Trend Micro Safe Lock™ Intelligent Manager

Administrator's Guide

A powerful lockdown solution for fixed-function computers

TXOne Edition

Endpoint Security

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

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

Document Part No.: SLEM08835/191007

Release Date: October 2019

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

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

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

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

Evaluate this documentation on the following site:

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

Privacy and Personal Data Collection Disclosure

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

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

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

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

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

Table of Contents

Preface

Chapter 1: Introduction

Chapter 2: Managing Safe Lock Agents

Chapter 3: Monitoring Safe Lock

Chapter 4: Configuring Administration Settings

Chapter 5: Using the Agent Console

Chapter 6: Using the Agent Command Line Interface (CLI)

Chapter 7: Managing Agents Remotely

Chapter 12: Technical Support

Chapter 13: Appendix: Reference

Index

Preface

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

Topics in this chapter include:

About the Documentation

Trend Micro Safe Lock Intelligent Manager documentation includes the following:

TABLE 1. Trend Micro Safe Lock Intelligent Manager Documentation

DOCUMENTATION	DESCRIPTION
Installation Guide	A PDF document that discusses requirements and procedures for installing Safe Lock Intelligent Manager.
Administrator's Guide	A PDF document that discusses getting started information and Safe Lock Intelligent Manager 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 Intelligent Manager documentation is intended for administrators responsible for Safe Lock Intelligent Manager management, including agent installation. These users are expected to have advanced networking and server management knowledge.

Document Conventions

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

TABLE 2. Document Conventions

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

Convention	Description
 Tip	Recommendations or suggestions
 Important	Information regarding required or default configuration settings and product limitations
 WARNING!	Critical actions and configuration options

Terminology

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

Table 3. Safe Lock Intelligent Manager Terminology

Terminology	Description
Server	The Safe Lock Intelligent Manager server program
Server endpoint	The host where the Safe Lock Intelligent Manager server is installed
Agents	The hosts running the Safe Lock program
NAT agents	The agents that are built under the routers with the Network Address Translation (NAT) function enabled
Managed agents Managed endpoints	The hosts running the Safe Lock program that are known to the Safe Lock Intelligent Manager server program
Target endpoints	The hosts where the Safe Lock Intelligent Manager managed agents will be installed

TERMINOLOGY	DESCRIPTION
Administrator (or Safe Lock Intelligent Manager administrator)	The person managing the Safe Lock Intelligent Manager server
Web console	The user interface for configuring and managing Safe Lock Intelligent Manager settings and managed agents
CLI	Command line interface
License activation	Includes the type of Safe Lock Intelligent Manager server installation and the allowed period of usage that you can use the application
Agent installation folder	The folder on the host that contains the Safe Lock agent files. If you accept the default settings during installation, you will find the installation folder at the following location: `"c:\Program Files\Trend Micro\Safe Lock"`
Server installation folder	The folder on the host that contains the Safe Lock Intelligent Manager server files. If you accept the default settings during installation, you will find the installation folder at the following location: `"c:\Program Files\Trend Micro\Safe Lock Intelligent Manager"`

Chapter 1

Introduction

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

Topics in this chapter include:

About Trend Micro™ Safe Lock Intelligent Manager™

Trend Micro™ Safe Lock Intelligent Manager™ provides centralized monitoring and management of Safe Lock agent deployment, status, and events. For example, administrators can remotely deploy agents, create initial agent Approved Lists, and change agent Application Lockdown states. Additionally, Safe Lock Intelligent Manager performs malware scans and administrators can view root cause information on files blocked from running by Safe Lock agents, reducing the time and effort needed to verify events and allowing quick responses to incidents.

What's New

Trend Micro Safe Lock Intelligent Manager TXOne Edition includes the following new features and enhancements:

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

FEATURE	DESCRIPTION
Agent Management enhancements	Safe Lock Intelligent Manager provides the the following new agent commands in this release: • **Configure Maintainance Mode**: You can define a time period when all file executions are allowed to perform patch updates on endpoints. • **Add Trusted USB Device**: When device control is enabled, you can configure trusted USB storage devices to allow USB device access on endpoints.
Agent transfer	A new command is provided on the Safe Lock Intelligent Manager server to allow you to transfer agents to a new server.

Server Features and Benefits

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

TABLE 1-2. Features and Benefits

FEATURE	BENEFIT
Dashboard	The web console dashboard provides summarized information about monitored Safe Lock agents. Administrators can check deployed Safe Lock agent status easily, and can generate security reports related to Safe Lock agent activity for specified periods.
Quick Scan	Trend Micro Intelligent Manager provides malware scans of files blocked by application protection and sets actions for the affected files, such as delete, quarantine, or add to Approved List.
Centralized Agent Management	Trend Micro Intelligent Manager allows administrators to peform the following tasks: • Monitor Safe Lock agent status • Examine connection status • View configurations • Collect agent logs on-demand or by policy • Turn agent Application Lockdown on or off • Enable or disable agent Device Control • Configure agent Maintenance Mode settings • Update agent components • Initialize the Approved List • Deploy agent patches • Add trusted files and USB devices

FEATURE	BENEFIT
Centralized Event Management	On endpoints protected by Safe Lock agents, administrators can monitor events and status and respond when files are blocked from running. Safe Lock Intelligent Manager provides event management features that let administrators know about blocked file events quickly and allows them to manage these events. For example, events can be marked open or closed for tracking, and the detailed event information needed to resolve events can be collected quickly and easily.
Root Cause Information Analysis	When blocked file events happen, administrators can determine if they are the result of a significant incident or not. Safe Lock Intelligent Manager provides malware scanning features and root cause information and diagrams to help administrators investigate blocked files quickly. For example, administrators can check if a blocked file is required to launch a mission-critical program, or if the blocked file is detected as malware. Administrators can also learn where blocked files are run from and what process launched them.
Server Event Auditing	Operations performed by Safe Lock Intelligent Manager web console accounts are logged. Safe Lock Intelligent Manager records an operating log for each account, tracking who logs on, who deletes event logs, and more.

Safe Lock Intelligent Manager Requirements

Important

- Trend Micro Safe Lock Intelligent Manager has specific requirements that vary based on other software running on the server endpoint.
- See the latest Safe Lock Intelligent Manager readme file for the most up-to-date list of supported operating systems.

TABLE 1-3. Required Software for Safe Lock Intelligent Manager

REQUIRED SOFTWARE	SPECIFICATIONS

Operating systems - Windows clients	• Windows 7 No-SP/SP1 (Enterprise/Ultimate) (32-bit and 64-bit)
	• Windows 8 No-SP (Professional/Enterprise) (32-bit and 64-bit)
	• Windows 8.1 No-SP (Professional/Enterprise) (32-bit and 64-bit)
	• Windows 10 (Enterprise/IoT Enterprise) (32-bit and 64-bit)
	  • Anniversary Update (Redstone 1)
	  • Creators Update (Redstone 2)

Operating systems - Windows server	• Windows Server 2008 SP1/SP2 (Standard/Enterprise/Storage) (32-bit and 64-bit) • Windows Server 2008 R2 No-SP/SP1 (Standard/Enterprise/ Storage) (64-bit) • Windows Server 2012 No-SP (Foundation/Essentials/Standard/ Datacenter) (64-bit) • Windows Server 2012 R2 No-SP (Foundation/Essentials/Standard/ Datacenter) (64-bit) • Windows Server 2012 R2 for Embedded Systems No-SP (64-bit) • Windows Server 2016 (Standard) (64-bit) • Windows Storage Server 2016

Required Software	Specifications
Web browser (for Safe Lock Intelligent Manager web console access)	• Microsoft Internet Explorer 9.0, 10.0, 11.0 (32/64bit) • Microsoft Edge • The latest version of Google Chrome / Chrome Portable • Mozilla Firefox 6 or later **Note** • Older versions of Internet Explorer are unsupported for security enhancement. • When accessed using iOS systems, Safe Lock Intelligent Manager does not support any export functions via the web console.

Table 1-4. Required Hardware for Safe Lock Intelligent Manager (without Safe Lock agent)

Required Hardware	Specification
RAM	• 2 GB minimum • 4 GB or more recommended
Processor	• 1 CPU core minimum • 1 CPU core or more recommended
Available disk space	• 10 GB minimum • 20 GB or more recommended

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

Required Hardware	Specification
RAM	• 2 GB minimum • 4 GB or more recommended

Required Hardware	Specification
Processor	• 1 CPU core minimum • 2 CPU cores or more recommended
Available disk space	• 10 GB minimum • 20 GB or more recommended

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

Required Hardware	Specification
RAM	• 4 GB minimum • 8 GB or more recommended
Processor	• 1 CPU core minimum • 2 CPU cores or more recommended
Available disk space	• 30 GB minimum • 50 GB or more recommended

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

Required Hardware	Specification
RAM	• 32 GB or more required
Processor	• 2 CPU cores minimum • 4 CPU cores or more recommended
Available disk space	• 1 TB minimum • 2 TB or more recommended

Server Accounts Overview

Trend Micro Safe Lock Intelligent Manager features web console accounts with different privileges and limitations. Use these accounts to configure Safe Lock Intelligent Manager and to monitor or manage Safe Lock agents.

The following table outlines typical Safe Lock Intelligent Manager tasks and the account privileges required to perform them.

	TASK	ACCOUNT PRIVILEGE REQUIRED
1	Add Safe Lock Intelligent Manager accounts	• Admin
2	Use remote deployment tools (`SLrst.exe`) to centrally deploy agents from the server	• N/A **Note** Using the `SLrst.exe` tool does not require specific account privileges, but does require the Safe Lock agent password to deploy tasks.
3	Use the Safe Lock Intelligent Manager console and remote deployment tools (`SLtasks.exe`) to manage the Approved List and Write Protection List on Safe Lock agents	• Admin • Full Control
4	Monitor Server Event logs	• Admin • Full Control • Manage Storage Device Control only • Manage Application Lockdown only

	TASK	ACCOUNT PRIVILEGE REQUIRED
5	Monitor Agent Event logs	• Admin • Full Control • Manage Storage Device Control only • Manage Application Lockdown only • Read Only
6	Download Trend Micro Safe Lock agent installer image	• Admin • Full Control • Manage Storage Device Control only • Manage Application Lockdown only • Read Only
7	Change the administrator password remotely	• Admin
8	Update Safe Lock Intelligent Manager license information	• Admin • Full Control
9	Deploy agent patch	• Admin • Full Control
10	Add trusted files	• Admin • Full Control
11	Manage application lockdown	• Admin • Full Control • Manage Application Lockdown Only

	TASK	ACCOUNT PRIVILEGE REQUIRED
12	Manage storage device control	• Admin • Full Control • Manage Storage Device Control only
13	Check connection	• Admin • Full Control • Manage Storage Device Control only • Manage Application Lockdown only • Read Only
14	Add trusted USB devices	• Admin • Full Control
15	Configure Maitnenance Mode	• Admin • Full Control
16	Update agent components	• Admin • Full Control
17	Agent transfer	• Admin • Full Control

About Trend Micro Safe Lock

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

What's New

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

TABLE 1-8. What's New in Trend Micro Safe Lock TXOne Edition

FEATURE	DESCRIPTION
New prescan parameters for agent installation	You can specify the prescan parameters (`FORCE_PRESCAN` and `PRESCANCLEANUP`) in the setup file for Windows installer to perform mandatory endpoint scanning before agent installation.
Maintenance Mode	To perform updates on endpoints, you can configure Maintenance Mode settings to define a period when Safe Lock allows all file executions and adds all files that are created, executed, or modified to the Approved List.
Trusted USB devices	When device control is enabled, you can configure trusted USB storage devices to allow USB device access on endpoints.

Agent Features and Benefits

Trend Micro Safe Lock includes the following features and benefits.

Application Lockdown

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

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

Exploit Prevention

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

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

Approved List Management

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

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

Small Footprint

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

Role Based Administration

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

Graphical and Command Line Interfaces

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

Trend Micro Portable Security Compatible

Out-of-the-box compatibility with Trend Micro Portable Security ensures straightforward removal of any threats that do get on to the endpoint, without the need to update the Approved List or unlock the endpoint.

Safe Lock Requirements

This section introduces Safe Lock system requirements and upgrade limitations.

Hardware Requirements

Trend Micro Safe Lock does not have specific hardware requirements beyond those specified by the operating system, with the following exceptions:

TABLE 1-9. Required Hardware for Safe Lock

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

Important

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

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

Operating Systems

Important

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

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

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

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

Note

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

Windows clients:

- Windows 2000 SP4 (32-bit)

Note

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

To support these features, install Filter Manager:

- For Windows 2000 Service Pack 4, apply the update KB891861 from the Microsoft Update Catalog website.
- For Windows XP SP1, upgrade to Windows XP SP2.

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

Note

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

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

  - Anniversary Update (Redstone 1)

  - Creators Update (Redstone 2)

  - Fall Creators Update (Redstone 3)

- April 2018 Update (Redstone 4)

- October 2018 Update (Redstone 5)

Note

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

Windows Server:

- Windows 2000 Server SP4* (32-bit)

Note

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

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

Note

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

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

Note

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

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

Windows Embedded Standard:

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

Note

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

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

Windows Embedded POSReady:

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

Windows Embedded Enterprise:

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

Note

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

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

Windows Embedded Server:

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

Note

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

- Windows Embedded Server 2003 R2 (32-bit)

Note

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

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

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

Windows Storage Server

- Windows Storage Server 2016

Agent Upgrade Preparation

Note

The TXOne Edition installation package does not support Safe Lock agent upgrade from previous versions to TXOne Edition. You must install a fresh copy of the Safe Lock TXOne Edition agent on endpoints.

WARNING!

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

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

TABLE 1-10. Upgrade Actions Required by Installation Method and Installed Agent Version

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

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

Supported Methods for Updating Safe Lock Agents

Safe Lock agents can be updated using the local or remote methods .

Note

The TXOne Edition installation package does not support Safe Lock agent upgrade from previous versions to TXOne Edition. You must install a fresh copy of the Safe Lock TXOne Edition agent on endpoints.

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:

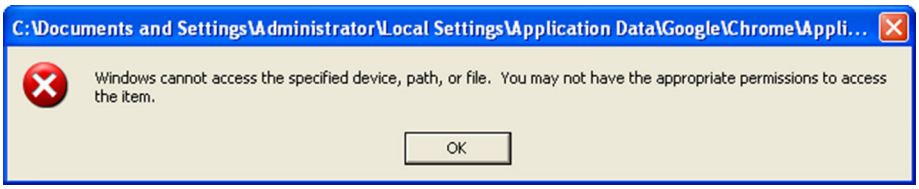


FIGURE 1-1. Trend Micro Safe Lock blocking message

Chapter 2

Managing Safe Lock Agents

This chapter introduces the web console screen for agent management.

Topics in this chapter include:

About the Agent Management Screen

To display the **Agent Management** screen, go to **Agents** in the navigation at the top of the web console. This screen displays a list of agents managed by Safe Lock Intelligent Manager and allows you to perform configuration tasks.

For more information, see:

- *Managing the Agent Tree on page 2-2*
- *Configuring Agent Settings on page 2-8*

Managing the Agent Tree

Safe Lock Intelligent Manager allows you to organize the agent tree and manage Safe Lock agent information.

TABLE 2-1. Agent Tree Management Tasks

TASK	DETAILS
Search for agents/ endpoints	For more information, see *Searching for Agents on page 2-3*.
Create agent groups	For more information, see *Grouping Agents on page 2-4*.
Remove agent groups	For more information, see *Removing Agents and Groups on page 2-4*.
View individual agent information	For more information, see *Checking Agent Statuses and Settings on page 2-5*.
Move agents or groups	Select one or more agents or groups and click **Move**.
Edit tags	Edit tags to help you identify and search for agents. For more information, see *Editing Tags on page 2-7*.

TASK	DETAILS
Export agent settings and summary in a CSV file	Select one or more agents and click **Export**.

Searching for Agents

Procedure

1. Go to **Agents** in the navigation at the top of the web console.

   The **Agent Management** screen appears.

2. Search for specific endpoints by selecting criteria from the drop-down list and specifying additional search criteria as required.

Tip

Safe Lock Intelligent Manager supports partial string matching.

OPTION	DESCRIPTION
Endpoint	Type the full endpoint host name to locate the specific endpoint.
Tags	Type the tag name.
IP Address	Type the IPv4 address.
IP Range	Type the IPv4 address.
Operating System	Select an operating system.
Application Lockdown State	Select the Application Lockdown state: **Application Lockdown On** or **Application Lockdown Off**.
Last Connection	Select from the default time ranges or **Custom** and specify your own range.

3. Click **Search** (if required).

   Safe Lock Intelligent Manager displays all hosts that match the search criteria.

Grouping Agents

Group agents according to location, type, or purpose to help you manage multiple agents.

Procedure

1. Go to **Agents** in the navigation at the top of the web console.

   The **Agent Management** screen appears.

2. From the directory on the left, click the group folder where you want to add a sub group, and click **Add Group**.

   Note

   - The group name must be within 64 characters.
   - You can establish up to 9 layers of subfolders to the Group directory, with up to 100 folders at each group layer.

3. Click **All Agents** from the directory, select agents from the table, and click **Move**.

   Tip

   Alternatively drag-and-drop agents and groups to another group in the directory.

Removing Agents and Groups

Remove groups, ungroup agents, or unregister agents from the Safe Lock Intelligent Manager server.

Agents unregister from Safe Lock Intelligent Manager during uninstallation. However, if you are unable to uninstall an agent before removing it from the environment, the agent

may continue to appear on the **Agent Management** screen. To remove the endpoints that Safe Lock Intelligent Manager no longer manages from the list of monitored agents, use the **Remove** feature to "unregister" the agents.

Note

Removing an agent from the list of monitored agents does not delete any preexisting agent event logs.

Procedure

1. Go to **Agents** in the navigation at the top of the web console.

   The **Agent Management** screen appears.

2. Select the agents and groups in the list that you want to remove, ungroup, or unregister.

3. Click **Remove**.

4. Confirm that you want to remove, ungroup, or unregister the selected items.

   Safe Lock Intelligent Manager removes the agents from the list.

Checking Agent Statuses and Settings

You can look up the following information of a managed endpoint from the **Agent Management** screen.

- Endpoint information: This includes the IP address, operating system, and tags.
- Agent summary: This includes summary information such as the last update time of the Approved List, NAT frequency, last NAT connection time, license status, license expiration date, agent version, the last agent upgrade time, and Maintenance Mode information.
- Agent settings: This includes the current agent settings and the date and time for the last change.

- Pending commands: This is a list of commands to be deployed to NAT agents upon their next connection with the Intelligent Manager. For more information on configuring the connection frequency, see *Customizing Installation Parameters on page 8-17*.

Procedure

1. Go to **Agents** in the navigation at the top of the web console.

   The **Agent Management** screen appears.

2. Click a target endpoint.

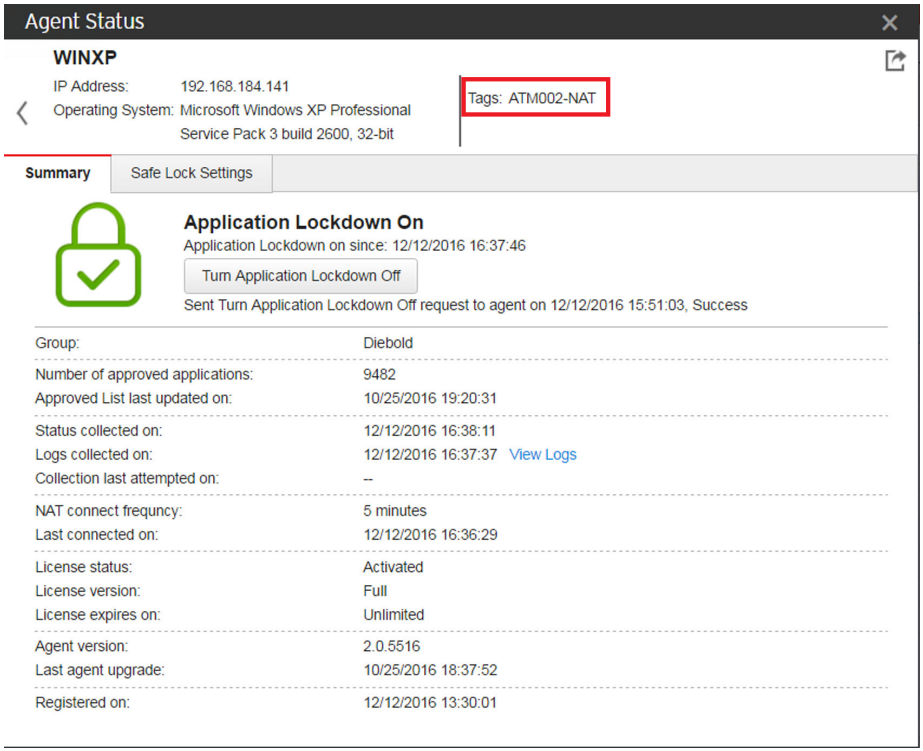
   The **Agent Status** screen appears.

   Note

   You can use the **Export** function to export and download the endpoint information to a comma-separated value (`.csv`) file.

Editing Tags

You can edit tags to help you identify and search for agents.



To edit tags, follow the steps below.

Procedure

1. Go to **Agents** in the navigation at the top of the web console.

   The **Agent Management** screen appears.

2. Select one or more agents.

3. Click **Edit Tags**.

4. Type or modify the agent tags.

Tip

Safe Lock Intelligent Manager does not use a delimiter for tags.

5. Click **OK**.

Configuring Agent Settings

You can use the **Send Command** menu located on the **Agent Management** screen to control agent configuration settings.

TABLE 2-2. Safe Lock Agent Commands

TASK	DETAILS
Configure Application Lockdown	For more information, see *Remotely Changing Application Lockdown Status on page 2-9*.
Configure Device Control	Allow or block storage devices (CD/DVD drives, floppy disks, and network drives) from accessing the managed endpoint Select one or more endpoints and click **Send Command** > **Configure Device Control**.
Configure Maintenance Mode	Configure Maintenance Mode settings to enable patch updates on endpoints without blocking new file operations. For more information, see *Configuring Maintenance Mode Settings on page 2-10*.
Add Trusted USB Device	Configure agents to allow access of trusted USB devices on endpoints based on the device information. For more information, see *Remotely Adding Trusted USB Devices on page 2-14*.

TASK	DETAILS
Add Trusted Files	Configure agents to allow all files and installers added to the list to run based on hash values For more information, see *Remotely Adding Trusted Applications and Files on page 2-12*.
Update Approved List	Update the Approved List on selected agents by performing an inventory scan For more information, see *Updating the Approved List on Safe Lock Agents on page 2-15*.
Collect event logs	For more information, see *Collecting Event Logs on page 2-17*.
Check Connection	Check the connection status of selected Safe Lock Agents For more information, see *Checking Agent Connections on page 2-17*.
Export Settings	Export the Approved List or configuration settings for selected agents For more information, see *Remotely Exporting Agent Settings on page 2-18*.
Import Settings	Import the Approved List or configuration settings for selected agents For more information, see *Remotely Importing Agent Settings on page 2-19*.
Deploy Agent Patch	Upgrade selected agents by uploading a patch file. For more information, see *Remotely Deploying Patches to Safe Lock Agents on page 2-21*.

Remotely Changing Application Lockdown Status

Note

Safe Lock agent administrators can also change the Application Lockdown status from the Safe Lock agent console.

Procedure

1. Go to **Agents** in the navigation at the top of the web console.
2. For a single agent, click the endpoint name to display agent status details, and then click the button to change the Application Lockdown status.
   - **Turn Application Lockdown On**
   - **Turn Application Lockdown Off**
3. For multiple agents and groups, select these items from the **Agent Management** table, click **Send Command**, select **Configure Application Lockdown**, and click the button to change the Application Lockdown status.
   - **Turn On**
   - **Turn Off**

Configuring Maintenance Mode Settings

To perform updates on endpoints, you can configure Maintenance Mode settings to define a period when Safe Lock allows all file executions and adds all files that are created, executed, or modified to the Approved List.

For added security, you can enable file scanning and select the scan action after the maintenance period.

Important

Before using Maintenance Mode, apply the required updates on the following supported platforms:

- For Windows 2000 Service Pack 4, apply the update KB891861 from the Microsoft Update Catalog website.
- For Windows XP SP1, upgrade to Windows XP SP2.

Note

- Before starting Maintenance Mode, perform an agent update on endpoints.
- To reduce risk of infection, run only applications from trusted sources on endpoints during the maintenance period.
- Agents start one scheduled maintenance period at a time. If you configure a new maintenance period, the system overwrites existing maintenance schedule that has not started yet.
- When the agent is about to leave Maintenance Mode, restarting the agent endpoint prevents Safe Lock from adding files in the queue to the Approved List.
- During the maintenance period, you cannot perform agent patch updates on endpoints.
- When Maintenance Mode is enabled, Safe Lock does not support Windows updates that require restarting an endpoint during the maintenance period.
- To run an installer that deploys files to a network folder during the maintenance period, Safe Lock must have access permission to the network folder.

Procedure

1. Go to **Agents** in the navigation at the top of the web console.

   The **Agent Management** screen appears.

2. Select one or more agents and groups.

3. Click **Send Command** and select **Configure Maintenance Mode**.

   The **Configure Maintenance Mode** screen appears.

4. Select **Enable** and configure the settings.

   Select **Disable** to stop Maintenance Mode or cancel scheduled maintenance period on endpoints.

5. Under **Schedule**, specify the duration of the maintenance period.

6. Select **Scan endpoints when Maintenance Mode stops** and a scan action to scan endpoints for threats when the maintenance period is over.

Note

Safe Lock scans files that are created, executed, or modified on endpoints during the maintenance period.

7. Click **Deploy**.

   A confirmation screen appears.

8. Click **Yes** to deploy the settings to the selected agents or groups.

Remotely Adding Trusted Applications and Files

Remotely allow applications and files to run on managed endpoints using hash values.

Procedure

1. Go to **Agents** in the navigation at the top of the web console.

   The **Agent Management** screen appears.

2. Select one or more agents and groups.

3. Click **Send Command** and select **Add Trusted Files**.

   The **Add Trusted Files** screen appears.

4. Click **Download File Hash Generator** to download the tool for calculating hash values.

   For detailed steps, see *Calculating the Hash Values on page 2-13*.

5. Click **Add** to add a single hash value or click **Import** to add a batch of hash values.

6. To allow files created or modified by trusted installation packages to be automatically added to the Approved List, select **application installers** in the **Installer** column.

Note

Safe Lock Intelligent Manager supports the batch import/export of `.txt` files containing lists of trusted hash values where the installer flag has been marked.

However, the import/export process automatically converts any `tab` character in the **Notes** field (as displayed on the trusted hash deployment window) to a `space` character.

Calculating the Hash Values

Use File Hash Generator to calculate hash values. To download this tool, see *Remotely Adding Trusted Applications and Files on page 2-12*.

Procedure

1. Execute WKFileHashGen.exe from the downloaded folder.

   The Trend Micro File Hash Generator screen appears.

2. Use any of the following methods to select files and calculate hash values:

   Note

   - To ensure that all necessary files are calculated for hash values, Trend Micro recommends adding the root folder of the target application to the File Hash Generator for calculation.
   - The **Add Folder** button will only calculate installer files, script files, and files in the Portable Executable format.

   - Drag-and-drop folders or files to the File Hash Generator screen.
   - Click the drop-down button and click **Add Files** to select files.
   - Click the drop-down button and click **Add Folder** to add all the files in the selected folder.

   Hash values appear in the File Hash (SHA-1) column.

3. For a single file, right-click the item and select **Copy hash**. For multiple files, click **Export All** to generate a list of hash values.

Remotely Adding Trusted USB Devices

You can specify USB storage devices that are allowed to access managed endpoints based on the device information.

Procedure

1. Go to **Agents** in the navigation at the top of the web console.

   The **Agent Management** screen appears.

2. Select one or more agents and groups.

3. Click **Send Command** and select **Add Trusted USB Device**.

   The **Add Trusted USB Device** screen appears.

4. Specify at least one of the following information for the trusted USB device:

   - Vendor ID
   - Product ID
   - Serial number

   Note

   For information on obtaining the device information, see *Getting Device Information on page 2-15*.

5. Click **Deploy** to deploy the setting to the selected agents or groups.

Note

- To view the list of trusted USB devices on an endpoint, export the agent settings.
- To manually configure the trusted USB device list on an endpoint, do one of the following:
  - Export the agent settings, make changes, and then import the updated settings file
  - Use the `SLCmd` command

Getting Device Information

You can use one of the following methods to get the information of a connected device to a endpoint:

- Open the Device Manager on the agent endpoint
- Use the `SLCmd.exe show USBinfo` command on the agent endpoint

  For more information, see *Trusted USB Device Commands on page 6-58*.
- Go to the **Agent Events** screen for agent events on the Intelligent Manager web consolde and click **View Event Details** for removable devices with event ID 5001

Updating the Approved List on Safe Lock Agents

You may want to periodically update the Approved List on Safe Lock Agents after installing new applications that you want to run during a Lockdown situation. Updating the Approved List performs an inventory scan on selected agents and adds any new applications found on the agent to the global Approved List.

Procedure

1. Go to **Agents** in the navigation at the top of the web console.

   The **Agent Management** screen appears.

2. Select one or more agents and groups.
3. Click **Send Command** and select **Update Approved List**.

   The **Update Approved List** dialog appears.
4. Click **Update** to begin inventorying the selected agents.

Note

Do not restart or turn off the endpoint during the update. The update process may take more than 30 minutes to complete.

You can monitor the status of the Approved List update using the **Details** screen. The icons on the **Approved List** column display the current progress status.

Remotely Updating Agent Components

You can start the agent component update process on selected endpoints from Safe Lock Intelligent Manager. The agents download the latest component updates from the Trend Micro ActiveUpdate server.

Update agent components regularly to protect endpoints from the latest security risks.

Procedure

1. Go to **Agents** in the navigation at the top of the web console.

   The **Agent Management** screen appears.
2. Select one or more agents and groups.
3. Click **Send Command** and select **Update Agent Components**.
4. Click **Yes**.

The system sends the componant update command to the selected agents. The update process may take some time. You can check the status on the **Agent Events** screen.

Collecting Event Logs

Logs contain information about agent activity. Collecting event logs updates the Safe Lock Intelligent Manager database with the latest information from the selected agents.

Procedure

1. Go to **Agents** in the navigation at the top of the web console.

   The **Agent Management** screen appears.

2. Select one or more agents.

3. Click **Send Command** and select **Collect Event Logs**.

   Safe Lock Intelligent Manager updates the date and time displayed in the **Last Connection** column after each Safe Lock agent successfully sends logs and status to Safe Lock Intelligent Manager.

Checking Agent Connections

Procedure

1. Go to **Agents** in the navigation at the top of the web console.

   The **Agent Management** screen appears.

2. Select one or more agents and groups.

3. Click **Send Command** and select **Check Connection**.

   Safe Lock Intelligent Manager automatically attempts to contact the selected Safe Lock Agents.

Important

Intelligent Manager is unable to check the connection to NAT agents due to a lack of direct communication.

After the connection check completes, a list of all Safe Lock Agents to which Safe Lock Intelligent Manager was unable to connect to displays.

4. Ensure that **Show disconnected agents in Agent Management** is selected and click **Close** to display a complete list of disconnected agents in the agent tree search results.

   After determining which agents cannot connect to the Safe Lock Intelligent Manager server, Trend Micro recommends checking the network connectivity of the disconnected agents.

Remotely Exporting Agent Settings

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

Procedure

1. Click **Agents** from the Intelligent Manager console.

   The **Agent Management** screen appears.

2. Select a target endpoint.

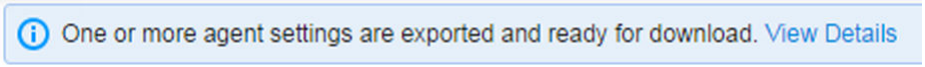
3. Click **Send Command**, select **Export Settings**, and select one of the following:

   - **Approved List**
   - **Agent Configuration**

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

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

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



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

Note

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

Remotely Importing Agent Settings

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

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

Procedure

1. Prepare a customized agent configuration file or Approved List.
   a. Export and download an agent configuration file or Approved List. For detailed steps, see *Remotely Exporting Agent Settings on page 2-18*.
   b. Customize the downloaded file.

Note

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

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

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

   The **Agent Management** screen appears.

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

   a. From the Endpoint column, select one or more agents.

   b. Click **Send Command**.

   c. Select **Import Settings**.

   d. Select **Approved List** or **Agent Configuration**.

      The import dialog appears.

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

   a. From the left panel, right-click an agent group and go to **Send Command** > **Import Settings**.

   b. Select **Approved List** or **Agent Configuration**.

      The import dialog appears.

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

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

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

Remotely Deploying Patches to Safe Lock Agents

You can upgrade agents directly from the web console page by using Intelligent Manager to deploy an uploaded patch file to selected Safe Lock agents.

Procedure

1. Click **Agents** from the Intelligent Manager console.

   The **Agent Management** screen appears.
2. Select one or more agents or groups.
3. Click **Send Command** > **Deploy Agent Patch**.
4. Select the patch file for deployment.
5. Click **Deploy**.

   Wait for the upload process to complete. After Intelligent Manager verifies the validity of the file, it deploys the patch file to the selected agents.

Chapter 3

Monitoring Safe Lock

This chapter introduces Trend Micro Safe Lock Intelligent Manager monitoring practices.

Topics in this chapter include:

About the Dashboard

The Safe Lock Intelligent Manager dashboard provides at-a-glance information using tabs and widgets. The dashboard displays the following components in a customized view for each web console account:

- **Tabs**: Allow users to organize widgets on customizable screens
- **Widgets**: Provide various data summaries on a tab

Use the **Generate Report** screen to manually download Safe Lock Intelligent Manager reports in Adobe PDF format (.PDF). For information on scheduling custom reports, see *Scheduled Reports on page 3-20*.

About Web Console Accounts and the Dashboard

Each web console account can customize the dashboard tabs and widgets for that account's specific needs. Customizing the tabs or widgets for one account has no effect on the tabs or widgets for a different account.

Note

When an account logs on to Safe Lock Intelligent Manager for the first time, default tabs and widgets appear on the dashboard.

See *About Default Tabs on page 3-3*.

About Dashboard Tabs

The Safe Lock Intelligent Manager dashboard uses tabs to provide a flexible data monitoring solution for administrators. Tabs provide a container for widgets, allowing web console accounts to create their own customized dashboard. The dashboard supports up to 30 tabs per account.

Closing tabs permanently removes them from that account. There is no way to recover closed tabs, but you can re-create similar tabs later. Closing a tab has no impact on the dashboard of other user accounts.

Use the slide show function to assist in monitoring widgets on different tabs by using the following controls:

- Click **Play Tab Slide Show** to rotate through tabs automatically at a specified interval.

  Tip

  Configure the duration of rotation intervals in **Tab Settings**.

  See *Configuring Tab Settings on page 3-5*.

- Click **Pause Tab Slide Show** to stop the slide show at the current tab.

  Tip

  Navigating to a different tab also stops the slide show.

About Default Tabs

The dashboard provides the following default tabs:

- **Event Overview**: This tab contains widgets that display information relating to agent events on managed Safe Lock endpoints.

WIDGET	DESCRIPTION
Open Warnings	Displays the latest open warnings.
Top Blocked Files	Displays the files that are blocked the most.
Blocked Event History	Displays blocked events during the specified time period.
Top Endpoints with Blocked Events	Displays the endpoints that triggered the most blocked events.
Blocked File Scan Results	Displays malware scan results for blocked files.

- **Agent Overview**: This tab contains widgets that display information relating to managed Safe Lock endpoints.

WIDGET	DESCRIPTION
Application Lockdown State	Displays the Application Lockdown status for agents.
Versions	Displays the number of endpoints with specific versions of Safe Lock installed.
Latest Component Updates	Displays the latest versions of components.

Note

Change the default names of tabs on the **Tab Settings** screen.

See *Configuring Tab Settings on page 3-5*.

Adding Tabs

Add tabs to the dashboard to provide a customized information summary to your Safe Lock Intelligent Manager account.

Procedure

1. Go to **Dashboard** in the navigation at the top of the web console.
2. Click the **+** tab.

   The **New Tab** screen appears.
3. In the **Title** field, type a meaningful title for the tab.
4. Select a layout for the tab.

Note

The number of widgets that you can add to a tab depends on the layout for the tab. Once the tab contains the maximum number of widgets, you must remove a widget from the tab or create a new tab for the widget.

5. Configure slide show and auto-fit settings.
6. Click **Save**.

   The empty tab appears on the dashboard.
7. Click **Add Widgets** to populate the tab with widgets.

Configuring Tab Settings

Procedure

1. Go to **Dashboard** in the navigation at the top of the web console.
2. Click **Tab Settings**.

   The **Tab Settings** screen appears.
3. In the **Title** field, type a meaningful title for the tab.
4. Select a layout for the tab.
5. Configure slide show and auto-fit settings.

   You may specify the length of time each tab displays before switching to the next tab. The number must be an integer between 5 and 3,600.

About Widgets

Widgets are the core components for the dashboard. Tabs provide the layout and widgets provide the actual data summary for the dashboard.

You can configure the data scope on many widgets individually. For example, some widgets allow you to specify the following:

- Time period
- Pie chart or line chart

- Legend

Move widgets in tabs by dragging and dropping widgets to various locations on a tab. The layout for a tab determines where you can move a widget.

Safe Lock Application Lockdown State

This widget displays an overview of the Application Lockdown status of the network.

By default, the widget is displayed on the **Agent Overview** tab of the **Dashboard**.

The widget displays the following data in a pie chart:

STATUS	DESCRIPTION
Application Lockdown On	Number and percentage of agents in the network that have Application Lockdown enabled
Application Lockdown Off	Number and percentage of agents in the network that have Application Lockdown disabled

Click a pie chart section to view more details about each status.

Safe Lock Versions

This widget displays a summary of the Safe Lock agent versions managed by Safe Lock Intelligent Manager.

By default, the widget is displayed on the **Agent Overview** tab of the **Dashboard**.

COLUMN	DESCRIPTION
Agent Version	Version number reported by the Safe Lock agent
Endpoints	Total number of endpoints that have the specific agent version installed

Click a value in the **Endpoints** column to view all endpoints that have the specific agent version installed.

Safe Lock Open Warnings

This widget displays the latest open warnings reported by Safe Lock agents.

By default, the widget is displayed on the **Event Overview** tab of the **Dashboard**.

COLUMN	DESCRIPTION
Event Time	Date and time when the open warning occurred
Endpoint Name	Name of the affected endpoint
Event	Event message for the open warning
File / Folder	File or folder that triggered the open warning

Click a value in the **Event** column to view more details for that event. To view all events, click **View all open warning events**.

To specify the number of events to display, open the **Widget Settings** dialog, then select a different value for **Latest Events**.

Safe Lock Top Endpoints with Blocked Events

This widget displays the endpoints with the most blocked events.

By default, the widget is displayed on the **Event Overview** tab of the **Dashboard**.

COLUMN	DESCRIPTION
Endpoint Name	Name of the endpoint
Tags	Tags assigned to the endpoint
IP Address	IP address of the endpoint
Blocked Events	Total number of events blocked on the endpoint

Click a value in the **Blocked Events** column to view more details for that event.

Use the **Time Period** drop-down to display only the event data for the period specified.

To specify the number of events to display, open the **Widget Settings** dialog, then select a different value for **Events to display**.

Safe Lock Blocked Event History

This widget displays a summary of blocked events for the specified time period.

By default, the widget is displayed on the **Event Overview** tab of the **Dashboard**.

Click the display icons to display the data as a pie chart or a line chart.

- Use the **Time Period** drop-down to display only the event data for the period specified.
- Click an entry on the legend to show or hide data for that event.
- Click a value on the chart to view more details about the blocked event.

Safe Lock Top Blocked Files

This widget displays a list of files that triggered the most blocked events.

By default, the widget is displayed on the **Event Overview** tab of the **Dashboard**.

COLUMN	DESCRIPTION
File Name	Name of the file that triggered the blocked events
Scan Result	Indicates if the file is malicious or not
File Hash	SHA1 hash of the file that triggered the blocked events
Endpoints	Number of endpoints which reported a blocked event for the file
Blocked Events	Total number of blocked events reported for the file

Click a value in the **Blocked Events** column to view more details for that event.

To specify the number of events to display, open the **Widget Settings** dialog, then select a different value for **Events to display**.

Safe Lock Blocked File Scan Results

This widget displays malware scan results for blocked files.

By default, the widget is displayed on the **Event Overview** tab of the **Dashboard**.

The data is displayed as a pie chart.

- Use the **Time Period** drop-down to display only the event data for the period specified.
- Click an entry on the legend to show or hide data for that scan result.
- Click a value on the chart to view more details about the blocked event.

Safe Lock Latest Component Updates

This widget displays the latest versions of components.

By default, the widget is displayed on the **Agent Overview** tab of the **Dashboard**.

COLUMN	DESCRIPTION
Pattern/ Template Engine	Name of the component
Version	Version number reported by the Safe Lock agent
Time	Time when the component was last updated

Adding Widgets

The number of widgets that you can add to a tab depends on the layout for the tab. Once the tab contains the maximum number of widgets, you must remove a widget from the tab or create a new tab for the widget.

Procedure

1. Go to **Dashboard** in the navigation at the top of the web console.
2. Go to the tab on the dashboard that you want to add the widget to.
3. Click **Add Widgets**.

   The **Add Widgets** screen appears.
4. Optionally, click one of the following to filter the widgets that display:

CATEGORY	DESCRIPTION
Most Recent Widgets	Queries for widgets added to a tab recently
All Widgets	Queries for all widgets available
Agent Status	Queries for only widgets that display data about managed Safe Lock agents.
Events	Queries for only widgets that display data about managed Safe Lock agent events.
Server Status	Queries for only widgets that display data about Safe Lock Intelligent Manager.

5. Select one or more widgets to add to the current tab.
6. Click **Add**.

Using Widgets

Perform the following tasks on each widget:

Task	Steps
Move a widget	Move widgets on tabs by clicking and holding on the title bar at the top of the widget and dragging to various locations on a tab. **Tip** The layout for a tab determines where you can move a widget. As you drag, a red, dotted border appears when the widget is able to move to an area.
Resize a widget	Horizontally resize a widget on a multi-column tab by doing the following: 1. Hover the pointer at the edge of a widget. A vertical, gray bar appears. 2. Drag the pointer left or right. Vertically resize widgets on a multi-column tab by enabling **Auto-fit** in the **Tab Settings**. This automatically adjusts widgets to be the same height as the widgets beside them.
Refresh widget data	Click the **Refresh** icon at the top of the widget.
Specify automatic refresh settings	1. Click the **More Options** icon at the top of the widget. 2. Select **Refresh Settings**. The **Refresh Settings** screen appears. 3. To enable automatic refresh for this widget, do the following: a. Select **Automatically refresh the widget**. b. Specify a frequency.
Rename a widget	1. Click the **More Options** icon at the top of the widget. 2. Select **Widget Settings**. The **Widget Settings** screen appears. 3. Type a meaningful title for the widget.

Task	Steps
Close a widget	1. Click the **More Options** icon at the top of the widget. 2. Select **Close Widget**.

About the Agent Events Screen

To display the **Agent Events** screen, go to **Logs & Reports** > **Agent Events** in the navigation at the top of the web console.

This screen displays a list of events related to applications not in the Approved List on agents managed by Safe Lock Intelligent Manager.

Depending on the feature status, Safe Lock generates a log and performs the action for the events listed in the following table. Event logs contain information from managed agents about files not in the Approved List and any action taken.

Table 3-1. Agent events

Event	Feature Status	Safe Lock Action
A file not on an agent's Approved List attempts to run or make changes to the endpoint	Lockdown disabled	Allows the file to run
	Lockdown enabled	Blocks the file and prompts for user action
A storage device (CD/DVD drive, floppy disk, or USB device) attempts to access the endpoint	Device Control disabled	Allows access for the device
	Device Control enabled	Denies access for the device (when the device type is removable device) and prompts for user action

The following table describes the user actions for the events.

TABLE 3-2. User actions

USER ACTION	DESCRIPTION
Add to Approved List	Prevent the file from executing or deny the USB device access to the endpoint for this instance but add the file or USB device to the agent's Approved List. This allows the file to execute or USB device access for subsequent detections.
Ignore	Prevent the file from executing but do not move or change the file.
Quarantine	Prevent the file from executing and hold the file in quarantine for later analysis.
Delete	Prevent the file from executing and delete the file.

Querying Agent Event Logs

Querying refines the list of displayed agent event logs.

Procedure

1. Go to **Logs & Reports** > **Agent Events** in the navigation at the top of the web console.

   The **Agent Events** screen appears.

2. To filter by period, click the **Time Period** drop down and specify a criteria.

   Perform one of the following:

   - Click a listed time range.
   - Click **Custom**, specify a time range, and click **Search**.

3. To filter by endpoints, click the **All Endpoints** drop down and specify a criteria.

   The following options are available:

   - **Endpoint name**: Type the beginning or all of an endpoint host name and click **Search**.

- **Group Name**: Type the group name and click **Search**.
- **IP Address**: Type the IPv4 address and click **Search**.
- **IP Range**: Type the IPv4 address range and click **Search**.
- **Tag**: Type all or part of the tag and click **Search**.

4. To filter by events, click the **All Events** drop down and specify a criteria.

   The following options are available:

   - **Event Type**: Select a specific event and click **Apply**.
   - **Source**: Select **Safe Lock** or **Portable Security** as the event source.
   - **Severity Level**: Select **Information** or **Warning** as the event level.
   - **Marked**: Select **Open** or **Closed**.
   - **Integrity Monitoring**: Select **File or folder** or **Registry key or value**, and click **Search**. **File or folder** searches support partial string matching.
   - **Blocked File**: Select **File name** or **File hash (SHA-1)**, and click **Search**. **File name** searches support partial string matching.
   - **Malware Detection**: Select **All detections**, **Unsuccessful actions**, **Cleaned**, **Quarantined**, **Deleted**, **Ignored** or **Rolled back**.

5. The table displays only the entries that match the filters selected.

Exporting Agent Events

Save data about selected agent event log entries as a CSV file.

Procedure

1. Go to **Logs & Reports** > **Agent Events** in the navigation at the top of the web console.

   The **Agent Events** screen appears.

2. Select the agent log entries in the list that you want to export information for.

   a. To export all entries, click **Export** > **All Logs**.

   b. To export selected entries only, perform one of the following:

      - To select a single entry, click the entry to be exported.
      - To select a range of entries, press and hold SHIFT, and then click the first and last entries to be exported.
      - To select multiple non-consecutive entries, press and hold CONTROL, and then click each entry to be exported.

   c. Click **Export** > **Selected Logs**.

3. Save the file.

Importing Agent Events

Safe Lock Intelligent Manager supports importing agent events from the following applications:

- Trend Micro Safe Lock Intelligent Manager: Logs exported by Safe Lock Intelligent Manager 2.0 in CSV format
- Trend Micro Portable Security: Collect logs from Safe Lock agents running versions 1.1 and 2.0 in DB format

Note

Portable Security exports Safe Lock logs to the `tmsllog.db` file by default.

Procedure

1. Go to **Logs & Reports** > **Agent Events** in the navigation at the top of the web console.

   The **Agent Events** screen appears.

2. Click **Import**.

   The **Import** screen appears.

3. Select the CSV file you want to import.

4. Click **Open**.

5. Click **OK**.

   The event logs are imported into Safe Lock Intelligent Manager.

> **Note**
>
> If you interrupt or cancel the import, no data will be added to the Safe Lock Intelligent Manager database.

Marking Warning Events

To help you track **Warning** events, change the status displayed for them under **Marked** in the list.

> **Note**
>
> Safe Lock Intelligent Manager does not display a **Marked** status for **Information** events.

Procedure

1. Go to **Logs & Reports** > **Agent Events** in the navigation at the top of the web console.

   The **Agent Events** screen appears.

2. Select the **Warning** event or events you want to change the status of.

3. Change the status by doing one of the following:

   - Click **Mark Open**.

- Click **Mark Closed** .

About the Server Events Screen

To display the **Server Events** screen, go to **Logs & Reports** > **Server Events** in the navigation at the top of the web console.

This screen displays a log of audited Safe Lock Intelligent Manager web console account activity.

Note

Server event logs contain collected information about actions taken by Safe Lock Intelligent Manager web console account users and policies.

Querying Server Event Logs

Querying refines the list of displayed server event logs.

Procedure

1. Go to **Logs & Reports** > **Server Events** in the navigation at the top of the web console.

   The **Server Events** screen appears.

2. Click the drop-down list under **Server Events**.

   A list of search criteria.

3. Select the type of search criteria.

   Appropriate search fields appear for the selected criteria.

4. Follow the appropriate steps depending on the selected criteria:

Option	Description
Time Period	Do one of the following: • Select a listed time range. • Specify a custom time range. a. Go to **Custom** in the list. b. Specify your custom time range. c. Click **Search**.
All Users	Displays all events logged by all users.
User Name	Displays all events logged by a specific user.
Endpoint name	Type the endpoint host name (first few letters or complete name), and click **Search**.
Group name	Displays all events logged by the specific groups.
All Events	Displays all events logged by agents.
Event Type	Select a specific event.

Your search results appear in the list of server event logs.

Exporting Server Event Logs

Save data about selected server event log entries as a CSV file.

Procedure

1. Go to **Logs & Reports** > **Server Events** in the navigation at the top of the web console.

   The **Server Events** screen appears.

2. Select the server log entries in the list that you want to export information for.

   a. To export all entries, click **Export** > **All Logs**.

b. To export selected entries only, perform one of the following:

- To select a single entry, click the entry to be exported.
- To select a range of entries, press and hold SHIFT, and then click the first and last entries to be exported.
- To select multiple non-consecutive entries, press and hold CONTROL, and then click each entry to be exported.

c. Click **Export** > **Selected Logs**.

3. Save the file.

Maintaining Logs

Purge older logs to reduce the size of the Safe Lock Intelligent Manager database.

Procedure

1. Go to **Logs & Reports** > **Log Settings** in the navigation at the top of the web console.

   The **Log Settings** screen appears.

2. Click the **Maintenance** tab.

3. Under **Purge agent event log entries older than**, specify the maximum age of agent event log entries to keep.

4. Under **keep at most**, specify the maximum number of agent event entries to keep.

Note

- If the number of entries exceeds the limit set under **keep at most**, Safe Lock Intelligent Manager purges agent event logs newer than the age specified in the **Purge agent event log entries older than** field.

5. Under **Purge server auditing log entries older than**, specify the maximum age of server event log entries that will be preserved.

6. To prohibit automatically purging without a backup, do the following:

   a. Select **Always back up logs before automatically purging**.

   b. Click **Backup Path**.

   c. Specify the full path for backups.

   d. If you want Safe Lock Intelligent Manager to create folders in the specified path that do not exist, select **Create missing folders**.

7. To manually purge log entries based on their age, do the following:

   a. In the **Manual Purge** section, select the minimum age of entries to preserve.

   b. Click **Purge Now**.

WARNING!

Safe Lock Intelligent Manager does not automatically back up manually purged log entries.

To back up existing log entries, perform the appropriate steps to export the entries manually.

See *Exporting Agent Events on page 3-14*.

See *Exporting Server Event Logs on page 3-18*.

Scheduled Reports

The **Scheduled Reports** screen provides a list of all reports that automatically generate on a user-defined schedule. You can use this screen to view basic information about previously configured scheduled reports, report content, recipients, as well as enabling and disabling scheduled reports.

The following table outlines the available tasks on the **Scheduled Reports** screen.

TASK	DESCRIPTION
Enable sending scheduled reports	Select the **Send scheduled reports** check box to enable scheduled reports.
Edit scheduled report content	Select the type of content you want to include in your report. For more information, see *About Default Tabs on page 3-3*
Send scheduled reports	Set the frequency and time for the scheduled reports on a daily, weekly, or monthly basis. **Note** Scheduled tasks will be skipped for the months that do not contain the specific day. To carry out the task regularly, we recommend avoiding the 29th, 30th, or 31st.
Specify scheduled report recipients	A valid email address is required for specifying the report recipients.

Important

Ensure that your SMTP server settings are properly configured in order to send scheduled reports.

For more information, see *Configuring SMTP Server Settings on page 4-9*.

Forwarding Events to an External Syslog Server

You can forward server and agent event logs to an external syslog server for additional managing and monitoring capabilities. The Intelligent Manager forwards logs in the Common Event Format (CEF). Make sure your syslog server supports the Common Event Format (CEF).

Procedure

1. Go to **Logs & Reports** > **Log Settings**.
2. Click the **Syslog Server** tab.
3. Select **Forward logs to syslog server (CEF only)**.
4. Specify the protocol, IP address, and port of the syslog server.

Apex Central Integration

Safe Lock Intelligent Manager supports integration with Apex Central . After integration, use the Apex Central console to monitor the status of Safe Lock agents.

Note

Safe Lock Intelligent Manager also supports integration with Trend Micro Control Manager 7.0.

Procedure

1. Register with the Apex Central server.
   a. On the Apex Central server management console, go to **Administration** > **Managed Servers** > **Server Registration**.
   b. Select **Trend Micro Safe Lock** as the **Server Type**.
   c. Click **Add** to open the **Add Server** screen.
   d. Provide the server information for the Safe Lock Intelligent Manager server to be integrated.
   e. Click **Save**.
2. Add the Safe Lock widgets to the Apex Central dashboard.
   a. On the Apex Central server management console, go to the **Dashboard**.

b. Determine which tab should contain the widgets.

   - To add a new tab, click the plus icon (+) and specify a tab name.
   - To select an existing tab, click the tab name.

c. Click the gear icon, and click **Add Widgets**.

d. On the **Add Widgets** screen, locate and select the Safe Lock widgets to be added.

   - Use the drop down to filter the widgets by product.
   - Use the search box to filter the widgets by name.

   For more details on the widgets, see *About Widgets on page 3-5*.

e. Click **Add**.

   Back in the **Dashboard**, verify that the selected widgets are displayed.

Chapter 4

Configuring Administration Settings

This chapter introduces Trend Micro Safe Lock Intelligent Manager administration settings.

Topics in this chapter include:

About the Component Updates Screen

To display the **Component Updates** screen, go to **Administration** > **Components** > **Updates** in the navigation at the top of the web console.

This screen displays the list of components used by Safe Lock Intelligent Manager.

The following table describes the tasks you are perform on this screen.

FUNCTION	DESCRIPTION
Update	Manually update the selected components that are used to scan files for malware on endpoints.
Schedule Updates	Configure the update schedule. Enable or disable scheduled updates for each component.
Download Agent Installer Package	Download an up-to-date agent installer package.

Manually Updating Components

Procedure

1. Go to **Administration** > **Components** > **Updates** in the navigation at the top of the web console.

   The **Component Updates** screen appears.

2. Click **Update**.

3. Select the components you want to update.

4. Click **Update**.

   The **Update Progress** screen appears. Safe Lock Intelligent Manager updates **Current Version** and **Latest Update** information after components update successfully.

Scheduling Component Updates

Procedure

1. Go to **Administration** > **Components** > **Updates** in the navigation at the top of the web console.

   The **Component Updates** screen appears.

2. Click **Scheduled Updates**.

3. Enable the components you want to update on a schedule.

4. In the **Update Schedule** section, select the schedule you want to use.

Important

If you select **Monthly, on day** and select a number higher than the actual number of days in a given month, Safe Lock Intelligent Manager updates selected components on the last day of that month instead.

To ensure that your tasks are properly scheduled, we recommend avoiding selecting the 29th, 30th, or 31st of each month.

Downloading an Up-to-Date Agent Installer Package

Procedure

1. Go to **Administration** > **Components** > **Updates** in the navigation at the top of the web console.

   The **Component Updates** screen appears.

2. Click **Download Agent Installer Package**.

3. Select the language the installation package.

   Your browser downloads the most up-to-date agent installer package.

Note

The agent installer package is considered up-to-date by Safe Lock Intelligent Manager based on the component versions displayed on the **Component Updates** screen. If the cached agent installer package is not up-to-date, Safe Lock Intelligent Manager prepares and caches an up-to-date package before starting the download.

Preparing an up-to-date agent installer package is system-intensive. Depending on the hardware running Safe Lock Intelligent Manager, preparing an up-to-date agent installer package can take a while.

4. To use the downloaded agent installer package for remote installations using the **`SLrst`** program at the command line interface (CLI), copy the downloaded agent installer package to the path used by **`SLrst`**.

   For example, if you installed Safe Lock Intelligent Manager to the default path on the C drive, copy the downloaded agent installer package to the following path: `c:\Program Files\Trend Micro\Safe Lock Intelligent Manager \CmdTools\RemoteAgentSetupTool\`.

Important

Users should manually compress the downloaded file into the package file (`.zip`).

The package file name must follow the format:
`TMSL_TXOne_<language_abbreviation>.zip`

For example:

VALID	NOT VALID
`TMSL_TXOne_EN.zip`	`TMSL_TXOne_EN (1).zip`
`TMSL_TXOne_JA.zip`	`TMSL_TXOne_EN_1.zip`

About Modifying the Agent Installer Package

Safe Lock Intelligent Manager supports specific modifications to the agent installer package. If you choose to modify the agent installer package, use caution and observe the following requirements:

- Modify only the `Setup.ini` and `trend.cer` files.
- Maintain the internal directory structure of the agent installer package.
- Modify the agent installer package at your own risk.

Configuring Component Download Locations

Procedure

1. Go to **Administration** > **Components** > **Update Source** in the navigation at the top of the web console.

   The **Server Update Source** screen appears.

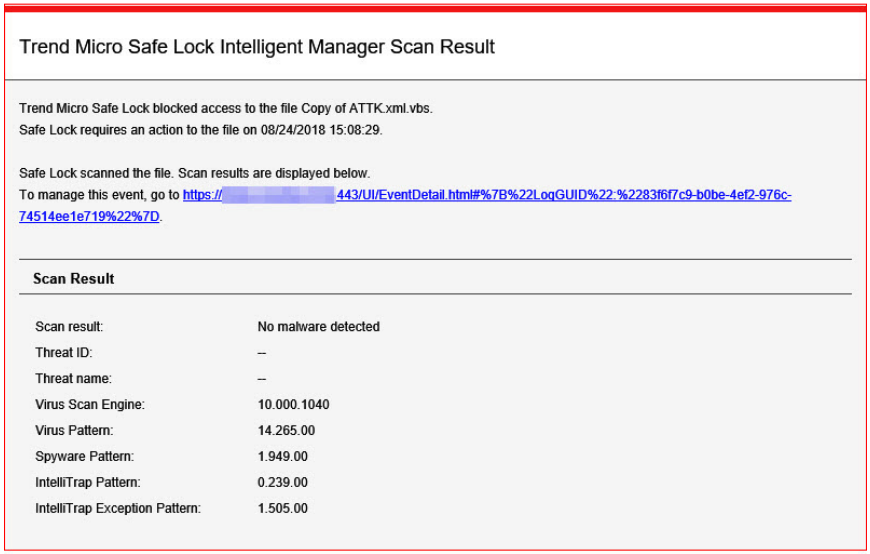
2. Select the appropriate download location for your environment:

OPTION	DESCRIPTION
Trend Micro ActiveUpdate server	Use the Trend Micro-managed update server on the Internet.
Internet or local server	Specify an update server that does not require authentication.
Local server requiring authentication	Specify a local, private update server that requires authentication.

Configuring Notification Settings

Safe Lock Intelligent Manager sends the following types of notifications based on configured settings:

- **General**: Notification of information and warning messages sent to Safe Lock Intelligent Manager by endpoints after blocking files



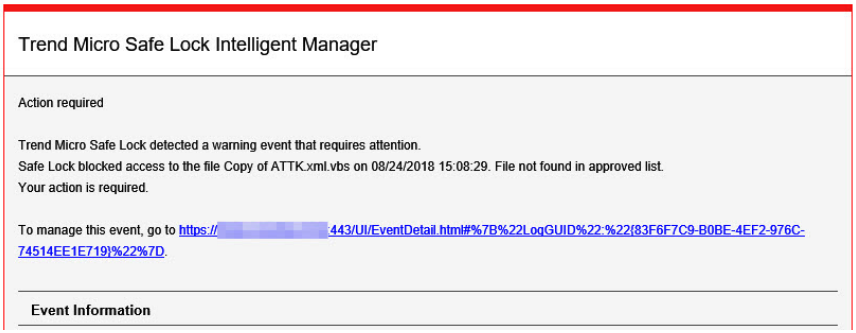
Trend Micro Safe Lock Intelligent Manager Scan Result

Trend Micro Safe Lock blocked access to the file Copy of ATTK.xml.vbs.
Safe Lock requires an action to the file on 08/24/2018 15:08:29.

Safe Lock scanned the file. Scan results are displayed below.
To manage this event, go to https://[redacted]:443/UI/EventDetail.html#%7B%22LogGUID%22:%2283f6f7c9-b0be-4ef2-976c-74514ee1e719%22%7D.

Scan Result

Scan result:	No malware detected
Threat ID:	--
Threat name:	--
Virus Scan Engine:	10.000.1040
Virus Pattern:	14.265.00
Spyware Pattern:	1.949.00
IntelliTrap Pattern:	0.239.00
IntelliTrap Exception Pattern:	1.505.00



Trend Micro Safe Lock Intelligent Manager

Action required

Trend Micro Safe Lock detected a warning event that requires attention.
Safe Lock blocked access to the file Copy of ATTK.xml.vbs on 08/24/2018 15:08:29. File not found in approved list.
Your action is required.

To manage this event, go to https://[redacted]:443/UI/EventDetail.html#%7B%22LogGUID%22:%22{83F6F7C9-B0BE-4EF2-976C-74514EE1E719}%22%7D.

Event Information

- **Outbreak**: Notification sent when the specified number of open warning messages in the specified time period has passed the threshold

See *Example Notification Messages on page 4-8*.

Procedure

1. Go to **Administration** > **Notification Settings** in the navigation at the top of the web console.

   The **Notification Settings** screen appears, open to the **General** tab.

2. To send general notifications using email:

   a. Select **Send notifications using email**.

   b. Specify the recipient email addresses.

   c. Specify your SMTP server settings. For details, see *Configuring SMTP Server Settings on page 4-9*.

   d. If your SMTP server requires authentication, select **SMTP authentication** and specify credentials.

   e. To send a test message using this configuration, click **Send Test**.

   For more information, see *Configuring SMTP Server Settings on page 4-9*

3. To send general notifications using SNMP:

   a. Select **Send notifications using SNMP**.

   b. Specify your SNMP server IPv4 address or Fully Qualified Domain Name (FQDN).

c. Specify your SNMP Community string.

4. To send general notifications using third party applications:

   a. Select **Launch a third-party application**.

   b. Specify the full path to the third-party application.

   c. Optionally, specify any run-time parameters for the application.

5. To send outbreak notifications:

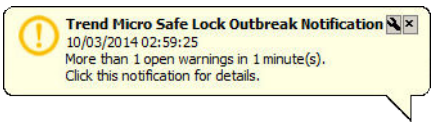
   a. Go to the **Outbreak** tab.

   b. Select **Send outbreak notifications**.

   c. Specify the threshold number of open warnings in a time period.

   d. Specify the threshold time period of those warnings.

   e. To display a Windows notification on the screen of the physical Safe Lock Intelligent Manager server endpoint during outbreaks, select **Display pop-up outbreak notification balloon on the physical Trend Micro Safe Lock Intelligent Manager server**.



Example Notification Messages

If you configure Safe Lock Intelligent Manager to send SMTP or SNMP notifications, Safe Lock Intelligent Manager sends the notifications for all types of events.

TABLE 4-1. Example Notifications

EVENT TYPE	CAUSE	EXAMPLE NOTIFICATION MESSAGE
Outbreak	Outbreak	Trend Micro Safe Lock: Outbreak notification

EVENT TYPE	CAUSE	EXAMPLE NOTIFICATION MESSAGE
Action Required	Blocked file	Trend Micro Safe Lock: [Action required] File access blocked on <computer_name> (<file_name>)
Scan Result	Malware detection	Trend Micro Safe Lock: [Scan Result] Malware detected on <computer_name> (<file_name>)
Warning	Unauthorized change	Trend Micro Safe Lock: [Warning] Unauthorized change of File/Folder allowed on <computer_name>
Warning	Application Lockdown status change	Trend Micro Safe Lock: [Warning] Application Lockdown Turned Off on <computer_name>
Warning	Device access blocked	Trend Micro Safe Lock: [Warning] Device access blocked on <computer_name>

Configuring SMTP Server Settings

This screen allows users to specify SMTP server settings for sending out notifications and scheduled reports.

Procedure

1. Go to **Administration** > **SMTP Server Settings**.

   The **SMTP Server Settings** screen appears.

2. Type the IP address or fully qualified domain name (FQDN) of the SMTP server in the **SMTP server** field.

3. Type the port number.

4. Type the sender's email address in the **Sender** field.

   Safe Lock Intelligent Manager uses this address as the sender address (a requirement for some SMTP servers).

5. If the SMTP server requires authentication, select **SMTP authentication**.

6. Type the user name and password.

7. Click **Save**.

   To send a test email from Safe Lock Intelligent Manager, select the **Send Test Email** button.

> **Note**
>
> You can send a test email to only one email address or recipient at a time.

About the Account Management Screen

To display the **Account Management** screen, go to **Administration** > **Account Management** in the navigation at the top of the web console.

Use this screen to manage Safe Lock Intelligent Manager web console accounts.

Trend Micro Safe Lock Intelligent Manager web console accounts have the following privileges:

ACCOUNT TYPE	PRIVILEGES
Administrator	• Add, edit, enable, disable, or delete Safe Lock Intelligent Manager web console accounts from the **Account Management** screen. • Modify their own account description, email address, and password • Specify actions to take on files blocked by agents • View the Safe Lock Intelligent Manager web console **Logs & Reports** > **Server Events** screen • Allow or block storage device access on managed endpoints.

ACCOUNT TYPE	PRIVILEGES
Full Control	• Modify their own account description, email address, and password • Specify actions to take on files blocked by agents • View the Safe Lock Intelligent Manager web console **Logs & Reports** > **Server Events** screen • Allow or block storage device access on managed endpoints.
Manage Storage Device Control Only	• Modify their own account description, email address, and password • Allow or block storage device access on managed endpoints.
Manage Application Lockdown Only	• Modify their own account description, email address, and password • Configure application lockdown on managed endpoints.
Read Only	• Modify their own account description, email address, and password

Note

The default account created during installation is named "admin" and is the only account that has Administrator privileges.

Adding Accounts

Procedure

1. Log on the web console using the "admin" account.
2. Go to **Administration** > **Account Management** in the navigation at the top of the web console.

   The **Account Management** screen appears.

3. Click **Add**.

   The **Add User** screen appears.

4. Specify the privileges for the account.

   See *About the Account Management Screen on page 4-10*.

5. Specify the account name.

   Note

   Only lowercase a to z, 0 to 9, - and _ are supported.

6. Specify whether the account should be **Enabled** or **Disabled** upon creation.

7. Optionally, type an account description.

   Note

   The following characters are not supported:

   > < & " '

8. Optionally, specify an email address for this account.

9. Specify the password.

   Note

   The password must be 8 to 64 alphanumeric characters. The following characters are not supported:

   | > " : < \ spaces

Editing Accounts

Only an account with Administrator privileges is able to add, enable or disable, or delete accounts. All other accounts are only able to edit their own account description, email address, and password.

Procedure

1. Go to **Administration** > **Account Management** in the navigation at the top of the web console.

   The **Account Management** screen appears.

2. Click the user name of the account.

   The **Edit User** screen appears.

3. Modify settings.

Configuring Proxy Settings

Procedure

1. Go to **Administration** > **Proxy Settings** in the navigation at the top of the web console.

   The **Proxy Settings** screen appears.

2. To configure proxy settings for updates:

   a. Select **Use a proxy server for pattern and engine updates**.

   b. Specify the IPv4 address or FQDN of the proxy server.

   c. Specify the port.

   d. If your proxy server requires authentication, select **Proxy server authentication** and specify credentials.

3. To configure proxy settings used by Safe Lock Intelligent Manager when sending messages to Safe Lock agents:

   a. Select **Use a proxy server when Safe Lock Intelligent Manager communicates to Safe Lock agents**.

b. Specify the IPv4 address or FQDN of the proxy server.

c. Specify the port.

d. If your proxy server requires authentication, select **Proxy server authentication** and specify credentials.

Tip

To configure proxy settings used by Safe Lock agents when sending messages to Safe Lock Intelligent Manager:

- Before remote installation: Add the proxy information to the configuration file used by the agent installer package.
- After remote installation: Use the **`SLCmd.exe`** Command Line Interface tool on the local Safe Lock agent.

About the License Management Screen

To display the **License Management** screen, go to **Administration** > **License Management** in the navigation at the top of the web console.

The following details appear on this screen:

ITEM	DESCRIPTION
Status	Displays “Activated” or “Expired”
Type	Displays “Full” or “Trial”
Expiration	Displays the date when features and support end
Activation Code	Displays the Activation Code For more information, see *Changing Activation Codes on page 4-15*
Last Updated	Displays the last time the Activation Code was updated

Changing Activation Codes

Procedure

1. Go to **Administration** > **License Management** in the navigation at the top of the web console.

   The **License Management** screen appears.

2. Click **Specify Activation Code**.

3. Type your new Trend Micro Safe Lock Intelligent Manager Activation Code.

   To remotely renew agent licenses, see *Renewing Agent Licenses on page 7-25*.

Note

Click **Refresh** to update your product license. A connection with the Trend Micro product license server is required.

Chapter 5

Using the Agent Console

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

Topics in this chapter include:

Setting Up the Approved List

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

Procedure

1. Open the Safe Lock console.

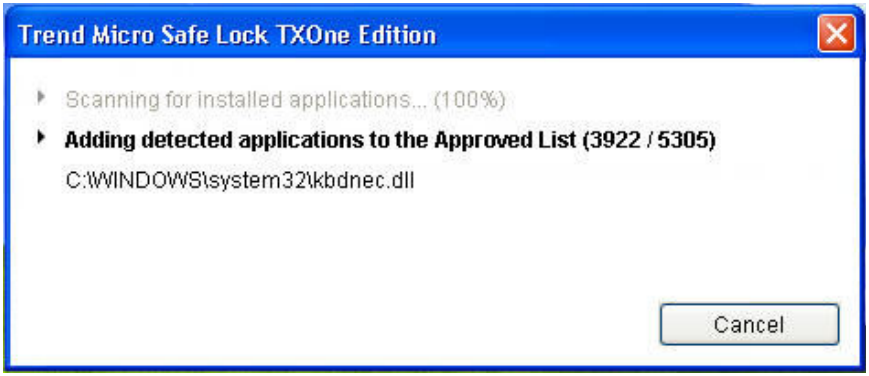
   The Safe Lock log on screen appears.

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

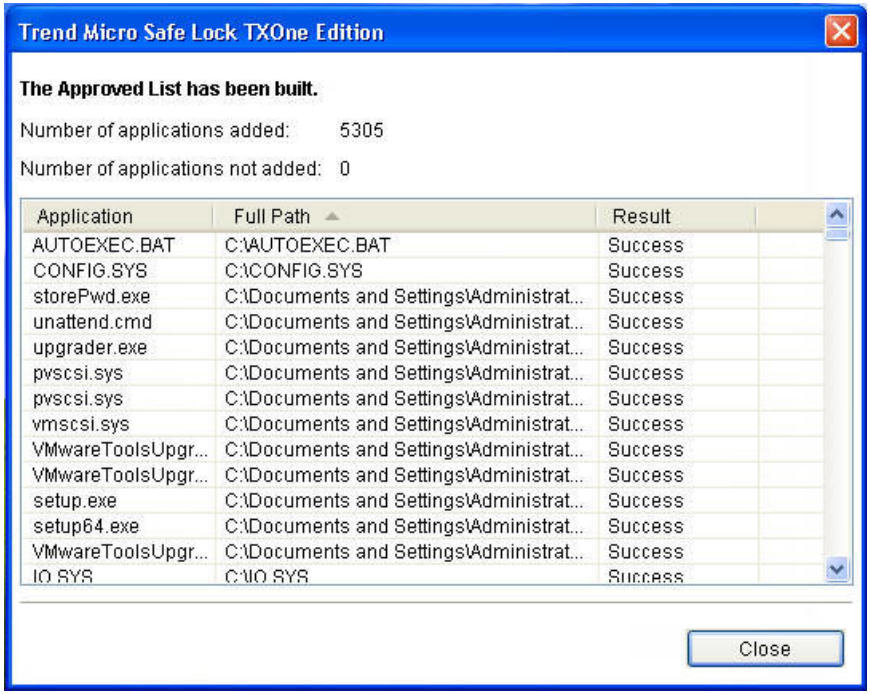
   Safe Lock asks if you want to set up the Approved List now.

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

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



Safe Lock displays the Approved List Configuration Results.



Note

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

4. Click **Close**.

Configuring Pop-up Notifications for Blocked Files

The administrator can set up a notification that displays on managed endpoints when Safe Lock blocks and prevents unapproved files from running or making changes to

managed endpoints. This notification alerts the administrator of any blocking event and provides details about the blocked file.

Note

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

TABLE 5-1. Configuring Pop-up Notifications for Blocked Files

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

About the Agent Console

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

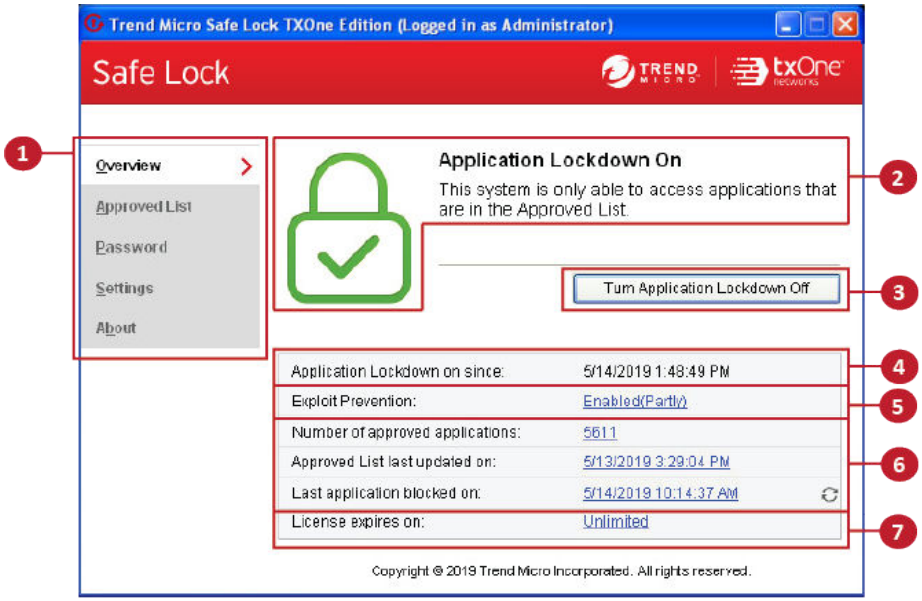


FIGURE 5-1. The Safe Lock console

The following table describes the features available on the console:

TABLE 5-2. Console Feature Descriptions

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

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

#	ITEM	DESCRIPTION
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.

Viewing Safe Lock Statuses

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

Note

System Tray icons display if they were enabled during installation.

TABLE 5-3. Status Icon Descriptions

CONSOLE ICON	SYSTEM TRAY ICON	STATUS	DESCRIPTION
		Locked	The Approved List is being enforced. Unauthorized applications cannot be run.
		Unlocked	The Approved List is not being enforced. Unauthorized applications can be run.

Console Icon	System Tray Icon	Status	Description
		Locked and in Maintenance Mode	In Maintenance Mode with the Approved List enforced. All applications can be run.
		Unlocked and in Maintenance Mode	In Mainteance Mode without Approved List enforced. All applications can be run.
N/A		Expired	The Safe Lock license has expired, and the system cannot be locked. Update the Activation Code by clicking on the expiration date.
N/A		Blocked	The Safe Lock has blocked and prevented an unapproved application not from running or making changes to the managed endpoint.

About the Approved List

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

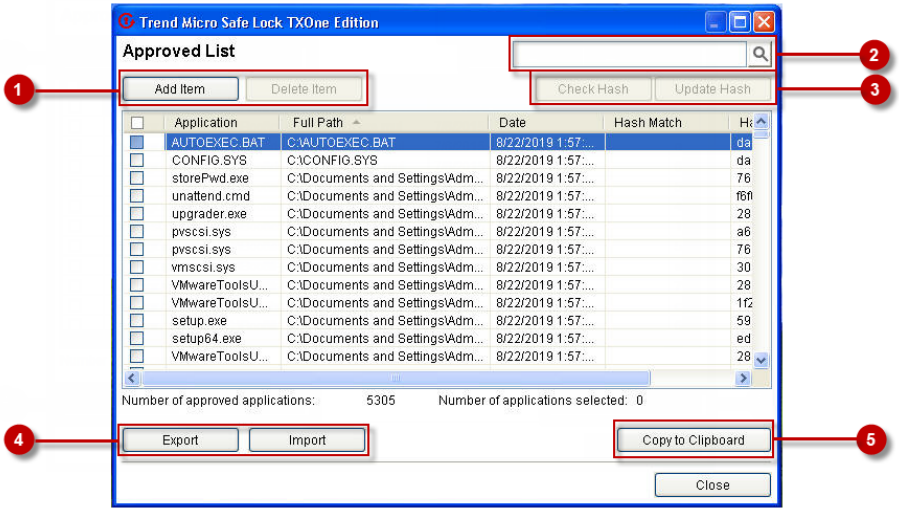


FIGURE 5-2. The Safe Lock Approved List

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

TABLE 5-4. Approved List Item Descriptions

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

About Hashes

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

The following table describes the hash check status icons.

TABLE 5-5. Hash Check Status Icons

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

Moving or overwriting files manually (without using the Trusted Updater) can result in the hash values not matching, but the mismatch could result from other applications (including malware) altering or overwriting existing files. If unsure why a hash value mismatch has occurred, scan the endpoint for threats with Trend Micro Portable Security.

Checking or Updating Hashes

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

Procedure

1. Open the Trend Micro Safe Lock console using the desktop icon (if available) or the **Start** menu by clicking **All Programs** > **Trend Micro Safe Lock**.
2. Provide the password and click **Login**.
3. Click the **Approved List** menu item to open the list.

   To check the file hash values:

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

b. Click **Check Hash**.

To update the file hash values:

a. Select the files to update.

b. Click **Update Hash**.

Important

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

Configuring the Approved List

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

TABLE 5-6. Methods for Adding Applications to the Approved List

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

Adding or Removing Files

Procedure

1. Open the Trend Micro Safe Lock console using the desktop icon (if available) or the **Start** menu by clicking **All Programs** > **Trend Micro Safe Lock**.
2. Provide the password and click **Login**.
3. Click the **Approved List** menu item to open the list.

   To add an item:

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

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

      A selection window appears.

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

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

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

   To remove an item:

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

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

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

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

Updating or Installing Using the Trusted Updater

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

Procedure

1. Open the Trend Micro Safe Lock console using the desktop icon (if available) or the **Start** menu by clicking **All Programs** > **Trend Micro Safe Lock**.
2. Provide the password and click **Login**.
3. Click the **Approved List** menu item to open the list.
4. To install or update an application, select the installer that the Trusted Updater should temporarily allow to run:
   a. Click **Add Item**, select **Automatically add files created or modified by the selected application installer**, and click **Next**.
   b. In the window that opens, choose **Specific installers**, **All installers in folders and subfolders**, or **All installers in a folder** from the drop-down list.
   c. Select the desired installation package or folder to add, and click **Open**.

      Note

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

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

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

FIGURE 5-3. The Safe Lock Trusted Updater

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

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

Exporting or Importing the Approved List

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

WARNING!

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

Procedure

1. Open the Trend Micro Safe Lock console using the desktop icon (if available) or the **Start** menu by clicking **All Programs** > **Trend Micro Safe Lock**.
2. Provide the password and click **Login**.
3. Click the **Approved List** menu item to open the list.

   To export the Approved List:

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

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

   To import an Approved List:

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

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

Account Types

Trend Micro Safe Lock Intelligent Manager 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 5-7. Safe Lock Accounts

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

ACCOUNT	DETAILS
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 5-18*. To sign in with a specific account, specify the password for that account.

Configuring Passwords

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

Important

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

Procedure

1. Open the Trend Micro Safe Lock console using the desktop icon (if available) or the **Start** menu by clicking **All Programs** > **Trend Micro Safe Lock**.
2. Provide the Safe Lock administrator password and click **Login**.
3. Click the **Password** menu item to display the administrator password page.

   To change the Safe Lock administrator password:

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

WARNING!

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

To create a Restricted User password:

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

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

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

To change an existing Restricted User password:

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

About Feature Settings

Safe Lock offers the following protection features.

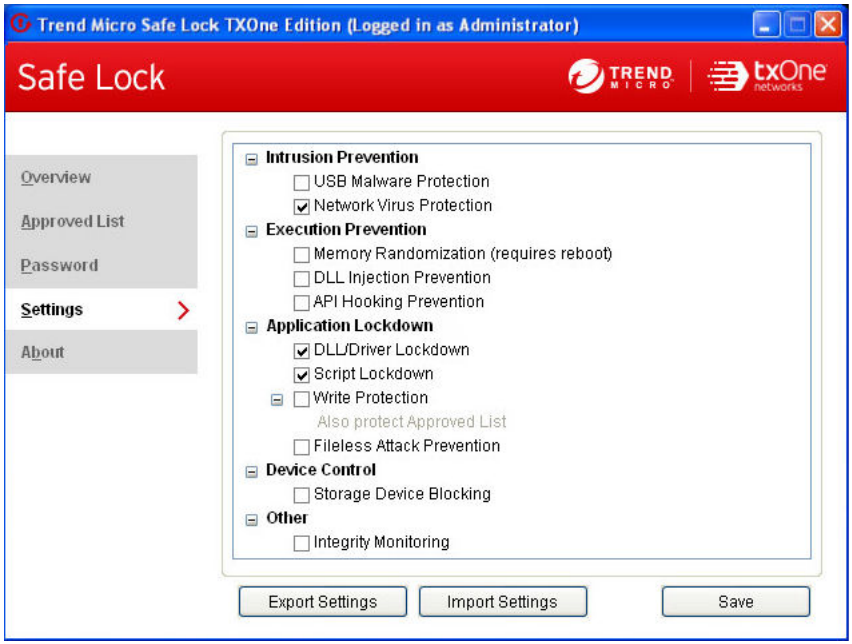


FIGURE 5-4. Safe Lock settings screen

TABLE 5-8. Intrusion Prevention

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

TABLE 5-9. Execution Prevention

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

SETTING	DESCRIPTION
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 5-10. Application Lockdown

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

TABLE 5-11. Device Control

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

TABLE 5-12. Other

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

Enabling or Disabling Feature Settings

Note

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

Procedure

1. Open the Trend Micro Safe Lock console using the desktop icon (if available) or the **Start** menu by clicking **All Programs** > **Trend Micro Safe Lock**.
2. Provide the password and click **Login**.
3. Click the **Settings** menu item to configure Exploit Prevention settings.
4. Enable or disable the desired features.
5. Click **Save**.

Chapter 6

Using the Agent Command Line Interface (CLI)

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

Topics in this chapter include:

Using SLCmd at the Command Line Interface (CLI)

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

Procedure

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

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

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

3. Type **SLCmd.exe**.

SLCmd Program and Console Function Comparison

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

TABLE 6-1. SLCmd Program at the Command Line Interface (CLI) and Console Function Comparison

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

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

Not all settings are available through the command line interface (CLI) or console. See *Working with the Agent Configuration File on page 9-2* 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 6-2. 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

PARAMETER	ABBREVIATION	USE
service	srv	Manage the Safe Lock service

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

TABLE 6-3. General Commands

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

COMMAND	PARAMETER	DESCRIPTION
		Note The default status is `disable`.
	`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`**
`set` `blockedfilenotification`		Display the current notification setting For example, type: **`SLCmd.exe -p <admin_password> set blockedfilenotification`** **Note** The default setting is `disable`.
	`enable`	Display a notification on the managed endpoint when Safe Lock blocks a file. For example, type: **`SLCmd.exe -p <admin_password> set blockedfilenotification enable`**
	`disable`	Do not display any notification when Safe Lock blocks a file. For example, type: **`SLCmd.exe -p <admin_password> set blockedfilenotification disable`**

COMMAND	PARAMETER	DESCRIPTION
show blockedlog		Display a list of applications blocked by Safe Lock For example, type: **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

COMMAND	PARAMETER	DESCRIPTION
		For example, type: **`SLCmd.exe -p <admin_password> version`**

Central Management Commands

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

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

The following table lists the available abbreviated forms of parameters.

TABLE 6-4. 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 6-5. Central Management Commands

COMMAND	PARAMETER	DESCRIPTION
`decrypt` `managedmodeconfiguration`	<path_of_encrypted_file> <path_of_decrypted_output_file>	Decrypt the configuration file used by Managed Mode
`encrypt` `managedmodeconfiguration`	<path_of_file> <path_of_encrypted_output_file>	Encrypt the configuration file used by Managed Mode

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

COMMAND	PARAMETER	DESCRIPTION
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 6-6. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
apihookingprevention	api	Manage API Hooking Prevention
customaction	ca	Manage actions taken when Safe Lock blocks specific types of events
dlldriverlockdown	dd	Manage DLL/Driver Lockdown
dllinjectionprevention	dll	Manage DLL Injection Prevention
exceptionpath	ep	Manage exceptions to Application Lockdown
integritymonitoring	in	Manage Integrity Monitoring
memoryrandomization	mr	Manage Memory Randomization
networkvirusprotection	net	Manage Network Virus Protection
script	scr	Manage Script Lockdown

PARAMETER	ABBREVIATION	USE
storagedeviceblocking	sto	Allows or blocks storage devices (CD/DVD drives, floppy disks, and network drives) from accessing the managed endpoint.
usbmalwareprotection	usb	Manage USB Malware Protection
writeprotection	wp	Manage Write Protection
writeprotection-includes-approvedlist	wpal	Manage Write Protection includes Approved List

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

TABLE 6-7. Optional Feature Commands

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

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

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

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

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

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

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

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

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

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

Restricted User Account Commands

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

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

The following table lists the available abbreviated forms of parameters.

TABLE 6-8. 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 6-9. Restricted User Account Commands

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

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

Script Commands

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

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

The following table lists the available abbreviated forms of parameters.

TABLE 6-10. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
script	scr	Manage script commands

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

TABLE 6-11. Script Commands

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

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

Note

Safe Lock uses the following default script rules:

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

Approved List Commands

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

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

The following table lists the available abbreviated forms of parameters.

TABLE 6-12. Abbreviations and Uses

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

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

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

TABLE 6-13. Approved List Commands

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

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

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

Application Lockdown Commands

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

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

The following table lists the available abbreviated forms of parameters.

TABLE 6-14. 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 6-15. Application Lockdown Commands

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

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

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

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

Write Protection Commands

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

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

The following table lists the available abbreviated forms of parameters.

TABLE 6-16. Abbreviations and Uses

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

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

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

TABLE 6-17. Write Protection List "File" Commands

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

TABLE 6-18. Write Protection List "Registry" Commands

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

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

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

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

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

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

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

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

Trusted Certification Commands

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

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

The following table lists the available abbreviated forms of parameters.

TABLE 6-19. Abbreviations and Uses

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

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

TABLE 6-20. Trusted Certificate Commands

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

Trusted Hash List Commands

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

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

The following table lists the available abbreviated forms of parameters.

TABLE 6-21. Abbreviations and Uses

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

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

TABLE 6-22. Trusted Hash List Commands

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

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

Trusted Updater Commands

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

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

The following table lists the available abbreviated forms of parameters.

TABLE 6-23. Abbreviations and Uses

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

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

TABLE 6-24. Trusted Updater Commands

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

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

Trusted USB Device Commands

Configure the trusted USB device 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 6-25. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
trustedusbdevice	tud	Manage the trusted USB device list

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

TABLE 6-26. Trusted USB Device Commands

COMMAND	PARAMETER	DESCRIPTION
show usbinfo	**<drive_letter>**	Display the identifiers (VID/PID/SN) of a USB storage device For example, type: `SLCmd.exe -p <admin_password> show usbinfo d`
show `trustedusbdevice`		Display all trusted USB storage devices For example, type: `SLCmd.exe -p <admin_password> show trustedusbdevice`
add `trustedusbdevice`	**[-vid <VID>] [-pid <PID>] [-sn <SN>]**	Add a trusted USB storage device with the specified identifiers. You must specify at least one device identifier. For example, type: `add trustedusbdevice -sn 123456`

COMMAND	PARAMETER	DESCRIPTION
remove trustedusbdevice	**[-vid <VID>] [-pid <PID>] [-sn <SN>]**	Remove a trusted USB storage device with the specified identifiers. You must specify at least one device identifier. For example, type: `remove trustedusbdevice -sn 123456`

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 6-63*.

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

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

The following table lists the available abbreviated forms of parameters.

TABLE 6-27. 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 6-28. Predefined Trusted Updater Commands

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

COMMAND	PARAMETER	DESCRIPTION
		Important The **add** command for adding files to the Predefined Trusted Updater List follows a different format than the other commands specified in the this list. For details on adding files to the Predefined Trusted Updater List (not the Predefined Trusted Updater Exception List), see *Predefined Trusted Updater "Add" Command on page 6-63*. For example, to add `notepad.exe` to the Predefined Trusted Updater Exception List, type: **`SLCmd.exe -p <admin_password> add predefinedtrustedupdater -e C:\Windows\notepad.exe`**
`decrypt` `predefinedtrustedupdater`	<path_of_encrypted_file> <path_of_decrypted_output_file>	Decrypt a file to the specified location For example, to decrypt `C:\Notepad.xen` to `C:\Editors\notepad.xml`, type: **`SLCmd.exe -p <admin_password> decrypt predefinedtrustedupdater C:\Notepad.xen C:\Editors\notepad.xml`**

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

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

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

Predefined Trusted Updater "Add" Command

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

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

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

TABLE 6-29. 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 6-30. Predefined Trusted Updater "Add" Additional Values

<table>
<tr><th>VALUE</th><th>REQUIRED / OPTIONAL</th><th>DESCRIPTION</th><th>EXAMPLE</th></tr>
<tr><td>-u <folder_or_file></td><td>Required</td><td>Add the specified file or folder to the Predefined Trusted Updater List</td><td>N/A

Note
This parameter requires the use of the -t <type_of_object> value.</td></tr>
<tr><td>-t <type_of_object></td><td>Required</td><td>Specify the type of object to add to the Predefined Trusted Updater List located in -u <folder_or_file>

Available objects types are as follows:

process — Indicates only EXE file types

file — Indicates only MSI and BAT file types

folder — Indicates all EXE, MSI, and BAT files in the specified folder

folderandsub — Indicates all EXE, MSI, and BAT files in the specified folder and related subfolders</td><td>SLCmd.exe -p <admin_password> add predefinedtrustedupdater -u C:\Windows\notepad.exe -t process</td></tr>
<tr><td>-p <parent_process></td><td>Optional</td><td>Add the full file path to the specified parent process used to invoke the</td><td>SLCmd.exe -p <admin_password> add predefinedtrust</td></tr>
</table>

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

Windows Update Support

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

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

The following table lists the available abbreviated forms of parameters.

TABLE 6-31. Abbreviations and Uses

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

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

TABLE 6-32. Windows Update Support Commands

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

Blocked File Notification Commands

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

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

The following table lists the available abbreviated forms of parameters.

TABLE 6-33. Abbreviations and Uses

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

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

TABLE 6-34. Blocked File Notification Commands

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

Configuration File Commands

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

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

The following table lists the available abbreviated forms of parameters.

TABLE 6-35. Abbreviations and Uses

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

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

TABLE 6-36. Configuration File Commands

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

Fileless Attack Prevention Commands

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

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

The following table lists the available abbreviated forms of parameters.

TABLE 6-37. Abbreviations and Uses

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

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

TABLE 6-38. Fileless Attack Prevention Commands

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

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

Note

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

Maintenance Mode Commands

Perform actions related to Maintenance Mode 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 6-39. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
approvedlist	al	Manage Approved List in Maintenance Mode
maintenancemode	mtm	Manage Maintenance Mode
maintenancemodeschedule	mtms	Manage Maintenance Mode schedule

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

TABLE 6-40. Maintenance Mode Commands

COMMAND	PARAMETER	DESCRIPTION
start maintenancemode		Start Maintenance Mode For example, type: SLCmd.exe -p <admin_password> start maintenancemode
	-scan quarantine	Start Maintenance Mode and enable file scanning after the maintenance period. Safe Lock scans files that are created/executed/modified during the period and quarantine detected files. Safe Lock adds files that are not detected as malicious to the Approved List. For example, type: SLCmd.exe -p <admin_password> start maintenancemode -scan quarantine

COMMAND	PARAMETER	DESCRIPTION
	`-scan al`	Start Maintenance Mode and enable file scanning after the maintenance period. Safe Lock scans files that are created/ executed/modified files during the period and adds these files (including files that are detected as malicious) to the Approved List. For example, type: `SLCmd.exe -p <admin_password> start maintenancemode -scan al`
`stop` `maintenancemode`		Stop Maintenance Mode For example, type: `SLCmd.exe -p <admin_password> stop maintenancemode` **Note** You cannot stop Maintenance Mode when an agent is preparing to leave Maintenance Mode.
	`-discard`	Stop Maintenance Mode and do not add files in the file queue to the Approved List For example, type: `SLCmd.exe -p <admin_password> stop maintenancemode discard` **Note** You cannot stop Maintenance Mode when an agent is preparing to leave Maintenance Mode.
`set` `maintenancemodeschedule`	`-start` YYYY-MM-DDTHH:MM:SS `-end` YYYY-MM-DDTHH:MM:SS	Set the schedule for Maintenance Mode For example, type: `SLCmd.exe -p <admin_password> set maintenancemodeschedule -start`

COMMAND	PARAMETER	DESCRIPTION
		`2019-04-07T01:00:00 -end 2019-04-07T05:00:00` **Note** • You cannot set the Maintenance Mode schedule when an agent is already in Maintenance Mode or is preparing to leave Maintenance Mode. • If you configure the Maintenance Mode schedule to start earlier than the current time, the system starts the maintenance period immediately after you save the settings.
	`-start` YYYY-MM-DDTHH:MM:SS `-end` YYYY-MM-DDTHH:MM:SS `-scan qaurantine`	Use this command to configure the following: • Set the schedule for Maintenance Mode • Enable file scanning after the maintenance period. Safe Lock scans files that are created/executed/modified during the period and quarantine detected files. Safe Lock adds files that are not detected as malicious to the Approved List. For example, type: `SLCmd.exe -p <admin_password> set maintenancemodeschedule -start 2019-04-07T01:00:00 -end 2019-04-07T05:00:00 -scan quarantine`

COMMAND	PARAMETER	DESCRIPTION
		Note • You cannot set the Maintenance Mode schedule when an agent is already in Maintenance Mode or is preparing to leave Maintenance Mode. • If you configure the Maintenance Mode schedule to start earlier than the current time, the system starts the maintenance period immediately after you save the settings.
	`-start` YYYY-MM-DDTHH:MM:SS `-end` YYYY-MM-DDTHH:MM:SS `-scan al`	Use this command to configure the following: • Set the schedule for Maintenance Mode • Enable file scanning after the maintenance period. Safe Lock scans files that are created/executed/modified during the period and adds these files (including files that are detected as malicious) to the Approved List. For example, type: `SLCmd.exe -p <admin_password> set maintenancemodeschedule -start 2019-04-07T01:00:00 -end 2019-04-07T05:00:00 -scan al`

COMMAND	PARAMETER	DESCRIPTION
		Note • You cannot set the Maintenance Mode schedule when an agent is already in Maintenance Mode or is preparing to leave Maintenance Mode. • If you configure the Maintenance Mode schedule to start earlier than the current time, the system starts the maintenance period immediately after you save the settings.
remove `maintenancemodeschedule`		Clear the Maintenance Mode schedule settings For example, type: `SLCmd.exe -p <admin_password> remove maintenancemodeschedule` **Note** You cannot delete the schedule settings when an agent is already in Maintenance Mode or is preparing to leave Maintenance Mode.
show `maintenancemode`		Display the Maintenance Mode status For example, type: `SLCmd.exe -p <admin_password> show maintenancemode`
show `maintenancemodeschedule`		Display the Maintenance Mode schedule settings

COMMAND	PARAMETER	DESCRIPTION
		For example, type: `SLCmd.exe -p <admin_password> show maintenancemodeschedule`

Important

Before using Maintenance Mode, apply the required updates on the following supported platforms:

- For Windows 2000 Service Pack 4, apply the update KB891861 from the Microsoft Update Catalog website.
- For Windows XP SP1, upgrade to Windows XP SP2.

Note

- Before starting Maintenance Mode, perform an agent update on endpoints.
- To reduce risk of infection, run only applications from trusted sources on endpoints during the maintenance period.
- Agents start one scheduled maintenance period at a time. If you configure a new maintenance period, the system overwrites existing maintenance schedule that has not started yet.
- When the agent is about to leave Maintenance Mode, restarting the agent endpoint prevents Safe Lock from adding files in the queue to the Approved List.
- During the maintenance period, you cannot perform agent patch updates on endpoints.
- When Maintenance Mode is enabled, Safe Lock does not support Windows updates that require restarting an endpoint during the maintenance period.
- To run an installer that deploys files to a network folder during the maintenance period, Safe Lock must have access permission to the network folder.

Chapter 7

Managing Agents Remotely

This chapter describes remote Trend Micro Safe Lock agent management.

Topics in this chapter include:

The Remote Setup Tool (SLrst)

You can use the Remote Setup Tool to perform silent installations, patching, and uninstallations of the Safe Lock agent program using a command line interface (CLI).

`SLrst.exe` remotely performs operations on target endpoints while target endpoints directly access the Safe Lock Intelligent Manager server.

By default, Safe Lock Intelligent Manager stores the `SLrst.exe` file in the following location:

```
<Safe_Lock_Intelligent_Manager_installation_folder>\CmdTools
\RemoteAgentSetupTool\
```

The Remote Setup Tool uses the following syntax for all CLI functions:

`SLrst` `<targets CSV file>` `<parameter>`

Type **`SLrst`** at the command prompt and press ENTER to view an example of the Remote Setup Tool syntax.

Important

Only a Safe Lock Intelligent Manager administrator with Windows administrator privileges can use **`SLrst`** at the command line interface (CLI).

Tip

Optionally, copy the entire `RemoteAgentSetupTool` folder containing `SLrst.exe` from the `Program Files` folder to other locations to run the program. `SLrst.exe` is designed to run from within the `RemoteAgentSetupTool` folder on any endpoint in your network with .NET Framework 2.0 or 3.5 installed, with `SLrst.exe` added to the Safe Lock Approved List or with Application Lockdown turned off, and with access to the Safe Lock Intelligent Manager server.

The following table lists the functions available using the **`SLrst`** program.

TABLE 7-1. SLrst Remote Agent Setup Parameters

PARAMETER	FUNCTION
`--install`	Deploys and installs the Safe Lock agent on the endpoint See *Remote Installation Considerations on page 7-3*.
`--patch`	Patches the Safe Lock agent
`--reboot`	Restarts the endpoint (required if you want to reinstall the Safe Lock agent) See *Restarting Agents Remotely on page 7-21* **Note** The `reboot` function is not compatible on systems running Windows 2000 platforms. Manually restart endpoints running Windows 2000 platforms if you want to reinstall the Safe Lock agent.
`--uninstall`	Uninstalls the Safe Lock agent from the endpoint See *Uninstalling Agents Remotely on page 7-20*

Remote Installation Considerations

Before you remotely install Safe Lock agents, ensure the following:

- Safe Lock Intelligent Manager is installed on the server endpoint.
- Safe Lock agent versions earlier than 1.1 are not installed on target endpoints.

  See *Agent Upgrade Preparation on page 1-20*.
- Network, target endpoints, and the server endpoint firewall settings allow for the following:
  - Safe Lock Intelligent Manager ports (by default 8000, 8001, and 14336)
  - File sharing services
  - WMI services

    - IPC services
- Target endpoints have the following settings:
    - Simple File Sharing is disabled. (Windows XP)
    - File sharing is enabled.
    - A local account has access to the default share `admin$`.
    - Windows Management Instrumentation (WMI) service is enabled.
    - Windows Interprocess Communications (IPC) service is enabled.
- Target endpoints are not running Windows Installer sessions. Specifically, confirm that Windows Update is not updating the endpoint in the background.

Preparing Windows Server 2003 for Remote Installations

Before running Safe Lock remote installations, follow this procedure to prepare components for the following Windows versions:

- Windows Server 2003
- Windows Server 2003 R2

Procedure

1. Turn off Windows Firewall.
2. Turn on File and Printer Sharing for Microsoft Networks.
    a. Go to **Start** > **Control Panel** > **Network Connections**.
    b. Right-click **Local Area Connection** and then select **Properties**.
    c. Select **File and Printer Sharing for Microsoft Networks**.

Preparing Windows Server 2008 for Remote Installations

Before running Safe Lock remote installations, follow this procedure to prepare components for the following Windows versions:

- Windows Server 2008
- Windows Server 2008 R2

Procedure

1. Turn off Windows Firewall.
2. Turn off User Account Control by editing the registry.
   a. Open **`Registry Editor`** (**`regedit.exe`**).

      For example, go to **Start** > **Run...**, type `regedit`, and then press ENTER.

   b. Locate and click the following registry subkey: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`.

   c. On the right, locate the following entry: `LocalAccountTokenFilterPolicy`.

      If the entry does not exist, do the following to create it:

      i. Go to **Edit** > **New**.

      ii. Select **DWORD Value**.

      iii. Type `LocalAccountTokenFilterPolicy` and then press ENTER.

   d. Right-click `LocalAccountTokenFilterPolicy` and then select **Modify**.

   e. In the **Value** field, type `1`.

   f. Click **OK**.

   g. Close **`Registry Editor`**.
3. Turn on Network Discovery for each user account that will log on the endpoint.

a. Go to **Start** > **Control Panel** > **Network and Sharing Center**.

b. Right-click **Local Area Connection** and then select **Properties**.

c. Select **File and Printer Sharing for Microsoft Networks**.

Preparing Windows Server 2012 for Remote Installations

Before running Safe Lock remote installations, follow this procedure to prepare components for the following Windows versions:

- Windows Server 2012
- Windows Server 2012 R2

Procedure

1. Turn off Windows Firewall.
2. Turn off User Account Control by editing the registry.

   a. Open **`Registry Editor`** (**`regedit.exe`**).

      For example, go to **Start** > **Run...**, type `regedit`, and then press ENTER.

   b. Locate and click the following registry subkey: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`.

   c. On the right, locate the following entry: `LocalAccountTokenFilterPolicy`.

      If the entry does not exist, do the following to create it:

      i. Go to **Edit** > **New**.

      ii. Select **DWORD Value**.

      iii. Type `LocalAccountTokenFilterPolicy` and then press ENTER.

   d. Right-click `LocalAccountTokenFilterPolicy` and then select **Modify**.

e. In the **Value** field, type `1`.

f. Click **OK**.

g. Close **`Registry Editor`**.

3. Turn on Network Discovery for each user account that will log on the endpoint.

   a. Go to **Start** > **Control Panel** > **All Control Panel Items** > **Network and Sharing Center**.

   b. From the left panel, click **Change advanced sharing settings** and click **Domain (current profile)** drop-down list.

   c. Select **Turn on network discovery**.

Preparing Windows Server 2016 for Remote Installations

Before running Safe Lock remote installations, follow this procedure to prepare components for the following Windows versions:

- Windows Server 2016 (Standard) (64-bit)
- Windows Storage Server 2016

Procedure

1. Turn off Windows Firewall.
2. Turn off User Account Control by editing the registry.

   a. Open **`Registry Editor`** (**`regedit.exe`**).

   For example, go to **Start** > **Run...**, type `regedit`, and then press ENTER.

   b. Locate and click the following registry subkey: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`.

   c. On the right, locate the following entry: `LocalAccountTokenFilterPolicy`.

If the entry does not exist, do the following to create it:

i. Go to **Edit** > **New**.

ii. Select **DWORD Value**.

iii. Type `LocalAccountTokenFilterPolicy` and then press ENTER.

d. Right-click `LocalAccountTokenFilterPolicy` and then select **Modify**.

e. In the **Value** field, type `1`.

f. Click **OK**.

g. Close **`Registry Editor`**.

3. Turn on Network Discovery for each user account that will log on the endpoint.

a. Go to **Start** > **Control Panel** > **All Control Panel Items** > **Network and Sharing Center** > **Advanced sharing settings**.

b. Select **Turn on network discovery** and **Turn on automatic setup of network connected devices**.

Preparing Windows XP for Remote Installations

Before running Safe Lock remote installations, follow this procedure to prepare components for the following Windows versions:

- Windows XP

Procedure

1. Turn off Windows Firewall.
2. Turn on File and Printer Sharing for Microsoft Networks.

a. Go to **Start** > **Control Panel** > **Network Connections**.

b. Right-click **Local Area Connection** and then select **Properties**.

c. Select **File and Printer Sharing for Microsoft Networks**.

3. Disable Simple File Sharing.

Preparing Windows 7 for Remote Installations

Before running Safe Lock remote installations, follow this procedure to prepare components for the following Windows versions:

- Windows 7

Procedure

1. Turn off Windows Firewall.
2. Turn off User Account Control by editing the registry.
   a. Open **`Registry Editor`** (**`regedit.exe`**).

      For example, go to **Start** > **Run...**, type `regedit`, and then press ENTER.

   b. Locate and click the following registry subkey: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`.

   c. On the right, locate the following entry: `LocalAccountTokenFilterPolicy`.

      If the entry does not exist, do the following to create it:

      i. Go to **Edit** > **New**.

      ii. Select **DWORD Value**.

      iii. Type `LocalAccountTokenFilterPolicy` and then press ENTER.

   d. Right-click `LocalAccountTokenFilterPolicy` and then select **Modify**.

   e. In the **Value** field, type `1`.

   f. Click **OK**.

   g. Close **`Registry Editor`**.

3. Turn on Network Discovery for each user account that will log on the endpoint.

Preparing Windows 8 for Remote Installations

Before running Safe Lock remote installations, follow this procedure to prepare components for the following Windows versions:

- Windows 8
- Windows 8.1

Procedure

1. Turn off Windows Firewall.
2. Turn off User Account Control by editing the registry.
   a. Open **`Registry Editor`** (**`regedit.exe`**).

      For example, go to **Start** > **Run...**, type `regedit`, and then press ENTER.

   b. Locate and click the following registry subkey: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`.

   c. On the right, locate the following entry: `LocalAccountTokenFilterPolicy`.

      If the entry does not exist, do the following to create it:

      i. Go to **Edit** > **New**.

      ii. Select **DWORD Value**.

      iii. Type `LocalAccountTokenFilterPolicy` and then press ENTER.

   d. Right-click `LocalAccountTokenFilterPolicy` and then select **Modify**.

   e. In the **Value** field, type `1`.

   f. Click **OK**.

g. Close **Registry Editor**.

3. Turn on Network Discovery for each user account that will log on the endpoint.

   a. Go to **Start** > **Control Panel** > **Network and Sharing Center**.

   b. Right-click **Local Area Connection** and then select **Properties**.

   c. Select **File and Printer Sharing for Microsoft Networks**.

Preparing Windows 10 for Remote Installations

Before running Safe Lock remote installations, follow this procedure to prepare components for the following Windows versions:

- Windows 10 Enterprise
- Windows 10 IoT Enterprise
- Windows 10 Professional
- Windows 10 Creators Update (Redstone 2)
- Windows 10 Fall Creators Update (Redstone 3)
- Windows 10 April 2018 Update (Redstone 4)
- Windows 10 October 2018 Update (Redstone 5)

Procedure

1. Turn off Windows Firewall.
2. Turn off User Account Control by editing the registry.

   a. Open **Registry Editor** (**regedit.exe**).

   For example, go to **Start** > **Run...**, type `regedit`, and then press ENTER.

   b. Locate and click the following registry subkey: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`.

c. On the right, locate the following entry: `LocalAccountTokenFilterPolicy`.

   If the entry does not exist, do the following to create it:

   i. Go to **Edit** > **New**.

   ii. Select **DWORD Value**.

   iii. Type `LocalAccountTokenFilterPolicy` and then press ENTER.

d. Right-click `LocalAccountTokenFilterPolicy` and then select **Modify**.

e. In the **Value** field, type `1`.

f. Click **OK**.

g. Close **`Registry Editor`**.

3. Turn on Network Discovery for each user account that will log on the endpoint.

   a. Go to **Start** > **Control Panel** > **All Control Panel Items** > **Network and Sharing Center** > **Advanced sharing settings**.

   b. Select **Turn on network discovery** and **Turn on automatic setup of network connected devices**.

Preparing the Agent Target Files

The Remote Setup Tool utilizes two files when processing commands.

- `endpoint_info.csv`: Stores relevant connection information for agent endpoints
- `targets.csv`: Targets specific endpoints for the current deployment

Important

To edit `endpoint_info.csv` or `targets.csv` files that are in the Program Files folder, copy them to a path with file write priveleges, edit them, then copy them back to the suggested path below.

Procedure

1. Prepare the "endpoint info" file and save it as `endpoint_info.csv` in the following path:

   ```
   <Safe_Lock_Intelligent_Manager_installation_folder>
   \CmdTools\RemoteAgentSetupTool\
   ```

   See *Endpoint Info File Specifications on page 7-14*.

2. Create the "targets" file or batches of files and save them in the following path:

   ```
   <Safe_Lock_Intelligent_Manager_installation_folder>
   \CmdTools\RemoteAgentSetupTool\
   ```

   See *Targets File Specifications on page 7-13*.

Targets File Specifications

The "targets" file used during remote agent installation contains the IP address of target endpoints. The targets file uses CSV format and has the file name `targets.csv` by default.

Tip

Remote agent setup using the **`SLrst`** command line program can be done in batches using more than one targets file and the same endpoint info file. The endpoint info file can contain information for endpoints outside the scope of the target endpoints listed in the targets file.

To create customized "targets" CSV files, specify the IP address of each target endpoint. Use one line per record. Use of spaces, quotation marks, or other delimiters is not supported.

For example:

VALID
Targeted IP 10.1.199.199 10.1.199.201 192.168.1.20

NOT VALID
10.1.199.199,10.1.199.201
"10.1.199.199" "10.1.199.201" "192.168.1.20"

Tip

The targets file can be reused. Therefore, you can use the same targets file to deploy, patch, and uninstall a batch of target endpoints. Check the log information and make backups of any critical information each time you run the **SLrst** program. **SLrst** ignores and overwrites any log information in the file each time it is run.

Endpoint Info File Specifications

The "endpoint info" file used during remote agent installation contains the IP address, user name, and password of a local account on each target endpoint with access to the default share `admin$`.

Tip

Trend Micro recommends using the local administrator account on each target endpoint for deployment.

The endpoint info file uses CSV format. The filename must be `endpoint_info.csv`.

Note

To create the "endpoint info" CSV file, divide the records into fields for IP address, user name, and password. Use one line per record. Separate these fields using a comma. Use of spaces, quotation marks, or other delimiters is not supported.

For example:

VALID

```
IP,Username,Password
10.1.199.199,Administrator,password1
10.1.199.200,Administrator,password2
10.1.199.201,Administrator,password3
192.168.1.20,Daniel,his_pwd
192.168.1.21,Sophia,her_pwd
```

NOT VALID

```
10.1.199.201,Administrator,password3,192.168.1.20,Daniel,his_pwd
```

```
"10.1.199.199","Administrator","password1"
"10.1.199.200""Administrator","password2"
"10.1.199.201","Administrator","password3"
"192.168.1.20","Daniel","his_pwd"
"192.168.1.21","Sophia","her_pwd"
```

Microsoft Excel will save a chart as a CSV using valid formatting.

Downloading an Up-to-Date Agent Installer Package

Procedure

1. Go to **Administration** > **Components** > **Updates** in the navigation at the top of the web console.

   The **Component Updates** screen appears.

2. Click **Download Agent Installer Package**.

3. Select the language the installation package.

   Your browser downloads the most up-to-date agent installer package.

Note

The agent installer package is considered up-to-date by Safe Lock Intelligent Manager based on the component versions displayed on the **Component Updates** screen. If the cached agent installer package is not up-to-date, Safe Lock Intelligent Manager prepares and caches an up-to-date package before starting the download.

Preparing an up-to-date agent installer package is system-intensive. Depending on the hardware running Safe Lock Intelligent Manager, preparing an up-to-date agent installer package can take a while.

4. To use the downloaded agent installer package for remote installations using the **`SLrst`** program at the command line interface (CLI), copy the downloaded agent installer package to the path used by **`SLrst`**.

   For example, if you installed Safe Lock Intelligent Manager to the default path on the C drive, copy the downloaded agent installer package to the following path: `c:\Program Files\Trend Micro\Safe Lock Intelligent Manager \CmdTools\RemoteAgentSetupTool\`.

Important

Users should manually compress the downloaded file into the package file (`.zip`).

The package file name must follow the format:
`TMSL_TXOne_<language_abbreviation>.zip`

For example:

VALID	NOT VALID
`TMSL_TXOne_EN.zip`	`TMSL_TXOne_EN (1).zip`
`TMSL_TXOne_JA.zip`	`TMSL_TXOne_EN_1.zip`

Installing Agents Remotely

Important

- Before remotely managing Safe Lock agents using the Remote Setup Tool, prepare the "endpoint info" and "targets" files.

  See *Preparing the Agent Target Files on page 7-12*.

- Before remotely installing Safe Lock agents, download an up-to-date agent installer package.

  See *Downloading an Up-to-Date Agent Installer Package on page 4-3*.

Use the **SLrst.exe** program at the command line interface (CLI) to install one or more Safe Lock agents connected to the network.

Procedure

1. Open a command prompt window with Windows administrator privileges.
2. Navigate to the Trend Micro Safe Lock Intelligent Manager "Safe Lock Remote Setup Tool" program folder using the **cd** command.

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

   cd /d "c:\Program Files\Trend Micro\Safe Lock Intelligent Manager\CmdTools\RemoteAgentSetupTool\"
3. To remotely install agents using the default targets file `targets.csv`, type the following at the command prompt:

   SLrst.exe `targets.csv --install`

   The remote setup tool looks for targets in the `targets.csv` file. For large production environments, Trend Micro recommends that you install agents in batches. Run the remote setup tool separately for each CSV batch file.
4. At the prompt, provide a password used to access the Safe Lock agent program and then confirm the password.

5. Select the target language.
6. Select to perform a prescan for malware on the target endpoints before installing the Safe Lock agent.
7. Select to enable root cause analysis on the target endpoints.
8. Monitor the progress of the remote installation process. Safe Lock writes log information directly in the CSV file (by default, `targets.csv`) specified in the command line argument.

Customizing Agent Installation Remotely Using a Setup.ini File

Procedure

1. Navigate to the "package" folder of the Trend Micro Safe Lock Intelligent Manager installation folder.

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

   "C:\Program Files\Trend Micro\Safe Lock Intelligent Manager\CmdTools \RemoteAgentSetupTool\package"

2. Unzip the `TMSL3.0_EN` file.
3. In the unzipped file, open the `Setup.ini` file and make changes to installation parameters as required. For details on installation parameters and their possible values, see *Setup.ini File Arguments on page 8-18*.
4. Zip the `TMSL3.0_EN` file and make sure it is saved to the installed path.
5. Install agents remotely. For details, see *Installing Agents Remotely on page 7-17*.

Applying Patches and Hotfixes to Agents Remotely

Important

- Before remotely managing Safe Lock agents using the Remote Setup Tool, prepare the "endpoint info" and "targets" files.

  See *Preparing the Agent Target Files on page 7-12*.

- Before remotely updating Safe Lock agents, download the latest agent patch or hotfix file using the Trend Micro Technical Support Download Center website: http://downloadcenter.trendmicro.com/

Use the **SLrst.exe** program at the command line interface (CLI) to install one or more Safe Lock agents connected to the network.

Procedure

1. Copy the downloaded agent patch or hotfix to the path used by **SLrst**.

   For example, if you installed Safe Lock Intelligent Manager to the default path on the C drive, copy the downloaded agent installer patch or hotfix to the following path: `c:\Program Files\Trend Micro\Safe Lock Intelligent Manager\CmdTools\RemoteAgentSetupTool\package\`

   Important

   The patch or hot fix file name must follow the format: `TMSL_TXOne_Hotfix_<language_abbreviation>.zip`

   For example:

VALID	NOT VALID
`TMSL_TXOne_Hotfix_EN.zip`	`TMSL_TXOne_Hotfix_EN (1).zip`
`TMSL_TXOne_Hotfix_JA.zip`	`TMSL_TXOne_Hotfix_EN_1.zip`

2. Navigate to the Trend Micro Trend Micro "Safe Lock Remote Setup Tool" folder inside the installation folder using the **cd** command.

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

cd /d "c:\Program Files\Trend Micro\Safe Lock Intelligent Manager\CmdTools\RemoteAgentSetupTool\"

3. To remotely patch or hotfix agents using the default targets file `targets.csv`, type the following at the command prompt:

   SLrst.exe `targets.csv --patch`

   The remote setup tool looks for targets in the `targets.csv` file. For large production environments, Trend Micro recommends that you patch or hotfix agents in batches. Run the remote setup tool separately for each CSV batch file.

4. At the prompt, provide the password used to access the Safe Lock agent program.

5. Monitor the progress of the remote patch or hotfix. Safe Lock writes log information directly in the CSV file (by default, `targets.csv`) specified in the command line argument.

Uninstalling Agents Remotely

Important

Before remotely managing Safe Lock agents using the Remote Setup Tool, prepare the "endpoint info" and "targets" files.

See *Preparing the Agent Target Files on page 7-12*.

Use the **SLrst.exe** program at the command line interface (CLI) to uninstall one or more Safe Lock agents connected to the network.

Procedure

1. Open a command prompt window with Windows administrator privileges.

2. Navigate to the Trend Micro Safe Lock Intelligent Manager "Safe Lock Remote Setup Tool" folder inside the installation folder using the **cd** command.

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

```
cd /d "c:\Program Files\Trend Micro\Safe Lock Intelligent Manager\CmdTools
\RemoteAgentSetupTool\"
```

3. To remotely install agents using the default targets file `targets.csv`, type the following at the command prompt:

   ```
   SLrst.exe targets.csv --uninstall
   ```

   The remote setup tool looks for targets in the `targets.csv` file. For large production environments, Trend Micro recommends that you uninstall agents in batches. Run the remote setup tool separately for each CSV batch file.

4. At the prompt, provide the password used to access the Safe Lock agent program.

5. Monitor the progress of the remote uninstallation process. Safe Lock writes log information directly in the CSV file (by default, `targets.csv`) specified in the command line argument.

6. Restart endpoints to complete the uninstallation process.

Restarting Agents Remotely

Important

Before remotely managing Safe Lock agents using the Remote Setup Tool, prepare the "endpoint info" and "targets" files.

See *Preparing the Agent Target Files on page 7-12*.

Use the **SLrst.exe** program at the command line interface (CLI) to restart one or more Safe Lock agents connected to the network.

Procedure

1. Open a command prompt window with Windows administrator privileges.

2. Navigate to the Trend Micro Safe Lock Intelligent Manager "Safe Lock Remote Setup Tool" folder inside the installation folder using the **cd** command.

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

```
cd /d "c:\Program Files\Trend Micro\Safe Lock Intelligent Manager\CmdTools
\RemoteAgentSetupTool\"
```

3. To remotely install agents using the default targets file `targets.csv`, type the following at the command prompt:

   ```
   SLrst.exe targets.csv --reboot
   ```

   The remote setup tool looks for targets in the `targets.csv` file. For large production environments, Trend Micro recommends that you restart agents in batches. Run the remote setup tool separately for each CSV batch file.

4. Monitor the progress of the remote restart process. Safe Lock writes log information directly in the CSV file (by default, `targets.csv`) specified in the command line argument.

   Endpoints restart automatically after receiving the command.

The Remote Tasks Tool (SLtasks)

You can use the Remote Tasks Tool to perform the following tasks:

- Initialize agent Approved Lists
- Lock down agents
- Match licenses
- Deploy patch or hotfixes without disabling firewall settings on agents
- Query the status of agents using the command line interface (CLI)
- Move agents to a new Safe Lock Intelligent Manager server using the CLI
- Remotely change the administrator password

By default, Safe Lock Intelligent Manager stores the `SLtasks.exe` file is the following location:

```
<Safe_Lock_Intelligent_Manager_installation_folder>\CmdTools
\RemoteAgentTasksTool\
```

Important

Only a Safe Lock Intelligent Manager administrator with Windows administrator privileges can use **SLtasks** at the command line interface (CLI).

Removing Files from Agent Approved Lists

Procedure

1. Open a command prompt window with Windows administrator privileges.
2. Navigate to the Trend Micro Safe Lock Intelligent Manager "Safe Lock Remote Tasks Tool" folder inside the installation folder using the **cd** command.

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

   cd /d "c:\Program Files\Trend Micro\Safe Lock Intelligent Manager\CmdTools\RemoteAgentTasksTool\"
3. Log on the Safe Lock Intelligent Manager server by typing the following command:

   SLtasks.exe --logon
4. Type your Safe Lock Intelligent Manager credentials.

   The CLI confirms a successful log on to the server.

   Important

   - The logged on account must have "admin" or "Full Control" privilege to send tasks to agents.
   - To reduce network and endpoint impact, Safe Lock Intelligent Manager queries target agents for their configurations and then sends only tasks it determines are needed.
5. Generate a list of target agents. To limit the query to agents before or after a specific version, append --minversion and --maxversion to the command and type the agent version.

- **SLtasks.exe** --query --minversion <agent_version>
- **SLtasks.exe** --query --maxversion <agent_version>

Important

The <agent_version> must be in the form of x.x.xxxx. For example, 2.0.5000.

The results of the query are saved in query_results.csv.

Tip

Trend Micro recommends querying agent statuses before deploying any tasks. A warning message appears if the query results are out-of-date when attempting to deploy tasks.

6. List the target files in a CSV file of UTF-8 format. List the files in any of the following variations:

   - File name
   - File path with file name
   - File path with SHA-1 hash
   - File name and SHA-1 hash
   - SHA-1 hash

   For example, the following are all valid ways of listing the files:

   - cal.exe,
   - C:\Windows\system32\calc.exe,
   - C:\Windows \system32\9018A7D6CDBE859A430E794E73381F77C840BE0,
   - cal.exe,9018A7D6CDBE859A430E794E73381F77C840BE0
   - ,9018A7D6CDBE859A430E794E73381F77C840BE0,

7. Type the following syntax to remove items from all agent Approved Lists:

   SLtasks.exe `--removeitems <target_list_file_name>`

   Tip

   - To only remove approved items from a specific agent, append `--targetPC` to the command and type the endpoint name.

     For example:

     SLtasks.exe `<task_parameter> --targetPC <endpoint_name>`

8. Log off the Safe Lock Intelligent Manager server by typing the following command:

   SLtasks.exe `--logoff`

   The CLI confirms a successful log off from the server.

Renewing Agent Licenses

Procedure

1. Update the Intelligent Manager license.
2. Open a command prompt window with Windows administrator privileges.
3. Navigate to the Trend Micro Safe Lock Intelligent Manager "Safe Lock Remote Tasks Tool" folder inside the installation folder using the **cd** command.

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

   cd `/d` "c:\Program Files\Trend Micro\Safe Lock Intelligent Manager\CmdTools\RemoteAgentTasksTool\"

4. Log on the Safe Lock Intelligent Manager server by typing the following command:

   SLtasks.exe `--logon`

5. Type your Safe Lock Intelligent Manager credentials.

   The CLI confirms a successful log on to the server.

   Important

   - The logged on account must have "admin" or "Full Control" privilege to send tasks to agents.
   - To reduce network and endpoint impact, Safe Lock Intelligent Manager queries target agents for their configurations and then sends only tasks it determines are needed.

6. Generate a list of target agents. To limit the query to agents before or after a specific version, append `--minversion` and `--maxversion` to the command and type the agent version.

   - **`SLtasks.exe`** `--query --minversion <agent_version>`
   - **`SLtasks.exe`** `--query --maxversion <agent_version>`

   Important

   The `<agent_version>` must be in the form of `x.x.xxxx`. For example, `2.0.5000`.

   The results of the query are saved in `query_results.csv`.

   Tip

   Trend Micro recommends querying agent statuses before deploying any tasks. A warning message appears if the query results are out-of-date when attempting to deploy tasks.

7. Type the following command.

   `SLtasks.exe` `--match`

   The license of the target agents are immediately updated to match the Safe Lock Intelligent Manager's license.

8. Log off the Safe Lock Intelligent Manager server by typing the following command:

   SLtasks.exe --logoff

   The CLI confirms a successful log off from the server.

Applying Message Time Groups

Message time groups use message-sending cycles to add additional bandwidth control to automated messages sent from Safe Lock agents to the Safe Lock Intelligent Manager.

During a message-sending cycle, agents in the active group send automated messages, which include log and status as well as quarantined files to be scanned, to Safe Lock Intelligent Manager. When a message-sending cycle ends, the next group of agents becomes active and sends automated messages.

Agents outside the active group do not send automated messages. However, agents in all groups respond as soon as possible to direct requests from Safe Lock Intelligent Manager. For example, a request to send logs and status from the web console will be replied to by the target agent as soon as network connectivity allows.

Note

The following conditions apply to automated messages:

By default, Safe Lock Intelligent Manager puts all agents into one "always on" group.

During a message-sending cycle, messages are sent in the following order:

- Higher priority first
- Oldest (least recent) first

Applying Message Time Groups Using the Remote Tasks Tool

Use **SLtasks.exe** to apply message time groups to agents.

Procedure

1. Open a command prompt window with Windows administrator privileges.
2. Navigate to the Trend Micro Safe Lock Intelligent Manager "Safe Lock Remote Tasks Tool" folder inside the installation folder using the **cd** command.

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

   cd /d "c:\Program Files\Trend Micro\Safe Lock Intelligent Manager\CmdTools\RemoteAgentTasksTool\"
3. Log on the Safe Lock Intelligent Manager server by typing the following command:

   SLtasks.exe --logon
4. Type your Safe Lock Intelligent Manager credentials.

   The CLI confirms a successful log on to the server.
5. Query message time groups by typing the following command:

   SLtasks.exe --querygroup

   The results of the query are saved in group_info.csv.

   Important

   Applying message time groups requires querying message time groups, editing the results as needed, and then applying the configured message time groups to agents. A warning message appears if the query results are out-of-date when attempting to apply message time groups to agents.
6. Edit the group_info.csv to configure the following message time group controls:

COLUMN NAME	CONTROL DESCRIPTION
`Total Group Num`	Divide agents into any number of groups. **Tip** Set this value to 1 to turn the feature off.
`Own Group Index`	Set the message group ID number for the Safe Lock agent.
`Time Period`	Set a duration for how long each group is allowed to send messages to Safe Lock Intelligent Manager when that group's message-sending cycle is active.

7. Apply message time groups to agents using the configured `group_info.csv` file by typing the following command:

   `SLtasks.exe` `--applygroups`

   Important

   - The logged on account must have "admin" or "Full Control" privilege to apply message time groups to agents.
   - Only agents listed in `group_info.csv` receive the command.

8. Log off the Safe Lock Intelligent Manager server by typing the following command:

   `SLtasks.exe` `--logoff`

   The CLI confirms a successful log off from the server.

Applying Message Time Groups Using the Configuration File

Procedure

1. Access the **Export/Import Configuration** section from the Trend Micro Safe Lock console.

a. 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**.

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

c. Click the **Settings** menu item.

2. 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**.

3. Decrypt the configuration file.

4. From Windows Notepad or another text editor, edit the `MessageRandomization` parameter in the `ManagedMode` section:

COLUMN NAME	CONTROL DESCRIPTION
`TOTAL_GROUP_NUM`	Divide agents into any number of groups.
`OWN_GROUP_INDEX`	Set the message group ID number for the Safe Lock agent.
`TIME_PERIOD`	Set a duration for how long each group is allowed to send messages to Safe Lock Intelligent Manager when that group's message-sending cycle is active.

5. From the **Export/Import Configuration** section of the Trend Micro Safe Lock console, 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 new settings in the database file.

Applying Message Time Groups Using the Setup.ini File

Procedure

1. Edit the `MESSAGERANDOMIZATION` arguments in the `Setup.ini` file.

   a. From the Trend Micro Safe Lock Intelligent Manager folder, double-click `Setup.ini`.

   b. Edit the following arguments in the `MESSAGERANDOMIZATION` section:

Column Name	Control Description
`TOTAL_GROUP_NUM`	Divide agents into any number of groups.
`OWN_GROUP_INDEX`	Set the message group ID number for the Safe Lock agent.
`TIME_PERIOD`	Set a duration for how long each group is allowed to send messages to Safe Lock Intelligent Manager when that group's message-sending cycle is active.

2. Install the Safe Lock Intelligent Manager using Windows Installer or the command line interface (CLI) installer. For details, see *Installing from Windows* and *Installation Using the Command Line* from the Trend Micro Safe Lock Intelligent Manager™ Installation Guide.

Updating the Agent Password Remotely

Update the Safe Lock agent password remotely using Safe Lock Intelligent Manager.

Note

- This function is only available for users with administrator privileges. Full Control/ Read Only/Storage Device Control should be unable to change admin password remotely.
- If you are running Safe Lock agents with expired licenses and versions earlier than 2.0 Service Pack 1 Patch 2, updating the password remotely will not be functional.

Procedure

1. Open a command prompt window with Windows administrator privileges.
2. Navigate to the Trend Micro Safe Lock Intelligent Manager "Safe Lock Remote Tasks Tool" folder inside the installation folder using the **cd** command.
3. Log on the Safe Lock Intelligent Manager server by typing the following command:

   SLtasks.exe `--logon`
4. Type your Safe Lock Intelligent Manager credentials.

   The CLI confirms a successful log on to the server.
5. Generate a list of target agents. To limit the query to agents before or after a specific version, append `--minversion` and `--maxversion` to the command and type the agent version.

   - **SLtasks.exe** `--query --minversion <agent_version>`
   - **SLtasks.exe** `--query --maxversion <agent_version>`

   The results of the query are saved in `query_results.csv`.
6. Set the new administrator password on the target agents identified in `query_results.csv` by typing the following command:

   `--changepassword`

   Note

   - The password must be 8 to 64 alphanumeric characters. The following characters are not supported: | > < \ " spaces
   - Safe Lock Intelligent Manager does not require the old agent password to create a new one.
   - Ensure the new password matches the confirm password, otherwise the command will abort.
7. Log off the Safe Lock Intelligent Manager server by typing the following command:

SLtasks.exe --logoff

The CLI confirms a successful log off from the server.

Transferring Agents to Another Server

Procedure

1. On the target Safe Lock Intelligent Manager server, Do the following to generate the `results.ini` file:

   a. Open a command prompt window with Windows administrator privileges.

   b. Go to `%INSTALL_FOLDER%\CmdTools\Installer\` or include the directory in the system path.

   c. Type `Setup.exe -src registry -get -server_info` to generate the `results.ini`.

   Note

   By default, the system generates the `results.ini` file in the `%INSTALL_FOLDER%\CmdTools\Installer\` folder.

2. Copy the `results.ini` file to the source Safe Lock Intelligent Manager server with the agents you want to transfer.

3. On the source server, open a command prompt window with Windows administrator privileges.

4. Navigate to the Trend Micro Safe Lock Intelligent Manager "Safe Lock Remote Tasks Tool" folder inside the installation folder using the **cd** command.

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

   cd /d "c:\Program Files\Trend Micro\Safe Lock Intelligent Manager\CmdTools \RemoteAgentTasksTool\"

5. Log on the Safe Lock Intelligent Manager server by typing the following command:

   SLtasks.exe --logon

6. Type your Safe Lock Intelligent Manager credentials.

   The CLI confirms a successful log on to the server.

   Important

   - The logged on account must have "admin" or "Full Control" privilege to send tasks to agents.
   - To reduce network and endpoint impact, Safe Lock Intelligent Manager queries target agents for their configurations and then sends only tasks it determines are needed.

7. Generate a list of target agents. To limit the query to agents before or after a specific version, append `--minversion` and `--maxversion` to the command and type the agent version.

   - **`SLtasks.exe`** `--query --minversion <agent_version>`
   - **`SLtasks.exe`** `--query --maxversion <agent_version>`

   Important

   The `<agent_version>` must be in the form of `x.x.xxxx`. For example, `3.0.0000`.

   The results of the query are saved in `query_results.csv`.

   Tip

   Trend Micro recommends querying agent statuses before deploying any tasks. A warning message appears if the query results are out-of-date when attempting to deploy tasks.

8. (Optional) Edit the `query_results.csv` file to remove one or more agents from the list.

9. Start the agent migration process. Do the following:

   a. Execute the `SLtasks.exe --migratenewserver` command.

b. Type the path of the `results.ini` file.

10. On the target Safe Lock Intelligent Manager server, verify that migrated agents display on the Agent Management screen.

Chapter 8

Local Agent Installation

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

Topics in this chapter include:

Local Installation Overview

Procedure

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

   For details, see *Safe Lock Requirements on page 1-13*.

   WARNING!

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

   For details, see *Agent Upgrade Preparation on page 1-20*.

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

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

TABLE 8-1. Safe Lock Local Installation Methods

INSTALLATION METHOD	BENEFITS
Windows Installer	The Windows Installer provides simplified step-by-step installation wizard for first-time or single installation and is also suitable for preparing for mass deployment for cloned endpoint systems. For details, see *Installing from Windows on page 8-3*.
Command line interface installer	The command line interface (CLI) installer provides silent installation and can be integrated into a batch file for mass deployment. For details, see *Installation Using the Command Line on page 8-14*.

Note

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

For details, see *Customizing Installation Parameters on page 8-17*.

3. Configure the new installation.

   a. Open the Trend Micro Safe Lock console and set up the Approved List.

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

      For details, see *Setting Up the Approved List on page 5-2*.

   b. Modify the Trend Micro Safe Lock settings.

      Note

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

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

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

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

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

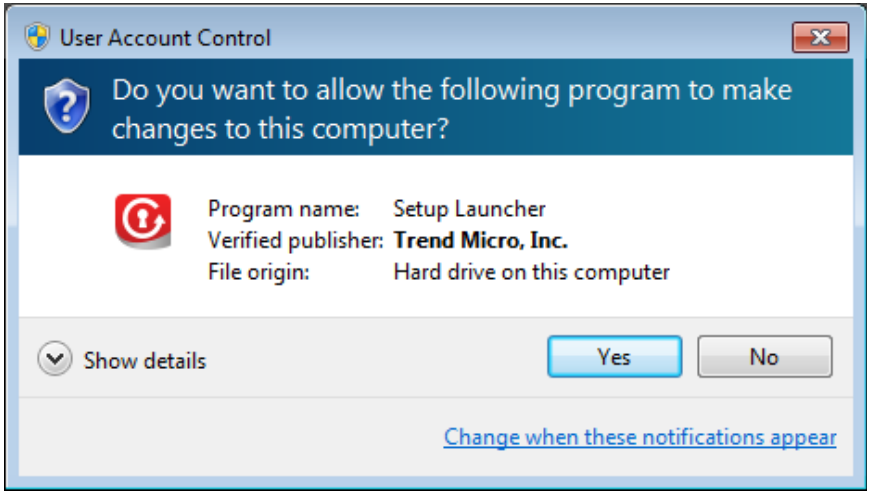
Installing from Windows

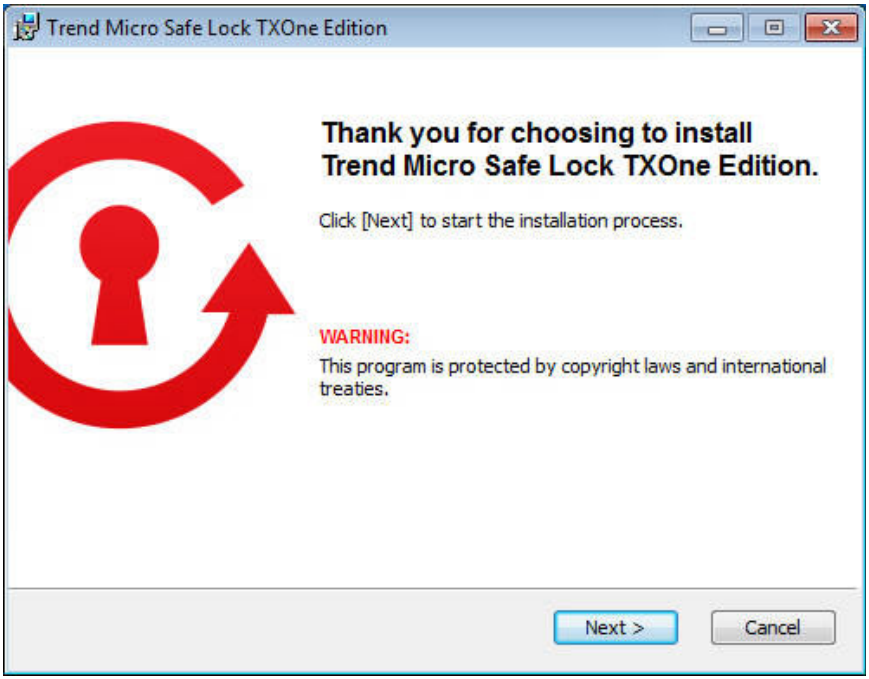
To install Trend Micro Safe Lock, you must log on using an account with administrator privileges.

Procedure

1. Double-click `SL_Install.exe`.

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

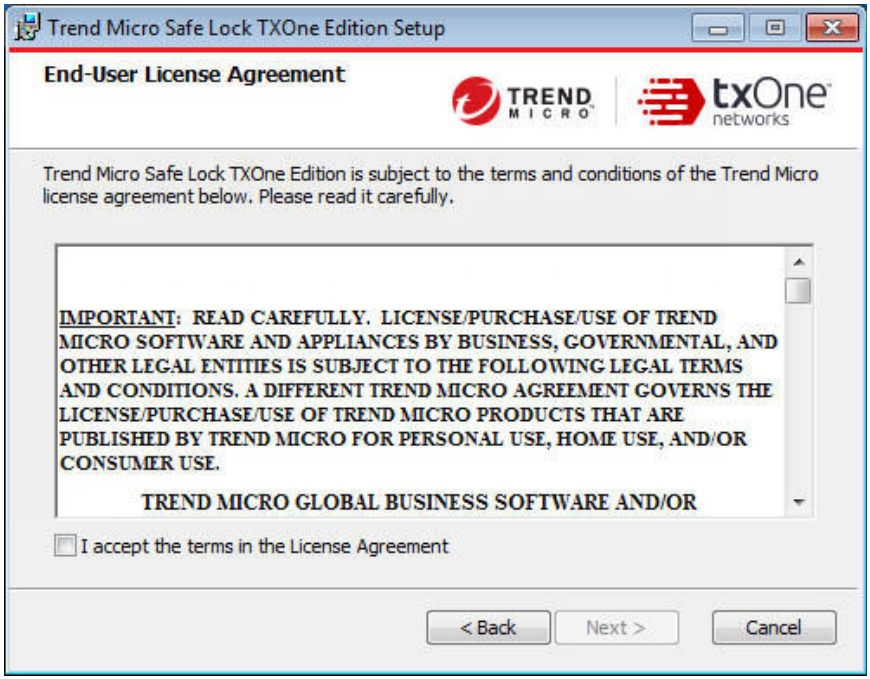




2. When the installation wizard opens, click **Next**.

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

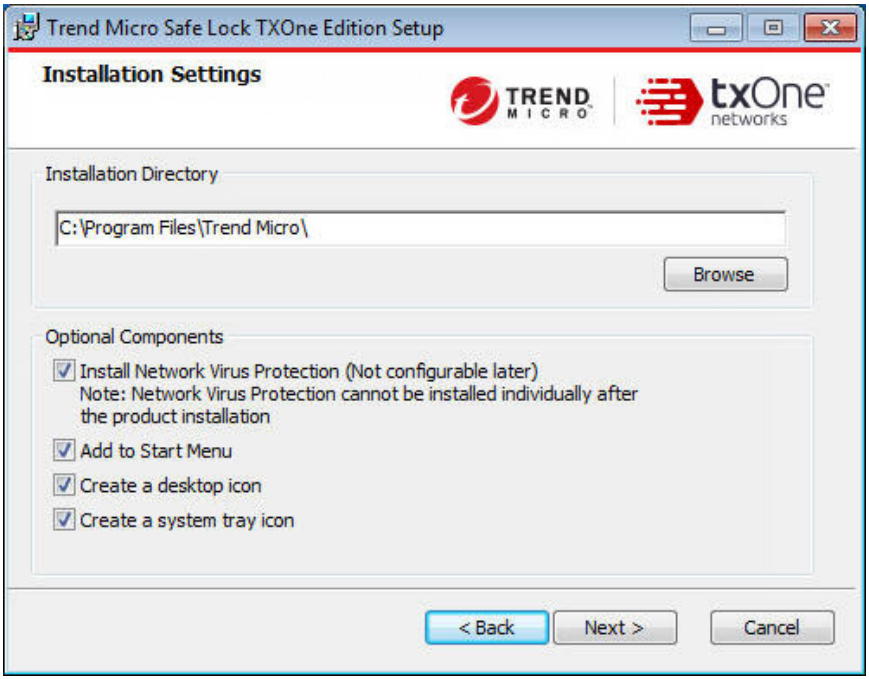
3. Read the license agreement, select **I accept the terms in the License Agreement**, and click **Next**.



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

Important

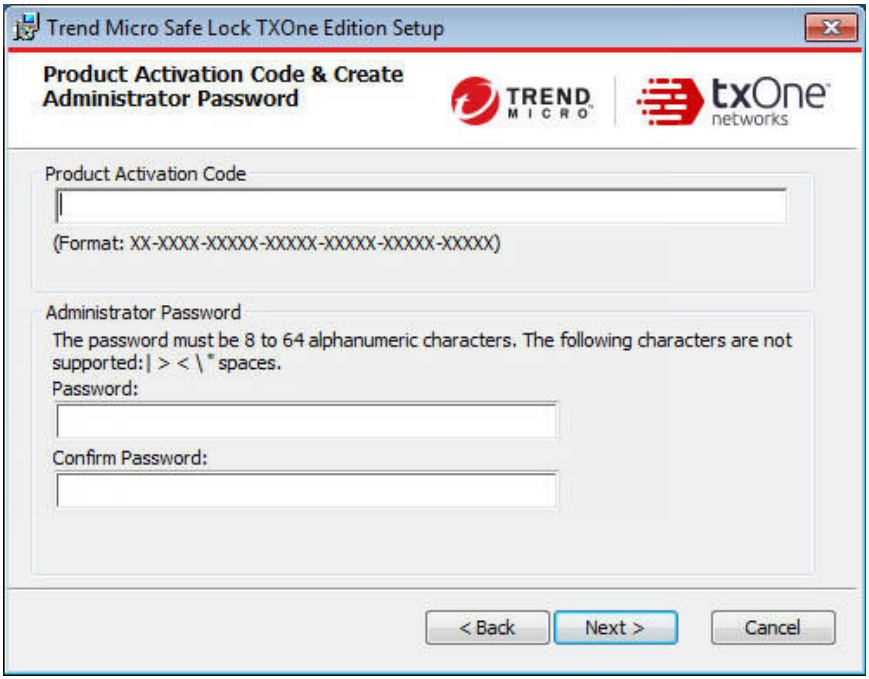
Network Virus Protection can only be installed during the initial program installation, but it can be disabled after installation, if necessary. See *Exploit Prevention Settings* in the Administrator's Guide for more information.



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

Note

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

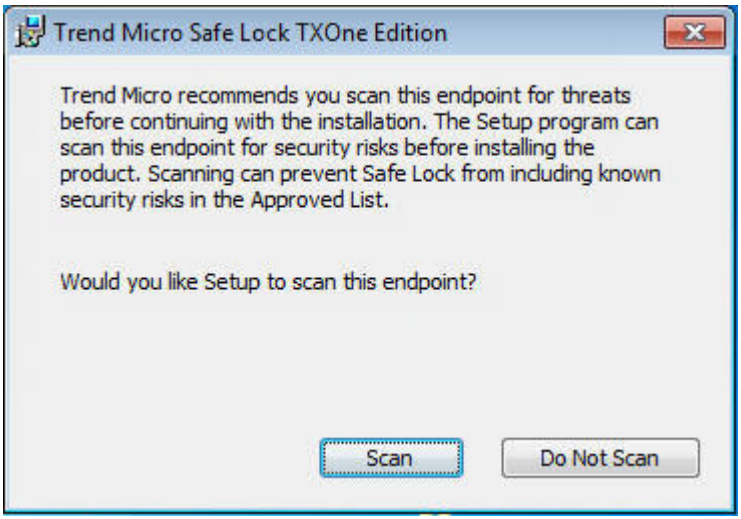


WARNING!

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

6. Click **Next**.

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



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

   - To scan the endpoint for threats, click **Scan**.

     a. The **Endpoint Prescan** window appears.

     b. To customize the scan settings, click **Edit Scan Settings**.

     c. Click **Scan Now**.

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

Note

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

For more information, see *Prescan Section on page 8-38*.

Tip

Trend Micro provides solutions for detecting and removing threats. For endpoints with limited or no network access, Trend Micro recommends using Trend Micro Portable Security. See *Trend Micro Portable Security Compatible on page 1-13*. For more information about this and other solutions from Trend Micro, go to http://trendmicro.com/.

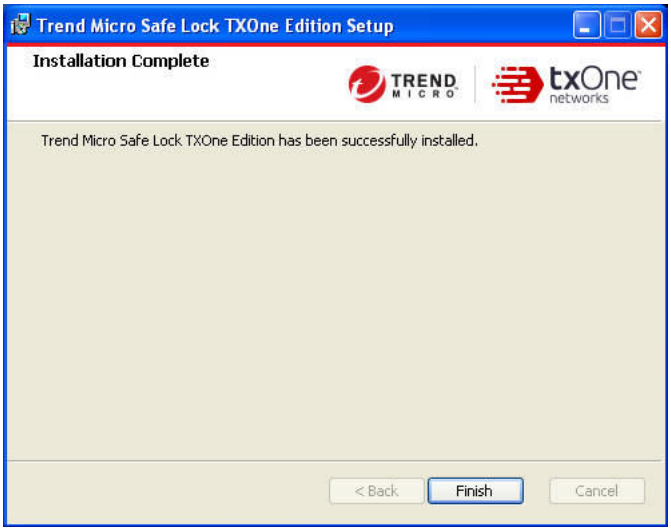
- To skip scanning, click **Do Not Scan**.

Note

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

For more information, see *Prescan Section on page 8-38*.

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



Note

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

Setting Up the Approved List

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

Procedure

1. Open the Safe Lock console.

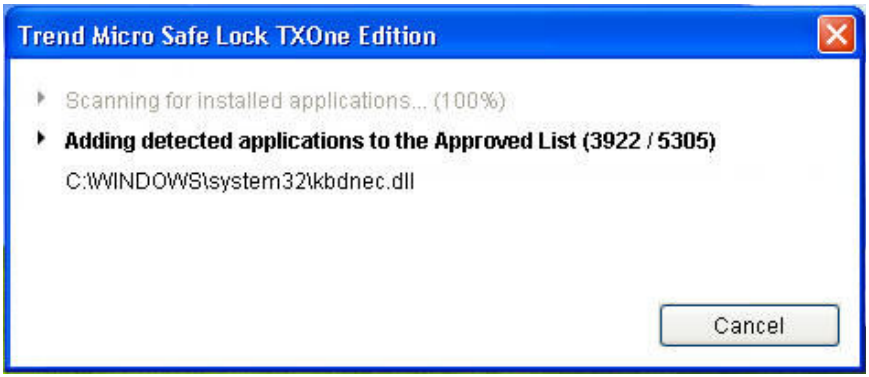
The Safe Lock log on screen appears.

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

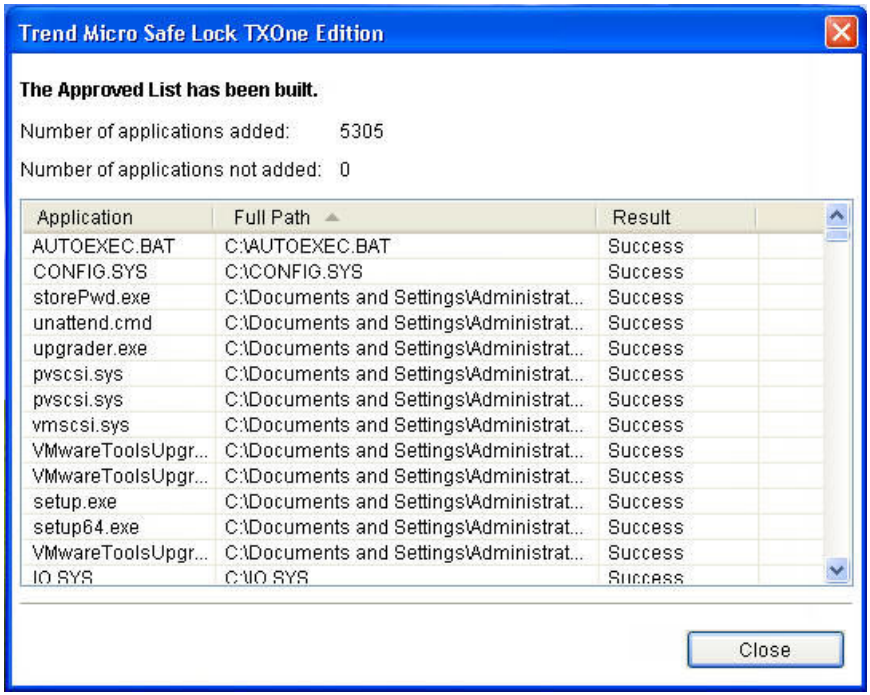
Safe Lock asks if you want to set up the Approved List now.

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

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



Safe Lock displays the Approved List Configuration Results.



Note

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

4. Click **Close**.

Installation Using the Command Line

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

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

WARNING!

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

Important

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

Note

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

Installer Command Line Interface Parameters

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

TABLE 8-2. Safe Lock Intelligent Manager Installer Command Line Options

PARAMETER	VALUE	DESCRIPTION
`-q`		Run the installer silently
`-p`	<administrator_password>	Specify the administrator password

PARAMETER	VALUE	DESCRIPTION
-d	<path>	Specify the installation path
-ac	<activation_code>	Specify the activation code
-nd		Do not create a desktop shortcut
-fw		Enable Network Virus Protection
-ns		Do not add a shortcut to the Start menu
-ni		Hide the task tray icon
-cp	<path>	Specify the Safe Lock configuration file **Note** The Safe Lock configuration file can be exported after installing Safe Lock.
-lp	<path>	Specify the Approved List **Note** After installing Safe Lock and creating the Approved List, the list can be exported.
-qp	<path>	Specify the folder path for quarantined files when custom action is set to “quarantine” mode.
-nrca		Disable the Root Cause Analysis (RCA) report
-nps		Do not execute Prescan
-ips		Do not cancel installation when Prescan detects threats

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

```
SL_Install.exe -q -ac XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX -p
P@ssW0Rd -nd
```

Important

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

Customizing Installation Parameters

Note

Arguments specified at the command line interface (CLI) take higher priority than the setup file, which takes higher priority over the default values. For example, if the switch `-nd` is added to `SL_Install.exe`, and `setup.ini` contains `NO_DESKTOP=0`, the switch will take precedence, and a Safe Lock Intelligent Manager desktop shortcut will not be created.

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

Procedure

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

   For information on installation parameters and their possible values, see *Setup.ini File Arguments on page 8-18*.
3. Optionally encrypt the Setup.ini file to prevent unauthorized access to important settings.

   a. From the installation folder, copy the Setup.ini file and the WKSupportTool.exe file to your desktop.

   b. Run a command prompt window as administrator.

   c. Navigate to the desktop and type `WKSupportTool.exe encryptsetupini Setup.ini Setup.bin` to encrypt the Setup.ini file and name the encrypted file as "Setup.bin".

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

Setup.ini File Arguments

Note

Arguments specified at the command line interface (CLI) take higher priority than the setup file, which takes higher priority over the default values. For example, if the switch `-nd` is added to `SL_Install.exe`, and `setup.ini` contains `NO_DESKTOP=0`, the switch will take precedence, and a Safe Lock Intelligent Manager desktop shortcut will not be created.

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

Property Section

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

TABLE 8-3. Setup.ini File `[PROPERTY]` Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
`ACTIVATION_CODE`	Activation Code	<activation_code>	<empty>	No
`NO_DESKTOP`	Create a shortcut on desktop	• `0`: Create shortcut • `1`: Do not create shortcut	`0`	No
`NO_STARTMENU`	Create a shortcut in the Start menu	• `0`: Create shortcut • `1`: Do not create shortcut	`0`	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
NO_SYSTRAY	Display the system tray icon and Windows notifications	• 0: Create system tray icon • 1: Do not create system tray icon	0	No
NO_NSC	Install firewall	• 0: Create firewall • 1: Do not create firewall	0	No
CONFIG_PATH	Configuration file path	<path>	<empty>	No
LIST_PATH	Approved List path for import	<path>	<empty>	No
APPLICATION FOLDER	Installation path for agent program	<path>	<empty>	No
MANAGED_MODE	Specify if Safe Lock is managed by the Safe Lock Intelligent Manager server	• 0: Standalone mode • 1: Managed mode	0	No
PASSWORD	Password which is used for **SLCmd.exe** and Safe Lock console	<password>	<empty>	No
CUSTOM_ACTION	Custom action for blocked events	• 0: Ignore • 1: Quarantine • 2: Ask server	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
QUARANTINE_FOLDER_PATH	Quarantine path for agent program	<path>	<empty>	No
ROOT_CAUSE_ANALYSIS	Enable root cause analysis reporting	• 0: Disable • Other value: Enable	1	No
INTEGRITY_MONITOR	Enable Integrity Monitor	• 0: Disable • 1: Enable	0	No
PREDEFINED_TRUSTED_UPDATER	Enable Predefined Trusted Updater	• 0: Disable • 1: Enable	0	No
WINDOWS_UPDATE_SUPPORT	Enable Window Update Support	• 0: Disable • 1: Enable	0	No
PRESCAN	Prescan the endpoint before installing Safe Lock	• 0: Do not prescan the endpoint • 1: Prescan the endpoint	1	No
MAX_EVENT_DB_SIZE	Maximum database file size (MB)	Positive integer	1024	No
WEL_SIZE	Windows Event Log size (KB)	Positive integer	10240	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		Note Default value for new installations. Upgrading Safe Lock does not change any user-defined `WEL_SIZE` values set in the previous installation.		
`WEL_RETENTION`	Windows Event Log option when maximum event log size is reached on Windows Event Log.	For Windows XP or earlier platforms: • `0`: Overwrite events as needed • `1 - 365`: Overwrite events older than (1-365) days • `-1`: Do not overwrite events (Clear logs manually) For Windows Vista or later platforms: • `0`: Overwrite events as needed (oldest events first) • `1`: Archive the log when full, do	`0`	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		not overwrite events • `-1`: Do not overwrite events (Clear logs manually)		
`WEL_IN_SIZE`	Windows Event Log size for Integrity Monitor events (KB)	Positive integer	`10240`	No
`WEL_IN_RETENTION`	Windows Event Log option when maximum event log size for Integrity Monitor events is reached on Windows Event Log.	For Windows XP or earlier platforms: • `0`: Overwrite events as needed • `1 - 365`: Overwrite events older than (1-365) days • `-1`: Do not overwrite events (Clear logs manually) For Windows Vista or later platforms: • `0`: Overwrite events as needed (oldest events first) • `1`: Archive the log when full, do not overwrite events	`0`	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		• -1: Do not overwrite events (Clear logs manually)		
USR_DEBUGLOG_ENABLE	Enable debug logging for user sessions	• 0: Do not log • 1: Log	0	No
USR_DEBUGLOGLEVEL	The number of debug log entries allowed for user sessions	• 273	273	No
SRV_DEBUGLOG_ENABLE	Enable debug logging for service sessions.	• 0: Do not log • 1: Log	0	No
SRV_DEBUGLOGLEVEL	The number of debug log entries allowed for service sessions	• 273	273	No
SILENT_INSTALL	Execute installation in silent mode	• 0: Do not use silent mode • 1: Use silent mode	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED

	Important
	To use silent mode, you must also specify the ACTIVATION_CODE and PASSWORD keys and values. For example:
	`[PROPERTY]`
	`ACTIVATION_CODE=XX-XXXXX-XXXXX-XXXXX-XXXXX`
	`PASSWORD=P@ssW0Rd`
	`SILENT_INSTALL=1`			

`STORAGE_DEVICE_BLOCKING`	Blocks storage devices, including CD/DVD drives, floppy disks, and USB devices, from accessing managed endpoints.	• `0`: Allow access from storage devices • `1`: Block access from storage devices	`0`	No
`INIT_LIST`	Initialize the Approved List during installation	• `0`: Do not initialize the Approved List during installation • `1`: Initialize the Approved List during installation	`0`	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED

	Note
	`LIST_PATH` has priority over `INIT_LIST`.
	For example:
	`[PROPERTY]`
	`LIST_PATH=liststore.db`
	`INIT_LIST=1`
	In this case, `liststore.db` is imported and `INIT_LIST` is ignored.			

`INIT_LIST_PATH`	A folder path to be traversed for the Approved List initialization. Each local disk's root directory will be traversed if empty.	<folder path>	<empty>	No
`INIT_LIST_PATH_OPTIONAL`	A folder path to be traversed for the Approved List initialization. Each local disk's root directory will be traversed if empty.	<folder path>	<empty>	No
`INIT_LIST_EXCLUDED_FOLDER`	An absolute folder path to exclude from	<folder path>	<empty>	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED

	automatic file enumeration for Approved List initialization.
	
	The configuration applies to the Approved List first initialized and all subsequent Approved List updates.
	
	Specify multiple folders by creating new entries with names that start with `INIT_LIST_EXCLUDED_FOLDER`. Ensure each entry name is unique. For example:
	
	`INIT_LIST_EXCLUDED_FOLDER=c:\folder1`
	
	`INIT_LIST_EXCLUDED_FOLDER2=c:\folder2`
	
	`INIT_LIST_EXCLUDED_FOLDER3=c:\folder3`
		Note
		• Folder path supports a maximum length of 260 characters.
		• Folder paths that do not exist may be specified.
		• The exclusion applies to subfolders.		

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
INIT_LIST_EXCLUDED_EXTENSION	A file extension to exclude from automatic file enumeration for Approved List initialization. The configuration applies to the Approved List first initialized and all subsequent Approved List updates. Specify multiple extensions by creating new entries with names that start with INIT_LIST_EXCLUDED_EXTENSION. Ensure each entry name is unique. For example: INIT_LIST_EXCLUDED_EXTENSION=bmp INIT_LIST_EXCLUDED_EXTENSION2=png	<file extension> **Note** Specifying file extensions of executable files (e.g. exe, dll and sys) may cause issues with Application Lockdown.	<empty>	No
LOCKDOWN	Turn Application	• 0: Turn off Application Lockdown	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
	Lockdown on after installation	• `1`: Turn on Application Lockdown		
`FILELESS_ATTACK_PREVENTION`	Enable the Fileless Attack Prevention feature	• `0`: Disable feature • `1`: Enable feature	`0`	No
`SERVICE_CREATION_PREVENTION`	Enable the Service Creation Prevention feature	• `0`: Disable feature • `1`: Enable feature	`0`	No
	Note Safe Lock temporarily disables the Service Creation Prevention feature under the following conditions: • Updating or installing new applications using installers allowed by Trusted Updater. The feature is automatically re-enabled after the Trusted Updater process is complete. • Enabling Windows Update Support. Disabling Windows Update Support automatically re-enables the feature.			
`VERIFY_PATCH_SIGNATURE`	Verify signature of patch received from Safe Lock Intelligent	• `0`: Do not verify patch signature • `1`: Verify patch signature	`2`	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
	Manager before continuing	• 2 or other: Verify patch signature on Windows 7 or later, but skip verification on Windows Vista or earlier		
USR_DEBUGLOG_ENABLE	Enable debug log in user session	• 0: Disable debug log • 1: Enable debug log	0	No
USR_DEBUGLOGLEVEL	Debug level in user session	273	273	No
SRV_DEBUGLOG_ENABLE	Enable debug log in service session	• 0: Disable debug log • 1: Enable debug log	0	No
SRV_DEBUGLOGLEVEL	Debug level in service session	• 273	273	No
FW_USR_DEBUGLOG	Enable debug log in user session of firewall	• 0: Disable debug log • 1: Enable debug log	0	No
FW_USR_DEBUGLOG_LEVEL	Debug level in user session of firewall	number	273	No
FW_SRV_DEBUGLOG_ENABLE	Enable debug log in service session of firewall	• 0: Disable debug log • 1: Enable debug log	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
FW_SRV_DEBUGLOG_LEVEL	Debug level in service session of firewall	number	273	No
BM_SRV_DEBUGLOG_ENABLE	Enable debug log of Behavior Monitoring Core service	• 0: Disable debug log • 1: Enable debug log	0	No
BM_SRV_DEBUGLOG_LEVEL	Debug level of Behavior Monitoring Core service	• 51	51	No

EventLog Section

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

TABLE 8-4. Setup.ini File [EVENTLOG] Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
ENABLE	Log events related to Safe Lock	• 1: Log • 0: Do not log	1	No
LEVEL_WARNINGLOG	Log “Warning” level events related to Safe Lock	• 1: Log • 0: Do not log	1	No
LEVEL_INFORMATIONLOG	Log “Information” level events related to Safe Lock	• 1: Log • 0: Do not log	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
BLOCKEDACCESSLOG	Log files blocked by Safe Lock	• 1: Log • 0: Do not log	1	No
APPROVEDACCESSLOG	Log files approved by Safe Lock	• 1: Log • 0: Do not log	1	No
APPROVEDACCESSLOG_TRUSTEDUPDATER	Log Trusted Updater approved access	• 1: Log • 0: Do not log	1	No
APPROVEDACCESSLOG_TRUSTEDHASH	Log Trusted Hash approved access	• 1: Log • 0: Do not log	1	No
APPROVEDACCESSLOG_DLLDRIVER	Log DLL/Driver approved access	• 1: Log • 0: Do not log	0	No
APPROVEDACCESSLOG_EXCEPTIONPATH	Log Application Lockdown exception path approved access	• 1: Log • 0: Do not log	1	No
APPROVEDACCESSLOG_TRUSTEDCERT	Log Trusted Certifications approved access	• 1: Log • 0: Do not log	1	No
APPROVEDACCESSLOG_WRITEPROTECTION	Log Write Protection approved access	• 1: Log • 0: Do not log	1	No
SYSTEMEVENTLOG	Log events related to the system	• 1: Log • 0: Do not log	1	No

Key	Description	Possible Values	Default Value	Encrypted
SYSTEMEVENTLOG_EXCEPTIONPATH	Log exceptions to Application Lockdown	• 1: Log • 0: Do not log	1	No
SYSTEMEVENTLOG_WRITEPROTECTION	Log Write Protection events	• 1: Log • 0: Do not log	1	No
LISTLOG	Log events related to the Approved list	• 1: Log • 0: Do not log	1	No
USBMALWAREPROTECTIONLOG	Log events that trigger USB Malware Protection	• 1: Log • 0: Do not log	1	No
EXECUTIONPREVENTIONLOG	Log events that trigger Execution Prevention	• 1: Log • 0: Do not log	1	No
NETWORKVIRUSPROTECTIONLOG	Log events that trigger Network Virus Protection	• 1: Log • 0: Do not log	1	No
INTEGRITYMONITORINGLOG_FILECREATED	Log file and folder created events	• 1: Log • 0: Do not log	1	No
INTEGRITYMONITORINGLOG_FILEMODIFIED	Log file modified events	• 1: Log • 0: Do not log	1	No
INTEGRITYMONITORINGLOG_FILEDELETED	Log file and folder deleted events	• 1: Log • 0: Do not log	1	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
INTEGRITYMONITORINGLOG_FILERENAMED	Log file and folder renamed events	• 1: Log • 0: Do not log	1	No
INTEGRITYMONITORINGLOG_REGVALUEMODIFIED	Log registry value modified events	• 1: Log • 0: Do not log	1	No
INTEGRITYMONITORINGLOG_REGVALUEDELETED	Log registry value deleted events	• 1: Log • 0: Do not log	1	No
INTEGRITYMONITORINGLOG_REGKEYCREATED	Log registry key created events	• 1: Log • 0: Do not log	1	No
INTEGRITYMONITORINGLOG_REGKEYDELETED	Log registry key deleted events	• 1: Log • 0: Do not log	1	No
INTEGRITYMONITORINGLOG_REGKEYRENAMED	Log registry key renamed events	• 1: Log • 0: Do not log	1	No
DEVICECONTROLLOG	Log events related to device access control	• 1: Log • 0: Do not log	1	No

Server Section

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

TABLE 8-5. Setup.ini File [SERVER] Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
HOSTNAME	Server host name	<host_name>	<empty>	No
PORT_FAST	Server listen port for fast lane	1 - 65535	<empty>	No
PORT_SLOW	Server listen port for slow lane	1 - 65535	<empty>	No
CERT	Certificate file name	<certificate_file_name>	<empty>	No
API_KEY	API key	<API_key>	<empty>	No

Agent Section

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

TABLE 8-6. Setup.ini File [AGENT] Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
PORT	Agent listening port	1 - 65535	<empty>	No
SSL_ALLOW_BEAST	Handles possible security flaws in SSL3 and TLS 1.0 protocols for BEAST attacks	• 0: Protect against BEAST attacks • 1: Do not implement any security workarounds for	1	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		BEAST vulnerabilities		
POLL_SERVER	Identify the agent as an NAT agent	• 0: Non-NAT agent • 1: NAT agent	0	No
POLL_SERVER_INTERVAL	Set the NAT connection frequency	• 1 - 64800: Connect to the Safe Lock Intelligent Manager server every (1 - 64800) minutes	10	No

Note

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

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

Message Section

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

TABLE 8-7. Setup.ini File [MESSAGE] Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
REGISTER_TRIGGER	Register message trigger	• 1: Immediately • 2: On demand	1	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
UNREGISTER_TRIGGER	Unregister message trigger	• 1: Immediately • 2: On demand	1	No
UPDATESTATUS_TRIGGER	Update status message trigger	• 1: Immediately • 2: On demand	1	No
UPLOADBLOCKEDEVENT_TRIGGER	Upload blocked event message trigger	• 1: Immediately • 2: On demand	1	No
CHECKFILEHASH_TRIGGER	Check file hash message trigger	• 1: Immediately • 2: On demand	1	No
QUICKSCANFILE_TRIGGER	Quick scan file message trigger	• 1: Immediately • 2: On demand	1	No
INITIAL_RETRY_INTERVAL	Starting interval, in seconds, between attempts to resend an event to Intelligent Manager. This interval doubles in size for each unsuccessful attempt, until it exceeds the MAX_RETRY_INTERVAL value.	• 0 ~ 2147483647	120	No
MAX_RETRY_INTERVAL	Maximum interval, in seconds,	• 0 ~ 2147483647	7680	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
	between attempts to resend events to Intelligent Manager.			

MessageRandomization Section

Note

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

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

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

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

Proxy Section

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

TABLE 8-9. Setup.ini File `[PROXY]` Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
`MODE`	Proxy mode	• `0`: No proxy used • `1`: Proxy used with manual settings • `2`: Proxy used with settings retrieved from Internet Explorer automatically	`0`	No
`HOSTNAME`	Proxy host name	<host_name>	<empty>	No
`PORT`	Proxy port	`1` - `65535`	<empty>	No
`USERNAME`	Proxy user name	<user_name>	<empty>	No
`PASSWORD`	Proxy password	<password>	<empty>	No

Prescan Section

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

TABLE 8-10. Setup.ini File [PRESCAN] Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
IGNORE_THREAT	Cancel installation after detecting malware threat during prescan	• 0: Cancel • 1: Continue installation after detecting malware threat during prescan • 2: Continue installation when no malware is detected, or after all detected malware is cleaned, deleted, or quarantined successfully without a system reboot.	0	No
REPORT_FOLDER	An absolute folder path where prescan result reports are saved.	• <folder_path> • <empty>: Defaults to %windir%\temp\prescan\log	<empty>	No
SCAN_TYPE	The type of scan executed during silent installation	• Full: Scan all folders on the endpoint. • Quick: Scans the following folders: • Fixed root drives	Full	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED

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

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		`c:\Users\Trend\AppData\Local\Temp` • Desktop folder including sub folders and files For example, `c:\Users\Trend\Desktop` • `Specific`: Scan folders specified with `SPECIFIC_FOLDER` entries		
`COMPRESS_LAYER`	The number of compressed layers to scan when a compressed file is scanned.	• `0`: Do not scan compressed files • `1 - 20`: Scan up to the specified number of layers of a compressed file	`2`	No
`MAX_FILE_SIZE`	The largest file allowed for scan	• `0`: Scan files of any sizes • `1 - 9999`: Only scan files equal to or smaller than the	`0`	No

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

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

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED

		`EXCLUDED_EXTENSION=bmp`
		
		`EXCLUDED_EXTENSION2=png`		

`PRESCANCLEANUP`	Attempt to clean detected files during prescan **Note** You must manually include this option in the Setup.ini file. Only valid during silent installations.	• `0`: No action. This is the default setting for installations using the Windows Installer. • `1`: Clean, or delete if the clean action is unsuccessful • `2`: Clean, or quarantine if the clean action is unsuccessful • `3`: Clean, or ignore if the clean action is unsuccessful	`2`	No
`FORCE_PRESCAN`	Perform a prescan before installation	• `0`: Disable • `1`: Enable	`0`	No

BlockNotification Section

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

See *Property Section on page 8-18* for more information.

Important

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

TABLE 8-11. Setup.ini File `[BlockNotification]` Section Arguments

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

Chapter 9

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 9-3* for more information.

Changing Advanced Settings

Some settings can only be changed though the configuration file using the command line interface (CLI). See *Using SLCmd at the Command Line Interface (CLI) on page 6-2* for more information.

Procedure

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

Important

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

Tip

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

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

Exporting or Importing a Configuration File

Note

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

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

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

Procedure

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

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

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

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

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

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

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

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

Configuration File Syntax

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

Important

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

Refer to the following example of the configuration file.

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

```
                    <Extension Id="bat">
                        <Interpreter>cmd.exe</Interpreter>
                    </Extension>
                    <Extension Id="cmd">
                        <Interpreter>cmd.exe</Interpreter>
                    </Extension>
                    <Extension Id="com">
                        <Interpreter>ntvdm.exe</Interpreter>
                    </Extension>
                    <Extension Id="dll">
                        <Interpreter>ntvdm.exe</Interpreter>
                    </Extension>
                    <Extension Id="drv">
                        <Interpreter>ntvdm.exe</Interpreter>
                    </Extension>
                    <Extension Id="exe">
                        <Interpreter>ntvdm.exe</Interpreter>
                    </Extension>
                    <Extension Id="js">
                        <Interpreter>cscript.exe</Interpreter>
                        <Interpreter>wscript.exe</Interpreter>
                    </Extension>
                    <Extension Id="msi">
                        <Interpreter>msiexec.exe</Interpreter>
                    </Extension>
                    <Extension Id="pif">
                        <Interpreter>ntvdm.exe</Interpreter>
                    </Extension>
                    <Extension Id="ps1">
                        <Interpreter>powershell.exe</Interpret
er>
                    </Extension>
                    <Extension Id="sys">
                        <Interpreter>ntvdm.exe</Interpreter>
                    </Extension>
                    <Extension Id="vbe">
                        <Interpreter>cscript.exe</Interpreter>
                        <Interpreter>wscript.exe</Interpreter>
                    </Extension>
                    <Extension Id="vbs">
                        <Interpreter>cscript.exe</Interpreter>
                        <Interpreter>wscript.exe</Interpreter>
```

```
                    </Extension>
                </ScriptLockdown>
                <TrustedUpdater>
                    <PredefinedTrustedUpdater Enable="no">
                        <RuleSet/>
                    </PredefinedTrustedUpdater>
                    <WindowsUpdateSupport Enable="no"/>
                </TrustedUpdater>
                <DllDriverLockDown Enable="yes"/>
                <ExceptionPath Enable="no">
                    <ExceptionPathList/>
                </ExceptionPath>
                <TrustedCertification Enable="yes"/>
                <TrustedHash Enable="no"/>
                <WriteProtection Enable="no" ActionMode="1"
ProtectApprovedList="yes"/>
                <CustomAction ActionMode="0"/>
                <FilelessAttackPrevention Enable="no">
                    <ExceptionList/>
                </FilelessAttackPrevention>
            </ApplicationLockDown>
            <UsbMalwareProtection Enable="no" ActionMode="1"/>
            <NetworkVirusProtection Enable="yes" ActionMode=
"1"/>
            <IntegrityMonitoring Enable="no"/>
            <StorageDeviceBlocking Enable="no" ActionMode="1"/>
            <Log>
                <EventLog Enable="yes">
                    <Level>
                        <WarningLog Enable="yes"/>
                        <InformationLog Enable="no"/>
                    </Level>
                    <BlockedAccessLog Enable="yes"/>
                    <ApprovedAccessLog Enable="yes">
                        <TrustedUpdaterLog Enable="yes"/>
                        <DllDriverLog Enable="no"/>
                        <ExceptionPathLog Enable="yes"/>
                        <TrustedCertLog Enable="yes"/>
                        <TrustedHashLog Enable="yes"/>
                        <WriteProtectionLog Enable="yes"/>
                    </ApprovedAccessLog>
                    <SystemEventLog Enable="yes">
```

```
                        <ExceptionPathLog Enable="yes"/>
                        <WriteProtectionLog Enable="yes"/>
                    </SystemEventLog>
                    <ListLog Enable="yes"/>
                    <UsbMalwareProtectionLog Enable="yes"/>
                    <ExecutionPreventionLog Enable="yes"/>
                    <NetworkVirusProtectionLog Enable="yes"/>
                    <IntegrityMonitoringLog>
                        <FileCreatedLog Enable="yes"/>
                        <FileModifiedLog Enable="yes"/>
                        <FileDeletedLog Enable="yes"/>
                        <FileRenamedLog Enable="yes"/>
                        <RegValueModifiedLog Enable="yes"/>
                        <RegValueDeletedLog Enable="yes"/>
                        <RegKeyCreatedLog Enable="yes"/>
                        <RegKeyDeletedLog Enable="yes"/>
                        <RegKeyRenamedLog Enable="yes"/>
                    </IntegrityMonitoringLog>
                    <DeviceControlLog Enable="yes"/>
                </EventLog>
                <DebugLog Enable="no"/>
            </Log>
        </Feature>
        <ManagedMode Enable="no">
            <Agent>
                <Port/>
                <SslAllowBeast>1</SslAllowBeast>
                <PollServer>0</PollServer>
                <PollServerInterval>10</PollServerInterval>
            </Agent>
            <Server>
                <HostName/>
                <FastPort/>
                <SlowPort/>
                <ApiKey/>
            </Server>
            <Message InitialRetryInterval="120"
MaxRetryInterval="7680">
                <Register Trigger="1"/>
                <Unregister Trigger="1"/>
                <UpdateStatus Trigger="1"/>
                <UploadBlockedEvent Trigger="1"/>
```

```
                <CheckFileHash Trigger="1"/>
                <QuickScanFile Trigger="1"/>
            </Message>
            <MessageRandomization TotalGroupNum="1" OwnGroupIn
dex="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"/>
            <UIControl Id="SupportToolUninstall" State="no"/>
        </AccountRef>
    </Permission>
</Configurations>
```

Configuration File Parameters

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

TABLE 9-1. Configuration File Sections and Descriptions

SECTION	DESCRIPTION	ADDITIONAL INFORMATION
`Configuration`	Container for the Configuration section	

SECTION			DESCRIPTION	ADDITIONAL INFORMATION
	AccountGroup		Parameters to configure the Restricted User account	See *AccountGroup Section on page 9-10*. See *Account Types on page 5-17*.
	UI		Parameters to configure the display of the system tray icon	See *UI Section on page 9-11*.
	Feature		Container for the Feature section	
		ApplicationLockDown	Parameters to configure Safe Lock features and functions	See *Feature Section on page 9-13*.
		UsbMalwareProtection		
		DllInjectionPrevention		
		ApiHookingPrevention		
		MemoryRandomization		
		NetworkVirusProtection		
		IntegrityMonitoring		
		StorageDeviceBlocking	A parameter to control storage device access to managed endpoints	
		Log	Parameters to configure individual log types	See *Log Section on page 9-27*. See *Agent Event Log Descriptions on page 13-4*.

Section	Description	Additional Information
ManagedMode	Parameters to configure Centralized Management functions	See *ManagedMode Section on page 9-31*.
Permission	Container for the Permission section	
AccountRef	Parameters to configure the Safe Lock console controls available to the Restricted User account	See *AccountRef Section on page 9-35*. See *Account Types on page 5-17*.

AccountGroup Section

Parameters to configure the Restricted User account

See *Account Types on page 5-17*.

TABLE 9-2. Configuration File `AccountGroup` Section Parameters

Parameter	Setting	Value	Description
Configuration			Container for the Configuration section
AccountGroup			Container for the AccountGroup section
Account	ID	<GUID>	Restricted User account GUID
	Enable	yes	Enable the Restricted User account
		no	Disable the Restricted User account
	Password	<Safe_Lock_password>	Password for the Restricted User account to access the Safe Lock console

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 9-3. Configuration File `UI` Section Parameters

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

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

Feature Section

Parameters to configure Safe Lock features and functions

See *About Feature Settings on page 5-19*.

TABLE 9-4. Configuration File `Feature` Section Parameters

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

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

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

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

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

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

Parameter			Setting	Value	Description
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: • 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

PARAMETER				SETTING	VALUE	DESCRIPTION
						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
				Name	<reg_value_name>	Registry value name
		ExceptionList				Container for the Write Protection Exception List

PARAMETER	SETTING	VALUE	DESCRIPTION
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 • HKEY_CLASSES_ROOT\test HKCR\test • HKEY_CURRENT_USER\test HKCU\test

Parameter	Setting	Value	Description
			• 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
	Name	<reg_value_name>	Registry value name

PARAMETER	SETTING	VALUE	DESCRIPTION
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

Parameter	Setting	Value	Description
IntegrityMonitoring	Enable	yes	Enable Integrity Monitoring
		no	Disable Integrity Monitoring
StorageDeviceBlocking	Enable	yes	Blocks access of storage devices (CD/DVD drives, floppy disks, and USB devices) to managed endpoints
	Disable	no	Allows access of storage devices (CD/DVD drives, floppy disks, and USB devices) to managed endpoints
	ActionMode	0	Allow actions such as edit, rename, and delete
		1	Block actions such as edit, rename, and delete
	Log		Container for configuring logs See *Log Section on page 9-27*.
FilelessAttackPrevention	Enable	yes	Enable Fileless Attack Prevention
		no	Disable Fileless Attack Prevention
ExceptionList			Container for the Fileless Attack

Parameter				Setting	Value	Description
						Prevention Exception List
			Exception	Target	<monitored process>	Specify powershell.exe, wscript.exe, CScript.exe, or mshta.exe
				Label	<label>	Unique name of this exception
			Arguments		<arguments>	Arguments to be approved
				Regex	yes	Specify yes if argument includes a regular exception
					no	Specify no if argument does not include a regular exception
			Parent1		<parent process>	Parent process of the monitored process
			Parent2		<grandparent process>	Grandparent process of the monitored process
			Parent3		<greatgrandparent process>	Great grandparent process of the monitored process
			Parent4		<great great grandp	Great great grandparent process of the monitored process

PARAMETER	SETTING	VALUE	DESCRIPTION
arent proces s>			

Log Section

Parameters to configure individual log types

See *Agent Event Log Descriptions on page 13-4*.

TABLE 9-5. Configuration File Log Section Parameters

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

Parameter	Setting	Value	Description
		no	Do not log “Information” level events related to Safe Lock
BlockedAccessLog	Enable	yes	Log files blocked by Safe Lock
		no	Do not log files blocked by Safe Lock
ApprovedAccessLog	Enable	yes	Log files approved by Safe Lock
		no	Do not log files approved by Safe Lock
TrustedUpdaterLog	Enable	yes	Log Trusted Updater approved access
		no	Do not log Trusted Updater approved access
DLLDriverLog	Enable	yes	Log DLL/Driver approved access
		no	Do not log DLL/Driver approved access
ExceptionPathLog	Enable	yes	Log Application Lockdown exception path approved access
		no	Do not log Application Lockdown exception path approved access
TrustedCertLog	Enable	yes	Log Trusted Certifications approved access
		no	Do not log Trusted Certifications approved access
WriteProtectionLog	Enable	yes	Log Write Protection approved access

PARAMETER	SETTING	VALUE	DESCRIPTION
		no	Do not log Write Protection approved access
SystemEventLog	Enable	yes	Log events related to the system
		no	Do not log events related to the system
ExceptionPathLog	Enable	yes	Log exceptions to Application Lockdown
		no	Do not log exceptions to Application Lockdown
WriteProtectionLog	Enable	yes	Log Write Protection events
		no	Do not log Write Protection events
ListLog	Enable	yes	Log events related to the Approved list
		no	Do not log events related to the Approved list
USBMalwareProtectionLog	Enable	yes	Log events that trigger USB Malware Protection
		no	Do not log events that trigger USB Malware Protection
ExecutionPreventionLog	Enable	yes	Log events that trigger Execution Prevention
		no	Do not log events that trigger Execution Prevention
NetworkVirusProtectionLog	Enable	yes	Log events that trigger Network Virus Protection
		no	Do not log events that trigger Network Virus Protection

Parameter	Setting	Value	Description
IntegrityMonitoringLog			Container for configuring Integrity Monitoring logs
FileCreatedLog	Enable	yes	Log file and folder created events
		no	Do not log file and folder created events
FileModifiedLog	Enable	yes	Log file modified events
		no	Do not log file modified events
FileDeletedLog	Enable	yes	Log file and folder deleted events
		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

PARAMETER	SETTING	VALUE	DESCRIPTION
		no	Do not log registry key deleted events
RegKeyRenamedLog	Enable	yes	Log registry key renamed events
		no	Do not log registry key renamed events
DeviceControlLog	Enable	yes	Log storage device control events.
		no	Do not log storage device control events.
DebugLog	Enable	yes	Log debugging information
		no	Do not log debugging information

ManagedMode Section

Parameters to configure Centralized Management functions

TABLE 9-6. Configuration File `ManagedMode` Section Parameters

PARAMETER	SETTING	VALUE	DESCRIPTION
Configuration			Container for the Configuration section
ManagedMode	Enable	yes	Enable managed mode
		no	Disable managed mode
Agent			Container for configuring Safe Lock agents
Port		<server_messages_port>	Specify the secure port for server communications

PARAMETER	SETTING	VALUE	DESCRIPTION
			(formerly the agent listening port)
SslAllowBeast		0	Allow upload of large files (>10MB) on Windows Server 2008 platforms
		1	Prevent the unsuccessful upload of large files (>10MB) on Windows Server 2008 platforms (default value)
PollServer		0	Identify the agent as a non-NAT agent
		1	Identify the agent as a NAT agent.
PollServerInterval		<interval_period>	Specify a NAT connection frequency from 1 to 64800 minutes (connect to the Safe Lock server every 1-64800 minutes)
Server			Container for configuring Safe Lock Intelligent Manager
HostName		<hostname>	Specify the host name of the Intelligent Manager server
FastPort		<logs_port>	Specify secure port for collecting logs and status (formerly Fast Lane)
SlowPort		<files_port>	Specify secure port for collecting files for

PARAMETER	SETTING	VALUE	DESCRIPTION
			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

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

Note

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

	TotalGroupNum	Positive Integer (>= 1)	Specify the total number of message time groups
	OwnGroupIndex	Zero or Positive Integer, < TotalGroupNum	Specify the message time group ID number of this Safe Lock agent
	TimePeriod	Zero or Positive Integer	Specify the duration of time in whole seconds that this message time group ID number will send automated messages to Intelligent Manager when this group's message-sending cycle is active

PARAMETER	SETTING	VALUE	DESCRIPTION
			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
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 5-17*.

TABLE 9-7. Configuration File `AccountRef` Section Parameters

PARAMETER	SETTING	VALUE	DESCRIPTION
`Configuration`			Container for the Configuration section
`Permission`			Container for the Permission section
`AccountRef`			Container for the AccountRef section
`UIControl`	`ID`	`DetailSetting`	Access the features and functions on the Safe Lock console **Settings** page **Note** The **Password** page is not available to the Restricted User account.
		`LockUnlock`	Access the Application Lockdown setting on the **Overview** screen
		`LaunchUpdater`	Access the **Automatically add files created or modified by the selected application installer** option when a Restricted User clicks **Add Item** on the **Approved List** screen
		`RecentHistoryUnapprovedFIles`	Access the Block logs if a Restricted User clicks **Last application blocked** on the **Overview**screen
		`ImportExportList`	Access the **Import List** and **Export List** buttons
		`ListManagement`	Access the following items on the **Approved List** screen: • The **Delete Item** button

PARAMETER				SETTING	VALUE	DESCRIPTION
						• 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 10

Local Agent Uninstallation

This chapter describes Trend Micro Safe Lock agent uninstallation procedures.

Topics in this chapter include:

Uninstalling Agents from Windows

Note

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

Procedure

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

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

OPTION	DESCRIPTION
If you use one of the following operating systems: • Windows 10 Enterprise • Windows 10 IoT Enterprise • Windows 10 Professional • Windows 10 Fall Creators Update (Redstone 3) • Windows 10 April 2018 Update (Redstone 4) • Windows 10 October 2018 Update (Redstone 5)	a. Go to **Start** > **Settings**. b. Depending on your version of Windows 10, locate the **Apps & features** section under one of the following categories: • **System** • **Apps** c. On the left pane, click **Apps & features**. d. In the list, click Trend Micro Safe Lock. e. Click **Uninstall**.
If you use one of the following operating systems: • Windows Server 2016 • Windows Server 2012 • Windows Server 2008 • Windows Storage Server 2016	a. Go to **Start** > **Control Panel** > **Prorgrams and Features**. b. In the list, double-click Trend Micro Safe Lock.

OPTION	DESCRIPTION
• Windows 8 • Windows 7 • Windows Vista	
If you use one of the following operating systems: • Windows Server 2003 • Windows XP • Windows 2000	a. Go to **Start** > **Control Panel** > **Add or Remove Programs**. b. In the list, select Trend Micro Safe Lock. c. Click **Remove**.

Safe Lock Setup opens in uninstaller mode.

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

Chapter 11

Troubleshooting & FAQs

This chapter provides a list of resources you can use to troubleshoot Trend Micro Safe Lock Intelligent Manager issues.

Topics in this chapter include:

Troubleshooting Remote Agent Installations

Remote installations performed using the **`SLrst`** command line interface (CLI) program may result in the following messages:

Unable to Run: The network or firewall is not correctly configured or a version of Safe Lock earlier than 1.1 is installed. Check configurations and remove older versions of Safe Lock from the target endpoint, then run Setup again.

Went Offline: The endpoint went offline while Setup was running. The tool is unable to determine if the installation completed successfully. If the endpoint appears in the Intelligent Manager web console, the installation was completed successfully. If the endpoint does not appear, then check the endpoint locally.

Frequently Asked Questions

Is a reboot required after installation or uninstallation?

Safe Lock agents do not require reboot after installation except for the following scenarios.

Scenario Type	Scenario
Setting Changes	When the **Memory Randomization** setting is configured and changed, the managed endpoints require a reboot to apply the change.
Installation	When Safe Lock detects a third-party program during its installation and then uninstalls the program, a reboot is required before continuing with the installation.
Installation	When a firewall module requests for a reboot during Safe Lock installation, a reboot is required before continuing with the installation.
Uninstallation	When Safe Lock agents are uninstalled using the Diagnostic Toolkit, a reboot is required before re-installing Safe Lock agents.

How to migrate Safe Lock agents to another Intelligent Manager?

Procedure

1. On an endpoint, open a command window and navigate to the Safe Lock agent installation directory.
2. Export the configuration file to a local drive.

   The following shows a command example:

   ```
   SLCmd.exe -p <admin_password> export mmc c:\config.xen
   ```

   For more information, see *Configuration File Commands on page 6-67*.
3. Decrypt and convert the exported configuration file into XML format.

   The following shows a command example:

   ```
   SLCmd.exe -p <admin_password> decrypt mmc c:\config.xen
   c:\config.xml
   ```
4. Use a text editor to open the decrypted configuration file and update the following parameters for the target Intelligent Manager server:

   - `host-name`
   - `FastPort`
   - `SlowPort`
   - `ApiKey`

   Tip

   On the Intelligent Manager server, you can obtain the information in `C:\Program Files\Trend Micro\Safe Lock Intelligent Manager\CmdTools\Installer\settings.xml`.
5. Encrypt and convert the configuration file into XEN file format.

The following shows a command example:

```
SLCmd.exe -p <admin_password> encrypt mmc c:\config.xml
c:\config.xen
```

6. Obtain the agent certification from the target Intelligent Manager server. Do the following to obtain the agent certificate in the agent installer package:

   a. Access the Intelligent Manager management console and click **Administrator** > **Updates**.

   b. Click **Download Agent Installer Package** to save the installer package to a local drive.

   c. Extract the installer package to obtain the agent certificate.

7. Copy the agent certificate to the same location as the updated configuration file on the endpoint.

8. Import the agent certificate and the updated configuration file.

   The following shows a command example:

   ```
   SLCmd.exe -p <admin_password> set mm enable -cfg
   c:\config.xen -sc c:\trend.cer
   ```

What if the endpoint becomes infected by a threat?

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

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

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

Procedure

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

   For details, see *Enabling or Disabling Feature Settings on page 5-22*.

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

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

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

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

   For details, see *Adding or Removing Files on page 5-14*.

   Note

   To determine the required modules, contact Trend Micro support.

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

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

Chapter 12

Technical Support

Learn about the following topics:

Troubleshooting Resources

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

Using the Support Portal

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

Procedure

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

Tip

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

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

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

Threat Encyclopedia

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

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

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

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

Contacting Trend Micro

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

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

- Worldwide support offices:

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

- Trend Micro product documentation:

  http://docs.trendmicro.com

Speeding Up the Support Call

To improve problem resolution, have the following information available:

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

Sending Suspicious Content to Trend Micro

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

Email Reputation Services

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

https://ers.trendmicro.com/

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

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

File Reputation Services

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

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

Record the case number for tracking purposes.

Web Reputation Services

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

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

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

Other Resources

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

Download Center

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

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

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

Documentation Feedback

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

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

Chapter 13

Appendix: Reference

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

Topics in this chapter include:

Enabling Local Administrator Accounts

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

Procedure

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

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

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

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

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

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

Enabling Local Accounts for Default Shares

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

Tip

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

Procedure

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

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

3. Locate the `LocalAccountTokenFilterPolicy` registry entry.

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

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

7. Exit **Registry Editor**.

Agent Event Log Descriptions

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

Tip

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

- Before installation, modify the Setup.ini file. See *Setup.ini File Arguments* > *EventLog Section* in the Safe Lock Installation Guide.
- After installation, modify the configuration file. See *Configuration File Parameters* > *Log Section on page 9-27*.

TABLE 13-1. Windows Event Log Descriptions

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

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

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

Event ID	Task Category	Level	Log Description
1049	System	Information	Write Protection enabled.
1050	System	Warning	Write Protection disabled.
1051	System	Information	Write Protection set to Allow.
1052	System	Information	Write Protection set to Block.
1055	System	Information	Added file to Write Protection List. Path: %path%
1056	System	Information	Removed file from Write Protection List. Path: %path%
1057	System	Information	Added file to Write Protection Exception List. Path: %path% Process: %process%
1058	System	Information	Removed file from Write Protection Exception List. Path: %path% Process: %process%
1059	System	Information	Added folder to Write Protection List. Path: %path% Scope: %scope%
1060	System	Information	Removed folder from Write Protection List. Path: %path% Scope: %scope%
1061	System	Information	Added folder to Write Protection Exception List.

Event ID	Task Category	Level	Log Description
			Path: %path% Scope: %scope% Process: %process%
1062	System	Information	Removed folder from Write Protection Exception List. Path: %path% Scope: %scope% Process: %process%
1063	System	Information	Added registry value to Write Protection List. Registry Key: %regkey% Registry Value Name: %regvalue%
1064	System	Information	Removed registry value from Write Protection List. Registry Key: %regkey% Registry Value Name: %regvalue%
1065	System	Information	Added registry value to Write Protection Exception List. Registry Key: %regkey% Registry Value Name: %regvalue% Process: %process%
1066	System	Information	Removed registry value from Write Protection Exception List. Registry Key: %regkey% Registry Value Name: %regvalue% Process: %process%

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

Event ID	Task Category	Level	Log Description
1075	System	Information	Quarantined file is deleted. [Details] Original Location: %path% Source: %source%
1076	System	Information	Integrity Monitoring enabled.
1077	System	Information	Integrity Monitoring disabled.
1078	System	Information	Root cause analysis report unsuccessful. [Details] Access Image Path: %path%
1079	System	Information	Server certification imported: %path%
1080	System	Information	Server certification exported to: %path%
1081	System	Information	Managed mode configuration imported: %path%
1082	System	Information	Managed mode configuration exported to: %path%
1083	System	Information	Managed mode enabled.
1084	System	Information	Managed mode disabled.
1085	System	Information	Protection applied to Write Protection List and Approved List while Write Protection is enabled
1086	System	Warning	Protection applied to Write Protection List while Write Protection is enabled.
1088	System	Information	Windows Update Support enabled.
1089	System	Information	Windows Update Support disabled.

Event ID	Task Category	Level	Log Description
1094	System	Information	Trend Micro Safe Lock updated. File applied: %file_name%
1096	System	Information	Trusted Hash List enabled.
1097	System	Information	Trusted Hash List disabled.
1099	System	Information	Storage device access set to Allow
1100	System	Information	Storage device access set to Block
1101	System	Information	Storage device control enabled
1102	System	Warning	Storage device control disabled
1103	System	Information	Event Log settings changed. [Details] Windows Event Log: %ON|off% Level: Warning Log: %ON|off% Information Log: %ON|off% System Log: %ON|off% Exception Path Log: %ON|off% Write Protection Log: %ON|off% List Log: %ON|off% Approved Access Log: DllDriver Log: %ON|off% Trusted Updater Log: %ON|off% Exception Path Log: %ON|off% Trusted Certification Log: %ON|off% Trusted Hash Log: %ON|off%

Event ID	Task Category	Level	Log Description
			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% Device Control Log: %ON|off% Debug Log: %ON|off%
1104	System	Warning	Memory Randomization is not available in this version of Windows.
1105	System	Information	Blocked File Notification enabled.
1106	System	Information	Blocked File Notification disabled.
1107	System	Information	Administrator password changed remotely.
1111	System	Information	Fileless Attack Prevention enabled.
1112	System	Warning	Fileless Attack Prevention disabled.

Event ID	Task Category	Level	Log Description
1500	List	Information	Trusted Update started.
1501	List	Information	Trusted Update stopped.
1502	List	Information	Approved List import started: %path%
1503	List	Information	Approved List import complete: %path%
1504	List	Information	Approved List exported to: %path%
1505	List	Information	Added to Approved List: %path%
1506	List	Information	Added to Trusted Updater List: %path%
1507	List	Information	Removed from Approved List: %path%
1508	List	Information	Removed from Trusted Updater List: %path%
1509	List	Information	Approved List updated: %path%
1510	List	Information	Trusted Updater List updated: %path%
1511	List	Warning	Unable to add to or update Approved List: %path%
1512	List	Warning	Unable to add to or update Trusted Updater List: %path%
1513	System	Information	Added to Exception Path List. [Details] Type: %exceptionpathtype% Path: %exceptionpath%
1514	System	Information	Removed from Exception Path List. [Details] Type: %exceptionpathtype% Path: %exceptionpath%

Event ID	Task Category	Level	Log Description
1515	System	Information	Added to Trusted Certification List. [Details] Label: %label% Hash: %hashvalue% Type: %type% Subject: %subject% Issuer: %issuer%
1516	System	Information	Removed from Trusted Certification List. [Details] Label: %label% Hash: %hashvalue% Type: %type% Subject: %subject% Issuer: %issuer%
1517	System	Information	Added to the Trusted Hash List.%n [Details] Label : %label% Hash : %hashvalue% Type : %type% Add to Approved List: %yes|no% Path : %path% Note: %note%
1518	System	Information	Removed from the Trusted Hash List.%n

Event ID	Task Category	Level	Log Description
			[Details] Label : %label% Hash : %hashvalue% Type : %type% Add to Approved List: %yes|no% Path : %path% Note: %note%
1519	List	Information	Removed from Approved List remotely: %path%
1520	List	Warning	Unable to create Approved List because an unexpected error occurred during enumeration of the files in %1 %n Error Code: %2 %n
1521	System	Information	Added Fileless Attack Prevention exception. [Details] Label : %label% Target Process: %process_name% Arguments: %arguments% %regex_flag% Parent Process 1 Image Path: %path% Parent Process 2 Image Path: %path% Parent Process 3 Image Path: %path% Parent Process 4 Image Path: %path%
1522	System	Information	Removed Fileless Attack Prevention exception. [Details]

Event ID	Task Category	Level	Log Description
			Label : %label% Target Process: %process_name% Arguments: %arguments% %regex_flag% Parent Process 1 Image Path: %path% Parent Process 2 Image Path: %path% Parent Process 3 Image Path: %path% Parent Process 4 Image Path: %path%
1523	System	Information	Maintenance Mode started
1524	System	Information	Leaving Maintenance Mode
1525	System	Information	Maintenance Mode stopped
1526	List	Information	Added to Approved List in Maintenance Mode. Path: %1 Hash: %2
1527	List	Information	Approved List updated in Maintenance Mode. Path: %1 Hash: %2
2000	Access Approved	Information	File access allowed: %path% [Details] Access Image Path: %path% Access User: %username% Mode: %mode% List: %list%

Event ID	Task Category	Level	Log Description
2001	Access Approved	Warning	File access allowed: %path% [Details] Access Image Path: %path% Access User: %username% Mode: %mode% File Hash allowed: %hash%
2002	Access Approved	Warning	File access allowed: %path% Unable to get the file path while checking the Approved List. [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2003	Access Approved	Warning	File access allowed: %path% Unable to calculate hash while checking the Approved List. [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2004	Access Approved	Warning	File access allowed: %path% Unable to get notifications to monitor process.

Event ID	Task Category	Level	Log Description
2005	Access Approved	Warning	File access allowed:%path% Unable to add process to non exception list.
2006	Access Approved	Information	File access allowed: %path% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2007	Access Approved	Warning	File access allowed: %path% An error occurred while checking the Exception Path List. [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2008	Access Approved	Warning	File access allowed: %path% An error occurred while checking the Trusted Certification List. [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2011	Access Approved	Information	Registry access allowed. Registry Key: %regkey% Registry Value Name: %regvalue%

Event ID	Task Category	Level	Log Description
			[Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2012	Access Approved	Information	Registry access allowed. Registry Key: %regkey% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2013	Access Approved	Information	Change of File/Folder allowed by Exception List: %path% [Details] Access Image Path: Access User: %username% Mode: %mode%
2015	Access Approved	Information	Change of Registry Value allowed by Exception List. Registry Key: %regkey% Registry Value Name: %regvalue% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%

Event ID	Task Category	Level	Log Description
2016	Access Approved	Information	Change of Registry Key allowed by Exception List. Registry Key: %regkey% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2017	Access Approved	Warning	Change of File/Folder allowed: %path% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2019	Access Approved	Warning	Change of Registry Value allowed. Registry Key: %regkey% Registry Value Name: %regvalue% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2020	Access Approved	Warning	Change of Registry Key allowed. Registry Key: %regkey% [Details] Access Image Path: %path% Access User: %username%

Event ID	Task Category	Level	Log Description
			Mode: %mode%
2021	Access Approved	Warning	File access allowed: %path% An error occurred while checking the Trusted Hash List. [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2022	Access Approved	Warning	Process allowed by Fileless Attack Prevention: %path% %argument% [Details] Access User: %username% Parent Process 1 Image Path: %path% Parent Process 2 Image Path: %path% Parent Process 3 Image Path: %path% Parent Process 4 Image Path: %path% Mode: Unlocked Reason: %reason%
2503	Access Blocked	Warning	Change of File/Folder blocked: %path% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2505	Access Blocked	Warning	Change of Registry Value blocked. Registry Key: %regkey%

Event ID	Task Category	Level	Log Description
			Registry Value Name: %regvalue% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2506	Access Blocked	Warning	Change of Registry Key blocked. Registry Key: %regkey% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2507	Access Blocked	Information	Action completed successfully: %path% [Details] Action: %action% Source: %source%
2508	Access Blocked	Warning	Unable to take specified action: %path% [Details] Action: %action% Source: %source%
2509	Access Blocked	Warning	File access blocked: %path% [Details] Access Image Path: %path% Access User: %username%

Event ID	Task Category	Level	Log Description
			Mode: %mode% Reason: Not in Approved List File Hash blocked: %hash%
2510	Access Blocked	Warning	File access blocked: %path% [Details] Access Image Path: %path% Access User: %username% Mode: %mode% Reason: Hash does not match expected value File Hash blocked: %hash%
2511	Access Blocked	Information	Change of File/Folder blocked: %path% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2512	Access Blocked	Warning	Change of Registry Value blocked. Registry Key: %regkey% Registry Value Name: %regvalue% [Details] Access Image Path: %path% Access User: %username%

Event ID	Task Category	Level	Log Description
			Note Enabling the Service Creation Prevention feature triggers Event ID 2512.
2513	Access Blocked	Warning	Process blocked by Fileless Attack Prevention: %path% %argument% [Details] Access User: %username% Parent Process 1 Image Path: %path% Parent Process 2 Image Path: %path% Parent Process 3 Image Path: %path% Parent Process 4 Image Path: %path% Mode: locked Reason: %reason%
2514	Access Blocked	Warning	File access blocked : %BLOCKED_FILE_PATH% [Details] Access Image Path: %PARENT_PROCESS_PATH% Access User: %USER_NAME% Reason: Blocked file is in a folder that has the case sensitive attribute enabled.
3000	USB Malware Protection	Warning	Device access allowed: %path% [Details] Access Image Path: %path% Access User: %username%

Event ID	Task Category	Level	Log Description
			Device Type: %type%
3001	USB Malware Protection	Warning	Device access blocked: %path% [Details] Access Image Path: %path% Access User: %username% Device Type: %type%
3500	Network Virus Protection	Warning	Network virus allowed: %name% [Details] Protocol: TCP Source IP Address: %ip_address% Source Port: %port% Destination IP Address: %ip_address% Destination Port: 80
3501	Network Virus Protection	Warning	Network virus blocked: %name% [Details] Protocol: TCP Source IP Address: %ip_address% Source Port: %port% Destination IP Address: %ip_address% Destination Port: 80
4000	Process Protection Event	Warning	API Hooking/DLL Injection allowed: %path%

Event ID	Task Category	Level	Log Description
			[Details] Threat Image Path: %path% Threat User: %username%
4001	Process Protection Event	Warning	API Hooking/DLL Injection blocked: %path% [Details] Threat Image Path: %path% Threat User: %username%
4002	Process Protection Event	Warning	API Hooking allowed: %path% [Details] Threat Image Path: %path% Threat User: %username%
4003	Process Protection Event	Warning	API Hooking blocked: %path% [Details] Threat Image Path: %path% Threat User: %username%
4004	Process Protection Event	Warning	DLL Injection allowed: %path% [Details] Threat Image Path: %path% Threat User: %username%
4005	Process Protection Event	Warning	DLL Injection blocked: %path% [Details] Threat Image Path: %path%

Event ID	Task Category	Level	Log Description
			Threat User: %username%
4500	Changes in System	Information	File/Folder created: %path% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4501	Changes in System	Information	File modified: %path% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4502	Changes in System	Information	File/Folder deleted: %path% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4503	Changes in System	Information	File/Folder renamed: %path% New Path: %path% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%

Event ID	Task Category	Level	Log Description
4504	Changes in System	Information	Registry Value modified. Registry Key: %regkey% Registry Value Name: %regvalue% Registry Value Type: %regvaluetype% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4505	Changes in System	Information	Registry Value deleted. Registry Key: %regkey% Registry Value Name: %regvalue% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4506	Changes in System	Information	Registry Key created. Registry Key: %regkey% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4507	Changes in System	Information	Registry Key deleted. Registry Key: %regkey%

Event ID	Task Category	Level	Log Description
			[Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4508	Changes in System	Information	Registry Key renamed. Registry Key: %regkey% New Registry Key: %regkey% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%
5000	Device Control	Warning	Storage device access allowed: %PATH% [Details] Access Image path: %PATH% Access User: %USERNAME% Device Type: %TYPE% %DEVICEINFO%
5001	Device Control	Warning	Storage device access blocked: %PATH% [Details] Access Image path: %PATH% Access User: %USERNAME% Device Type: %TYPE% %DEVICEINFO%
6000	System	Information	%Result% [Details]

Event ID	Task Category	Level	Log Description
			Update Source: %SERVER% [Original Version] Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION% Damage Cleanup Template: %VERSION% Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION% [Updated Version] Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION% Damage Cleanup Template: %VERSION% Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%

Event ID	Task Category	Level	Log Description
6001	System	Warning	Update failed: %ERROR_MSG% (%ERROR_CODE%) [Details] Update Source: %SERVER% [Original Version] Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION % Damage Cleanup Template: %VERSION % Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION% [Updated Version] Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION % Damage Cleanup Template: %VERSION % Damage Cleanup Engine Configuration: %VERSION%

Event ID	Task Category	Level	Log Description
			Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%
6002	System	Information	Malware scan started: %SCAN_TYPE% [Details] Files to scan: %SCAN_FOLDER_TYPE% Scanned folders: %PATHS% Excluded paths: %PATHS% Excluded files: %PATHS% Excluded extensions: %PATHS% [Components] Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION % Damage Cleanup Template: %VERSION % Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%
6003	System	Information	Malware scan completed: %SCAN_TYPE %. Number of infected files: %NUM%

Event ID	Task Category	Level	Log Description
			[Details] Files to scan: %SCAN_FOLDER_TYPE% Scanned folders: %PATHS% Excluded paths: %PATHS% Excluded files: %PATHS% Excluded extensions: %PATHS% Start date/time: %DATE_TIME% End date/time: %DATE_TIME% Number of scanned files: %NUM% Number of infected files: %NUM% Number of cleaned files: %NUM% Number of files cleaned after reboot: %NUM% [Components] Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION % Damage Cleanup Template: %VERSION % Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%

Event ID	Task Category	Level	Log Description
6004	System	Warning	Malware scan unsuccessful: %SCAN_TYPE% %ERROR% [Details] Files to scan: %SCAN_FOLDER_TYPE% Scanned folders: %PATHS% Excluded paths: %PATHS% Excluded files: %PATHS% Excluded extensions: %PATHS% Start date/time: %DATE_TIME% End date/time: %DATE_TIME% Number of scanned files: %NUM% Number of infected files: %NUM% Number of cleaned files: %NUM% Number of files cleaned after reboot: %NUM% [Components] Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION % Damage Cleanup Template: %VERSION % Damage Cleanup Engine Configuration: %VERSION%

Event ID	Task Category	Level	Log Description
			Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%
6005	System	Information	Malware detected: %ACTION% File path: %PATH% [Details] Reboot required: %NEED_REBOOT% [Scan Result] Threat type: %TYPE% Threat name: %NAME% [Components] Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION % Damage Cleanup Template: %VERSION % Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%
6006	System	Warning	Malware detected. Unable to perform scan actions: %PATH% [Details]

Event ID	Task Category	Level	Log Description
			First action: %1ST_ACTION% Second action: %2ND_ACTION% Threat type: %TYPE% Threat name: %NAME% [Components] Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION% Damage Cleanup Template: %VERSION% Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%
6007	Maintenance Mode	Warning	Malware detected in Maintenance Mode (file quarantine successful): %PATH% [Details] Component versions: Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION%

Event ID	Task Category	Level	Log Description
			Damage Cleanup Template: %VERSION % Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%
6008	Maintenance Mode	Warning	Malware detected in Maintenance Mode (file quarantine unsuccessful): %PATH% [Details] Component versions: Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION % Damage Cleanup Template: %VERSION % Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%
6009	Maintenance Mode	Warning	Malware detected in Maintenance Mode: %PATH% [Details] Component versions:

Event ID	Task Category	Level	Log Description
			Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION % Damage Cleanup Template: %VERSION % Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%

Agent Error Code Descriptions

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

Table 13-2. 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.

Code	Description
0x80040205	Invalid status.
0x80040206	Out of memory.
0x80040207	Busy. Request ignored.
0x00040208	Retry. (Usually the result of a task taking too long)
0x80040208	System Reserved. (Not used)
0x80040209	The file path is too long.
0x0004020a	System Reserved. (Not used)
0x8004020b	System Reserved. (Not used)
0x0004020c	System Reserved. (Not used)
0x0004020d	System Reserved. (Not used)
0x8004020d	System Reserved. (Not used)
0x0004020e	Reboot required.
0x8004020e	Reboot required for unexpected reason.
0x0004020f	Allowed to perform task.
0x8004020f	Permission denied.
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)

Code	Description
0x80040214	System Reserved. (Not used)
0x00040215	Not found.
0x80040215	"Expected, but not found."
0x80040216	Authentication is locked.
0x80040217	Invalid password length.
0x80040218	Invalid characters in password.
0x00040219	Duplicate password. Administrator and Restricted User passwords cannot match.
0x80040220	System Reserved. (Not used)
0x80040221	System Reserved. (Not used)
0x80040222	System Reserved. (Not used)
0x80040223	File not found (as expected, and not an error).
0x80040224	System Reserved. (Not used)
0x80040225	System Reserved. (Not used)
0x80040240	Library not found.
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)

Code	Description
0x80040270	System Reserved. (Not used)
0x80040271	System Reserved. (Not used)
0x80040272	System Reserved. (Not used)
0x80040273	System Reserved. (Not used)
0x80040274	System Reserved. (Not used)
0x80040275	System Reserved. (Not used)
0x80040280	Invalid Activation Code.
0x80040281	Incorrect Activation Code format.

Server Event Log Descriptions

To display the **Server Events** screen, go to **Logs & Reports** > **Server Events** in the navigation at the top of the web console.

Table 13-3. Server Event Log Descriptions

Event ID	Server Event	Description
1001	Log on console	Logged on web console.
1002	Log off console	Logged off web console.
1003	Session timeout	Web console session timed out. Account '%user_name%' was logged off automatically .
1011	Unable to send reports	Unable to send scheduled reports to %email_address%.
1012	Unable to send notifications	Unable to send notifications to %email_address%.
2001	Create account	Created Intelligent Manager account '%user_name %'.

EVENT ID	SERVER EVENT	DESCRIPTION
2002	Delete account	Deleted Intelligent Manager account '%user_name %'.
2003	Modify account	Modified Intelligent Manager account '%user_name %' %field_name%.
3001	Purge agent event logs - automatic	Automatic purge of agent event logs.
3002	Purge agent event logs - manual	Manual purge of agent event logs.
3003	Back up agent event logs	Automatic back up of agent event logs. Path: %filepath%.
3004	Purge server event logs - automatic	Automatic purge of server event logs.
3005	Purge server event logs - manual	Manual purge of server event logs.
3006	Back up server event logs	Automatic back up of server event logs. Path: %filepath%.

EVENT ID	SERVER EVENT	DESCRIPTION
4001	Take action on unapproved blocked file	Request sent to endpoint(s): Add blocked file to Approved List. File name: %file_name% File hash: %file_hash% (SHA-1) Request sent to endpoint(s): Delete the blocked file. File name: %file_name% File hash: %file_hash% (SHA-1) Request sent to endpoint(s): Ignore the blocked file. File name: %file_name% File hash: %file_hash% (SHA-1) Request sent to endpoint(s): Quarantine the file. File name: %file_name% File hash: %file_hash% (SHA-1) Request sent to endpoint(s): Restore the file from quarantine. File name: %file_name% File hash: %file_hash% (SHA-1)
4002	Mark as closed	Marked %num% event(s) closed.
4003	Mark as open	Marked %num% event(s) opened.
4004	Release the quarantined malicious file	Request sent to endpoint(s): Restore the file from quarantine. File name: %file_name% File hash: %file_hash% (SHA-1)
4005	Delete the quarantined malicious file	Request sent to endpoint(s): Delete the file from quarantine. File name: %file_name% File hash: %file_hash% (SHA-1)
4006	Take action on unapproved fileless attack	Request sent to endpoint(s): Add blocked process chain and command argument. Process chain: %process_name% Command argument: %parameter% Request sent to endpoint(s): Ignore blocked process chain and command argument. Process chain: %process_name% Command argument: %parameter%

Event ID	Server Event	Description
5001	Turn Application Lockdown on	Turned Application Lockdown on for endpoint(s).
5002	Turn Application Lockdown off	Turned Application Lockdown off for endpoint(s).
5011	Add trusted file hashes	Added 1 trusted file hash to endpoint(s). Added %num% trusted file hashes to endpoint(s).
5013	Delete approved files	Removed specified items from the Approved List on endpoint(s) using SLtasks.exe.
5021	Block access from storage devices	Blocked access from storage devices on endpoint(s).
5023	Allow access from storage devices	Allowed access from storage devices on endpoint(s).
5025	Add trusted USB device	Add trusted USB device on selected endpoint(s)
5601	Export agent settings	Exported (%file_desc%) from %endpoint_name%.
5602	Import agent settings	Imported (%file_desc%) to endpoint(s).
5800	Change agent administrator password	Changed password on endpoint(s).
5700	Scan for malware	Scanned endpoint(s) for malware.
5701	Update agent components	Updated agent components on endpoint(s).
5900	Update agent Approved List	Updated Approved List on endpoint(s).
6001	Deploy agent patch	Deploy agent patch to endpoint(s). Patch name: %patch_name%

EVENT ID	SERVER EVENT	DESCRIPTION
6101	Agent transfer	Agent transferred to new Intelligent Manager server
6201	Turn Maintenance Mode on	Turned Maintenance Mode on for endpoint(s).
6202	Turn Maintenance Mode off	Turned Maintenance Mode off for endpoint(s).

Index

T

U

W

TREND MICRO INCORPORATED

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

www.trendmicro.com

Item Code: SLEM08835/191007