



# 2.0 TREND MICRO™ Safe Lock™ Intelligent Manager Service Pack 1 Patch 3 Administrator's Guide

A powerful lockdown solution for fixed-function computers



Endpoint Security

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

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

© 2018 Trend Micro Incorporated. All Rights Reserved. Trend Micro, the Trend Micro t-ball logo, Trend Micro Safe Lock, Safe Lock Intelligent Manager, Trend Micro Portable Security, Trend Micro Portable Security 2, and TrendLabs are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Document Part No.: SLEM28239/180418

Release Date: July 2018

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](mailto: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](https://www.trendmicro.com/en_us/about/legal/privacy-policy-product.html)

# Table of Contents

## Preface

Preface .....	vii
About the Documentation .....	vii
Audience .....	viii
Document Conventions .....	viii
Terminology .....	ix

## Chapter 1: Introduction

About Trend Micro Safe Lock Intelligent Manager .....	1-2
What's New .....	1-2
Server Features and Benefits .....	1-4
Safe Lock Intelligent Manager Requirements .....	1-6
Server Accounts Overview .....	1-9
About Trend Micro Safe Lock .....	1-11
What's New .....	1-11
Agent Features and Benefits .....	1-13
Safe Lock Requirements .....	1-15
Agent Use Overview .....	1-23

## Chapter 2: Managing Safe Lock Agents

About the Agent Management Screen .....	2-2
Managing the Agent Tree .....	2-2
Searching for Agents .....	2-3
Grouping Agents .....	2-4
Removing Agents and Groups .....	2-4
Checking Agent Statuses and Settings .....	2-5
Editing Tags .....	2-7
Configuring Agent Settings .....	2-8
Remotely Changing Application Lockdown Status .....	2-9

Remotely Adding Trusted Applications and Files .....	2-10
Updating the Approved List on Safe Lock Agents .....	2-12
Collecting Event Logs .....	2-12
Checking Agent Connections .....	2-13
Remotely Exporting Agent Settings .....	2-14
Remotely Importing Agent Settings .....	2-15
Remotely Deploying Patches to Safe Lock Agents .....	2-16

### **Chapter 3: Monitoring Safe Lock**

About the Dashboard .....	3-2
About Web Console Accounts and the Dashboard .....	3-2
About Dashboard Tabs .....	3-2
About Widgets .....	3-5
About the Agent Events Screen .....	3-9
Querying Agent Event Logs .....	3-9
Marking Warning Events .....	3-12
About the Server Events Screen .....	3-13
Querying Server Event Logs .....	3-13
Maintaining Logs .....	3-15
Scheduled Reports .....	3-17
Forwarding Events to an External Syslog Server .....	3-18

### **Chapter 4: Configuring Administration Settings**

About the Component Updates Screen .....	4-2
Manually Updating Components .....	4-2
Scheduling Component Updates .....	4-3
Downloading an Up-to-Date Agent Installer Package .....	4-3
Configuring Component Download Locations .....	4-5
Configuring Notification Settings .....	4-5
Example Notification Messages .....	4-8
Configuring SMTP Server Settings .....	4-9
About the Account Management Screen .....	4-10
Adding Accounts .....	4-11

Editing Accounts .....	4-12
Configuring Proxy Settings .....	4-13
About the License Management Screen .....	4-14
Changing Activation Codes .....	4-15

## **Chapter 5: Using the Agent Console**

Setting Up the Approved List .....	5-2
Configuring Pop-up Notifications for Blocked Files .....	5-5
About the Agent Console .....	5-6
Viewing Safe Lock Statuses .....	5-9
About the Approved List .....	5-10
About Hashes .....	5-12
Configuring the Approved List .....	5-13
Account Types .....	5-17
Configuring Passwords .....	5-18
About Feature Settings .....	5-19
Enabling or Disabling Feature Settings .....	5-22

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

Using SLCmd at the Command Line Interface (CLI) .....	6-2
SLCmd Program and Console Function Comparison .....	6-2
SLCmd Program Commands .....	6-4

## **Chapter 7: Managing Agents Remotely**

The Remote Setup Tool (SLrst) .....	7-2
Remote Installation Considerations .....	7-3
Preparing the Agent Target Files .....	7-12
Downloading an Up-to-Date Agent Installer Package .....	7-15
Installing Agents Remotely .....	7-17
Customizing Agent Installation Remotely Using a Setup.ini File .	7-18
Applying Patches and Hotfixes to Agents Remotely .....	7-19
Uninstalling Agents Remotely .....	7-20
Restarting Agents Remotely .....	7-21

The Remote Tasks Tool (SLtasks) .....	7-22
Removing Files from Agent Approved Lists .....	7-23
Renewing Agent Licenses .....	7-25
Applying Message Time Groups .....	7-27
Updating the Agent Password Remotely .....	7-31

## **Chapter 8: Local Agent Installation**

Local Installation Overview .....	8-2
Installing from Windows .....	8-3
Setting Up the Approved List .....	8-11
Installation Using the Command Line .....	8-13
Installer Command Line Interface Parameters .....	8-14
Customizing Installation Parameters .....	8-16
Setup.ini File Arguments .....	8-17

## **Chapter 9: Working with the Agent Configuration File**

Working with the Agent Configuration File .....	9-2
Changing Advanced Settings .....	9-2
Configuration File Syntax .....	9-3
Configuration File Parameters .....	9-8

## **Chapter 10: Local Agent Uninstallation**

Uninstalling Agents from Windows .....	10-2
--	------

## **Chapter 11: Troubleshooting & FAQs**

Troubleshooting Remote Agent Installations .....	11-2
Frequently Asked Questions .....	11-2
Is a reboot required after installation or uninstallation? .....	11-2
How to migrate Safe Lock agents to another Intelligent Manager? .....	11-3



## Chapter 12: Technical Support

Troubleshooting Resources .....	12-2
Using the Support Portal .....	12-2
Threat Encyclopedia .....	12-2
Contacting Trend Micro .....	12-3
Speeding Up the Support Call .....	12-4
Sending Suspicious Content to Trend Micro .....	12-4
Email Reputation Services .....	12-4
File Reputation Services .....	12-5
Web Reputation Services .....	12-5
Other Resources .....	12-5
Download Center .....	12-5
Documentation Feedback .....	12-6

## Chapter 13: Appendix: Reference

Enabling Local Administrator Accounts .....	13-2
Enabling Local Accounts for Default Shares .....	13-3
Agent Event Log Descriptions .....	13-4
Agent Error Code Descriptions .....	13-31
Server Event Log Descriptions .....	13-34

## Index

Index .....	IN-1
-------------	------



# 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 on page vii*
- *Audience on page viii*
- *Document Conventions on page viii*
- *Terminology on page ix*

## 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:  <a href="http://esupport.trendmicro.com">http://esupport.trendmicro.com</a>

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
<b>Bold</b>	Menus and menu commands, command buttons, tabs, and options
<i>Italics</i>	References to other documents
Monospace	Sample command lines, program code, web URLs, file names, and program output
<b>Navigation &gt; Path</b>	The navigation path to reach a particular screen For example, <b>File &gt; Save</b> means, click <b>File</b> and then click <b>Save</b> on the interface
 <b>Note</b>	Configuration notes

CONVENTION	DESCRIPTION
 <b>Tip</b>	Recommendations or suggestions
 <b>Important</b>	Information regarding required or default configuration settings and product limitations
 <b>WARNING!</b>	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

<b>TERMINOLOGY</b>	<b>DESCRIPTION</b>
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:  <code>"c:\Program Files\Trend Micro\Safe Lock"</code>
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:  <code>"c:\Program Files\Trend Micro\Safe Lock Intelligent Manager"</code>

# Chapter 1

## Introduction

Trend Micro Safe Lock Intelligent Manager 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™ on page 1-2*
- *About Trend Micro Safe Lock on page 1-11*

# 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 2.0 Service Pack 1 Patch 3 includes the following new features and enhancements:



**TABLE 1-1. What's New in Trend Micro Safe Lock Intelligent Manager 2.0 Service Pack 1 Patch 3**

FEATURE	DESCRIPTION
Fileless Attack Prevention	<p>Safe Lock Intelligent Manager introduces Fileless Attack Prevention to this release, and provides the following features:</p> <ul style="list-style-type: none"> <li>• Monitors processes, process chains and command line arguments commonly associated with fileless attacks</li> <li>• Manage events based on the last 5 parent processes involved in the process chain</li> <li>• Manage events based on the command line arguments used</li> <li>• Apply action to other endpoints with the same blocked process chains and command line arguments</li> </ul> <hr/> <p> <b>Note</b></p> <p>Since Fileless Attack Prevention blocks the execution of all target processes by default, ensure that the Fileless Attack Prevention feature has been properly configured to allow the execution of processes required in your environment.</p>
Agent Management enhancements	<p>Safe Lock Intelligent Manager introduces the following enhancements for agent management:</p> <ul style="list-style-type: none"> <li>• Apply update patch to selected agents remotely</li> <li>• Sort agents according to agent version</li> </ul>

FEATURE	DESCRIPTION
Audit Log enhancements	Safe Lock Intelligent Manager introduces the following enhancements for the audit logs: <ul style="list-style-type: none"> <li>• Support for multiple filters on the <b>Agent Event</b> and <b>Server Event</b> screens</li> <li>• Export list of deployed endpoints and trusted hashes in the <b>Server Events</b> screen</li> <li>• Improved deployment details screen:               <ul style="list-style-type: none"> <li>• Easier access from the <b>Server Events</b> screen</li> <li>• Filter and export of deployment details</li> <li>• Inclusion of IP address information</li> </ul> </li> </ul>
Installer flag for trusted hash list import/export	Safe Lock Intelligent Manager adds the installer flag to the resulting <code>.txt</code> file when importing or exporting the trusted hash list.

## 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.

FEATURE	BENEFIT
Centralized Agent Management	<p>Trend Micro Intelligent Manager allows administrators to perform the following tasks:</p> <ul style="list-style-type: none"> <li>• Monitor Safe Lock agent status</li> <li>• Examine connection status</li> <li>• View configurations</li> <li>• Collect agent logs on-demand or by policy</li> <li>• Remotely turn agent Application Lockdown on or off</li> <li>• Initialize the Approved List</li> <li>• Deploy agent patches</li> <li>• Add trusted files</li> </ul>
Centralized Event Management	<p>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.</p>
Root Cause Information Analysis	<p>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.</p>
Server Event Auditing	<p>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.</p>

## 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	<ul style="list-style-type: none"><li>• Windows 7 No-SP/SP1 (Enterprise/Ultimate) (32-bit and 64-bit)</li><li>• Windows 8 No-SP (Professional/Enterprise) (32-bit and 64-bit)</li><li>• Windows 8.1 No-SP (Professional/Enterprise) (32-bit and 64-bit)</li><li>• Windows 10 (Enterprise/IoT Enterprise) (32-bit and 64-bit)<ul style="list-style-type: none"><li>• Anniversary Update (Redstone 1)</li><li>• Creators Update (Redstone 2)</li></ul></li></ul>

REQUIRED SOFTWARE	SPECIFICATIONS
Operating systems -  Windows server	<ul style="list-style-type: none"> <li>• Windows Server 2008 SP1/SP2 (Standard/Enterprise/Storage) (32-bit and 64-bit)</li> <li>• Windows Server 2008 R2 No-SP/SP1 (Standard/Enterprise/Storage) (64-bit)</li> <li>• Windows Server 2012 No-SP (Foundation/Essentials/Standard/Datacenter) (64-bit)</li> <li>• Windows Server 2012 R2 No-SP (Foundation/Essentials/Standard/Datacenter) (64-bit)</li> <li>• Windows Server 2012 R2 for Embedded Systems No-SP (64-bit)</li> <li>• Windows Server 2016 (Standard) (64-bit)</li> <li>• Windows Storage Server 2016</li> </ul> <hr/> <p> <b>Note</b> Safe Lock Intelligent Manager Intelligent Manager 2.0 SP1 Patch 2 or later no longer supports installation on Windows XP or Windows Server 2003. To update existing installations of Safe Lock Intelligent Manager Intelligent Manager 2.0 SP1 Patch 1 or earlier on these platforms, please install the SP1 Patch 2 or later cumulative patch module.</p>
Web browser (for Safe Lock Intelligent Manager web console access)	<ul style="list-style-type: none"> <li>• Microsoft Internet Explorer 9.0, 10.0, 11.0 (32/64bit)</li> <li>• The latest version of Google Chrome / Chrome Portable</li> <li>• Mozilla Firefox 6 or later</li> </ul> <hr/> <p> <b>Note</b></p> <ul style="list-style-type: none"> <li>• Older versions of Internet Explorer are unsupported for security enhancement.</li> <li>• When accessed using iOS systems, Safe Lock Intelligent Manager does not support any export functions via the web console.</li> </ul>

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

REQUIRED HARDWARE	SPECIFICATION
RAM	<ul style="list-style-type: none"> <li>• 2 GB minimum</li> <li>• 4 GB or more recommended</li> </ul>
Processor	<ul style="list-style-type: none"> <li>• 1 CPU core minimum</li> <li>• 1 CPU core or more recommended</li> </ul>
Available disk space	<ul style="list-style-type: none"> <li>• 10 GB minimum</li> <li>• 20 GB or more recommended</li> </ul>

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

REQUIRED HARDWARE	SPECIFICATION
RAM	<ul style="list-style-type: none"> <li>• 2 GB minimum</li> <li>• 4 GB or more recommended</li> </ul>
Processor	<ul style="list-style-type: none"> <li>• 1 CPU core minimum</li> <li>• 2 CPU cores or more recommended</li> </ul>
Available disk space	<ul style="list-style-type: none"> <li>• 10 GB minimum</li> <li>• 20 GB or more recommended</li> </ul>

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

REQUIRED HARDWARE	SPECIFICATION
RAM	<ul style="list-style-type: none"> <li>• 4 GB minimum</li> <li>• 8 GB or more recommended</li> </ul>
Processor	<ul style="list-style-type: none"> <li>• 1 CPU core minimum</li> <li>• 2 CPU cores or more recommended</li> </ul>

REQUIRED HARDWARE	SPECIFICATION
Available disk space	<ul style="list-style-type: none"> <li>• 30 GB minimum</li> <li>• 50 GB or more recommended</li> </ul>

**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	<ul style="list-style-type: none"> <li>• 32 GB or more required</li> </ul>
Processor	<ul style="list-style-type: none"> <li>• 2 CPU cores minimum</li> <li>• 4 CPU cores or more recommended</li> </ul>
Available disk space	<ul style="list-style-type: none"> <li>• 1 TB minimum</li> <li>• 2 TB or more recommended</li> </ul>

## 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.	<ul style="list-style-type: none"> <li>• Admin</li> </ul>

	TASK	ACCOUNT PRIVILEGE REQUIRED
2	Use remote deployment tools ( <code>SLrst.exe</code> ) to centrally deploy agents from the server.	<ul style="list-style-type: none"> <li>N/A</li> </ul> <hr/>  <b>Note</b> Using the <code>SLrst.exe</code> 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 ( <code>SLtasks.exe</code> ) to manage the Approved List and Write Protection List on Safe Lock agents.	<ul style="list-style-type: none"> <li>Admin</li> <li>Full Control</li> </ul>
4	Monitor Server Event logs.	<ul style="list-style-type: none"> <li>Admin</li> <li>Full Control</li> </ul>
5	Monitor Agent Event logs.	<ul style="list-style-type: none"> <li>Admin</li> <li>Full Control</li> <li>Storage Device Control</li> <li>Read Only</li> </ul>
6	Download Trend Micro Safe Lock agent installer image.	<ul style="list-style-type: none"> <li>Admin</li> <li>Full Control</li> <li>Storage Device Control</li> <li>Read Only</li> </ul>
7	Change the administrator password remotely	<ul style="list-style-type: none"> <li>Admin</li> </ul>
8	Update Safe Lock Intelligent Manager license information	<ul style="list-style-type: none"> <li>Admin</li> <li>Full Control</li> </ul>



	<b>TASK</b>	<b>ACCOUNT PRIVILEGE REQUIRED</b>
9	Deploy agent patch	<ul style="list-style-type: none"><li>• Admin</li><li>• Full Control</li></ul>
10	Add trusted files	<ul style="list-style-type: none"><li>• Admin</li><li>• Full Control</li></ul>



## About Trend Micro Safe Lock

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

## What's New

Trend Micro Safe Lock 2.0 Service Pack 1 Patch 3 includes the following new features and enhancements.

**TABLE 1-8. What's New in Trend Micro Safe Lock 2.0 Service Pack 1 Patch 3**

FEATURE	DESCRIPTION
Platform support enhancements	<p data-bbox="538 293 1049 318">Safe Lock adds support for the following platforms:</p> <ul data-bbox="538 337 1063 496" style="list-style-type: none"> <li data-bbox="538 337 838 362">• Windows 10 Professional</li> <li data-bbox="538 381 1060 406">• Windows 10 Fall Creators Update (Redstone 3)</li> <li data-bbox="538 425 1033 449">• Windows 10 April 2018 Update (Redstone 4)</li> <li data-bbox="538 469 892 493">• Windows Storage Server 2016</li> </ul> <hr data-bbox="538 529 1089 532"/> <p data-bbox="538 542 1089 688">  <b>Note</b>            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.         </p> <hr data-bbox="538 695 1089 698"/> <p data-bbox="538 732 1089 781">For more information, see <a href="#">Operating Systems on page 1-16</a>.</p>
Fileless Attack Prevention	<p data-bbox="538 810 1029 859">Safe Lock adds Fileless Attack Prevention to this release, and provides the following features :</p> <ul data-bbox="538 878 1063 1101" style="list-style-type: none"> <li data-bbox="538 878 1063 956">• Monitors processes, process chains and command line arguments commonly associated with fileless attacks</li> <li data-bbox="538 976 1009 1024">• Manage events based on the last 5 parent processes involved in the process chain</li> <li data-bbox="538 1044 1022 1092">• Manage events based on the command line arguments used</li> </ul> <hr data-bbox="538 1151 1089 1154"/> <p data-bbox="538 1164 1089 1365">  <b>Note</b>            Since Fileless Attack Prevention blocks the execution of all target processes by default, ensure that the Fileless Attack Prevention feature has been properly configured to allow the execution of processes required in your environment.         </p>

FEATURE	DESCRIPTION
Windows Event Log enhancements	Safe Lock introduces the following enhancements for the Windows Event Log: <ul style="list-style-type: none"> <li>• Default log size increased from 1 MB to 10 MB</li> <li>• Hash value of the blocked file added to the Windows Event Log</li> </ul>
Support Secure Boot option	Safe Lock adds support for the Secure Boot feature of Windows 10.
Compatibility with Microsoft BitLocker	Safe Lock adds support for Microsoft BitLocker to ensure compatibility with the Safe Lock agents.
Trend Micro signature check enhancements	Safe Lock adds an option in <code>setup.ini</code> to enable/disable the Trend Micro signature check for remote patch.

## Agent Features and Benefits

Trend Micro Safe Lock includes the following features and benefits.

### Application Lockdown

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

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

### Exploit Prevention

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

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

## **Easy Management**

When software needs to be installed or updated, the Trusted Updater and Predefined Trusted Updater List provide an easy way to make changes to the endpoint and automatically add new or modified files to the Approved List, all without having to unlock Trend Micro Safe Lock.

## **Small Footprint**

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

## **Role Based Administration**

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

## **Graphical and Command Line Interfaces**

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

## **Trend Micro Portable Security Compatible**

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

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

---

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

**Note**

- Safe Lock installed on Windows 2000 SP4 (without update rollup), Windows XP SP1, or Windows Server 2003 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, and Predefined Trusted Updater.
  - Safe Lock does not support a custom action of “quarantine” on Windows XP or Windows 2003.
- 
- Windows Vista No-SP/SP1/SP2 (32-bit) (except Starter and Home editions)
  - Windows 7 No-SP/SP1 (32-bit and 64-bit) (except Starter and Home editions)
  - Windows 8 No-SP (32-bit and 64-bit)
  - Windows 8 No-SP (Professional/Enterprise) (32-bit and 64-bit)
  - Windows 8.1 No-SP (Professional/Enterprise with Bing) (32-bit and 64-bit)
  - Windows 8.1 No-SP (32-bit and 64-bit)
  - Windows 10 (Professional/Enterprise/IoT Enterprise) (32-bit and 64-bit)
    - Anniversary Update (Redstone 1)
    - Creators Update (Redstone 2)
    - Fall Creators Update (Redstone 3)
    - April 2018 Update (Redstone 4)



- Unlock the endpoint before updating your Windows 10 operating system to the Anniversary Update, Creators Update, Fall Creators Update or April 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.
    - Windows 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.
- 

Windows Server:

- Windows 2000 Server SP4\* (32-bit)
- 



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

---

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



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



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

**Note**

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

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

Windows Embedded Standard:

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

**Note**

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

- 
- Windows Embedded Standard 2009 (32-bit)
  - Windows Embedded Standard 7 (32-bit and 64-bit)
  - Windows Embedded Standard 8 (32-bit and 64-bit)

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

Windows Embedded POSReady:

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

Windows Embedded Enterprise:

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



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

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

Windows Embedded Server:

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

**Note**

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

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

**Note**

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

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

#### Windows Storage Server

- Windows Storage Server 2016

## Agent Upgrade Preparation

---

**WARNING!**

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

---

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

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

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



**Note**

Safe Lock supports remote installation using Safe Lock Intelligent Manager.

## Supported Methods for Updating Safe Lock Agents

Safe Lock agents can be updated using various methods depending on its current version.

**TABLE 1-11. Supported Methods for Updating Safe Lock Agents**

CURRENT VERSION	TARGET VERSION	SUPPORTED METHOD FOR UPDATING SAFE LOCK AGENTS			
		LOCAL INSTALLATION		REMOTE INSTALLATION	
		USING AN INSTALLER	USING A PATCH MODULE	REMOTE SETUP TOOL	REMOTE TASKS TOOL
1.1	Latest version	✓			
2.0			✓	✓	
2.0 Patch 1			✓	✓	
2.0 SP 1			✓	✓	✓
2.0 SP1 Patch 1			✓	✓	✓
2.0 SP1 Patch 2			✓	✓	✓

**Note**

If you are running Safe Lock Intelligent Manager on Windows 2003 or earlier versions, we recommend applying the hotfix for enforcing TLSv10 (`tmsl_20_win_en_hfb_enforce_TLSv10.exe`) to avoid possible communication issues between the Intelligent Manager and the agent. Refer to the **Product Patch** tab on the [Trend Micro Download Center](#) for details.

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

## 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 <a href="#">Searching for Agents on page 2-3</a> .
Create agent groups	For more information, see <a href="#">Grouping Agents on page 2-4</a> .
Remove agent groups	For more information, see <a href="#">Removing Agents and Groups on page 2-4</a> .
View individual agent information	For more information, see <a href="#">Checking Agent Statuses and Settings on page 2-5</a> .
Move agents or groups	Select one or more agents or groups and click <b>Move</b> .
Edit tags	Edit tags to help you identify and search for agents. For more information, see <a href="#">Editing Tags on page 2-7</a> .



TASK	DETAILS
Export agent settings and summary in a CSV file	Select one or more agents and click <b>Export</b> .

## Searching for Agents

### Procedure

- Go to **Agents** in the navigation at the top of the web console.  
The **Agent Management** screen appears.
- 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
<b>Endpoint</b>	Type the full endpoint host name to locate the specific endpoint.
<b>Tags</b>	Type the tag name.
<b>IP Address</b>	Type the IPv4 address.
<b>IP Range</b>	Type the IPv4 address.
<b>Operating System</b>	Select an operating system.
<b>Application Lockdown State</b>	Select the Application Lockdown state: <b>Application Lockdown On</b> or <b>Application Lockdown Off</b> .
<b>Last Connection</b>	Select from the default time ranges or <b>Custom</b> 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**.



- The group name must be within 64 characters.
  - You can establish up to 9 layers of subfolders to the Group directory, with up to 1000 folders at each group layer.
- 

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



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, and the last agent upgrade time.
- 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 8-16](#).

---

### 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.

**Agent Status**


**WINXP**

IP Address: 192.168.184.141

Operating System: Microsoft Windows XP Professional Service Pack 3 build 2600, 32-bit

Tags: ATM002-NAT

**Summary** | Safe Lock Settings

 **Application Lockdown On**

Application Lockdown on since: 12/12/2016 16:37:46

Sent Turn Application Lockdown Off request to agent on 12/12/2016 15:51:03, Success

Group:	Diebold
Number of approved applications:	9482
Approved List last updated on:	10/25/2016 19:20:31
Status collected on:	12/12/2016 16:38:11
Logs collected on:	12/12/2016 16:37:37 <a href="#">View Logs</a>
Collection last attempted on:	--
NAT connect frequency:	5 minutes
Last connected on:	12/12/2016 16:36:29
License status:	Activated
License version:	Full
License expires on:	Unlimited
Agent version:	2.0.5516
Last agent upgrade:	10/25/2016 18:37:52
Registered on:	12/12/2016 13:30:01

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 <a href="#">Remotely Changing Application Lockdown Status on page 2-9</a> .
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 <b>Send Command &gt; Configure Device Control</b> .
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 <a href="#">Remotely Adding Trusted Applications and Files on page 2-10</a> .
Update Approved List	Update the Approved List on selected agents by performing an inventory scan  For more information, see <a href="#">Updating the Approved List on Safe Lock Agents on page 2-12</a> .
Collect event logs	For more information, see <a href="#">Collecting Event Logs on page 2-12</a> .

TASK	DETAILS
Check Connection	Check the connection status of selected Safe Lock Agents For more information, see <a href="#">Checking Agent Connections on page 2-13</a> .
Export Settings	Export the Approved List or configuration settings for selected agents For more information, see <a href="#">Remotely Exporting Agent Settings on page 2-14</a> .
Import Settings	Import the Approved List or configuration settings for selected agents For more information, see <a href="#">Remotely Importing Agent Settings on page 2-15</a> .
Deploy Agent Patch	Upgrade selected agents by uploading a patch file. For more information, see <a href="#">Remotely Deploying Patches to Safe Lock Agents on page 2-16</a> .

## 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**
- 

## 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 2-11](#).
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 2-10](#).

---

### 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.
- 

## 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 **Command Deployment Status** screen. The icons on the **Approved List** column display the current progress status.

---

## 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 **Command Deployment Status** window.

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

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

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

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

**Note**

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

---

## Remotely Importing Agent Settings

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

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

---

### Procedure

1. Prepare a customized agent configuration file or Approved List.
  - a. Export and download an agent configuration file or Approved List. For detailed steps, see [Remotely Exporting Agent Settings on page 2-14](#).
  - b. Customize the downloaded file.

**Note**

Trend Micro Safe Lock Intelligent Manager can only import an Approved List of up to 20 MB and a configuration file of up to 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 on page 3-2*
- *About the Agent Events Screen on page 3-9*
- *About the Server Events Screen on page 3-13*
- *Maintaining Logs on page 3-15*

## 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 3-17*.

## 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 Triggering 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.

The following widgets are available:

WIDGET	CATEGORY	DESCRIPTION
Application Lockdown State	Agent Status	Displays the Application Lockdown State for agents.

<b>WIDGET</b>	<b>CATEGORY</b>	<b>DESCRIPTION</b>
Versions	Agent Status	Displays the number of endpoints with specific versions of Safe Lock installed.
Open Warnings	Events	Displays the latest open warnings.
Top Endpoints Triggering Blocked Events	Events	Displays the endpoints that triggered the most blocked events.
Blocked Event History	Events	Displays blocked events during a specified time period.
Top Blocked Files	Events	Displays the files that are blocked the most.
Blocked File Scan Results	Events	Displays malware scan results for blocked files.
Latest Component Updates	Server Status	Displays the latest versions of components.


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.

## Using Widgets

Perform the following tasks on each widget:

TASK	STEPS
Move a widget	<p>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.</p> <hr/> <p> <b>Tip</b> 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.</p>
Resize a widget	<p>Horizontally resize a widget on a multi-column tab by doing the following:</p> <ol style="list-style-type: none"> <li>1. Hover the pointer at the edge of a widget. A vertical, gray bar appears.</li> <li>2. Drag the pointer left or right.</li> </ol> <p>Vertically resize widgets on a multi-column tab by enabling <b>Auto-fit</b> in the <b>Tab Settings</b>. This automatically adjusts widgets to be the same height as the widgets beside them.</p>
Refresh widget data	Click the <b>Refresh</b> icon at the top of the widget.
Specify automatic refresh settings	<ol style="list-style-type: none"> <li>1. Click the <b>More Options</b> icon at the top of the widget.</li> <li>2. Select <b>Refresh Settings</b>. The <b>Refresh Settings</b> screen appears.</li> <li>3. To enable automatic refresh for this widget, do the following: <ol style="list-style-type: none"> <li>a. Select <b>Automatically refresh the widget</b>.</li> <li>b. Specify a frequency.</li> </ol> </li> </ol>
Rename a widget	<ol style="list-style-type: none"> <li>1. Click the <b>More Options</b> icon at the top of the widget.</li> <li>2. Select <b>Widget Settings</b>. The <b>Widget Settings</b> screen appears.</li> <li>3. Type a meaningful title for the widget.</li> </ol>

TASK	STEPS
Close a widget	<ol style="list-style-type: none"> <li>1. Click the <b>More Options</b> icon at the top of the widget.</li> <li>2. Select <b>Close Widget</b>.</li> </ol>

## 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 Widget**.

The **Add Widget** 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**.

---

# 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.

When Lockdown is off and a file not on an agent's Approved List attempts to run or make changes to the endpoint, Safe Lock logs the event but allows the file to run.

When Lockdown is on and a file not on an agent's Approved List attempts to run or make changes to the endpoint, Safe Lock stops the file and may prompt the user for the appropriate action. Event logs contain information from managed agents about files not in the Approved List and any action taken.

You can take the following actions on files not in the Approved List when Lockdown is on:

- “Add to Approved List”: Prevent the file from executing for this instance but add the file to the agent's Approved List.
- “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 **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 **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 or folder** or **Registry key or value**, and click **Search**. **File or folder** searches support partial string matching.
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 `tms11og.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
<b>Time Period</b>	Do one of the following: <ul style="list-style-type: none"> <li>• Select a listed time range.</li> <li>• Specify a custom time range.               <ol style="list-style-type: none"> <li>a. Go to <b>Custom</b> in the list.</li> <li>b. Specify your custom time range.</li> <li>c. Click <b>Search</b>.</li> </ol> </li> </ul>
<b>All Users</b>	Displays all events logged by all users.
<b>User Name</b>	Displays all events logged by a specific user.
<b>Endpoint name</b>	Type the endpoint host name (first few letters or complete name), and click <b>Search</b> .
<b>Group name</b>	Displays all events logged by the specific groups.
<b>All Events</b>	Displays all events logged by agents.
<b>Event Type</b>	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**

- Safe Lock Intelligent Manager only purges the agent events marked **Closed**.
  - 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 3-11*.

See *Exporting Server Event Logs on page 3-15*.

## 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 <b>Send scheduled reports</b> 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 <a href="#">About Default Tabs on page 3-3</a>
Send scheduled reports	Set the frequency and time for the scheduled reports on a daily, weekly, or monthly basis.  <div style="border: 1px solid black; padding: 5px;">  <b>Note</b>            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.         </div>

TASK	DESCRIPTION
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.
-

# 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 on page 4-2*
- *Configuring Component Download Locations on page 4-5*
- *Configuring Notification Settings on page 4-5*
- *About the Account Management Screen on page 4-10*
- *Configuring Proxy Settings on page 4-13*
- *About the License Management Screen on page 4-14*

## 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.

Perform the following tasks from this screen:

FUNCTION	DESCRIPTION
<b>Update</b>	Manually update the components you select.
<b>Schedule Updates</b>	Configure the update schedule. Enable or disable scheduled updates for each component.
<b>Download Agent Installer Package</b>	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:

TMSL2.0\_<language\_abbreviation>.zip

For example:

VALID	NOT VALID
TMSL2.0_EN.zip	TMSL2.0_EN (1).zip
TMSL2.0_JA.zip	TMSL2.0_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
<b>Trend Micro ActiveUpdate server</b>	Use the Trend Micro-managed update server on the Internet.
<b>Internet or local server</b>	Specify an update server that does not require authentication.
<b>Local server requiring authentication</b>	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 FileHash\_20170612110747.txt.bat.  
Safe Lock required action to the file on 10-02-2017 20:09:06.

Safe Lock scanned the file. Scan results are displayed below.  
To manage this event, go to <https://10.1.192.3:443/UI/EventDetail.html#%7B%22LogGUID%22%3A%22e5eddb80-d0b6-4c1c-a27e-56d925f23294%22%7D>.

---

**Scan Result**

---

Scan result:	No malware detected
Threat ID:	--
Threat name:	--
Virus Scan Engine:	9.850.1008
Virus Pattern:	12.475.00
Spyware Pattern:	1.723.00
IntelliTrap Pattern:	0.227.00
IntelliTrap Exception Pattern:	1.283.00

### 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 FileHash\_20170612110747.txt.bat on 10-02-2017 20:09:06. File not found in approved list.  
Your action is required.

To manage this event, go to <https://10.1.192.3:443/UI/EventDetail.html#%7B%22LogGUID%22%3A%22E5EDDB80-D0B6-4C1C-A27E-56D925F23294%22%7D>.

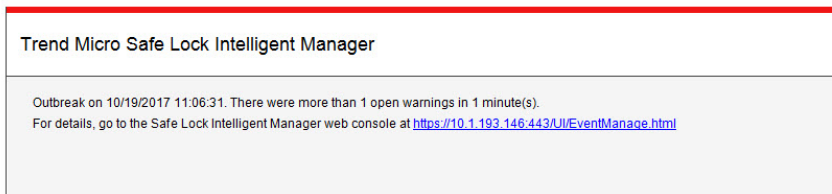
---

**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.

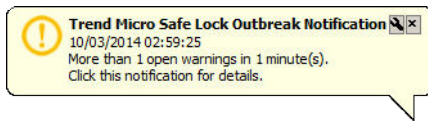
The **Notification Settings** screen appears, open to the **General** tab.

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	<ul style="list-style-type: none"><li>• Add, edit, enable, disable, or delete Safe Lock Intelligent Manager web console accounts from the <b>Account Management</b> screen.</li><li>• Modify their own account description, email address, and password</li><li>• Specify actions to take on files blocked by agents</li><li>• View the Safe Lock Intelligent Manager web console <b>Logs &amp; Reports &gt; Server Events</b> screen</li><li>• Allow or block storage device access on managed endpoints.</li></ul>

ACCOUNT TYPE	PRIVILEGES
Full Control	<ul style="list-style-type: none"> <li>• Modify their own account description, email address, and password</li> <li>• Specify actions to take on files blocked by agents</li> <li>• View the Safe Lock Intelligent Manager web console <b>Logs &amp; Reports &gt; Server Events</b> screen</li> <li>• Allow or block storage device access on managed endpoints.</li> </ul>
Storage Device Control	<ul style="list-style-type: none"> <li>• Modify their own account description, email address, and password</li> <li>• Allow or block storage device access on managed endpoints.</li> </ul>
Read Only	<ul style="list-style-type: none"> <li>• Modify their own account description, email address, and password</li> </ul>

**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.



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.



The following characters are not supported:

> < & " ' "

---

8. Optionally, specify an email address for this account.
9. Specify the password.



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 <a href="#">Changing Activation Codes on page 4-15</a>
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 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 on page 5-2*
- *About the Agent Console on page 5-6*
- *About the Approved List on page 5-10*
- *Account Types on page 5-17*
- *About Feature Settings on page 5-19*

## Setting Up the Approved List

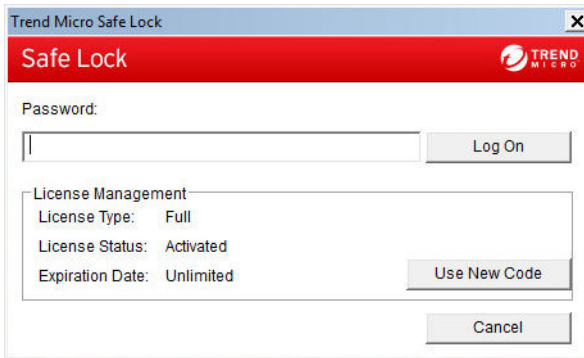
Before Trend Micro Safe Lock can protect the endpoint, it must check the endpoint for existing applications and files necessary for the system to run correctly.

---

### Procedure

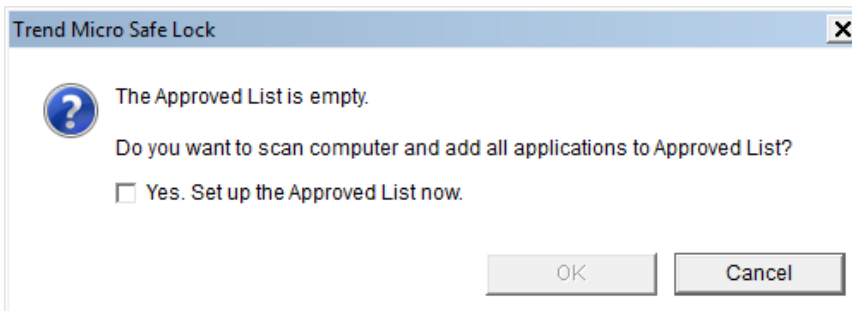
1. Open the Safe Lock console.

The Safe Lock log on screen appears.



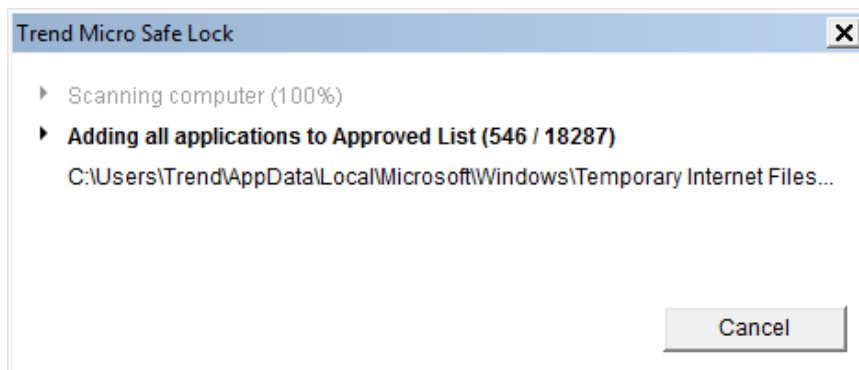
2. Provide the password and click **Login**.

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

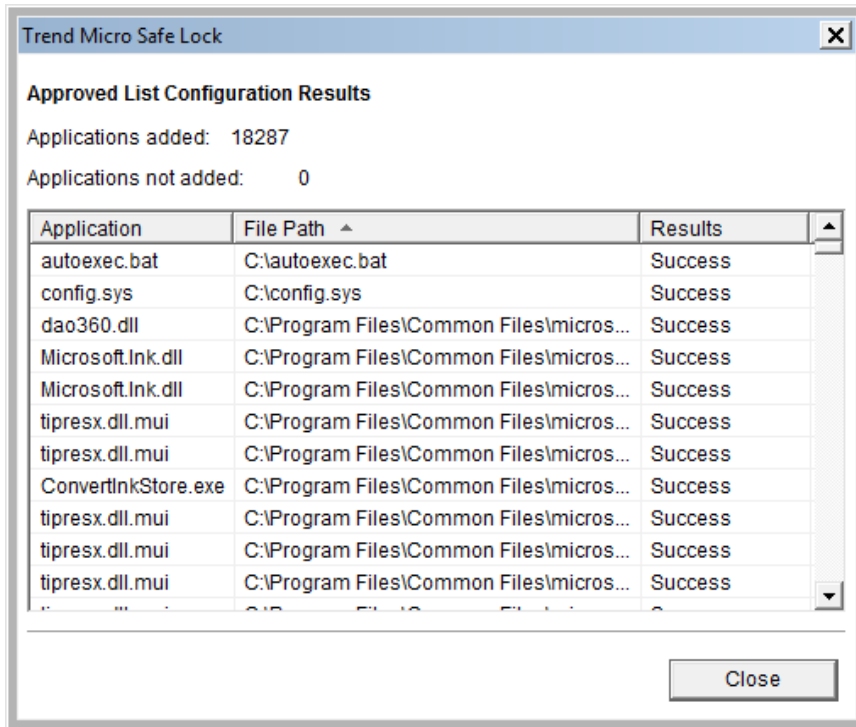


3. At the notification window, select **Yes. Set up the Approved List now** and click **OK**.

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.
-

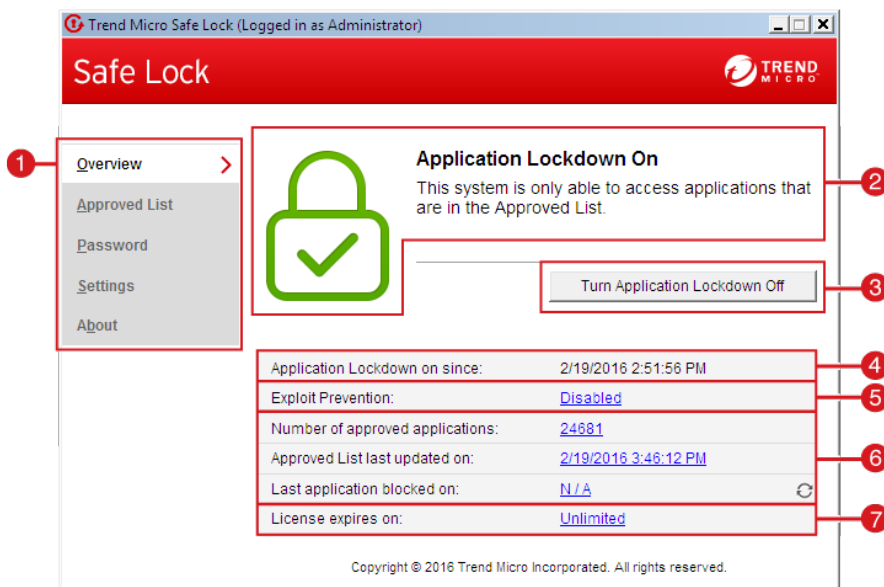
**TABLE 5-1. Configuring Pop-up Notifications for Blocked Files**

SETTING	DEFAULT	WHERE TO ACCESS THE SETTING	
		BEFORE AGENT DEPLOYMENT	AFTER AGENT DEPLOYMENT
Enable the notification	Disabled	Customize the <code>BlockNotification</code> section of the agent <code>Setup.ini</code> file.	Use agent Command Line Interface to issue a <code>blockedfilenotification</code> 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	<ul style="list-style-type: none"> <li>Title: Application Blocked</li> <li>Message: A program has been blocked by Trend Micro Safe Lock. Please contact your help desk or administrator.</li> </ul>		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	<b>Overview</b>	Display the software status
	<b>Approved List</b>	Display applications allowed to run and let users manage the list
	<b>Password</b>	Change the Safe Lock administrator or Restricted User passwords (only available to administrators)
	<b>Settings</b>	Enable or disable vulnerability protection settings and export or import the system configuration
	<b>About</b>	Display the product and component version numbers

#	ITEM	DESCRIPTION
2	Status information	The current status of the software
3	<b>Turn Application Lockdown On</b>	Lock down the system, blocking applications not on the Approved List from running
	<b>Turn Application Lockdown Off</b>	<p>Release the system from lock down, allowing applications not on the Approved List to run</p> <hr/> <p> <b>Note</b>            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.</p>
4	<b>Application Lockdown on since</b>	The date and time that Application Lockdown was last turned on
	<b>Application Lockdown off since</b>	The date and time that Application Lockdown was last turned off
5	<b>Exploit Prevention</b>	<p><b>Enabled:</b> All Exploit Prevention features are enabled</p> <p>Click the status to open the settings screen.</p>
		<p><b>Enabled (Partly):</b> Some Exploit Prevention features are enabled</p> <p>Click the status to open the settings screen.</p>
		<p><b>Disabled:</b> No Exploit Prevention features are enabled</p> <p>Click the status to open the settings screen.</p>

#	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	<b>License expires on</b>	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.

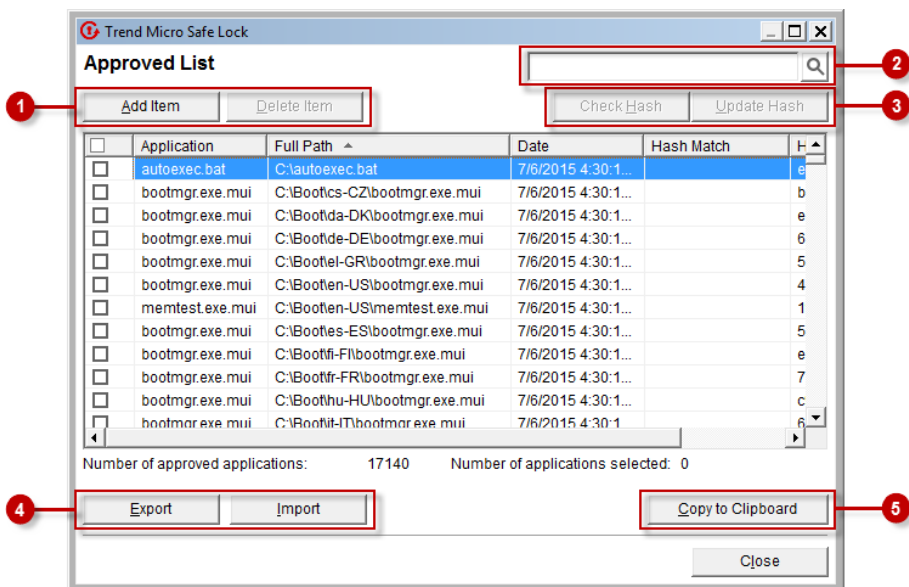
**TABLE 5-3. Status Icon Descriptions**

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
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	<b>Add Item/Delete Item</b>	Adds or removes selected items to or from the Approved List.
2	Search bar	Searches the <b>Application</b> and <b>File Path</b> columns.
3	<b>Check Hash/Update Hash</b>	Checks or updates the hash values for applications in the Approved List.
4	<b>Export/Import</b>	Exports or imports the Approved List using a SQL database (.db) file.
5	<b>Copy to Clipboard</b>	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
<b>Manually browse and select files</b>	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 ( <code>wmplayer.exe</code> ) is not in the Approved List after initial setup, users can add it to the list using the console.
<b>Automatically add files created or modified by the selected application installer (Trusted Updater)</b>	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**.

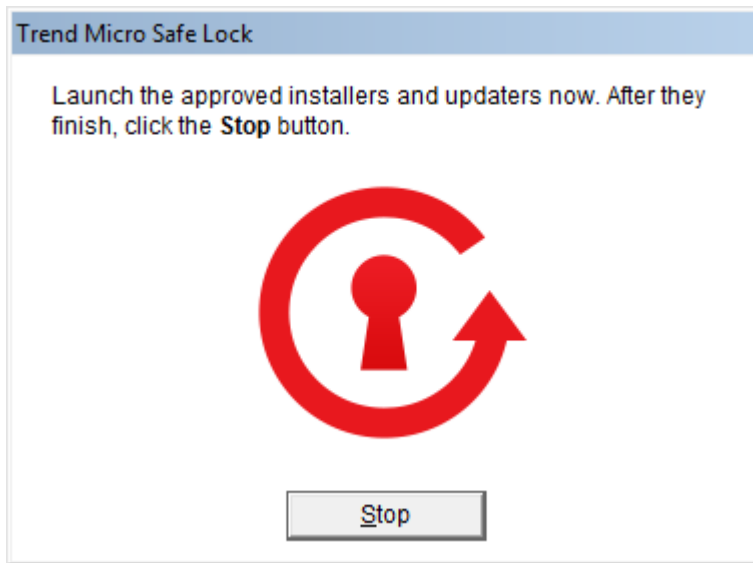


### Note

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	<ul style="list-style-type: none"> <li>• Default account</li> <li>• Full access to Safe Lock functions</li> <li>• Can use both the console and command line interface (CLI)</li> </ul>

ACCOUNT	DETAILS
Restricted User	<ul style="list-style-type: none"> <li>• Secondary maintenance account</li> <li>• Limited access to Safe Lock functions</li> <li>• Can only use the console</li> </ul>

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.

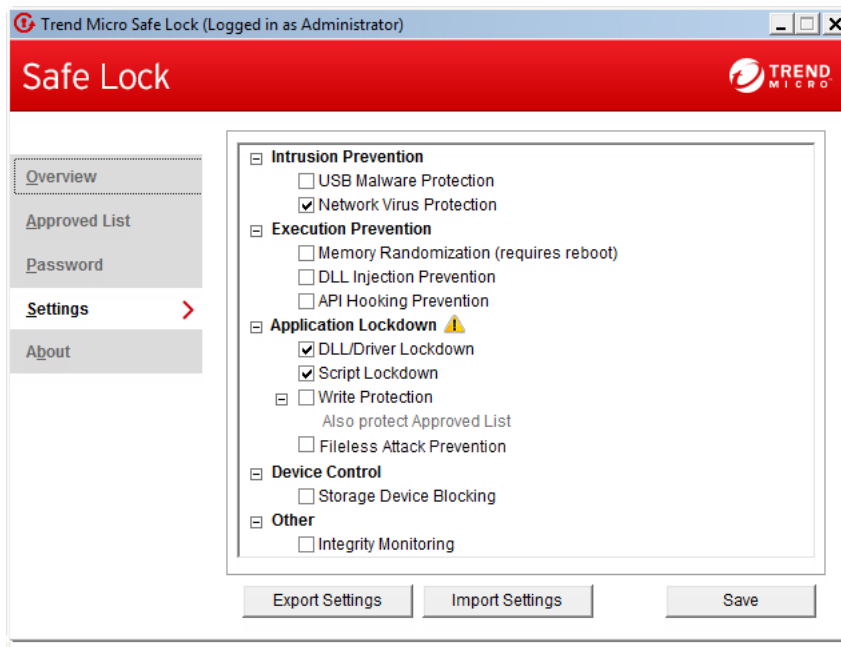



FIGURE 5-4. Safe Lock settings screen

**TABLE 5-8. Intrusion Prevention**


SETTING	DESCRIPTION
USB Malware Protection	<p>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.</p> <p>Enable this feature to prevent files on USB devices from automatically infecting the endpoint.</p>
Network Virus Protection	<p>Network Virus Protection scans incoming and outgoing network traffic, blocking threats from infected computers or other devices on the network.</p> <p>Enable this feature to prevent threats on the network from infecting the endpoint.</p>

**TABLE 5-9. Execution Prevention**

SETTING	DESCRIPTION
Memory Randomization	<p>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.</p> <p>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.</p> <hr/> <p> <b>Note</b> The endpoint must be restarted to enable or disable Memory Randomization.</p> <hr/>
DLL Injection Prevention	<p>DLL Injection Prevention detects and blocks API call behaviors used by malicious software. Blocking these threats helps prevent malicious processes from running.</p> <p>Never disable this feature except in troubleshooting situations since it protects the system from a wide variety of serious threats.</p>

SETTING	DESCRIPTION
API Hooking Prevention	<p>API Hooking Prevention detects and blocks malicious software that tries to intercept and alter messages used in critical processes within the operating system.</p> <p>Never disable this feature except in troubleshooting situations since it protects the system from a wide variety of serious threats.</p>


**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.	 <b>Important</b> 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	<p>Integrity Monitoring logs events related to changes for files, folders, and the registry on the managed endpoint.</p> <hr/> <p> <b>Note</b> To view Integrity Monitoring logs on the managed endpoint, go to <b>Start &gt; Control Panel &gt; Administrative Tools</b> and access Event Viewer.</p>

## 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.

### 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) on page 6-2*

## 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

<b>FUNCTION</b>	<b>SLCMD PROGRAM AT THE COMMAND LINE INTERFACE (CLI)</b>	<b>CONSOLE</b>
Export/Import configuration	Yes	Yes
Install	Yes	Yes
Windows Update Support	Yes	No
Application Lockdown	Yes	Yes
Write Protection	Yes	Yes
Write Protection Exceptions	Yes	No
Integrity Monitoring	Yes	Yes
Exception Paths	Yes	No
License Management	Yes	Yes
Administrator password	Yes	Yes
Turn on/off Application Lockdown	Yes	Yes
Enable/disable pop-up notifications for blocked files	Yes	No
Start/Stop Trusted Updater	Yes	Yes
Trusted Hash List	Yes	No
Start/Stop the service	Yes	No
Uninstall	No	No
Storage Device Control	Yes	Yes
Fileless Attack Prevention	Yes	Yes

Not all settings are available through the command line interface (CLI) or console. See *Working with the Agent Configuration File on page 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 administrator password
lock	lo	Manage Application Lockdown status
blockedlog	bl	Manage the applications blocked by Safe Lock
license	lc	Manage the Safe Lock license
settings	set	Manage the Safe Lock settings
service	srv	Manage the Safe Lock service

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

**TABLE 6-3. General Commands**

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

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

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

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



COMMAND	PARAMETER	DESCRIPTION
<b>import</b> managedmodeconfig uration	<path_of_encrypted_ input>	Import the encrypted configuration file used by Managed Mode
<b>import</b> servercertificati on	<path_of_certification _file>	Import the encrypted Safe Lock Intelligent Manager SSL communication certificate file
<b>set</b> managedmode	enable [-cfg <path_of_encrypte d_file>] [-sc <path_of_certific ation_file]	<p>Enable Managed Mode</p> <hr/> <p> <b>Note</b> The default setting is disable.</p> <hr/> <p>The following optional parameters are available:</p> <ul style="list-style-type: none"> <li>• -cfg &lt;path_of_encrypted_file&gt; Use -cfg value to specify the path of the configuration file</li> <li>• -sc &lt;path_of_certification_file&gt; Use -sc value to specify the path of the certificate file</li> </ul>
<b>set</b> managedmode		Display the current Managed Mode status
<b>show</b> managedmodeconfig uration		Display the configuration used by Managed Mode
<b>test</b> 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
storagedeviceblocking	sto	Allows or blocks storage devices (CD/DVD drives, floppy disks, and network drives) from accessing the managed endpoint.



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

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


**TABLE 6-7. Optional Feature Commands**



COMMAND	PARAMETER	DESCRIPTION
<b>set</b> apihookingprevention	enable	Enable API Hooking Prevention For example, type: <pre>SLCmd.exe -p &lt;admin_password&gt; set apihookingprevention enable</pre> <hr/>  <b>Note</b> The default status is Disabled.
	disable	Disable API Hooking Prevention For example, type: <pre>SLCmd.exe -p &lt;admin_password&gt; set apihookingprevention disable</pre>
		Display the current status of API Hooking Prevention For example, type: <pre>SLCmd.exe -p &lt;admin_password&gt; set apihookingprevention</pre>

COMMAND	PARAMETER	DESCRIPTION
<code>set customaction</code>		Display the current setting for actions taken when Safe Lock blocks specific types of events  <hr/>  <b>Note</b> The default setting is <code>Ask</code> .
	<code>ignore</code>	Ignore blocked files or processes when Application Lockdown blocks any of the following events: <ul style="list-style-type: none"> <li>• Process launch</li> <li>• DLL loading</li> <li>• Script file access</li> </ul> For example, type:  <pre>SICmd.exe -p &lt;admin_password&gt; set customaction ignore</pre>
	<code>quarantine</code>	Quarantine blocked files or processes when Application Lockdown blocks any of the following events: <ul style="list-style-type: none"> <li>• Process launch</li> <li>• DLL loading</li> <li>• Script file access</li> </ul> For example, type:  <pre>SICmd.exe -p &lt;admin_password&gt; set customaction quarantine</pre>


COMMAND	PARAMETER	DESCRIPTION
		 <b>Note</b> Safe Lock does not support a custom action of “quarantine” on Windows XP or Windows 2003.
	ask	Ask what to do for blocked files or processes when Application Lockdown blocks any of the following events: <ul style="list-style-type: none"> <li>• Process launch</li> <li>• DLL loading</li> <li>• Script file access</li> </ul> For example, type: <pre>SICmd.exe -p &lt;admin_password&gt; set customaction ask</pre>
set dlldriverlockdown		Display the current status of DLL/Driver Lockdown For example, type: <pre>SICmd.exe -p &lt;admin_password&gt; set dlldriverlockdown</pre> <hr/>  <b>Note</b> The default status is Enabled.
	enable	Enable DLL/Driver Lockdown For example, type: <pre>SICmd.exe -p &lt;admin_password&gt; set dlldriverlockdown enable</pre>
	disable	Disable DLL/Driver Lockdown For example, type:



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


COMMAND	PARAMETER	DESCRIPTION
	enable	<p>Enable exceptions to Application Lockdown</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set exceptionpath enable</pre>
	disable	<p>Disable exceptions to Application Lockdown</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set exceptionpath disable</pre>
<pre>set integritymonitoring</pre>		<p>Display the current status of Integrity Monitoring</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set integritymonitoring</pre> <hr/> <p> <b>Note</b> The default status is Disabled.</p> <hr/>
	enable	<p>Enable Integrity Monitoring</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set integritymonitoring enable</pre>
	disable	<p>Disable Integrity Monitoring</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set integritymonitoring disable</pre>


COMMAND	PARAMETER	DESCRIPTION
<b>set</b> memoryrandomization		Display the current status of Memory Randomization  For example, type:  <pre>SLCmd.exe -p &lt;admin_password&gt; set memoryrandomization</pre> <hr/>  <b>Note</b> The default status is Disabled.
	enable	Enable Memory Randomization  For example, type:  <pre>SLCmd.exe -p &lt;admin_password&gt; set memoryrandomization enable</pre>
	disable	Disable Memory Randomization  For example, type:  <pre>SLCmd.exe -p &lt;admin_password&gt; set memoryrandomization disable</pre>
<b>set</b> networkvirusprotecti on		Display the current status of Network Virus Protection  For example, type:  <pre>SLCmd.exe -p &lt;admin_password&gt; set networkvirusprotection</pre> <hr/>  <b>Note</b> The default status is Enabled.
	enable	Enable Network Virus Protection  For example, type:



COMMAND	PARAMETER	DESCRIPTION
		<pre>SLCmd.exe -p &lt;admin_password&gt; set networkvirusprotection enable</pre>
	disable	Disable Network Virus Protection For example, type: <pre>SLCmd.exe -p &lt;admin_password&gt; set networkvirusprotection disable</pre>
set script		Display the current status of Script Lockdown For example, type: <pre>SLCmd.exe -p &lt;admin_password&gt; set script</pre> <hr/>  <b>Note</b> The default status is Enabled.
	enable	Enable Script Lockdown For example, type: <pre>SLCmd.exe -p &lt;admin_password&gt; set script enable</pre>
	disable	Disable Script Lockdown For example, type: <pre>SLCmd.exe -p &lt;admin_password&gt; set script disable</pre>
set storagedeviceblockin g		Display the current status of Storage Device Blocking For example, type: <pre>SLCmd.exe -p &lt;admin_password&gt; set storagedeviceblocking</pre>

COMMAND	PARAMETER	DESCRIPTION
		 <b>Note</b> The default status is Disabled.
	enable	Enable Storage Device Blocking For example, type: <pre>SLCmd.exe -p &lt;admin_password&gt; set storagedeviceblocking enable</pre>
	disable	Disable Storage Device Blocking For example, type: <pre>SLCmd.exe -p &lt;admin_password&gt; set storagedeviceblocking disable</pre>
set usbmalwareprotection		Display the current status of USB Malware Protection For example, type: <pre>SLCmd.exe -p &lt;admin_password&gt; set usbmalwareprotection</pre> <hr/>  <b>Note</b> The default status is Disabled.
	enable	Enable USB Malware Protection For example, type: <pre>SLCmd.exe -p &lt;admin_password&gt; set usbmalwareprotection enable</pre>
	disable	Disable USB Malware Protection For example, type:

COMMAND	PARAMETER	DESCRIPTION
		<pre>SLCmd.exe -p &lt;admin_password&gt; set usbmalwareprotection disable</pre>
<code>set writeprotection</code>		<p>Display the current status of Write Protection</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set writeprotection</pre> <hr/> <p> <b>Note</b> The default status is Disabled.</p> <hr/>
	enable	<p>Enable Write Protection</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set writeprotection enable</pre>
	disable	<p>Disable Write Protection</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set writeprotection disable</pre>
<code>set writeprotection-includes-approvedlist</code>		<p>Display the current status of Write Protection includes Approved List</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set writeprotection-includes-approvedlist</pre>

COMMAND	PARAMETER	DESCRIPTION
		 <b>Note</b> 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:  <pre>SLCmd.exe -p &lt;admin_password&gt; set writeprotection-includes-approvedlist enable</pre>
	disable	Disable protection of the Approved List (in addition to the Write Protection List) when Write Protection is enabled  For example, type:  <pre>SLCmd.exe -p &lt;admin_password&gt; set writeprotection-includes-approvedlist disable</pre>

## 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
<b>set</b> user		Display the the Restricted User account status  For example, type:  <pre>S1Cmd.exe -p &lt;admin_password&gt; set user</pre> <hr/>  <b>Note</b> The default status is Disabled.
	enable	Enable the Restricted User account  For example, type:  <pre>S1Cmd.exe -p &lt;admin_password&gt; set user enable</pre>
	disable	Disable the Restricted User account  For example, type:  <pre>S1Cmd.exe -p &lt;admin_password&gt; set user disable</pre>
<b>set</b> userpassword		Prompt the currently logged on administrator to specify a new Restricted User account password  For example, type:

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

## 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 <code>JSP</code> with the interpreter file <code>jscript.js</code> , type:  <code>SLCmd.exe -p &lt;admin_password&gt; add script jsp C:\Scripts\jscript.js</code>

COMMAND	PARAMETER	DESCRIPTION
<pre>remove script</pre>	<pre>&lt;extension&gt; [interpreter1] [interpreter2] ...</pre>	<p>Remove the specified script extension and the interpreter(s) required to execute the script</p> <p>For example, to remove the script extension JSP with the interpreter file <code>jscript.js</code>, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; remove script jsp C:\Scripts\jscript.js</pre> <hr/> <p> <b>Note</b></p> <p>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.</p>
<pre>show script</pre>		<p>Display all script rules</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; show script</pre>

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

COMMAND	PARAMETER	DESCRIPTION
		<pre>SLCmd.exe -p &lt;admin_password&gt; check approvedlist -f</pre>
	-q	<p>Update the hash values in the Approved List and displays summarized results</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; check approvedlist -q</pre>
	-v	<p>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</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; check approvedlist -v</pre>
<code>export list</code>	<output_file>	<p>Export the Approved List to the file path and file name specified</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; export list c:\approvedlist\ap.db</pre> <hr/> <p> <b>Note</b> The output file type must be DB format.</p>
<code>import list</code>	[-o] <input_file>	<p>Import an Approved List from the file path and file name specified</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; import list c:\approvedlist\ap.db</pre>

COMMAND	PARAMETER	DESCRIPTION
		 <b>Note</b> The input file type must be DB format.  Using the optional <code>-o</code> 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:

**SICmd.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
<b>show</b> quarantinedfile		Display a list of quarantined files
<b>restore</b> quarantinedfile	<id> [-al] [-f]	Restore the specified file from quarantine  Using the optional <code>-al</code> value also adds the restored file to Approved List.  Using the optional <code>-f</code> value forces the restore.

COMMAND	PARAMETER	DESCRIPTION
<b>remove</b> quarantinedfile	<id>	Delete the specified file
<b>show</b> exceptionpath		Display current exceptions to Application Lockdown  For example, type: SLCmd.exe -p <admin_password> show exceptionpath
<b>add</b> 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: <ul style="list-style-type: none"> <li>• SLCmd.exe -p &lt;admin_password&gt; add exceptionpath -e c:\folder\.* -t regexp</li> <li>• SLCmd.exe -p &lt;admin_password&gt; add exceptionpath -e \\computer\folder\.*\file.exe -t regexp</li> </ul>

COMMAND	PARAMETER	DESCRIPTION
<b>remove</b> 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  <hr/>  <b>Note</b> 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  <hr/>  <b>Note</b> 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  <hr/>  <b>Note</b> Specify the exact <folder_path> originally specified in the corresponding add command.

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

## 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
<b>show</b>	writeprotection		Display the entire Write Protection List
	writeprotection-file		Display the files in the Write Protection List  For example, type:  <code>SLCmd.exe -p &lt;admin_password&gt; show writeprotection-file</code>


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





COMMAND	PARAMETER	VALUE	DESCRIPTION
			 <b>Note</b> The <file_path> value pattern matches from the end of the path toward the beginning of the path. For example, specifying <code>userfile.txt</code> matches <code>c:\Windows\userfile.txt</code> and <code>c:\Temp\userfile.txt</code> .
	<code>writeprotection-file-exception</code>	<code>-t &lt;file_path&gt;</code> <code>-p</code> <code>&lt;process_path&gt;</code> <code>&gt;</code>	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 <code>notepad.exe</code> to a file named <code>userfile.txt</code> , type:  <pre>SLCmd.exe -p &lt;admin_password&gt; add writeprotection-file-exception -t userfile.txt -p notepad.exe</pre>


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



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

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


COMMAND	PARAMETER	VALUE	DESCRIPTION
			 <b>Note</b> Using the optional <code>-r</code> value includes the specified folder and related subfolders.  The <code>&lt;folder_path&gt;</code> value pattern matches from the end of the path toward the beginning of the path. For example, specifying <code>userfile.txt</code> matches <code>c:\Windows\userfolder</code> and <code>c:\Temp\userfolder</code> .
	<code>writeprotection- folder-exception</code>	<code>[-r] -t &lt;folder_path&gt; -p &lt;process_path&gt; &gt;</code>	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 <code>notepad.exe</code> to a folder and related subfolders at <code>c:\Windows\System32\Temp</code> , type:  <pre>SLCmd.exe -p &lt;admin_password&gt; add writeprotection- folder-exception -r -t c:\Windows \System32\Temp -p notepad.exe</pre>



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


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


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





COMMAND	PARAMETER	VALUE	DESCRIPTION
			<pre>SICmd.exe -p &lt;admin_password&gt; remove writeprotection-file- exception -t userfile.txt -p notepad.exe</pre> <hr/> <p> <b>Note</b> Specify the exact &lt;file_path&gt; and &lt;process_path&gt; originally specified in the corresponding add command.</p> <hr/>
		-t <file_path>	<p>Remove the specified file from the Write Protection Exception List</p> <p>For example, type:</p> <pre>SICmd.exe -p &lt;admin_password&gt; remove writeprotection-file- exception -t userfile.txt</pre>

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

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



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



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

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



**TABLE 6-18. Write Protection List “Registry” Commands**



COMMAND	PARAMETER	VALUE	DESCRIPTION
<b>show</b>	<code>writeprotection</code>		Display the entire Write Protection List
	<code>writeprotection-regvalue</code>		Display the registry values in the Write Protection List
	<code>writeprotection-regvalue-exception</code>		Display the registry values in the Write Protection Exception List
	<code>writeprotection-regkey</code>		Display the registry keys in the Write Protection List
	<code>writeprotection-regkey-exception</code>		Display the registry keys in the Write Protection Exception List
<b>add</b>	<code>writeprotection-regvalue</code>	<code>&lt;path_of_registry_key&gt;</code> <code>&lt;registry_value&gt;</code>	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
			<pre>SIcmd.exe -p &lt;admin_password&gt; add writeprotection-regvalue HKEY\test testvalue</pre>
	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 <hr/>  <b>Note</b> 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 <hr/>  <b>Note</b> 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
			 <b>Note</b> This command allows write access by the specified process to any registry values.  The <code>-p</code> value pattern matches from the end of the process path toward the beginning of the path.
	<code>writeprotection-regkey</code>	<code>[-r] &lt;path_of_registry_key&gt;</code>	Add the specified registry key to the Write Protection List   <b>Note</b> Using the optional <code>-r</code> value includes the specified registry key and related subkeys.
	<code>writeprotection-regkey-exception</code>	<code>[-r] -t &lt;path_of_registry_key&gt; -p &lt;process_path&gt;</code>	Add the specified registry key and processes run from the specified path to the Write Protection Exception List





COMMAND	PARAMETER	VALUE	DESCRIPTION
			 <b>Note</b> This command allows write access by the specified process to the specified registry keys.  Using the optional <code>-r</code> value includes the specified registry key and related subkeys.  The <code>-p</code> value pattern matches from the end of the process path toward the beginning of the path.
		<code>[-r] -t            &lt;path_of            _registry            _key&gt;</code>	Add the specified registry key to the Write Protection Exception List  <hr/>  <b>Note</b> This command allows write access by any process to the specified registry keys.  Using the optional <code>-r</code> value includes the specified registry key and related subkeys.
		<code>-p            &lt;process            _path&gt;</code>	Add processes run from the specified paths to the Write Protection Exception List

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

COMMAND	PARAMETER	VALUE	DESCRIPTION
			 <b>Note</b> 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   <b>Note</b> 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
			 <b>Note</b> 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  <hr/>  <b>Note</b> 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
			 <b>Note</b> Using the optional <code>-r</code> value includes the specified registry key and related subkeys.
		<code>-p</code> <code>&lt;process_path&gt;</code>	Remove the specified process path from the Write Protection Exception List   <b>Note</b> The <code>-p</code> 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:

**SICmd.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
<b>set</b> trustedcertifica tion		Display current setting for using Trusted Certifications   <b>Note</b> The default setting is Enabled.
	enable	Enable using Trusted Certifications
	disable	Disable using Trusted Certifications
<b>show</b> trustedcertifica tion	[-v]	Display the certificate files in the Trusted Certifications List  Using the optional -v value displays detailed information.
<b>add</b> trustedcertifica tion	-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.
<b>remove</b> trustedcertifica tion	-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
<b>set</b> trustedhash		Display current setting for using Trusted Hash List   <b>Note</b> The default setting is Disabled.
	enable	Enable using Trusted Hash List
	disable	Disable using Trusted Hash List
<b>show</b> trustedhash		Display the hash values in the Trusted Hash List  For example, type:  <code>SLCmd.exe -p &lt;admin_password&gt; show trustedhash</code>
<b>add</b> trustedhash	<code>-v &lt;hash&gt; [-l &lt;label&gt;] [-u][-al] [-t&lt;file_path&gt;][-n&lt;note&gt;]</code>	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:  <code>SLCmd.exe -p &lt;admin_password&gt; add trustedhash -v xxx</code>  Using the optional <code>-l</code> value specifies the unique label for this hash value.

COMMAND	PARAMETER	DESCRIPTION
		<p>Using the optional <code>-u</code> value treats the file of the specified hash value as a Trusted Updater.</p> <hr/> <p> <b>Note</b> The <code>-u</code> value requires the Predefined Trusted Updater List enabled.</p> <hr/> <p>Using the optional <code>-al</code> value adds the file of the specified hash value to Approved List.</p> <p>Using the optional <code>-t</code> value specifies a file path to check for the hash value</p> <hr/> <p> <b>Note</b> The <code>-t</code> value pattern matches from the end of the path toward the beginning of the path. For example, specifying <code>userfile.txt</code> matches <code>c:\Windows\userfile.txt</code> and <code>c:\Temp\userfile.txt</code>.</p> <hr/> <p>Using the optional <code>-n</code> value adds a note for the file hash</p>
<code>remove trustedhash</code>	<code>-l &lt;label&gt;</code>	Remove a file from the Trusted Hash List by specifying its label
<code>remove trustedhash</code>	<code>-a</code>	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
<b>start</b> trustedupdater	[-r] <path_of_installer> r>	<p>Start Trusted Updater to add installer files (<code>EXE</code> and <code>MSI</code> file types) to the specified folder of the Approved List.</p> <hr/> <p> <b>Note</b> Using the optional <code>-r</code> value includes the specified folder and related subfolders.</p> <hr/> <p>For example, to include all installation packages in the <code>C:\Installers</code> folder and all sub-folders, type:</p> <pre>SILCmd.exe -p &lt;admin_password&gt; start trustedupdater -r C:\Installers</pre>
<b>stop</b> trustedupdater	[-f]	<p>Disable Trusted Updater to stop adding new or updated files to the Approved List.</p> <hr/> <p> <b>Note</b> Using the optional <code>-f</code> value specifies that the Trusted Updater does not prompt the administrator before committing a file to the Approved List.</p> <hr/> <p>For example, to stop the Trusted Updater and commit all identified installers (identified before receiving the stop command) to the Approved List after receiving a prompt, type:</p>

COMMAND	PARAMETER	DESCRIPTION
		<code>SLCmd.exe -p &lt;admin_password&gt; stop trustedupdater -f</code>

## 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 6-62](#).

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

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

The following table lists the available abbreviated forms of parameters.

**TABLE 6-25. Abbreviations and Uses**

PARAMETER	ABBREVIATION	USE
<code>predefinedtrustedupdate r</code>	<code>ptu</code>	Manage files in the Predefined Trusted Updater Lists


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

**TABLE 6-26. Predefined Trusted Updater Commands**

COMMAND	PARAMETER	DESCRIPTION
<code>add predefinedtrustedup dater</code>	<code>-e &lt;folder_or_file_exception&gt;</code>	Add the specified file or folder to the Predefined Trusted Updater Exception List

COMMAND	PARAMETER	DESCRIPTION
		<p> <b>Important</b></p> <p>The <code>add</code> 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 <a href="#">Predefined Trusted Updater "Add" Command on page 6-62</a>.</p> <hr/> <p>For example, to add <code>notepad.exe</code> to the Predefined Trusted Updater Exception List, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; add predefinedtrustedupdater -e C:\Windows\notepad.exe</pre>
<pre>decrypt predefinedtrustedup dater</pre>	<pre>&lt;path_of_encrypted_file&gt; &lt;path_of_decrypted_outp ut_file&gt;</pre>	<p>Decrypt a file to the specified location</p> <p>For example, to decrypt <code>C:\Notepad.xen</code> to <code>C:\Editors\notepad.exe</code>, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; decrypt predefinedtrustedupdater C: \notepad.xen C:\Editors \notepad.exe</pre>

COMMAND	PARAMETER	DESCRIPTION
<pre>encrypt predefinedtrustedup dater</pre>	<pre>&lt;path_of_file&gt; &lt;path_of_encrypted_outp ut_file&gt;</pre>	<p>Encrypt a file to the specified location</p> <p>For example, to encrypt C:\notepad.exe to C:\Editors\notepad.xen, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; encrypt predefinedtrustedupdater C: \Editors\notepad.exe C: \notepad.xen</pre>
<pre>export predefinedtrustedup dater</pre>	<pre>&lt;path_of_encrypted_outp ut&gt;</pre>	<p>Export the Predefined Trusted Updater List to the specified encrypted file</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; export predefinedtrustedupdater C: \Lists\ptu_list.xen</pre>
<pre>import predefinedtrustedup dater</pre>	<pre>&lt;path_of_encrypted_input &gt;</pre>	<p>Import a Predefined Trusted Updater List from the specified encrypted file</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; import predefinedtrustedupdater C: \Lists\ptu_list.xen</pre>
<pre>remove predefinedtrustedup dater</pre>	<pre>-l &lt;label_name&gt;</pre>	<p>Remove the specified labeled rule from the Predefined Trusted Updater List</p> <p>For example, to remove the "Notepad" rule, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; remove</pre>

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

COMMAND	PARAMETER	DESCRIPTION
		<code>SLCmd.exe -p &lt;admin_password&gt; show predefinedtrustedupdater -e</code>

## 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 6-27. Predefined Trusted Updater "Add" Command**

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

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

**TABLE 6-28. Predefined Trusted Updater “Add” Additional Values**

VALUE	REQUIRED / OPTIONAL	DESCRIPTION	EXAMPLE	
-u <folder_or_file >	Required	Add the specified file or folder to the Predefined Trusted Updater List	N/A   <b>Note</b> This parameter requires the use of the -t <type_of_object> value.	
-t <type_of_object>	Required	Specify the type of object to add to the Predefined Trusted Updater List located in -u <folder_or_file>  Available objects types are as follows:	SLCmd.exe -p <admin_password> add predefinedtrust edupdater -u C:\Windows\notepad.exe -t process	
		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	
-p <parent_process>	Optional	Add the full file path to the specified parent process used to invoke the	SLCmd.exe -p <admin_password> add predefinedtrust	

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



## 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 6-29. Abbreviations and Uses**

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

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

**TABLE 6-30. Windows Update Support Commands**

COMMAND	PARAMETER	DESCRIPTION
set windowsupdatesupport		Display current setting for Windows Update Support
		 <b>Note</b> 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 6-31. 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 6-32. Blocked File Notification Commands**

COMMAND	PARAMETER	DESCRIPTION
set blockedfilenotification		Display the current setting.   <b>Note</b> 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 6-33. Abbreviations and Uses**

PARAMETER	ABBREVIATION	USE
configuration	con	Manage the configuration file

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

**TABLE 6-34. Configuration File Commands**

COMMAND	PARAMETER	DESCRIPTION
<b>decrypt</b> 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:  <b>SLCmd.exe -p &lt;admin_password&gt; decrypt configuration C:\config.xen C:\config.xml</b>
<b>encrypt</b> 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:  <b>SLCmd.exe -p &lt;admin_password&gt; encrypt configuration C:\config.xml C:\config.xen</b>
<b>export</b> configuration	<path_of_encrypted_output>	Export the configuration file to the specified location  For example, type:  <b>SLCmd.exe -p &lt;admin_password&gt; export configuration C:\config.xen</b>
<b>import</b> configuration	<path_of_encrypted_input>	Import a configuration file from the specified location  For example, type:  <b>SLCmd.exe -p &lt;admin_password&gt; import configuration C:\config.xen</b>

## 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 6-35. Abbreviations and Uses**

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

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

**TABLE 6-36. Fileless Attack Prevention Commands**

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

COMMAND	PARAMETER	DESCRIPTION
<b>show</b> filelessattackprevention-process		Display the list of monitored processes  For example, type:  <pre>SLCmd.exe -p &lt;admin_password&gt; show filelessattackprevention-process</pre>
<b>add</b> filelessattackprevention-exception	<monitored_processes> <Parentprocess1> <Parentprocess2> <Parentprocess3> <Parentprocess4> -a <arguments> -regex -l <label>	Add a Fileless Attack Prevention exception  For example, given the following exception: <ul style="list-style-type: none"> <li>• Monitored Process: cscript.exe</li> <li>• Parentprocess1: a.exe</li> <li>• Parentprocess2:</li> <li>• Parentprocess3: c.exe</li> <li>• Parentprocess4:</li> <li>• Arguments: -abc -def</li> <li>• Use regular expression for arguments: No</li> </ul> To add the exception, type:  <pre>SLCmd.exe -p &lt;admin_password&gt; add flpe cscript.exe a.exe "" c.exe "" -a "-abc -def"</pre>
<b>remove</b> filelessattackprevention-exception	-l <label>	Remove a Fileless Attack Prevention exception  For example, type:  <pre>SLCmd.exe -p &lt;admin_password&gt; remove filelessattackprevention-exception -l &lt;label&gt;</pre>



**Note**

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

# Chapter 7

## Managing Agents Remotely

This chapter describes remote Trend Micro Safe Lock agent management.

Topics in this chapter include:

- *The Remote Setup Tool (SLrst) on page 7-2*
- *The Remote Tasks Tool (SLtasks) on page 7-22*

## 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 <a href="#">Remote Installation Considerations on page 7-3</a> .
--patch	Patches the Safe Lock agent
--reboot	Restarts the endpoint (required if you want to reinstall the Safe Lock agent) See <a href="#">Restarting Agents Remotely on page 7-21</a>
	 <b>Note</b> The <code>reboot</code> 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 <a href="#">Uninstalling Agents Remotely on page 7-20</a>

## 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 1-21](#).

- 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**.





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 privileges, 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:

<b>VALID</b>
<pre>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</pre>
<b>NOT VALID</b>
<pre>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"</pre>

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:

TMSL2.0\_<language\_abbreviation>.zip

For example:

VALID	NOT VALID
TMSL2.0_EN.zip	TMSL2.0_EN (1).zip
TMSL2.0_JA.zip	TMSL2.0_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 `TMSL2.0_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 8-17](#).
  4. Zip the `TMSL2.0_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:  
 TMSL2.0\_Hotfix\_<language\_abbreviation>.zip

For example:

VALID	NOT VALID
TMSL2.0_Hotfix_EN.zip	TMSL2.0_Hotfix_EN (1).zip
TMSL2.0_Hotfix_JA.zip	TMSL2.0_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 initialize agent Approved Lists, lockdown agents, match licenses, deploy patch or hotfixes without disabling firewall settings on agents, query the status of agents using a command line interface (CLI), and remotely change the administrator password.

By default, Safe Lock Intelligent Manager stores the `SLtasks.exe` file in 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 without byte order mark (BOM). 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:

```
SItasks.exe --removeitems <target_list_file_name>
```

**Tip**

- To only remove approved items from a specific agent, append `--targetPC` to the command and type the computer name.

For example:

```
SLtasks.exe <task_parameter> --targetPC <computer_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:

```
SItasks.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:

```
SItasks.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.   <b>Tip</b> Set this value to 1 to turn the feature off.
Own Group Index	Set the message group ID number for the Safe Lock agent.

COLUMN NAME	CONTROL DESCRIPTION
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.

- 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.

- 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

- Access the **Export/Import Configuration** section from the Trend Micro Safe Lock console.
  - 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**.
  - Provide the password and click **Login**.
  - 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
<code>TOTAL_GROUP_NUM</code>	Divide agents into any number of groups.
<code>OWN_GROUP_INDEX</code>	Set the message group ID number for the Safe Lock agent.
<code>TIME_PERIOD</code>	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_NUMBER	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.

---

# 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 on page 8-2*
- *Installing from Windows on page 8-3*
- *Setting Up the Approved List on page 5-2*
- *Installation Using the Command Line on page 8-13*
- *Customizing Installation Parameters on page 8-16*

## 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 1-15*.



#### **WARNING!**

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

For details, see *Agent Upgrade Preparation on page 1-21*.

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	<p>The Windows Installer provides simplified step-by-step installation wizard for first-time or single installation and is also suitable for preparing for mass deployment for cloned computer systems.</p> <p>For details, see <i>Installing from Windows on page 8-3</i>.</p>
Command line interface installer	<p>The command line interface (CLI) installer provides silent installation and can be integrated into a batch file for mass deployment.</p> <p>For details, see <i>Installation Using the Command Line on page 8-13</i>.</p>



**Note**

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

---

For details, see *Customizing Installation Parameters on page 8-16*.

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

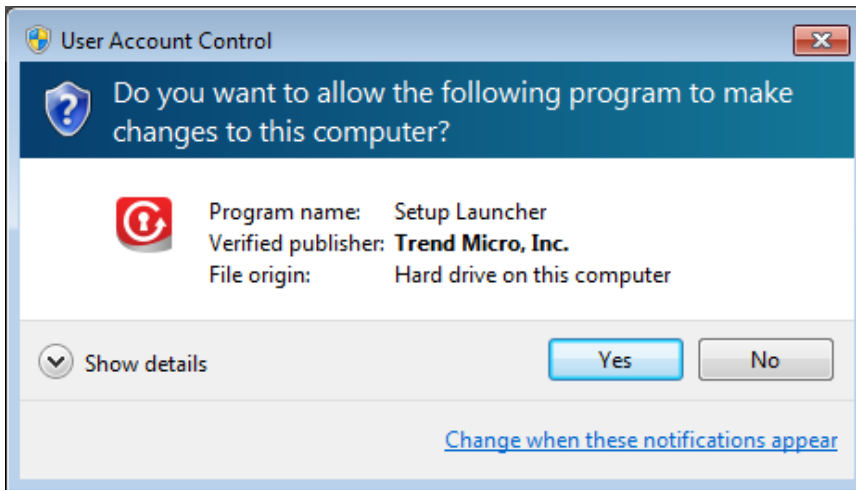
To install Trend Micro Safe Lock, you must log on using an account with administrator privileges.

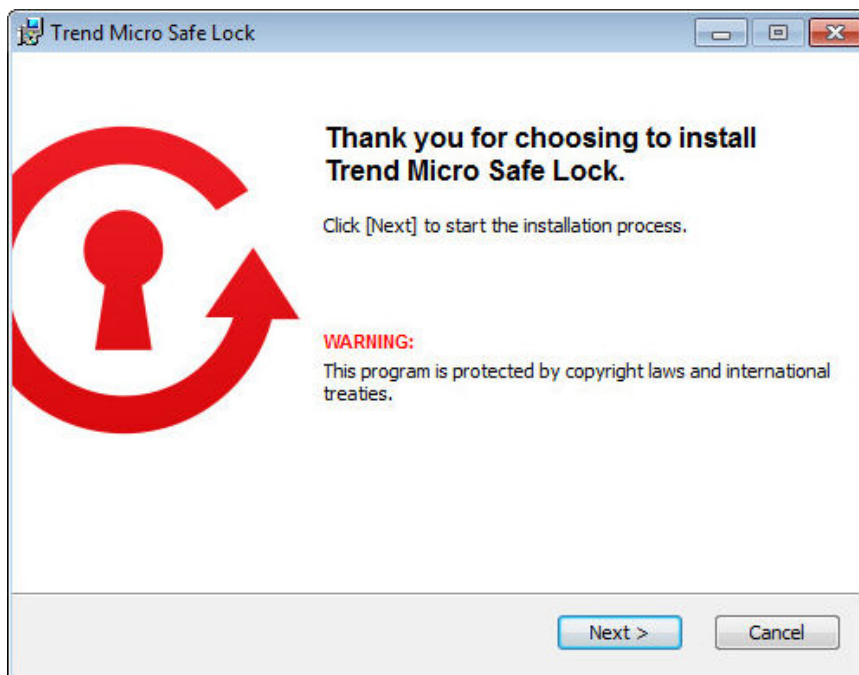
---

## Procedure

1. Double-click `SL_Install.exe`.

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



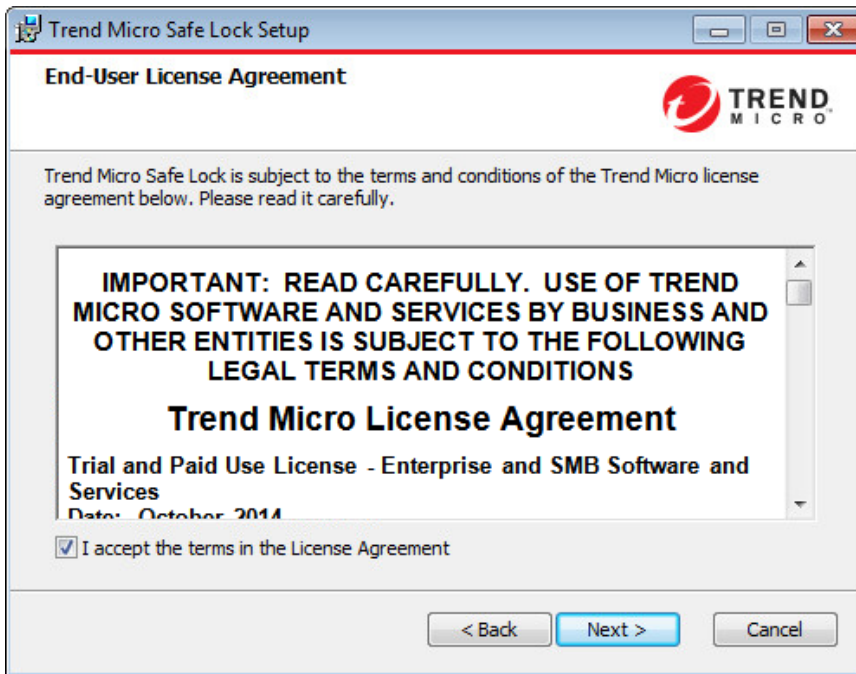


2. When the installation wizard opens, click **Next**.

**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**.

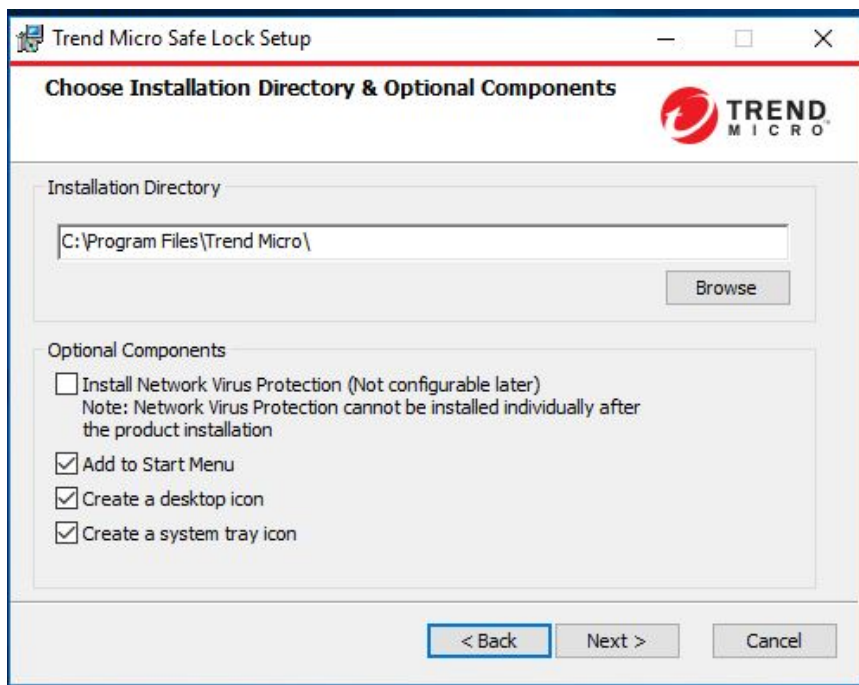


4. Make any necessary changes to the installation options, and click **Next**.



**Important**

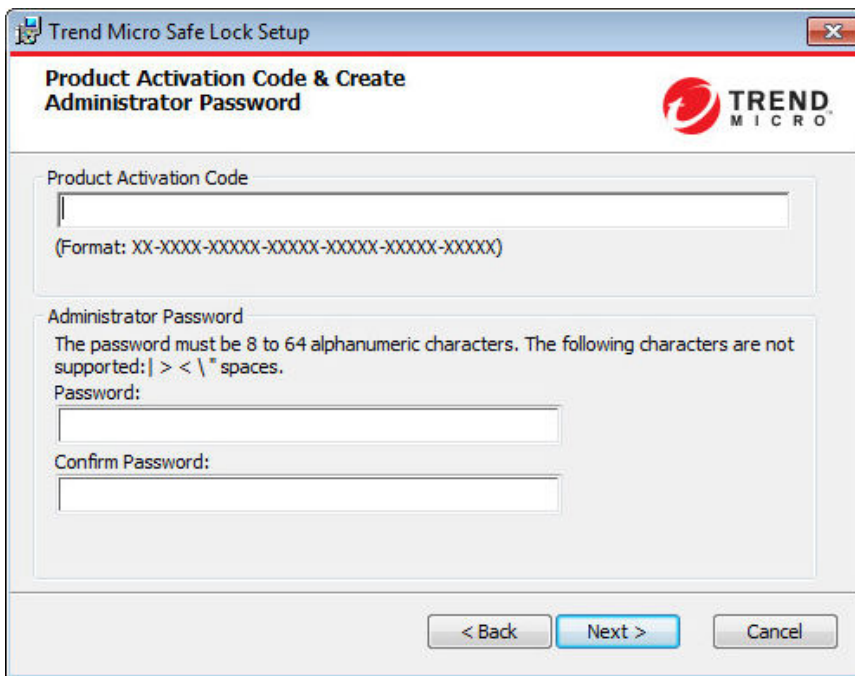
Network Virus Protection can only be installed during the initial program installation, but it can be disabled after installation, if necessary. See *Exploit Prevention Settings* in the Administrator's Guide for more information.



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. Optionally, scan the endpoint for threats before continuing with the installation. Trend Micro recommends you perform this scan.
  - To scan the endpoint for threats, click **Scan**.
    - a. The **Endpoint Prescan** window appears.
    - b. To customize the scan settings, click **Edit Scan Settings**.
    - c. Click **Scan Now**.

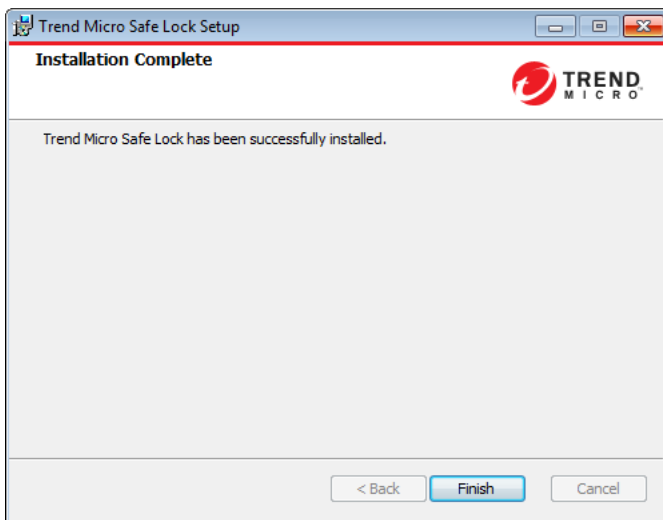
If Endpoint Prescan detects security risks, Trend Micro recommends canceling the installation. Remove threats from the endpoint and try again. If critical programs are detected as threats, confirm that the endpoint is secure and that the versions of the programs installed do not contain threats. Ignore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

**Tip**

Trend Micro provides solutions for detecting and removing threats. For endpoints with limited or no network access, Trend Micro recommends using Trend Micro Portable Security. See *Trend Micro Portable Security Compatible* on page 1-14. For more information about this and other solutions from Trend Micro, go to <http://trendmicro.com/>.

---

- To skip scanning, click **Do Not Scan**.
8. When the **Installation Complete** window displays, click **Finish**.

**Note**

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

---



## Setting Up the Approved List

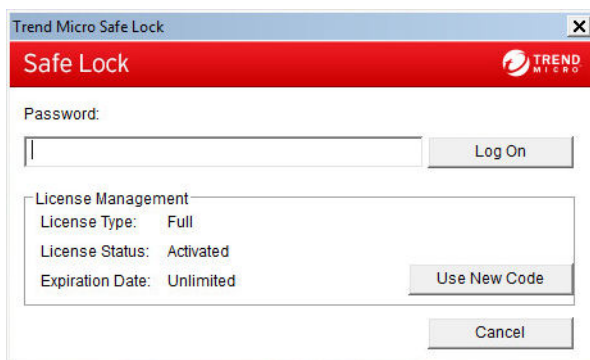
Before Trend Micro Safe Lock can protect the endpoint, it must check the endpoint for existing applications and files necessary for the system to run correctly.

---

### Procedure

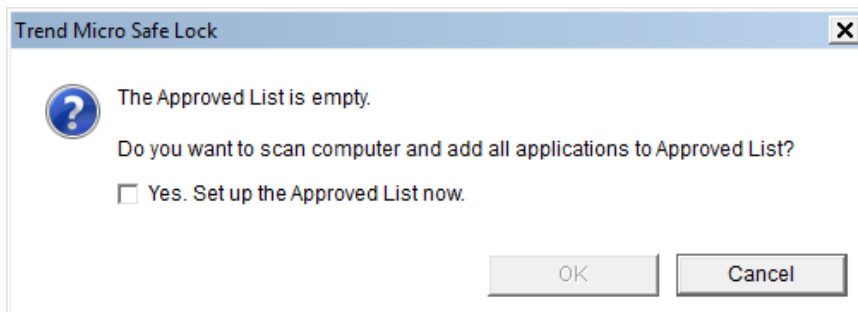
1. Open the Safe Lock console.

The Safe Lock log on screen appears.



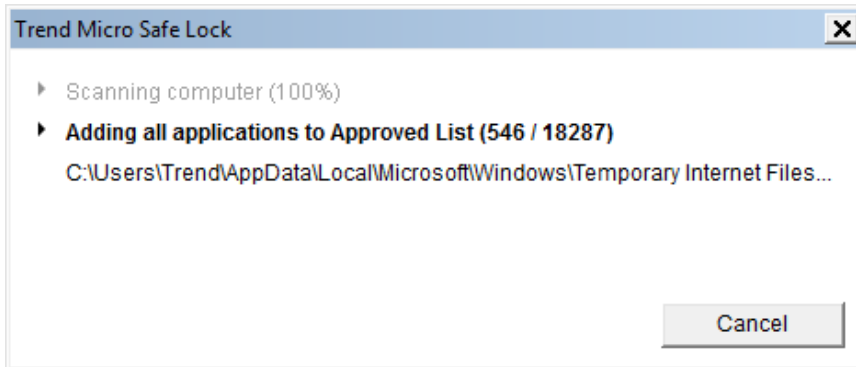
2. Provide the password and click **Login**.

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

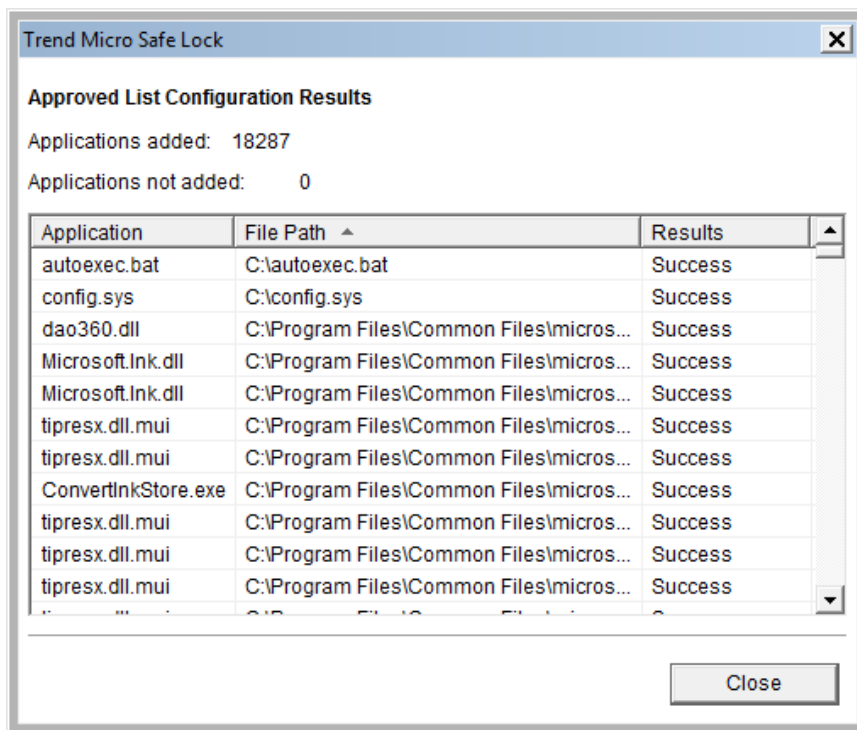


3. At the notification window, select **Yes. Set up the Approved List now** and click **OK**.

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 computer since a customized installation may require a valid configuration file and Approved List. See the Trend Micro Safe Lock Administrator's Guide for more information about the Approved List and configuration file.



### WARNING!

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



### Important

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



### Note



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

## Installer Command Line Interface Parameters

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

**TABLE 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   <b>Note</b> The Safe Lock configuration file can be exported after installing Safe Lock.
-lp	<path>	Specify the Approved List   <b>Note</b> 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 8-17](#).

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	<ul style="list-style-type: none"> <li>• 0: Create shortcut</li> <li>• 1: Do not create shortcut</li> </ul>	0	No
NO_STARTMENU	Create a shortcut in the Start menu	<ul style="list-style-type: none"> <li>• 0: Create shortcut</li> <li>• 1: Do not create shortcut</li> </ul>	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
NO_SYSTRAY	Display the system tray icon and Windows notifications	<ul style="list-style-type: none"> <li>0: Create system tray icon</li> <li>1: Do not create system tray icon</li> </ul>	0	No
TITLE	Title content for pop-up notifications	Text up to 64 characters	Application Blocked	No
MESSAGE	Message content for pop-up notifications	Text up to 200 characters	A program has been blocked by Trend Micro Safe Lock. Please contact your help desk or administrator.	No
FILEINFO	Display the name and path of a blocked file in the pop-up notification	<ul style="list-style-type: none"> <li>0: Disable</li> <li>1: Enable</li> </ul>	0	No
PASSWORD	Authenticate user identity by requesting for the administrator password before closing a pop-up notification	<ul style="list-style-type: none"> <li>0: Disable</li> <li>1: Enable</li> </ul>	0	No
NO_NSC	Install firewall	<ul style="list-style-type: none"> <li>0: Create firewall</li> <li>1: Do not create firewall</li> </ul>	0	No





KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
CONFIG_PATH	Configuration file path	<path>	<empty>	No
LIST_PATH	Approved List path for import	<path>	<empty>	No
APPLICATION FOLDER	Installation path for agent program	<path>	<empty>	No
MANAGED_MODE	Specify if Safe Lock is managed by the Safe Lock Intelligent Manager server	<ul style="list-style-type: none"> <li>• 0: Standalone mode</li> <li>• 1: Managed mode</li> </ul>	0	No
PASSWORD	Password which is used for <code>sLcmd.exe</code> and Safe Lock console	<password>	<empty>	No
CUSTOM_ACTION	Custom action for blocked events	<ul style="list-style-type: none"> <li>• 0: Ignore</li> <li>• 1: Quarantine</li> <li>• 2: Ask server</li> </ul>	0	No
QUARANTINE_FOLDER_PATH	Quarantine path for agent program	<path>	<empty>	No
ROOT_CAUSE_ANALYSIS	Enable root cause analysis reporting	<ul style="list-style-type: none"> <li>• 0: Disable</li> <li>• Other value: Enable</li> </ul>	1	No
INTEGRITY_MONITOR	Enable Integrity Monitor	<ul style="list-style-type: none"> <li>• 0: Disable</li> <li>• 1: Enable</li> </ul>	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
PREDEFINED_TRUSTED_UPDATER	Enable Predefined Trusted Updater	<ul style="list-style-type: none"> <li>0: Disable</li> <li>1: Enable</li> </ul>	0	No
WINDOWS_UPDATE_SUPPORT	Enable Window Update Support	<ul style="list-style-type: none"> <li>0: Disable</li> <li>1: Enable</li> </ul>	0	No
PRESCAN	Prescan the endpoint before installing Safe Lock	<ul style="list-style-type: none"> <li>0: Do not prescan the endpoint</li> <li>1: Prescan the endpoint</li> </ul>	1	No
MAX_EVENT_DATABASE_SIZE	Maximum database file size (MB)	Positive integer	1024	No
WEL_SIZE	Windows Event Log size (KB)	Positive integer <hr/>  <b>Note</b> Default value for new installations. Upgrading Safe Lock does not change any user-defined WEL_SIZE values set in the previous installation.	10240	No
WEL_RETENTION	Windows Event Log option when maximum event log size is reached on	For Windows XP or earlier platforms:	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
	Windows Event Log.	<ul style="list-style-type: none"> <li>• 0: Overwrite events as needed</li> <li>• 1 - 365: Overwrite events older than (1-365) days</li> <li>• -1: Do not overwrite events (Clear logs manually)</li> </ul> <p>For Windows Vista or later platforms:</p> <ul style="list-style-type: none"> <li>• 0: Overwrite events as needed (oldest events first)</li> <li>• 1: Archive the log when full, do not overwrite events</li> <li>• -1: Do not overwrite events (Clear logs manually)</li> </ul>		
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	<p>For Windows XP or earlier platforms:</p> <ul style="list-style-type: none"> <li>• 0: Overwrite events as needed</li> </ul>	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
	Monitor events is reached on Windows Event Log.	<ul style="list-style-type: none"> <li>• 1 - 365: Overwrite events older than (1-365) days</li> <li>• -1: Do not overwrite events (Clear logs manually)</li> </ul> <p>For Windows Vista or later platforms:</p> <ul style="list-style-type: none"> <li>• 0: Overwrite events as needed (oldest events first)</li> <li>• 1: Archive the log when full, do not overwrite events</li> <li>• -1: Do not overwrite events (Clear logs manually)</li> </ul>		
USR_DEBUGLOG_ENABLE	Enable debug logging for user sessions	<ul style="list-style-type: none"> <li>• 0: Do not log</li> <li>• 1: Log</li> </ul>	0	No
USR_DEBUGLOG_LEVEL	The number of debug log entries allowed for user sessions	<ul style="list-style-type: none"> <li>• 273</li> </ul>	273	No
SRV_DEBUGLOG_ENABLE	Enable debug logging for service sessions.	<ul style="list-style-type: none"> <li>• 0: Do not log</li> <li>• 1: Log</li> </ul>	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
SRV_DEBUGLOGLEVEL	The number of debug log entries allowed for service sessions	<ul style="list-style-type: none"> <li>273</li> </ul>	273	No
SILENT_INSTALL	<p>Execute installation in silent mode</p> <hr/> <p> <b>Important</b> To use silent mode, you must also specify the ACTIVATION_CODE and PASSWORD keys and values. For example:</p> <pre>[PROPERTY]  ACTIVATION_CODE=XX-XXXXX-XXXXX-XXXXX-XXXXX PASSWORD=P@ssW0rd  SILENT_INSTALL=1</pre>	<ul style="list-style-type: none"> <li>0: Do not use silent mode</li> <li>1: Use silent mode</li> </ul>	0	No
STORAGE_DEVICE_BLOCKING	Blocks storage devices, including CD/DVD drives, floppy disks, and network drives, from accessing managed endpoints.	<ul style="list-style-type: none"> <li>0: Allow access from storage devices</li> <li>1: Block access from storage devices</li> </ul>	0	No
INIT_LIST	Initialize the Approved List	<ul style="list-style-type: none"> <li>0: Do not initialize the Approved List</li> </ul>	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
	during installation	during installation <ul style="list-style-type: none"> <li>1: Initialize the Approved List during installation</li> </ul>		
	 <b>Note</b> 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	<folder path>	<empty>	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
	directory will be traversed if empty.			
LOCKDOWN	Turn Application Lockdown on after installation finish	<ul style="list-style-type: none"> <li>0: Turn off Application Lockdown</li> <li>1: Turn on Application Lockdown</li> </ul>	0	No
FILELESS_ATTACK_PREVENTION	Enable the Fileless Attack Prevention feature	<ul style="list-style-type: none"> <li>0: Disable feature</li> <li>1: Enable feature</li> </ul>	0	No
VERIFY_PATCH_SIGNATURE	Verify signature of patch received from Safe Lock Intelligent Manager before continuing	<ul style="list-style-type: none"> <li>0: Do not verify patch signature</li> <li>1: Verify patch signature</li> </ul>	1	No
USR_DEBUGLOG_ENABLE	Enable debug log in user session	<ul style="list-style-type: none"> <li>0: Disable debug log</li> <li>1: Enable debug log</li> </ul>	0	No
USR_DEBUGLOG_LEVEL	Debug level in user session	273	273	No
SRV_DEBUGLOG_ENABLE	Enable debug log in service session	<ul style="list-style-type: none"> <li>0: Disable debug log</li> <li>1: Enable debug log</li> </ul>	0	No
SRV_DEBUGLOG_LEVEL	Debug level in service session	<ul style="list-style-type: none"> <li>273</li> </ul>	273	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
FW_USR_DEBU GLOG	Enable debug log in user session of firewall	<ul style="list-style-type: none"> <li>0: Disable debug log</li> <li>1: Enable debug log</li> </ul>	0	No
FW_USR_DEBU GLOG_LEVEL	Debug level in user session of firewall	number	273	No
FW_SRV_DEBU GLOG_ENABLE	Enable debug log in service session of firewall	<ul style="list-style-type: none"> <li>0: Disable debug log</li> <li>1: Enable debug log</li> </ul>	0	No
FW_SRV_DEBU GLOG_LEVEL	Debug level in service session of firewall	number	273	No
BM_SRV_DEBU GLOG_ENABLE	Enable debug log of Behavior Monitoring Core service	<ul style="list-style-type: none"> <li>0: Disable debug log</li> <li>1: Enable debug log</li> </ul>	0	No
BM_SRV_DEBU GLOG_LEVEL	Debug level of Behavior Monitoring Core service	<ul style="list-style-type: none"> <li>51</li> </ul>	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	<ul style="list-style-type: none"> <li>• 1: Log</li> <li>• 0: Do not log</li> </ul>	1	No
LEVEL_WARNINGLOG	Log "Warning" level events related to Safe Lock	<ul style="list-style-type: none"> <li>• 1: Log</li> <li>• 0: Do not log</li> </ul>	1	No
LEVEL_INFORMATIONLOG	Log "Information" level events related to Safe Lock	<ul style="list-style-type: none"> <li>• 1: Log</li> <li>• 0: Do not log</li> </ul>	0	No
BLOCKEDACCESSLOG	Log files blocked by Safe Lock	<ul style="list-style-type: none"> <li>• 1: Log</li> <li>• 0: Do not log</li> </ul>	1	No
APPROVEDACCESSLOG	Log files approved by Safe Lock	<ul style="list-style-type: none"> <li>• 1: Log</li> <li>• 0: Do not log</li> </ul>	1	No
APPROVEDACCESSLOG_TRUSTEDUPDATER	Log Trusted Updater approved access	<ul style="list-style-type: none"> <li>• 1: Log</li> <li>• 0: Do not log</li> </ul>	1	No
APPROVEDACCESSLOG_TRUSTEDHASH	Log Trusted Hash approved access	<ul style="list-style-type: none"> <li>• 1: Log</li> <li>• 0: Do not log</li> </ul>	1	No
APPROVEDACCESSLOG_DLLDRIVER	Log DLL/Driver approved access	<ul style="list-style-type: none"> <li>• 1: Log</li> <li>• 0: Do not log</li> </ul>	0	No
APPROVEDACCESSLOG_EXCEPTIONPATH	Log Application Lockdown exception path	<ul style="list-style-type: none"> <li>• 1: Log</li> <li>• 0: Do not log</li> </ul>	1	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
	approved access			
APPROVEDACCESSLOG_TRUSTEDCERT	Log Trusted Certifications approved access	<ul style="list-style-type: none"> <li>• 1: Log</li> <li>• 0: Do not log</li> </ul>	1	No
APPROVEDACCESSLOG_WRITEPROTECTION	Log Write Protection approved access	<ul style="list-style-type: none"> <li>• 1: Log</li> <li>• 0: Do not log</li> </ul>	1	No
SYSTEMEVENTLOG	Log events related to the system	<ul style="list-style-type: none"> <li>• 1: Log</li> <li>• 0: Do not log</li> </ul>	1	No
SYSTEMEVENTLOG_EXCEPTIONONPATH	Log exceptions to Application Lockdown	<ul style="list-style-type: none"> <li>• 1: Log</li> <li>• 0: Do not log</li> </ul>	1	No
SYSTEMEVENTLOG_WRITEPROTECTION	Log Write Protection events	<ul style="list-style-type: none"> <li>• 1: Log</li> <li>• 0: Do not log</li> </ul>	1	No
LISTLOG	Log events related to the Approved list	<ul style="list-style-type: none"> <li>• 1: Log</li> <li>• 0: Do not log</li> </ul>	1	No
USBMALWAREPROTECTIONLOG	Log events that trigger USB Malware Protection	<ul style="list-style-type: none"> <li>• 1: Log</li> <li>• 0: Do not log</li> </ul>	1	No
EXECUTIONPREVENTIONLOG	Log events that trigger Execution Prevention	<ul style="list-style-type: none"> <li>• 1: Log</li> <li>• 0: Do not log</li> </ul>	1	No
NETWORKVIRUSPROTECTIONLOG	Log events that trigger Network Virus Protection	<ul style="list-style-type: none"> <li>• 1: Log</li> <li>• 0: Do not log</li> </ul>	1	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
INTEGRITYMONITORINGLOG_FILECREATED	Log file and folder created events	<ul style="list-style-type: none"> <li>• 1: Log</li> <li>• 0: Do not log</li> </ul>	1	No
INTEGRITYMONITORINGLOG_FILEMODIFIED	Log file modified events	<ul style="list-style-type: none"> <li>• 1: Log</li> <li>• 0: Do not log</li> </ul>	1	No
INTEGRITYMONITORINGLOG_FILEDELETED	Log file and folder deleted events	<ul style="list-style-type: none"> <li>• 1: Log</li> <li>• 0: Do not log</li> </ul>	1	No
INTEGRITYMONITORINGLOG_FILERENAMED	Log file and folder renamed events	<ul style="list-style-type: none"> <li>• 1: Log</li> <li>• 0: Do not log</li> </ul>	1	No
INTEGRITYMONITORINGLOG_REGVALUEMODIFIED	Log registry value modified events	<ul style="list-style-type: none"> <li>• 1: Log</li> <li>• 0: Do not log</li> </ul>	1	No
INTEGRITYMONITORINGLOG_REGVALUEDELETED	Log registry value deleted events	<ul style="list-style-type: none"> <li>• 1: Log</li> <li>• 0: Do not log</li> </ul>	1	No
INTEGRITYMONITORINGLOG_REGKEYCREATED	Log registry key created events	<ul style="list-style-type: none"> <li>• 1: Log</li> <li>• 0: Do not log</li> </ul>	1	No
INTEGRITYMONITORINGLOG_REGKEYDELETED	Log registry key deleted events	<ul style="list-style-type: none"> <li>• 1: Log</li> <li>• 0: Do not log</li> </ul>	1	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
INTEGRITYMONITORINGLOG_REGKEYRENAME	Log registry key renamed events	<ul style="list-style-type: none"> <li>1: Log</li> <li>0: Do not log</li> </ul>	1	No
DEVICECONTROLLOG	Log events related to device access control	<ul style="list-style-type: none"> <li>1: Log</li> <li>0: Do not log</li> </ul>	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	<ul style="list-style-type: none"> <li>0: Protect against BEAST attacks</li> <li>1: Do not implement any security workarounds for BEAST vulnerabilities</li> </ul>	1	No
POLL_SERVER	Identify the agent as an NAT agent	<ul style="list-style-type: none"> <li>0: Non-NAT agent</li> <li>1: NAT agent</li> </ul>	0	No
POLL_SERVER_INTERVAL	Set the NAT connection frequency	<ul style="list-style-type: none"> <li>1 - 64800: Connect to the Safe Lock Intelligent Manager server every (1 - 64800) minutes</li> </ul>	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	<ul style="list-style-type: none"> <li>• 1: Immediately</li> <li>• 2: On demand</li> </ul>	1	No
UNREGISTER_TRIGGER	Unregister message trigger	<ul style="list-style-type: none"> <li>• 1: Immediately</li> <li>• 2: On demand</li> </ul>	1	No
UPDATESTATUS_TRIGGER	Update status message trigger	<ul style="list-style-type: none"> <li>• 1: Immediately</li> <li>• 2: On demand</li> </ul>	1	No
UPLOADBLOCKED_EVENT_TRIGGER	Upload blocked event message trigger	<ul style="list-style-type: none"> <li>• 1: Immediately</li> <li>• 2: On demand</li> </ul>	1	No
CHECKFILEHASH_TRIGGER	Check file hash message trigger	<ul style="list-style-type: none"> <li>• 1: Immediately</li> <li>• 2: On demand</li> </ul>	1	No
QUICKSCANFILE_TRIGGER	Quick scan file message trigger	<ul style="list-style-type: none"> <li>• 1: Immediately</li> <li>• 2: On demand</li> </ul>	1	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
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, between attempts to resend events to Intelligent Manager.	• 0 ~ 2147483647	7680	No

## MessageRandomization Section



### Note

Safe Lock agents respond as soon as possible to direct requests from Safe Lock Intelligent Manager. For details, refer to Applying Message Time Groups in the Safe Lock 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_IN_DEX	Index of group which this agent belongs to	0 - 2147483646	0	No
TIME_PERIOD	Maximum amount of time agents have to upload data (in seconds)	0 - 2147483647	0	No

## Proxy Section

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

**TABLE 8-9. Setup.ini File [PROXY] Section Arguments**

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
MODE	Proxy mode	<ul style="list-style-type: none"> <li>• 0: No proxy used</li> <li>• 1: Proxy used with manual settings</li> <li>• 2: Proxy used with settings retrieved from Internet</li> </ul>	0	No





KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		Explorer automatically		
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	<p>Cancel installation after detecting malware threat during prescan</p> <hr/>  <b>Note</b> Only valid during silent installations.	<ul style="list-style-type: none"> <li>0: Cancel</li> <li>1: Continue installation after detecting malware threat during prescan</li> </ul>	0	No
REPORT_FOLDER	An absolute folder path where prescan	<ul style="list-style-type: none"> <li>&lt;folder_path&gt;</li> <li>&lt;empty&gt;: Defaults to</li> </ul>	<empty>	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
	result reports are saved.	%windir%\temp \prescan\log		
SCAN_TYPE	<p>The type of scan executed during silent installation</p> <hr/>  <b>Note</b> The selected value is used as the default value for a UI installation.	<ul style="list-style-type: none"> <li>• Full: Scan all folders on the endpoint.</li> <li>• Quick: Scans the following folders: <ul style="list-style-type: none"> <li>• Fixed root drives For example: c:\ d:\</li> <li>• System root folder For example, c:\Windows</li> <li>• System folder For example, c:\Windows\System</li> <li>• System32 folder For example, c:</li> </ul> </li> </ul>	Full	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		<p>\Windows \System32</p> <ul style="list-style-type: none"> <li>• <b>Driver folder</b>  For example, c: \Windows \System32 \Drivers</li> <li>• <b>Temp folder</b>  For example, c:\Users \Trend \AppData \Local \Temp</li> <li>• <b>Desktop folder including sub folders and files</b>  For example, c:\Users \Trend \Desktop</li> <li>• <b>Specific: Scan folders specified with SPECIFIC_FOLDER entries</b></li> </ul>		

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
COMPRESS_LAYER	The number of compressed layers to scan when a compressed file is scanned.	<ul style="list-style-type: none"> <li>0: Do not scan compressed files</li> <li>1 - 20: Scan up to the specified number of layers of a compressed file</li> </ul>	2	No
MAX_FILE_SIZE	The largest file allowed for scan	<ul style="list-style-type: none"> <li>0: Scan files of any sizes</li> <li>1 - 9999: Only scan files equal to or smaller than the specified size (MB)</li> </ul>	0	No
SCAN_REMOVABLE_DRIVE	Scan removable drives	<ul style="list-style-type: none"> <li>0: Do not scan removable drives</li> <li>1: Scan removable drives</li> </ul>	0	No
SPECIFIC_FOLDER	An absolute folder path to scan when the scan type is [Specific]	<p>&lt;folder_path&gt;</p> <p>Multiple folders can be specified by creating new entries whose name starting with SPECIFIC_FOLDER. Every entry name needs to be unique.</p> <p>For example:</p> <p>SPECIFIC_FOLDER=c:\folder1</p>	<empty>	No

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

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		EXCLUDED_FOLDER2= c:\file2.exe  EXCLUDED_FOLDER3= c:\file3.exe		
EXCLUDED_EXTENSION	A file extension to exclude from scanning	<file_extension>  Multiple extensions can be specified by creating new entries whose name starting with EXCLUDED_EXTENSION. Every entry name needs to be unique.  For example:  EXCLUDED_EXTENSION=bmp  EXCLUDED_EXTENSION2=png	<empty>	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 8-17](#) 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.	<ul style="list-style-type: none"> <li>• 0: Disable</li> <li>• 1: Enable</li> </ul>	0	No
ALWAYS_ON_TOP	Display the file blocking notification on top of other screens.	<ul style="list-style-type: none"> <li>• 0: Disable</li> <li>• 1: Enable</li> </ul>	1	No
SHOW_DETAILS	Display file name, file path, and event time in the notification.	<ul style="list-style-type: none"> <li>• 0: Disable</li> <li>• 1: Enable</li> </ul>	1	No
AUTHENTICATE	Authenticate the user by requesting the administrator password when closing the notification.	<ul style="list-style-type: none"> <li>• 0: Disable</li> <li>• 1: Enable</li> </ul>	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 on page 9-2*

## 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 through 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.org/2001/XMLSchema-i
  <Configuration>
    <AccountGroup>
      <Account Id="{24335D7C-1204-43d1-9CBB-332D688C85B6}" Enable="no">
        <Password/>
      </Account>
    </AccountGroup>
  </UI>
    <SystemTaskTrayIcon Enable="yes">
      <BlockNotification Enable="no" AlwaysOnTop="yes" ShowDetails="ye
        <Title/>
        <Message/>
      </BlockNotification>
    </SystemTaskTrayIcon>
  </UI>
  <Feature>
    <ApplicationLockDown LockDownMode="2">
      <WhiteList RecentHistoryUnapprovedFilesLimit="50"/>
      <ScriptLockdown Enable="yes">
        <Extension Id="bat">
          <Interpreter>cmd.exe</Interpreter>
        </Extension>
        <Extension Id="cmd">
          <Interpreter>cmd.exe</Interpreter>
        </Extension>
        <Extension Id="com">
          <Interpreter>ntvdm.exe</Interpreter>
        </Extension>
        <Extension Id="dll">
          <Interpreter>ntvdm.exe</Interpreter>
        </Extension>
        <Extension Id="drv">
          <Interpreter>ntvdm.exe</Interpreter>
        </Extension>
        <Extension Id="exe">
```

```

        <Interpreter>ntvdm.exe</Interpreter>
    </Extension>
    <Extension Id="js">
        <Interpreter>cscript.exe</Interpreter>
        <Interpreter>wscript.exe</Interpreter>
    </Extension>
    <Extension Id="msi">
        <Interpreter>msiexec.exe</Interpreter>
    </Extension>
    <Extension Id="pif">
        <Interpreter>ntvdm.exe</Interpreter>
    </Extension>
    <Extension Id="ps1">
        <Interpreter>powershell.exe</Interpreter>
    </Extension>
    <Extension Id="sys">
        <Interpreter>ntvdm.exe</Interpreter>
    </Extension>
    <Extension Id="vbe">
        <Interpreter>cscript.exe</Interpreter>
        <Interpreter>wscript.exe</Interpreter>
    </Extension>
    <Extension Id="vbs">
        <Interpreter>cscript.exe</Interpreter>
        <Interpreter>wscript.exe</Interpreter>
    </Extension>
</ScriptLockdown>
<TrustedUpdater>
    <PredefinedTrustedUpdater Enable="no">
        <RuleSet/>
    </PredefinedTrustedUpdater>
    <WindowsUpdateSupport Enable="no"/>
</TrustedUpdater>
<DllDriverLockDown Enable="yes"/>
<ExceptionPath Enable="no">
    <ExceptionPathList/>
</ExceptionPath>
<TrustedCertification Enable="yes"/>
<TrustedHash Enable="no"/>
<WriteProtection Enable="no" ActionMode="1" ProtectApprov
<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>
</Log>
```

```

        </EventLog>
        <DebugLog Enable="no"/>
    </Log>
</Feature>
<ManagedMode Enable="no">
    <Agent>
        <Port/>
        <SslAllowBeast>1</SslAllowBeast>
        <PollServer>0</PollServer>
        <PollServerInterval>10</PollServerInterval>
    </Agent>
    <Server>
        <HostName/>
        <FastPort/>
        <SlowPort/>
        <ApiKey/>
    </Server>
    <Message InitialRetryInterval="120" MaxRetryInterval="7680">
        <Register Trigger="1"/>
        <Unregister Trigger="1"/>
        <UpdateStatus Trigger="1"/>
        <UploadBlockedEvent Trigger="1"/>
        <CheckFileHash Trigger="1"/>
        <QuickScanFile Trigger="1"/>
    </Message>
    <MessageRandomization TotalGroupNum="1" OwnGroupIndex="0" Tim
    <Proxy Mode="0">
        <HostName/>
        <Port/>
        <UserName/>
        <Password/>
    </Proxy>
</ManagedMode>
</Configuration>
<Permission>
    <AccountRef Id="{24335D7C-1204-43d1-9CBB-332D688C85B6}">
        <UIControl Id="DetailSetting" State="no"/>
        <UIControl Id="LockUnlock" State="yes"/>
        <UIControl Id="LaunchUpdater" State="yes"/>
        <UIControl Id="RecentHistoryUnapprovedFiles" State="yes"/>
        <UIControl Id="ImportExportList" State="yes"/>
        <UIControl Id="ListManagement" State="yes"/>
    </AccountRef>
</Permission>

```

```

        <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	
	AccountGroup	Parameters to configure the Restricted User account	See <a href="#">AccountGroup Section on page 9-10</a> . See <a href="#">Account Types on page 5-17</a> .
	UI	Parameters to configure the display of the system tray icon	See <a href="#">UI Section on page 9-10</a> .
	Feature	Container for the Feature section	




SECTION		DESCRIPTION	ADDITIONAL INFORMATION
	ApplicationLockDown	Parameters to configure Safe Lock features and functions	See <a href="#">Feature Section on page 9-13</a> .
	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 <a href="#">Log Section on page 9-25</a> . See <a href="#">Agent Event Log Descriptions on page 13-4</a> .
	ManagedMode	Parameters to configure Centralized Management functions	See <a href="#">ManagedMode Section on page 9-29</a> .
Permission		Container for the Permission section	
	AccountRef	Parameters to configure the Safe Lock console controls available to the Restricted User account	See <a href="#">AccountRef Section on page 9-33</a> . See <a href="#">Account Types on page 5-17</a> .

## 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
			<hr/>  <b>Note</b> The Safe Lock administrator and Restricted User passwords cannot be the same. <hr/>

## 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	LockDown Mode	1	Turn on Application Lockdown
		2	Turn off Application Lockdown
WhiteList	RecentHistoryUnapprovedFilesLimit	0 - 65535	Maximum number of entries in the Blocked Files log
ScriptLockDown	Enable	yes	Enable Script Lockdown
		no	Disable Script Lockdown
Extension	ID	<file_extension>	File extension for Script Lockdown to block  For example, specify a value of <code>MSI</code> to block <code>.msi</code> files.
		Interpreter	<file_name>  Interpreter for the specified file extension  For example, specify <code>msiexec.exe</code> as the interpreter for <code>.msi</code> files.

PARAMETER		SETTING	VALUE	DESCRIPTION
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
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

PARAMETER				SETTING	VALUE	DESCRIPTION		
					folderandsub	Use the EXE, MSI OR BAT files in the specified folder and its subfolders		
				Path	<update_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 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							

PARAMETER	SETTING	VALUE	DESCRIPTION
		regex	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
		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



PARAMETER	SETTING	VALUE	DESCRIPTION	
	Hash	<SHA-1_hash_value>	SHA-1 hash value of this file	
	Label	<label>	Description of this file	
	AddToApprovedList	yes		Add the file matched by this hash value to the Approved List when it is accessed for the first time
		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 >	
	Folder	Path	<folder_path>	Folder path
		IncludesSubfolder	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: <ul style="list-style-type: none"> <li>• HKEY_LOCAL_MACHINE\test HKLM\test</li> <li>• HKEY_CURRENT_CONFIG\test HKCC\test</li> <li>• HKEY_CLASSES_ROOT\test HKCR\test</li> <li>• HKEY_CURRENT_USER\test HKCU\test</li> <li>• HKEY_USERS\test HKU\test</li> </ul>
IncludesSubkey				yes

PARAMETER				SETTING	VALUE	DESCRIPTION
					no	Do not include any subkeys
			RegistryValue	Key	<reg_key >	Registry key <reg_key> can be abbreviated or expanded as shown below: <ul style="list-style-type: none"> <li>• HKEY_LOCAL_MACHINE\test HKLM\test</li> <li>• HKEY_CURRENT_CONFIG\test HKCC\test</li> <li>• HKEY_CLASSES_ROOT\test HKCR\test</li> <li>• HKEY_CURRENT_USER\test HKCU\test</li> <li>• HKEY_USERS\test HKU\test</li> </ul>
				Name	<reg_value_name >	Registry value name
			ExceptionList			Container for the Write Protection Exception List
			Process	Path	<process_path>	Path of the process
			File	Path	<file_path >	File path

PARAMETER				SETTING	VALUE	DESCRIPTION
	Folder	Path	<folder_path>	Folder path		
		IncludesSubfolder	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:		
				<ul style="list-style-type: none"> <li>• HKEY_LOCAL_MACHINE\test HKLM\test</li> <li>• HKEY_CURRENT_CONFIG\test HKCC\test</li> <li>• HKEY_CLASSES_ROOT\test HKCR\test</li> <li>• HKEY_CURRENT_USER\test HKCU\test</li> <li>• HKEY_USERS\test HKU\test</li> </ul>		
	RegistryValue	Key	<reg_key >	Registry key		
				IncludesSubkey	yes	Include any subkeys
				no	Do not include any subkeys	

PARAMETER				SETTING	VALUE	DESCRIPTION
						<p>&lt;reg_key&gt; can be abbreviated or expanded as shown below:</p> <ul style="list-style-type: none"> <li>• HKEY_LOCAL_MACHINE\test</li> <li>• HKLM\test</li> <li>• HKEY_CURRENT_CONFIG\test</li> <li>• HKCC\test</li> <li>• HKEY_CLASSES_ROOT\test</li> <li>• HKCR\test</li> <li>• HKEY_CURRENT_USER\test</li> <li>• HKCU\test</li> <li>• HKEY_USERS\test</li> <li>• HKU\test</li> </ul>
				Name	<reg_value_name>	Registry value name
			CustomAction	ActionMode	0	<p>Ignore blocked files or processes when Application Lockdown blocks any of the following events:</p> <ul style="list-style-type: none"> <li>• Process launch</li> <li>• DLL loading</li> <li>• Script file access</li> </ul>
					1	<p>Quarantine blocked files or processes when Application Lockdown blocks any of the following events:</p>

PARAMETER	SETTING	VALUE	DESCRIPTION
			<ul style="list-style-type: none"> <li>Process launch</li> <li>DLL loading</li> <li>Script file access</li> </ul>
		2	Ask what to do for blocked files or processes when Application Lockdown blocks any of the following events: <ul style="list-style-type: none"> <li>Process launch</li> <li>DLL loading</li> <li>Script file access</li> </ul>
UsbMalwareProtection	Enable	yes	Enable USB Malware Protection
		no	Disable USB Malware Protection
	ActionMode	0	Allow action by detected malware
		1	Block action by detected malware
DllInjectionPrevention	Enable	yes	Enable DLL Injection Prevention
		no	Disable DLL Injection Prevention
	ActionMode	0	Allows DLL injections
		1	Blocks DLL injections
ApiHookingPrevention	Enable	yes	Enable API Hooking Prevention
		no	Disable API Hooking Prevention

PARAMETER	SETTING	VALUE	DESCRIPTION
	ActionMode	0	Allow API hooking
		1	Block API hooking
MemoryRandomization	Enable	yes	Enable Memory Randomization
		no	Disable Memory Randomization
NetworkVirusProtection	Enable	yes	Enable Network Virus Protection
		no	Disable Network Virus Protection
	ActionMode	0	Allow action by detected network viruses
		1	Block action by detected network viruses
IntegrityMonitoring	Enable	yes	Enable Integrity Monitoring
		no	Disable Integrity Monitoring
StorageDeviceBlocking	Enable	yes	Blocks access of storage devices (CD/DVD drives, floppy disks, and network drives) to managed endpoints
		no	Allows access of storage devices (CD/DVD drives, floppy disks, and network drives) to managed endpoints
	ActionMode	0	Allow actions such as edit, rename, and delete
		1	Block actions such as edit, rename, and delete

PARAMETER	SETTING	VALUE	DESCRIPTION
	Log		Container for configuring logs See <a href="#">Log Section on page 9-25</a> .
FilelessAttackPrevention	Enable	yes	Enable Fileless Attack Prevention
		no	Disable Fileless Attack Prevention
ExceptionList			Container for the Fileless Attack Prevention Exception List
Exception	Target	<monitored process>	Specify powershell.exe, wscript.exe, CScript.exe, or mshta.exe
	Label	<label>	Unique name of this exception
Arguments		<arguments>	Arguments to be approved
	Regex	yes	Specify yes if argument includes a regular exception
		no	Specify no if argument does not include a regular exception
Parent1		<parent process>	Parent process of the monitored process
Parent2		<grandparent process>	Grandparent process of the monitored process
Parent3		<great grandpar	Great grandparent process of the monitored process



PARAMETER				SETTING	VALUE	DESCRIPTION
					ent process>	
			Parent4		<great great grandpar ent process>	Great great grandparent process of the monitored process

## 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
EventLog					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

PARAMETER				SETTING	VALUE	DESCRIPTION	
				InformationLog	Enable	yes	Log "Information" level events related to Safe Lock
					no	Do not log "Information" level events related to Safe Lock	
				BlockedAccessLog	Enable	yes	Log files blocked by Safe Lock
						no	Do not log files blocked by Safe Lock
				ApprovedAccessLog	Enable	yes	Log files approved by Safe Lock
						no	Do not log files approved by Safe Lock
				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

PARAMETER		SETTING	VALUE	DESCRIPTION
	WriteProt ectionLog	Enable	no	Do not log Trusted Certifications approved access
			yes	Log Write Protection approved access
	SystemEventL og	Enable	no	Do not log Write Protection approved access
			yes	Log events related to the system
	Exception PathLog	Enable	no	Do not log events related to the system
			yes	Log exceptions to Application Lockdown
	WriteProt ectionLog	Enable	no	Do not log exceptions to Application Lockdown
			yes	Log Write Protection events
	ListLog	Enable	no	Do not log Write Protection events
			yes	Log events related to the Approved list
	USBMalwarePr otectionLog	Enable	no	Do not log events related to the Approved list
			yes	Log events that trigger USB Malware Protection
	ExecutionPre ventionLog	Enable	no	Do not log events that trigger USB Malware Protection
			yes	Log events that trigger Execution Prevention
			no	Do not log events that trigger Execution Prevention

PARAMETER		SETTING	VALUE	DESCRIPTION
	NetworkVirusProtectionLog	Enable	yes	Log events that trigger Network Virus Protection
			no	Do not log events that trigger Network Virus Protection
	IntegrityMonitoringLog			Container for configuring Integrity Monitoring logs
	FileCreatedLog	Enable	yes	Log file and folder created events
			no	Do not log file and folder created events
	FileModifiedLog	Enable	yes	Log file modified events
			no	Do not log file modified events
	FileDeletedLog	Enable	yes	Log file and folder deleted events
			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

PARAMETER				SETTING	VALUE	DESCRIPTION
			RegKeyCreatedLog	Enable	yes	Log registry key created events
					no	Do not log registry key created events
				Enable	yes	Log registry key deleted events
					no	Do not log registry key deleted events
				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

PARAMETER	SETTING	VALUE	DESCRIPTION
Agent			Container for configuring Safe Lock agents
Port		<server_messages_port>	Specify the secure port for server communications (formerly the agent listening port)
SslAllowBeast		0	Allow upload of large files (>10MB) on Windows Server 2008 platforms
		1	Prevent the unsuccessful upload of large files (>10MB) on Windows Server 2008 platforms (default value)
PollServer		0	Identify the agent as a non-NAT agent
		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

PARAMETER	SETTING	VALUE	DESCRIPTION
			status (formerly Fast Lane)
SlowPort		<files_port>	Specify secure port for collecting files for scanning (formerly Slow Lane)
ApiKey		<API_key>	Specify API key
Message			Container for configuring automated messages to Safe Lock Intelligent Manager
Register	Trigger	1	Send as soon as possible after the event occurs
		2	Do not send unless requested to by Intelligent Manager
Unregister	Trigger	1	Send as soon as possible after the event occurs
		2	Do not send unless requested to by Intelligent Manager
UpdateStatus	Trigger	1	Send as soon as possible after the event occurs
		2	Do not send unless requested to by Intelligent Manager
UploadBlockedEvent	Trigger	1	Send as soon as possible after the event occurs

PARAMETER	SETTING	VALUE	DESCRIPTION
		2	Do not send unless requested to by Intelligent Manager
CheckFileHash	Trigger	1	Send as soon as possible after the event occurs
		2	Do not send unless requested to by Intelligent Manager
QuickScanFile	Trigger	1	Send as soon as possible after the event occurs
		2	Do not send unless requested to by Intelligent Manager
MessageRandomization			
 <b>Note</b> 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 ( $\geq 1$ )	Specify the total number of message time groups
	OwnGroupIndex	Zero or Positive Integer, $< \text{TotalGroupNum}$	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




PARAMETER		SETTING	VALUE	DESCRIPTION
				<p>messages to Intelligent Manager when this group's message-sending cycle is active</p> <hr/> <p> <b>Note</b> Message time groups do not become active if their duration is set to zero (0).</p> <hr/>
	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_username>	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 <b>Settings</b> page   <b>Note</b> The <b>Password</b> page is not available to the Restricted User account.
		LockUnlock	Access the Application Lockdown setting on the <b>Overview</b> screen
		LaunchUpdater	Access the <b>Automatically add files created or modified by the selected application installer</b> option when a Restricted User clicks <b>Add Item</b> on the <b>Approved List</b> screen
		RecentHistoryUnapprovedFiles	Access the Block logs if a Restricted User clicks <b>Last application blocked</b> on the <b>Overview</b> screen
		ImportExportList	Access the <b>Import List</b> and <b>Export List</b> buttons
		ListManagement	Access the following items on the <b>Approved List</b> screen: <ul style="list-style-type: none"> <li>The <b>Delete Item</b> button</li> </ul>

PARAMETER				SETTING	VALUE	DESCRIPTION
						<ul style="list-style-type: none"><li>• The <b>Update Hash</b> button</li><li>• The <b>Add Item &gt; Add Files/Folders</b> menu</li></ul>
				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 on page 10-2*

## Uninstalling Agents from Windows



### Note

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

### Procedure

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

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

OPTION	DESCRIPTION
<p>If you use one of the following operating systems:</p> <ul style="list-style-type: none"> <li>• Windows 10 Enterprise</li> <li>• Windows 10 IoT Enterprise</li> <li>• Windows 10 Professional</li> <li>• Windows 10 Fall Creators Update (Redstone 3)</li> <li>• Windows 10 April 2018 Update (Redstone 4)</li> </ul>	<ol style="list-style-type: none"> <li>a. Go to <b>Start &gt; Settings</b>.</li> <li>b. Depending on your version of Windows 10, locate the <b>Apps &amp; features</b> section under one of the following categories: <ul style="list-style-type: none"> <li>• <b>System</b></li> <li>• <b>Apps</b></li> </ul> </li> <li>c. On the left pane, click <b>Apps &amp; features</b>.</li> <li>d. In the list, click Trend Micro Safe Lock.</li> <li>e. Click <b>Uninstall</b>.</li> </ol>
<p>If you use one of the following operating systems:</p> <ul style="list-style-type: none"> <li>• Windows Server 2016</li> <li>• Windows Server 2012</li> <li>• Windows Server 2008</li> <li>• Windows Storage Server 2016</li> </ul>	<ol style="list-style-type: none"> <li>a. Go to <b>Start &gt; Control Panel &gt; Programs and Features</b>.</li> <li>b. In the list, double-click Trend Micro Safe Lock.</li> </ol>

OPTION	DESCRIPTION
<ul style="list-style-type: none"><li>• Windows 8</li><li>• Windows 7</li><li>• Windows Vista</li></ul>	
If you use one of the following operating systems: <ul style="list-style-type: none"><li>• Windows Server 2003</li><li>• Windows XP</li><li>• Windows 2000</li></ul>	<ol style="list-style-type: none"><li>a. Go to <b>Start &gt; Control Panel &gt; Add or Remove Programs</b>.</li><li>b. In the list, select Trend Micro Safe Lock.</li><li>c. Click <b>Remove</b>.</li></ol>

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 on page 11-2](#)*

## 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 required reboot after installation except for the following scenarios.

SCENARIO TYPE	SCENARIO
Setting Changes	When the <b>Memory Randomization</b> 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. Collect the agent configuration file by exporting and importing from an existing agent.

For detailed steps, see [Exporting or Importing a Configuration File on page 9-3](#).

2. In the exported configuration file, specify the target Intelligent Manager by configuring the <Server> parameters under ManagedMode.

3. Encrypt the configuration file with the following command:

```
<TMSL>\SLCmd.exe encrypt managedmodeconfiguration test.xml  
test.xen
```

4. Import the encrypted configuration file and the certificate to Intelligent Manager with the following command:

```
<TMSL>\SLCmd.exe set managedmode enable -cfg test.xen -sc  
trend.cer
```

---



# Chapter 12

## Technical Support

Learn about the following topics:

- *Troubleshooting Resources on page 12-2*
- *Contacting Trend Micro on page 12-3*
- *Sending Suspicious Content to Trend Micro on page 12-4*
- *Other Resources on page 12-5*

## Troubleshooting Resources

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

### Using the Support Portal

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

---

#### Procedure

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



#### Tip

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

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

---

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

---

### Threat Encyclopedia

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

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

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

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

## Contacting Trend Micro

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

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

- 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 on page 13-2*
- *Enabling Local Accounts for Default Shares on page 13-3*
- *Agent Event Log Descriptions on page 13-4*
- *Agent Error Code Descriptions on page 13-31*

## 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 9-25*.

**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.

<b>EVENT ID</b>	<b>TASK CATEGORY</b>	<b>LEVEL</b>	<b>LOG DESCRIPTION</b>
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.



<b>EVENT ID</b>	<b>TASK CATEGORY</b>	<b>LEVEL</b>	<b>LOG DESCRIPTION</b>
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%

<b>EVENT ID</b>	<b>TASK CATEGORY</b>	<b>LEVEL</b>	<b>LOG DESCRIPTION</b>
1061	System	Information	Added folder to Write Protection Exception List. Path: %path% Scope: %scope% Process: %process%
1062	System	Information	Removed folder from Write Protection Exception List. Path: %path% Scope: %scope% Process: %process%
1063	System	Information	Added registry value to Write Protection List. Registry Key: %regkey% Registry Value Name: %regvalue%
1064	System	Information	Removed registry value from Write Protection List. Registry Key: %regkey% Registry Value Name: %regvalue%
1065	System	Information	Added registry value to Write Protection Exception List. Registry Key: %regkey% Registry Value Name: %regvalue% Process: %process%

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
1066	System	Information	Removed registry value from Write Protection Exception List. Registry Key: %regkey% Registry Value Name: %regvalue% Process: %process%
1067	System	Information	Added registry key to Write Protection List. Path: %regkey% Scope: %scope%
1068	System	Information	Removed registry key from Write Protection List. Path: %regkey% Scope: %scope%
1069	System	Information	Added registry key to Write Protection Exception List. Path: %regkey% Scope: %scope% Process: %process%
1070	System	Information	Removed registry key from Write Protection Exception List. Path: %regkey% Scope: %scope% Process: %process%
1071	System	Information	Custom Action set to Ignore.
1072	System	Information	Custom Action set to Quarantine.

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
1073	System	Information	Custom Action set to Ask Intelligent Manager
1074	System	Information	Quarantined file is restored. [Details] Original Location: %path% Source: %source%
1075	System	Information	Quarantined file is deleted. [Details] Original Location: %path% Source: %source%
1076	System	Information	Integrity Monitoring enabled.
1077	System	Information	Integrity Monitoring disabled.
1078	System	Information	Root cause analysis report failed. [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.

<b>EVENT ID</b>	<b>TASK CATEGORY</b>	<b>LEVEL</b>	<b>LOG DESCRIPTION</b>
1085	System	Information	When Write Protection is enabled, it includes the Write Protection List and the Approved List.
1086	System	Warning	When Write Protection is enabled, it includes the Write Protection List only.
1088	System	Information	Windows Update Support enabled.
1089	System	Information	Windows Update Support disabled.
1094	System	Information	Trend Micro Safe Lock updated. File applied: %file_name%
1096	System	Information	Trusted Hash List enabled.
1097	System	Information	Trusted Hash List disabled.
1099	System	Information	Storage device access set to Allow
1100	System	Information	Storage device access set to Block
1101	System	Information	Storage device control enabled
1102	System	Warning	Storage device control disabled

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
1103	System	Information	<p>Event Log settings changed.</p> <p>[Details]</p> <p>Windows Event Log: %ON off%</p> <p>Level:</p> <p>Warning Log: %ON off%</p> <p>Information Log: %ON off%</p> <p>System Log: %ON off%</p> <p>Exception Path Log: %ON off%</p> <p>Write Protection Log: %ON off%</p> <p>List Log: %ON off%</p> <p>Approved Access Log:</p> <p>DIIDriver Log: %ON off%</p> <p>Trusted Updater Log: %ON off%</p> <p>Exception Path Log: %ON off%</p> <p>Trusted Certification Log: %ON off%</p> <p>Trusted Hash Log: %ON off%</p> <p>Write Protection Log: %ON off%</p> <p>Blocked Access Log: %ON off%</p> <p>USB Malware Protection Log: %ON off%</p> <p>Execution Prevention Log: %ON off%</p> <p>Network Virus Protection Log: %ON off%</p> <p>Integrity Monitoring Log</p> <p>File Created Log: %ON off%</p> <p>File Modified Log: %ON off%</p> <p>File Deleted Log: %ON off%</p> <p>File Renamed Log: %ON off%</p> <p>RegValue Modified Log: %ON off%</p> <p>RegValue Deleted Log: %ON off%</p> <p>RegKey Created Log: %ON off%</p> <p>RegKey Deleted Log: %ON off%</p>

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
1104	System	Warning	Memory Randomization is not available in this version of Windows.
1105	System	Information	Blocked File Notification enabled.
1106	System	Information	Blocked File Notification disabled.
1107	System	Information	Administrator password changed remotely.
1111	System	Information	Fileless Attack Prevention enabled.
1112	System	Warning	Fileless Attack Prevention disabled.
1500	List	Information	Trusted Update started.
1501	List	Information	Trusted Update stopped.
1502	List	Information	Approved List import started: %path%
1503	List	Information	Approved List import complete: %path%
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%

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
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%
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%



EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
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 [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 happened during enumeration of the files in %drive_letter% Error Code: %error_code%

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
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] Label : %label% Target Process: %process_name% Arguments: %arguments% %regex_flag% Parent Process 1 Image Path: %path% Parent Process 2 Image Path: %path% Parent Process 3 Image Path: %path% Parent Process 4 Image Path: %path%

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
2000	Access Approved	Information	File access allowed: %path%  [Details] Access Image Path: %path% Access User: %username% Mode: %mode% List: %list%
2001	Access Approved	Warning	File access allowed: %path%  [Details] Access Image Path: %path% Access User: %username% Mode: %mode% File Hash allowed: %hash%
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%

<b>EVENT ID</b>	<b>TASK CATEGORY</b>	<b>LEVEL</b>	<b>LOG DESCRIPTION</b>
2003	Access Approved	Warning	File access allowed: %path% Unable to calculate hash while checking the Approved List.  [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2004	Access Approved	Warning	File access allowed: %path% Unable to get notifications to monitor process.
2005	Access Approved	Warning	File access allowed:%path% Unable to add process to non exception list.
2006	Access Approved	Information	File access allowed: %path%  [Details] Access Image Path: %path% Access User: %username% Mode: %mode%

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
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%  [Details] Access Image Path: %path% Access User: %username% Mode: %mode%

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
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%

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
2020	Access Approved	Warning	Change of Registry Key allowed. Registry Key: %regkey%  [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2021	Access Approved	Warning	File access allowed: %path% An error occurred while checking the Trusted Hash List.  [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
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%



EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
2503	Access Blocked	Warning	Change of File/Folder blocked: %path%  [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2505	Access Blocked	Warning	Change of Registry Value blocked. Registry Key: %regkey% Registry Value Name: %regvalue%  [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
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	Specified action is taken: %path%  [Details] Action: %action% Source: %source%  .

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
2508	Access Blocked	Warning	Failed to take specified action: %path%  [Details]  Action: %action%  Source: %source%  .
2509	Access Blocked	Warning	File access blocked: %path%  [Details]  Access Image Path: %path%  Access User: %username%  Mode: %mode%  Reason: Not in Approved List  File Hash blocked: %hash%
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%

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
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%
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%

<b>EVENT ID</b>	<b>TASK CATEGORY</b>	<b>LEVEL</b>	<b>LOG DESCRIPTION</b>
3000	USB Malware Protection	Warning	Device access allowed: %path%  [Details] Access Image Path: %path% Access User: %username% 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

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
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%  [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%

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
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% 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%

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
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%
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%

EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
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%  [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%



EVENT ID	TASK CATEGORY	LEVEL	LOG DESCRIPTION
4508	Changes in System	Information	Registry Key renamed. Registry Key: %regkey% New Registry Key: %regkey%  [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%

## Agent Error Code Descriptions

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

**TABLE 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.
0x80040205	Invalid status.
0x80040206	Out of memory.
0x80040207	Busy. Request ignored.

<b>CODE</b>	<b>DESCRIPTION</b>
0x00040208	Retry. (Usually the result of a task taking too long)
0x80040208	System Reserved. (Not used)
0x80040209	The file path is too long.
0x0004020a	System Reserved. (Not used)
0x8004020b	System Reserved. (Not used)
0x0004020c	System Reserved. (Not used)
0x0004020d	System Reserved. (Not used)
0x8004020d	System Reserved. (Not used)
0x0004020e	Reboot required.
0x8004020e	Reboot required for unexpected reason.
0x0004020f	Allowed to perform task.
0x8004020f	Permission denied.
0x00040210	System Reserved. (Not used)
0x80040210	Invalid or unexpected service mode.
0x00040211	System Reserved. (Not used)
0x80040211	Requested task not permitted in current status. Check license.
0x00040212	System Reserved. (Not used)
0x00040213	System Reserved. (Not used)
0x80040213	Passwords do not match.
0x00040214	System Reserved. (Not used)
0x80040214	System Reserved. (Not used)
0x00040215	Not found.
0x80040215	"Expected, but not found."

CODE	DESCRIPTION
0x80040216	Authentication is locked.
0x80040217	Invalid password length.
0x80040218	Invalid characters in password.
0x00040219	Duplicate password. Administrator and Restricted User passwords cannot match.
0x80040220	System Reserved. (Not used)
0x80040221	System Reserved. (Not used)
0x80040222	System Reserved. (Not used)
0x80040223	File not found (as expected, and not an error).
0x80040224	System Reserved. (Not used)
0x80040225	System Reserved. (Not used)
0x80040240	Library not found.
0x80040241	Invalid library status or unexpected error in library function.
0x80040260	System Reserved. (Not used)
0x80040261	System Reserved. (Not used)
0x80040262	System Reserved. (Not used)
0x80040263	System Reserved. (Not used)
0x80040264	System Reserved. (Not used)
0x00040265	System Reserved. (Not used)
0x80040265	System Reserved. (Not used)
0x80040270	System Reserved. (Not used)
0x80040271	System Reserved. (Not used)
0x80040272	System Reserved. (Not used)

CODE	DESCRIPTION
0x80040273	System Reserved. (Not used)
0x80040274	System Reserved. (Not used)
0x80040275	System Reserved. (Not used)
0x80040280	Invalid Activation Code.
0x80040281	Incorrect Activation Code format.

## 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 %'.
2002	Delete account	Deleted Intelligent Manager account '%user_name %'.
2003	Modify account	Modified Intelligent Manager account '%user_name %' %field_name%.

EVENT ID	SERVER EVENT	DESCRIPTION
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%.
4001	Take action on unapproved blocked file	<p>Requested to add blocked file to Approved List on endpoint(s). File name: %file_name% File hash: %file_hash% (SHA-1)</p> <p>Requested to delete the blocked file on endpoint(s). File name: %file_name% File hash: %file_hash% (SHA-1)</p> <p>Requested to quarantine the file on endpoint(s). File name: %file_name% File hash: %file_hash% (SHA-1)</p> <p>Requested to ignore the blocked file on endpoint(s). File name: %file_name% File hash: %file_hash% (SHA-1)</p> <p>Requested to restore the file from quarantine on endpoint(s). File name: %file_name% File hash: %file_hash% (SHA-1)</p>
4002	Mark as closed	Marked %num% event(s) closed.

EVENT ID	SERVER EVENT	DESCRIPTION
4003	Mark as open	Marked %num% event(s) opened.
4004	Release the quarantined malicious file	Requested to restore the file from quarantine on endpoint(s). File name: %file_name% File hash: %file_hash% (SHA-1)
4005	Delete the quarantined malicious file	Requested to delete the file from quarantine on endpoint(s). File name: %file_name% File hash: %file_hash% (SHA-1)
4006	Take action on unapproved fileless attack	Requested to add blocked process chain and command argument. Process chain: %process_name% Command argument: %parameter%  Requested to ignore blocked process chain and command argument. Process chain: %process_name% Command argument: %parameter%
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).
5012	Unable to add trusted file hashes	Unable to add 1 trusted file hash to %endpoint_name%. Unable to add %num% trusted file hashes to %endpoint_name%.
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).

EVENT ID	SERVER EVENT	DESCRIPTION
5022	Unable to block access from storage devices	Unable to block access from storage devices on %endpoint_name%.
5023	Allow access from storage devices	Allowed access from storage devices on endpoint(s).
5024	Unable to allow access from storage devices	Unable to allow access from storage devices on %endpoint_name%.
5601	Export agent settings	Exported (%file_desc%) from %endpoint_name%.
5602	Import agent settings	Imported (%file_desc%) to endpoint(s).
5603	Unable to import agent settings	Unable to import (%file_desc%) to %endpoint_name%.
5800	Change agent administrator password	Changed password on endpoint(s).
5801	Unable to change agent administrator password	Unable to change password to %endpoint_name%.
5900	Update agent Approved List	Updated Approved List on endpoint(s).
5901	Unable to update agent Approved List	Unable to update Approved List on %endpoint_name%.
6001	Deploy agent patch	Deploy agent patch to endpoint(s). Patch name: %patch_name%





# Index

## A

- agent configuration file, 9-2, 9-8
  - editing, 9-2
  - exporting or importing, 9-3
  - syntax, 9-3
- agent endpoint preparation
  - Windows 10, 7-7, 7-11
  - Windows 10 Enterprise, 7-7, 7-11
  - Windows 10 IoT Enterprise, 7-7, 7-11
  - Windows 7, 7-9
  - Windows 8, 7-10
  - Windows 8.1, 7-10
  - Windows Server 2003, 7-4
  - Windows Server 2003 R2, 7-4
  - Windows Server 2008, 7-5
  - Windows Server 2008 R2, 7-5
  - Windows Server 2012, 7-6
  - Windows Server 2012 R2, 7-6
  - Windows XP, 7-8
- agent events
  - exporting, 3-11
  - importing, 3-11
  - log maintenance, 3-15
  - notifications, 4-5
  - querying logs, 3-9
  - tracking, 3-9
- agent installer
  - approved list, 5-2, 8-11
  - command line interface, 8-13, 8-14
  - downloading, 4-3, 7-15
  - modified packages, 4-4
  - overview, 8-2
  - Setup.ini Agent section, 8-31
  - Setup.ini arguments, 8-17
  - Setup.ini BlockNotification section, 8-40
  - Setup.ini EventLog section, 8-26
  - Setup.ini MessageRandomization section, 8-33
  - Setup.ini Message section, 8-32
  - Setup.ini Prescan section, 8-35
  - Setup.ini Property section, 8-17
  - Setup.ini Proxy section, 8-34
  - Setup.ini Server section, 8-30
  - Setup.ini use, 8-16
  - upgrade preparation, 1-22
  - Windows Installer, 8-3
- agents, 1-11
  - account passwords, 5-18
  - accounts, 1-14, 5-17
  - changing lockdown, 2-9
  - collecting logs, 2-12
  - collecting status, 2-12
  - component update locations, 4-5
  - console, 5-6
  - editing tags, 2-7
  - error codes, 13-31
  - event ID codes, 13-4, 13-34
  - features and benefits, 1-13
  - manual component updates, 4-2
  - operating systems, 1-16
  - querying, 2-3
  - remote setup, 7-2
  - removing from list, 2-4
  - scheduled component updates, 4-3
  - settings, 5-19, 5-22
  - status icons, 5-9
  - system requirements, 1-15
  - uninstallation, 10-2

- use overview, 1-23
- Application Lockdown, 1-13
- Approved List, 5-10
  - adding or removing files, 5-14
  - checking or updating hashes, 5-12
  - configuring, 5-13
  - exporting or importing, 5-16
  - hashes, 5-12
  - installing or updating files, 5-14
  - setting up, 5-2, 8-11

## **C**

- configuration file
  - agents, 9-2
- console
  - feature comparison, 6-2

## **D**

- dashboard, 3-2
  - adding tabs, 3-4
  - default tabs, 3-3
  - tabs, 3-2
  - tab settings, 3-5
- dashboard widgets, 3-5
- default shares, 13-3
- documentation, vii
- documentation feedback, 12-6

## **E**

- error codes, 13-31
- event ID codes, 13-4, 13-34
- events
  - agent, 3-9
  - agent events, 3-9, 3-11, 3-15
  - server events, 3-13, 3-15
- Exploit Prevention, 1-13

## **F**

- features, 1-2
  - overview, 1-4
- features and benefits, 1-4

## **H**

- hashes, 5-12

## **I**

- installation
  - customization, 8-16
  - methods, 8-2
- installer
  - agent, 1-22

## **L**

- local accounts
  - enabling administrator, 13-2
  - enabling default shares, 13-3

## **N**

- Network Virus Protection, 8-6, 8-14
- notifications, 4-5, 4-8

## **O**

- operating systems, 1-6, 1-16

## **P**

- passwords, 5-18

## **R**

- remote tasks, 7-22
  - SLrst Program, 7-2
- requirements, 1-15
- Restricted User account
  - enabling, 5-19

## **S**

- Safe Lock, 1-2, 1-11

- Safe Lock Intelligent Manager, 1-2
  - server, 1-2
    - accounts, 1-9
    - features and benefits, 1-4
    - message time groups, 7-27
    - notifications, 4-8
    - remote tasks, 7-2, 7-22
    - system requirements, 1-6
  - server console, 2-2
  - server events
    - exporting, 3-15
    - log maintenance, 3-15
    - querying logs, 3-13
    - tracking, 3-13
  - SLCmd Commands, 6-4
    - For Application Lockdown, 6-27
    - For Approved List, 6-24
    - For Central Management, 6-8
    - For Configuration File, 6-66
    - For General Actions, 6-4
    - For notifications of file blocking, 6-65
    - For Optional Features, 6-10
    - For Predefined Trusted Updater, 6-58
    - For Predefined Trusted Updater "Add", 6-62
    - For Restricted User Accounts, 6-20
    - For Scripts, 6-22
    - For Trusted Certifications, 6-53
    - For Trusted Hash List, 6-54
    - For Trusted Updater, 6-56
    - For Windows Update Support, 6-65
    - For Write Protection, 6-30
  - SLCmd Program, 6-4
    - commands, 6-4
    - comparison to console functions, 6-2
    - using, 6-2
  - SLrst Program, 7-2
    - agent target files, 7-12–7-14
    - downloading installers, 4-3, 7-15
    - remote installation considerations, 7-3
    - remotely installing agents, 7-17
    - remotely restarting agents, 7-21
    - remotely uninstalling agents, 7-20
  - SLtasks Program, 7-22
    - message time groups, 7-27
  - support
    - resolve issues faster, 12-4
  - syslog server
    - forwarding, 3-18
  - system requirements, 1-6, 1-15
    - disk space, 1-8
    - operating systems, 1-6
    - processor, 1-8
    - RAM, 1-8
    - web browsers, 1-7
    - with SQL Express Server
      - disk space, 1-9
      - processor, 1-8, 1-9
      - RAM, 1-8, 1-9
- T**
- tabs, 3-2
  - tab widgets, 3-5
  - terminology, ix
  - Trend Micro Portable Security, 1-14
  - Trusted Updater, 5-15
- U**
- uninstallation, 10-2
  - upgrading, 1-22
- W**
- web console, 2-2

- accounts
    - web console accounts, 4-10
  - activation codes, 4-15
  - agent statuses and settings, 2-5
  - changing lockdown, 2-9
  - collecting logs, 2-12
  - component updates, 4-2
  - dashboard, 3-2
  - editing agent tags, 2-7
  - exporting agent events, 3-11
  - exporting server events, 3-15
  - importing agent events, 3-11
  - license management, 4-14, 4-15
  - log maintenance, 3-15
  - marking events, 3-12
  - proxy settings, 4-13
  - querying agent events, 3-9
  - querying agents, 2-3
  - querying server events, 3-13
  - removing agents, 2-4
  - syslog server, 3-18
  - widgets, 3-5
- web console accounts, 4-10
    - adding, 4-11
    - editing, 4-12
- what's new, 1-2
- widgets, 3-5
    - adding, 3-8
    - using, 3-6



**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](http://www.trendmicro.com)

Item Code: SLEM28239/180418