdown
script	scr	Manage Script Lockdown
writeprotection	wp	Manage Write Protection
writeprotection-includes-approvedlist	wpal	Manage Write Protection includes Approved List
integritymonitoring	in	Manage Integrity Monitoring
customaction	ca	Manage actions taken when Safe Lock blocks specific types of events
exceptionpath	ep	Manage exceptions to Application Lockdown

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

TABLE 3-7. Optional Feature Commands

COMMAND	PARAMETER	VALUE	DESCRIPTION
set	usbmalwareprotection	enable	Enable USB Malware Protection For example, type: **SLCmd.exe -p <admin_password> set usbmalwareprotection enable**
		disable	Disable USB Malware Protection For example, type: **SLCmd.exe -p <admin_password> set usbmalwareprotection disable**
			Display the current status of USB Malware Protection For example, type: **SLCmd.exe -p <admin_password> set usbmalwareprotection**
set	networkvirusprotection	enable	Enable Network Virus Protection For example, type: **SLCmd.exe -p <admin_password> set networkvirusprotection enable**
		disable	Disable Network Virus Protection For example, type: **SLCmd.exe -p <admin_password> set networkvirusprotection disable**
			Display the current status of Network Virus Protection For example, type:

COMMAND	PARAMETER	VALUE	DESCRIPTION
			SLCmd.exe -p <admin_password> set networkvirusprotection
set	memoryrandomization	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**
			Display the current status of Memory Randomization For example, type: **SLCmd.exe -p <admin_password> set memoryrandomization**
set	dllinjectionprevention	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**
			Display the current status of DLL Injection Prevention For example, type:

COMMAND	PARAMETER	VALUE	DESCRIPTION
			SLCmd.exe -p <admin_password> set dllinjectionprevention
set	apihookingprevention	enable	Enable API Hooking Prevention For example, type: **SLCmd.exe -p <admin_password> set apihookingprevention enable**
		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**
set	dlldriverlockdown	enable	Enable DLL/Driver Lockdown For example, type: **SLCmd.exe -p <admin_password> set dlldriverlockdown enable**
		disable	Disable DLL/Driver Lockdown For example, type: **SLCmd.exe -p <admin_password> set dlldriverlockdown disable**
			Display the current status of DLL/ Driver Lockdown For example, type:

COMMAND	PARAMETER	VALUE	DESCRIPTION
			SLCmd.exe -p <admin_password> set dlldriverlockdown
set	script	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**
			Display the current status of Script Lockdown For example, type: **SLCmd.exe -p <admin_password> set script**
set	writeprotection	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**
			Display the current status of Write Protection For example, type: **SLCmd.exe -p <admin_password> set writeprotection**

COMMAND	PARAMETER	VALUE	DESCRIPTION
set	writeprotection-includes-approvedlist	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**
			Display the current status of Write Protection includes Approved List For example, type: **SLCmd.exe -p <admin_password> set writeprotection-includes-approvedlist**
set	integritymonitoring	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	VALUE	DESCRIPTION
			Display the current status of Integrity Monitoring For example, type: **`SLCmd.exe -p <admin_password> set integritymonitoring`**
`set`	`customaction`	`ignore`	Ignore blocked files or processes when Application Lockdown blocks any of the following events: • Process launch • DLL loading • Script file access
		`quarantine`	Quarantine blocked files or processes when Application Lockdown blocks any of the following events: • Process launch • DLL loading • Script file access **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

COMMAND	PARAMETER	VALUE	DESCRIPTION
			• Script file access
			Display the current setting for actions taken when Safe Lock blocks specific types of events
set	exceptionpath	enable	Enable exceptions to Application Lockdown
		disable	Disable exceptions to Application Lockdown
			Display current setting for using exceptions to Application Lockdown

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	VALUE	DESCRIPTION
set	user	enable	Enable the Restricted User account For example, type:

COMMAND	PARAMETER	VALUE	DESCRIPTION
			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**
			Display the the Restricted User account status For example, type: **SLCmd.exe -p <admin_password> set user**
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**
			Prompt the currently logged on administrator to specify a new Restricted User account password For example, type: **SLCmd.exe -p <admin_password> set userpassword**

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	VALUE	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`**
`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`**

COMMAND	PARAMETER	VALUE	DESCRIPTION
			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**

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
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	VALUE	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	VALUE	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	VALUE	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	VALUE	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.

COMMAND	PARAMETER	VALUE	DESCRIPTION
			Using the optional `-f` value forces the restore.
remove	`quarantinedfile`	<id>	Delete the specified file
show	`exceptionpath`		Display current exceptions to Application Lockdown
add	`exceptionpath`	`-e` <file_path> `-t file`	Add an exception for the specified file
		`-e` <folder_path> `-t folder`	Add an exception for the specified folder
		`-e` <folder_path> `-t folderandsub`	Add an exception for the specified folder and related subfolders
remove	`exceptionpath`	`-e` <file_path> `-t file`	Remove an exception for the specified 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 **Note** Specify the exact <folder_path> originally specified in the corresponding add command.

COMMAND	PARAMETER	VALUE	DESCRIPTION
		-e <folder_path>-t folderandsub	Remove an exception for the specified folder and related subfolders **Note** Specify the exact <folder_path> originally specified in the corresponding add command.

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
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

Parameter	Abbreviation	Use
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**
	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**

COMMAND	PARAMETER	VALUE	DESCRIPTION
	`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`** **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`** **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`** **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

COMMAND	PARAMETER	VALUE	DESCRIPTION
			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`** **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`** **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:

COMMAND	PARAMETER	VALUE	DESCRIPTION
			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: **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`.
	`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`**

COMMAND	PARAMETER	VALUE	DESCRIPTION
			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`** **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`** **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: **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

COMMAND	PARAMETER	VALUE	DESCRIPTION
			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 **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

COMMAND	PARAMETER	VALUE	DESCRIPTION
			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 **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.

COMMAND	PARAMETER	VALUE	DESCRIPTION
		-p <process_path>	Add processes run from the specified paths to the Write Protection Exception List **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 **Note** Using the optional `-r` value includes the specified registry key and related subkeys.

COMMAND	PARAMETER	VALUE	DESCRIPTION
		-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	VALUE	DESCRIPTION
set	trustedcertification	enable	Enable using Trusted Certifications
		disable	Disable using Trusted Certifications
			Display current setting for using Trusted Certifications

COMMAND	PARAMETER	VALUE	DESCRIPTION
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 Updater Commands

Configure Trusted Updaters 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
trustedupdater	tu	Manage the Predefined Trusted Updater tool process

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

TABLE 3-22. Trusted Updater Commands

COMMAND	PARAMETER	VALUE	DESCRIPTION
start	trustedupdater	[-r] <path_of_installer>	Start the Trusted Updater and add the installation packages (EXE and MSI file types) in the specified folder to 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]	Stop the Trusted Updater function **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	VALUE	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 3-47*.

Configure Predefined Trusted Updaters 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 3-23. 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 3-24. Predefined Trusted Updater Commands

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

COMMAND	PARAMETER	VALUE	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 3-47*. 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.exe`, type: **`SLCmd.exe -p <admin_password> decrypt predefinedtrustedupdater C:\Notepad.xen C:\Editors\notepad.exe`**
encrypt	`predefinedtrustedupdater`	<path_of_file> <path_of_encrypted	Encrypt a file to the specified location For example, to encrypt `C:\notepad.exe` to `C:\Editors\Notepad.xen`, type:

COMMAND	PARAMETER	VALUE	DESCRIPTION
		_output_file>	**SLCmd.exe -p <admin_password> encrypt predefinedtrustedupdater C:\Editors\notepad.exe 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 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:

COMMAND	PARAMETER	VALUE	DESCRIPTION
			SLCmd.exe -p <admin_password> remove predefinedtrustedupdater -e C:\Windows\notepad.exe
set	predefinedtrustedupdater	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: **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 3-25. 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 3-26. 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	**`SLCmd.exe -p <admin_password> add predefinedtrustedupdater -u C:\Windows\notepad.exe -t process`**

VALUE	REQUIRED / OPTIONAL	DESCRIPTION		EXAMPLE
		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	
`-p` <parent_process>	Optional	Add the full file path to the specified parent process used to invoke the file(s) specified in `-u` <folder_or_file>		**`SLCmd.exe -p <admin_password> add predefinedtrustedupdater -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 predefinedtrustedupdater -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 predefinedtrustedupdater -u C:\Windows\notepad.exe -t process -al enable`**

VALUE	REQUIRED / OPTIONAL	DESCRIPTION	EXAMPLE
`-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 predefinedtrustedupdater -u C:\Windows\notepad.exe -t process -al disable`**

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 3-27. Abbreviations and Uses

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

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

TABLE 3-28. Configuration File Commands

COMMAND	PARAMETER	VALUE	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:

COMMAND	PARAMETER	VALUE	DESCRIPTION
			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**

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 4-2* 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.
4. Encrypt the edited configuration file.
5. Import the edited configuration file.

Exporting or Importing a Configuration File

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

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

The configuration file only supports UTF-8 encoding.

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-instance"
    xsi:noNamespaceSchemaLocation="WKConfig.xsd">
    <Configuration>
        <AccountGroup>
            <Account
                ID="{24335D7C-1204-43d1-9CBB-332D688C85B6}"
                Enable="no">
                <Password/>
            </Account>
        </AccountGroup>
        <UI>
            <SystemTaskTrayIcon Enable="yes"/>
```

```
        </UI>
        <Feature>
            <ApplicationLockDown LockDownMode="2">
                <WhiteList
                RecentHistoryUnapprovedFilesLimit="50"/>
                <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>
                </TrustedUpdater>
                <DllDriverLockDown Enable="yes"/>
                <ExceptionPath Enable="no">
                    <ExceptionPathList/>
                </ExceptionPath>
                <TrustedCertification Enable="yes"/>
                <WriteProtection Enable="yes" ActionMode="1"
                ProtectApprovedList=”yes”/>
                <CustomAction ActionMode="0"/>
            </ApplicationLockDown>
            <UsbMalwareProtection Enable="yes" ActionMode="1"/>
            <DllInjectionPrevention Enable="yes"
            ActionMode="1"/>
            <ApiHookingPrevention Enable="yes" ActionMode="1"/>
            <MemoryRandomization Enable="yes"/>
            <NetworkVirusProtection Enable="yes"
            ActionMode="1"/>
            <IntegrityMonitoring Enable="yes"/>
            <Log>
                <EventLog Enable="yes">
                    <BlockedAccessLog Enable="yes"/>
                    <ApprovedAccessLog Enable="yes">
                        <TrustedUpdaterLog Enable="yes"/>
                        <DllDriverLog Enable="yes"/>
                        <ExceptionPathLog Enable="yes"/>
                        <TrustedCertLog 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>
            </EventLog>
            <DebugLog Enable="no"/>
        </Log>
    </Feature>
    <ManagedMode Enable="yes">
        <Agent>
            <Port/>
            <SslAllowBeast>1</SslAllowBeast>
        </Agent>
        <Server>
            <HostName/>
            <FastPort/>
            <SlowPort/>
            <ApiKey/>
        </Server>
        <Message>
            <Register Trigger="1"/>
            <Unregister Trigger="1"/>
            <UpdateStatus Trigger="1"/>
            <UploadBlockedEvent Trigger="1"/>
            <CheckFileHash Trigger="1"/>
            <QuickScanFile Trigger="1"/>
        </Message>
        <MessageRandomization TotalGroupNum="1"
        OwnGroupIndex="0"
```

```
                TimePeriod="0"/>
            <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"/>
        </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 4-9*. See *Account Types on page 2-15*.

Section			Description	Additional Information
	UI		Parameters to configure the display of the system tray icon	See *UI Section on page 4-10*.
	Feature		Container for the Feature section	
		ApplicationLockDown	Parameters to configure Safe Lock features and functions	See *Feature Section on page 4-10*. See *About Feature Settings on page 2-17*.
		UsbMalwareProtection		
		DllInjectionPrevention		
		ApiHookingPrevention		
		MemoryRandomization		
		NetworkVirusProtection		
		IntegrityMonitoring		
		Log	Parameters to configure individual log types	See *Log Section on page 4-20*. See *Agent Event Log Descriptions on page 7-4*.
	ManagedMode		Parameters to configure Centralized Management functions	See *ManagedMode Section on page 4-24*.
Permission			Container for the Permission section	

Section	Description	Additional Information
AccountRef	Parameters to configure the Safe Lock console controls available to the Restricted User account	See *AccountRef Section on page 4-27*. See *Account Types on page 2-15*.

AccountGroup Section

Parameters to configure the Restricted User account

See *Account Types on page 2-15*.

Table 4-2. 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

Parameter	Setting	Value	Description
			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. UI Section Parameters

Parameter	Setting	Value	Description
`Configuration`			Container for the Configuration section
`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

Feature Section

Parameters to configure Safe Lock features and functions

See *About Feature Settings on page 2-17*.

Table 4-4. Feature Section Parameters

Parameter	Setting	Value	Description
`Configuration`			Container for the Configuration section

Parameter	Setting	Value	Description
Feature			Container for the Feature section
ApplicationLockDown	LockDown Mode	1	Turn on Application Lockdown
		2	Turn off Application Lockdown
WhiteList	RecentHistoryUnapprovedFilesLimit	0 - 65535	Maximum number of entries in the Blocked Files log
ScriptLockDown	Enable	yes	Enable Script Lockdown
		no	Disable Script Lockdown
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

Parameter			Setting	Value	Description
Condition			ID	<unique_ruleset_name>	Unique name for the set of rules
	ApprovedListCheck		Enable	yes	Enable hash checks for Trusted Updaters
				no	Disable hash checks for Trusted Updaters
	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>	Updater path
			ConditionRef	<condition_ID>	Condition ID to provide a more detailed rule for the updater
DLLDriverLockdown			Enable	yes	Enable DLL/Driver Lockdown

Parameter	Setting	Value	Description
		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
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 Updater
		lockdown	File signed by this certificate is not treated as a Trusted Updater
	Hash	<SHA-1_hash_value>	SHA1-hash value of this certificate
	Label	<label>	Description of this certificate
	Subject	<subject>	Subject of this certificate

Parameter			Setting	Value	Description
			Issuer	<issuer>	Issuer of this certificate
	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
		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:

Parameter	Setting	Value	Description
			• 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
		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

Parameter			Setting	Value	Description
					• 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
		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

Parameter	Setting	Value	Description
			• HKEY_CLASSES_ROOT\test HKCR\test • HKEY_CURRENT_USER\test HKCU\test • HKEY_USERS\test HKU\test
	IncludeSubkey	yes	Include any subkeys
		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

Parameter	Setting	Value	Description
	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 • 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

PARAMETER	SETTING	VALUE	DESCRIPTION
		1	Block action by detected malware
DllInjectionPrevention	Enable	yes	Enable DLL Injection Prevention
		no	Disable DLL Injection Prevention
	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

Parameter	Setting	Value	Description
Log			Container for configuring logs See *Log Section on page 4-20*.

Log Section

Parameters to configure individual log types

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

Table 4-5. Log Configuration 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 the Safe Lock events specified in the following elements
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	Enable the Trusted Updater approved access log
		no	Disable the Trusted Updater approved access log
DLLDriverLog	Enable	yes	Enable the DLL/Driver approved access log
		no	Disable the DLL/Driver approved access log
ExceptionPathLog	Enable	yes	Enable the Application Lockdown exception path approved access log
		no	Disable the Application Lockdown exception path approved access log
TrustedCertLog	Enable	yes	Enable the Trusted Certifications approved access log
		no	Disable the Trusted Certifications approved access log
WriteProtectionLog	Enable	yes	Enable the Write Protection approved access log
		no	Disable the Write Protection approved access log
SystemEventLog	Enable	yes	Log events related to the system
		no	Do not log events related to the system
ExceptionPathLog	Enable	yes	Enable exceptions to Application Lockdown

Parameter	Setting	Value	Description
		no	Disable exceptions to Application Lockdown
WriteProtectionLog	Enable	yes	Enable the Write Protection system log
		no	Disable the Write Protection system log
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

Parameter	Setting	Value	Description
		no	Do not log file modified events
FileDeletedLog	Enable	yes	Log file and folder deleted events
		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
EventLog	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. 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)
Server			Container for configuring Safe Lock Intelligent Manager
HostName		<hostname>	Specify the host name of the Intelligent Manager server

PARAMETER		SETTING	VALUE	DESCRIPTION
	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
	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

Parameter	Setting	Value	Description
QuickScanFile	Trigger	1	Send as soon as possible after the event occurs
		2	Do not send unless requested to by Intelligent Manager
MessageRandomization **Note** Safe Lock agents repond as soon as possible to direct requests from Safe Lock Intelligent Manager.	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
HostName		<proxy_hostname>	Specify the proxy host name

Parameter	Setting	Value	Description
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 2-15*.

Table 4-7. 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 **Note** The **Password** page is not available to the Restricted User account.

Parameter	Setting	Value	Description
		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.

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

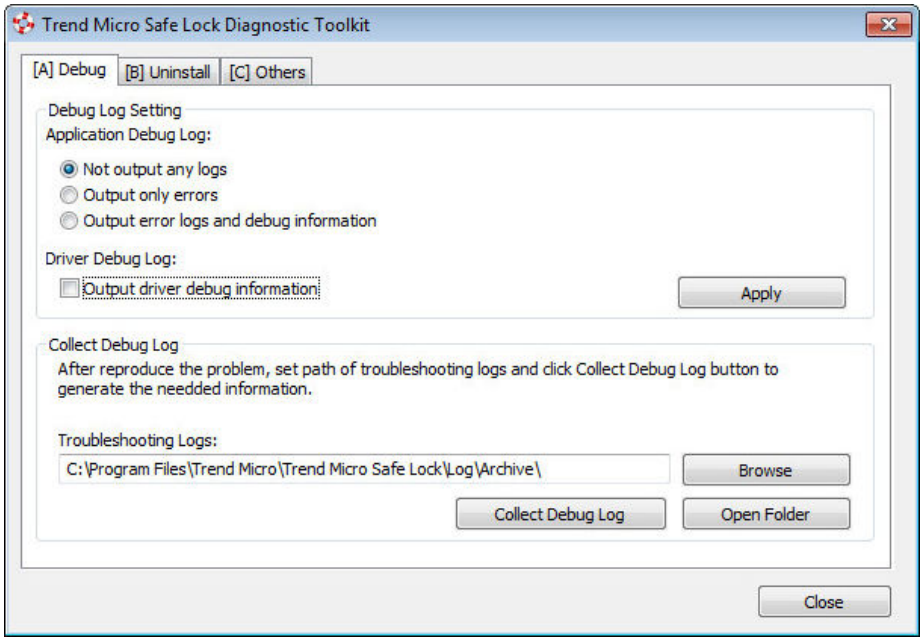


FIGURE 5-1. The Trend Micro Safe Lock Diagnostic Toolkit Debug Tab

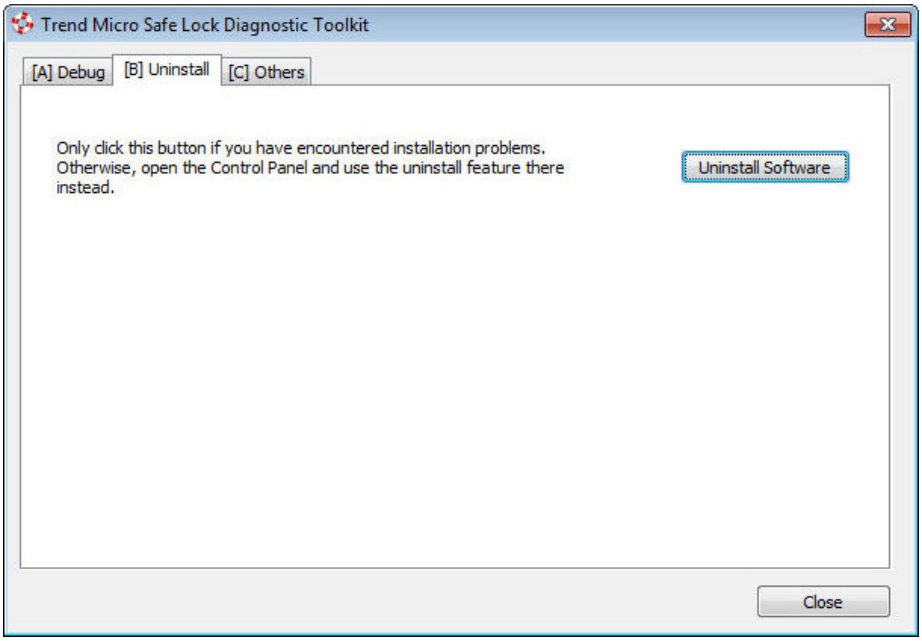


FIGURE 5-2. The Trend Micro Safe Lock Diagnostic Uninstall Tab

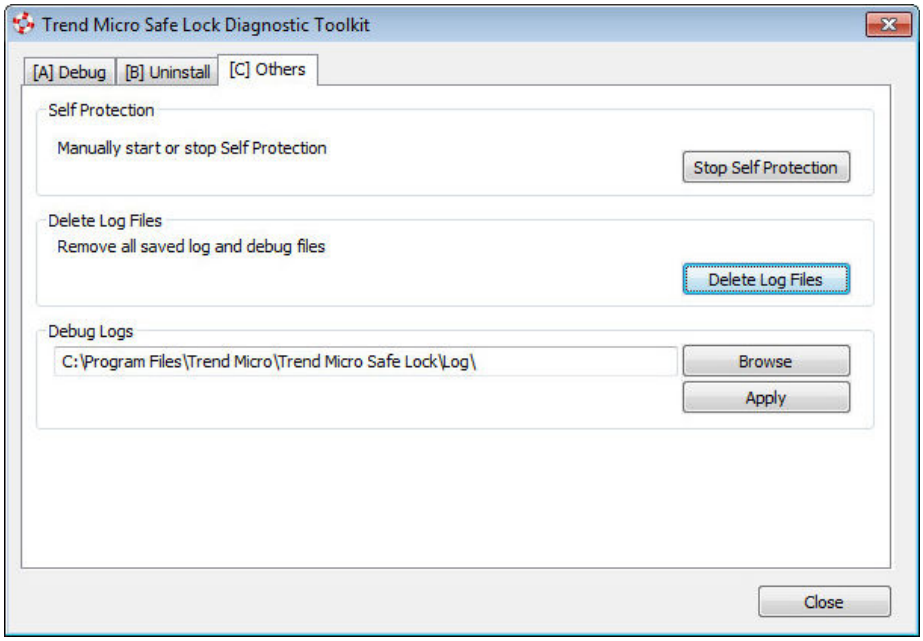


FIGURE 5-3. The Trend Micro Safe Lock Diagnostic Toolkit Others Tab

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 Safe Lock 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 \Trend Micro Safe Lock\`.

b. Provide the Safe Lockadministrator 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 \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.

Chapter 6

Technical Support

This chapter describes how to find solutions online, use the Support Portal, and contact Trend Micro.

Topics include:

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 a product or service from the appropriate drop-down list and specify any other related information.

   The **Technical Support** product page appears.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Submit a Support Case** from the left navigation and add any relevant details, or submit a support case here:

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

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

Trend Community

To get help, share experiences, ask questions, and discuss security concerns with other users, enthusiasts, and security experts, go to:

http://community.trendmicro.com/

Contacting Trend Micro

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

Address	Trend Micro, Inc. 10101 North De Anza Blvd., Cupertino, CA 95014
Phone	Toll free: +1 (800) 228-5651 (sales) Voice: +1 (408) 257-1500 (main)
Fax	+1 (408) 257-2003
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

Related information

↳ *Speeding Up the Support Call*

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 hardware connected to the endpoint
- Amount of memory and free hard disk space
- Operating system and service pack version
- Endpoint agent version

- Serial number or activation code
- Detailed description of install environment
- Exact text of any error message received

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.

Related information

↳ *TrendEdge*
↳ *Download Center*
↳ *TrendLabs*

TrendEdge

Find information about unsupported, innovative techniques, tools, and best practices for Trend Micro products and services. The TrendEdge database contains numerous documents covering a wide range of topics for Trend Micro partners, employees, and other interested parties.

See the latest information added to TrendEdge at:

http://trendedge.trendmicro.com/

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.

TrendLabs

TrendLabs℠ is a global network of research, development, and action centers committed to 24x7 threat surveillance, attack prevention, and timely and seamless solutions delivery. Serving as the backbone of the Trend Micro service infrastructure, TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services.

TrendLabs monitors the worldwide threat landscape to deliver effective security measures designed to detect, preempt, and eliminate attacks. The daily culmination of these efforts is shared with customers through frequent virus pattern file updates and scan engine refinements.

Learn more about TrendLabs at:

http://cloudsecurity.trendmicro.com/us/technology-innovation/experts/index.html#trendlabs

About Trend Micro

As a global leader in cloud security, Trend Micro develops Internet content security and threat management solutions that make the world safe for businesses and consumers to exchange digital information. With over 20 years of experience, Trend Micro provides top-ranked client, server, and cloud-based solutions that stop threats faster and protect data in physical, virtualized, and cloud environments.

As new threats and vulnerabilities emerge, Trend Micro remains committed to helping customers secure data, ensure compliance, reduce costs, and safeguard business integrity. For more information, visit:

http://www.trendmicro.com

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) requires 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 Server 2008 and Windows Server 2012) requires 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**.

TABLE 7-1. Windows Event Log Descriptions

EVENT ID	TASK CATEGORY	LEVEL	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.
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: <full_path>
1014	System	Information	Product configuration import complete: <full_path>

Event ID	Task Category	Level	Description
1015	System	Information	Product configuration exported to: <full_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.
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	Auto Trusted Update enabled.
1036	System	Information	Auto Trusted Update disabled.
1037	System	Information	DLL/Driver Lockdown enabled.

Event ID	Task Category	Level	Description
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.

EVENT ID	TASK CATEGORY	LEVEL	DESCRIPTION
1046	System	Information	Event Log settings changed. [Details] Windows Event Log: <ON|off> System Log: <on|OFF> Exception Path Log: <ON|off> Write Protection Log: <ON|off> List Log: <ON|off> Approved Access Log: <ON|off> DLL Driver Log: <on|OFF> Trusted Updater Log: <ON|off> Exception Path Log: <ON|off> Trusted Certification 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> 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> Debug Log: <on|OFF>

Event ID	Task Category	Level	Description
1047	System	Information	Trusted certificate enabled.
1048	System	Information	Trusted certificate disabled.
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: <full_path>
1056	System	Information	Removed file from Write Protection List. Path: <full_path>
1057	System	Information	Added file to Write Protection Exception List Path: <full_path> Process: <process>
1058	System	Information	Removed file from Write Protection Exception List. Path: <full_path> Process: <process>
1059	System	Information	Added folder to Write Protection List. Path: <full_path> Scope: Folder
1060	System	Information	Removed folder from Write Protection List. Path: <full_path> Scope: Folder

Event ID	Task Category	Level	Description
1061	System	Information	Added folder to Write Protection Exception List. Path: <full_path> Scope: Folder Process: <process>
1062	System	Information	Removed folder from Write Protection Exception List. Path: <full_path> Scope: Folder Process: <process>
1063	System	Information	Added registry value to Write Protection List. Registry Key: <reg_key> Registry Value Name: <reg_value>
1064	System	Information	Removed registry value from Write Protection List. Registry Key: <reg_key> Registry Value Name: <reg_value>
1065	System	Information	Added registry value to Write Protection Exception List. Registry Key: <reg_key> Registry Value Name: <reg_value> Process: <process>
1066	System	Information	Removed registry value from Write Protection Exception List. Registry Key: <reg_key> Registry Value Name: <reg_value> Process: <process>

Event ID	Task Category	Level	Description
1067	System	Information	Added registry key to Write Protection List. Registry Key: <reg_key> Scope: Registry Key
1068	System	Information	Removed registry key from Write Protection List. Registry Key: <reg_key> Scope: Registry Key
1069	System	Information	Added registry key to Write Protection Exception List. Registry Key: <reg_key> Scope: Registry Key Process: <process>
1070	System	Information	Removed registry key from Write Protection Exception List. Registry Key: <reg_key> Scope: Registry Key Process: <process>
1071	System	Information	Custom Action set to Ignore.
1072	System	Information	Custom Action set to Quarantine.
1073	System	Information	Custom Action set to Ask Intelligent Manager.
1074	System	Information	Quarantined file is restored. [Details] Original Location: <full_path> Source: <source>

Event ID	Task Category	Level	Description
1075	System	Information	Quarantined file is deleted. [Details] Original Location: <full_path> Source: <source>
1076	System	Information	Integrity Monitoring enabled.
1077	System	Information	Integrity Monitoring disabled.
1078	System	Information	Root cause analysis report failed. [Details] Access Image Path: <full_path>
1079	System	Information	Server certificate imported: <full_path>
1080	System	Information	Server certificate exported to: <full_path>
1081	System	Information	Managed mode configuration imported: <full_path>
1082	System	Information	Managed mode configuration exported to: <full_path>
1083	System	Information	Managed mode enabled.
1084	System	Information	Managed mode disabled.
1085	System	Information	When Write Protection is enabled, it includes the Write Protection List and the Approved List.
1086	System	Warning	When Write Protection is enabled, it includes the Write Protection List only.
1500	List	Information	Trusted Update started.
1501	List	Information	Trusted Update stopped.
1502	List	Information	Approved List import started: <full_path>

Event ID	Task Category	Level	Description
1503	List	Information	Approved List import complete: <full_path>
1504	List	Information	Approved List exported to: <full_path>
1505	List	Information	Added to Approved List: <full_path>
1506	List	Information	Added to Trusted Update List: <full_path>
1507	List	Information	Removed from Approved List: <full_path>
1508	List	Information	Removed from Trusted Update List: <full_path>
1509	List	Information	Approved List updated: <full_path>
1510	List	Information	Trusted Update List updated: <full_path>
1511	List	Warning	Unable to add to or update Approved List: <full_path>
1512	List	Warning	Unable to add to or update Trusted Update List: <full_path>
1513	List	Information	Added to Exception Path List. [Details] Type: <exception_path_type> Path: <exception_path>
1514	List	Information	Removed from Exception Path List. [Details] Type: <exception_path_type> Path: <exception_path>

Event ID	Task Category	Level	Description
1515	List	Information	Added to Trusted Certificate List. [Details] Label: <label> Hash: <hash_value> Type: <type> Subject: <subject> Issuer: <issuer>
1516	List	Information	Removed from Trusted Certificate List. [Details] Label: <label> Hash: <hash_value> Type: <type> Subject: <subject> Issuer: <issuer>
2000	Access Approved	Information	File access allowed: <full_path> [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode> List: <list>

Event ID	Task Category	Level	Description
2001	Access Approved	Warning	File access allowed: <full_path> [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode>
2002	Access Approved	Warning	File access allowed: <full_path> Unable to get the file path while checking the Approved List. [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode>
2003	Access Approved	Warning	File access allowed: <full_path> Unable to calculate hash while checking the Approved List. [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode>
2004	Access Approved	Warning	File access allowed: <full_path> Unable to get notifications to monitor process.
2005	Access Approved	Warning	File access allowed: <full_path> Unable to add process to non exception list.

Event ID	Task Category	Level	Description
2006	Access Approved	Information	File access allowed: <full_path> [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode>
2007	Access Approved	Warning	File access allowed: <full_path> An error occurred while checking the Exception Path List. [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode>
2008	Access Approved	Warning	File access allowed: <full_path> An error occurred while checking the Trusted Certificate List. [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode>

Event ID	Task Category	Level	Description
2011	Access Approved	Information	Trusted registry value access allowed. Registry Key: <reg_key> Registry Value Name: <reg_value> [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode>
2012	Access Approved	Information	Trusted registry key access allowed. Registry Key: <reg_key> [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode>
2013	Access Approved	Information	Change of File/Folder allowed by Exception List: <full_path> [Details] Access Image Path: Access User: <user_name> Mode: <mode>

Event ID	Task Category	Level	Description
2015	Access Approved	Information	Change of Registry Value allowed by Exception List. Registry Key: <reg_key> Registry Value Name: <reg_value> [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode>
2016	Access Approved	Information	Change of Registry Key allowed by Exception List. Registry Key: <reg_key> [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode>
2017	Access Approved	Warning	Change of File/Folder allowed: <full_path> [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode>

Event ID	Task Category	Level	Description
2019	Access Approved	Warning	Change of Registry Value allowed. Registry Key: <reg_key> Registry Value Name: <reg_value> [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode>
2020	Access Approved	Warning	Change of Registry Key allowed. Registry Key: <reg_key> [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode>
2503	Access Blocked	Warning	Change of File/Folder blocked: <full_path> [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode>

Event ID	Task Category	Level	Description
2505	Access Blocked	Warning	Change of Registry Value blocked. Registry Key: <reg_key> Registry Value Name: <reg_value> [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode>
2506	Access Blocked	Warning	Change of Registry Key blocked. Registry Key: <reg_key> [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode>
2507	Access Blocked	Information	Specified action is taken: <full_path> [Details] Action: <action> Source: <source>
2508	Access Blocked	Warning	Failed to take specified action: <full_path> [Details] Action: <action> Source: <source>

Event ID	Task Category	Level	Description
2509	Access Blocked	Warning	File access blocked: <full_path> [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode> Reason: Not in Approved List
2510	Access Blocked	Warning	File access blocked: <full_path> [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode> Reason: Hash does not match expected value
2511	Access Blocked	Information	Change of File/Folder blocked: <full_path> [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode>
3000	USB Malware Protection	Warning	Device access allowed: <full_path> [Details] Access Image Path: <full_path> Access User: <user_name> Device Type: <type>

Event ID	Task Category	Level	Description
3001	USB Malware Protection	Warning	Device access blocked: <full_path> [Details] Access Image Path: <full_path> Access User: <user_name> 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: <port>
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: <port>
4002	Process Protection Event	Warning	API Hooking allowed: <full_path> [Details] Threat Image Path: <full_path> Threat User: <user_name>

Event ID	Task Category	Level	Description
4003	Process Protection Event	Warning	API Hooking blocked: <full_path> [Details] Threat Image Path: <full_path> Threat User: <user_name>
4004	Process Protection Event	Warning	DLL Injection allowed: <full_path> [Details] Threat Image Path: <full_path> Threat User: <user_name>
4005	Process Protection Event	Warning	DLL Injection blocked: <full_path> [Details] Threat Image Path: <full_path> Threat User: <user_name>
4500	Changes in System	Information	File/Folder created: <full_path> [Details] Access Image Path: <full_path> Access Process ID: <proc_id> Access User: <user_name>
4501	Changes in System	Information	File modified: <full_path> [Details] Access Image Path: <full_path> Access Process ID: <proc_id> Access User: <user_name>

Event ID	Task Category	Level	Description
4502	Changes in System	Information	File/Folder deleted: <full_path> [Details] Access Image Path: <full_path> Access Process ID: <proc_id> Access User: <user_name>
4503	Changes in System	Information	File/Folder renamed: <full_path> New path: <full_path> [Details] Access Image Path: <full_path> Access Process ID: <proc_id> Access User: <user_name>
4504	Changes in System	Information	Registry Value modified. Registry Key: <reg_key> Registry Value Name: <reg_value> Registry Value Type: <reg_value_type> [Details] Access Image Path: <full_path> Access Process ID: <proc_id> Access User: <user_name>

Event ID	Task Category	Level	Description
4505	Changes in System	Information	Registry Value deleted. Registry Key: <reg_key> Registry Value Name: <reg_value> [Details] Access Image Path: <full_path> Access Process ID: <proc_id> Access User: <user_name>
4506	Changes in System	Information	Registry Key created. Registry Key: <reg_key> [Details] Access Image Path: <full_path> Access Process ID: <proc_id> Access User: <user_name>
4507	Changes in System	Information	Registry Key deleted. Registry Key: <reg_key> [Details] Access Image Path: <full_path> Access Process ID: <proc_id> Access User: <user_name>

Event ID	Task Category	Level	Description
4508	Changes in System	Information	Registry Key renamed. Registry Key: <reg_key> New Registry Key: <reg_key> [Details] Access Image Path: <full_path> Access Process ID: <proc_id> Access User: <user_name>

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.

Code	Description
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.
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."

Code	Description
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.
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)

Code	Description
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

10101 North De Anza Blvd. Cupertino, CA., 95014, USA

Tel:+1(408)257-1500/1-800 228-5651 Fax:+1(408)257-2003 info@trendmicro.com

www.trendmicro.com

Item Code: SLEM26722/141016