



2.0 TREND MICRO™ Safe Lock Intelligent Manager 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>

© 2014 Trend Micro Incorporated. All Rights Reserved. Trend Micro, the Trend Micro t-ball logo, Safe Lock, Intelligent Manager, Portable Security, 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.: SLEM26724/141016

Release Date: December 2014

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

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

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

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

Evaluate this documentation on the following site:

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

Table of Contents

Preface

Preface	v
About the Documentation	v
Audience	vi
Document Conventions	vi
Terminology	vii

Chapter 1: Introduction

About Trend Micro Safe Lock Intelligent Manager	1-2
Server Features and Benefits	1-2
Server Accounts Overview	1-6
About Trend Micro Safe Lock	1-7
What's New in This Version	1-7
Agent Features and Benefits	1-8
Agent Use Overview	1-15

Chapter 2: Working with Agents

About the Agents Screen	2-2
Querying Agents	2-2
Displaying Agent Status Details	2-3
Editing Tags	2-4
Collecting Logs and Status	2-4
Exporting Agent Data	2-5
Removing Agents	2-5
Remotely Changing Application Lockdown Status	2-6

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	3-8
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	3-14

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
About the Account Management Screen	4-8
Adding Accounts	4-9
Editing Accounts	4-10
Configuring Proxy Settings	4-11
About the License Management Screen	4-12
Changing Activation Codes	4-13

Chapter 5: Using the Agent Console

Setting Up the Approved List	5-2
About the Agent Console	5-5
About Status Icons	5-7
About the Approved List	5-8
About Hashes	5-10
Configuring the Approved List	5-11

Account Types	5-15
Configuring Passwords	5-16
About Feature Settings	5-17
Enabling or Disabling Feature Settings	5-20

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	6-3

Chapter 7: Managing Agents Remotely

The Remote Setup Tool (SLrst)	7-2
Remote Installation Considerations	7-3
Preparing the Agent Target Files	7-4
Downloading an Up-to-Date Agent Installer Package	7-7
Installing Agents Remotely	7-9
Applying Patches and Hot Fixes to Agents Remotely	7-10
Uninstalling Agents Remotely	7-12
Restarting Agents Remotely	7-13
The Remote Tasks Tool (SLtasks)	7-14
Sending Remote Tasks	7-14
Applying Message Time Groups	7-16

Chapter 8: Local Agent Installation

Local Installation Overview	8-2
Installing from Windows	8-2
Setting Up the Approved List	8-8
Installation Using the Command Line	8-11
Installer Command Line Interface Parameters	8-12
Installation Customization	8-13

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	9-7

Chapter 10: Local Agent Uninstallation

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

Chapter 11: Troubleshooting & FAQs

Troubleshooting Remote Agent Installations	11-2
--	------

Chapter 12: Technical Support

Troubleshooting Resources	12-2
Using the Support Portal	12-2
Trend Community	12-2
Contacting Trend Micro	12-3
Speeding Up the Support Call	12-3
Other Resources	12-4
TrendEdge	12-4
Download Center	12-4
TrendLabs	12-5
About Trend Micro	12-5

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	13-25

Index

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

Preface

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

Topics in this chapter include:

- *About the Documentation on page v*
- *Audience on page vi*
- *Document Conventions on page vi*
- *Terminology on page vii*

About the Documentation

Trend Micro Safe Lock Intelligent Manager documentation includes the following:

TABLE 1. Trend Micro Safe Lock Intelligent Manager Documentation

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

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

<http://docs.trendmicro.com>


Audience




Trend Micro Safe Lock Intelligent Manager documentation is intended for administrators responsible for Safe Lock Intelligent Manager management, including agent installation. These users are expected to have advanced networking and server management knowledge.

Document Conventions

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

TABLE 2. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
<i>Italics</i>	References to other documents
Monospace	Sample command lines, program code, web URLs, file names, and program output
Navigation > Path	The navigation path to reach a particular screen For example, File > Save means, click File and then click Save on the interface
 Note	Configuration notes

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

Terminology

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

TABLE 3. Safe Lock Intelligent Manager Terminology

TERMINOLOGY	DESCRIPTION
Server	The Safe Lock Intelligent Manager server program
Server endpoint	The host where the Safe Lock Intelligent Manager server is installed
Agents	The hosts running the Safe Lock program
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
Administrator (or Safe Lock Intelligent Manager administrator)	The person managing the Safe Lock Intelligent Manager server

TERMINOLOGY	DESCRIPTION
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 Intelligent Manager 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 1-7*

About Trend Micro Safe Lock Intelligent Manager

Trend Micro Safe Lock Intelligent Manager provides centralized monitoring and management of Trend Micro Safe Lock agent deployment, status, and events. For example, administrators can remotely deploy agents, deploy 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.

Server Features and Benefits

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

TABLE 1-1. 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.
Centralized Agent Management	Administrators can monitor Safe Lock agent status, examine connection status, view configurations, collect agent logs on-demand or by policy, and remotely turn agent Application Lockdown on or off.
Centralized Event Management	On endpoints protected by Safe Lock agents, administrators can monitor events and status and respond when files are blocked from running. Safe Lock Intelligent Manager provides event management features that let administrators know about blocked file events quickly and allows them to manage these events. For example, events can be marked open or closed for tracking, and the detailed event information needed to resolve events can be collected quickly and easily.

FEATURE	BENEFIT
Root Cause Information Analysis	When blocked file events happen, administrators can determine if they are the result of a significant incident or not. Safe Lock Intelligent Manager provides malware scanning features and root cause information and diagrams to help administrators investigate blocked files quickly. For example, administrators can check if a blocked file is required to launch a mission-critical program, or if the blocked file is detected as malware. Administrators can also learn where blocked files are run from and what process launched them.
Server Event Auditing	Operations performed by Safe Lock Intelligent Manager web console accounts are logged. Safe Lock Intelligent Manager records an operating log for each account, tracking who logs on, who deletes event logs, and more.

Safe Lock Intelligent Manager Requirements



Important

Trend Micro Safe Lock Intelligent Manager has specific requirements that vary based on other software running on the server endpoint.

TABLE 1-2. Required Software for Safe Lock Intelligent Manager

REQUIRED SOFTWARE	SPECIFICATIONS
Operating systems	<ul style="list-style-type: none"> • Windows XP SP2/SP3 (32-bit) • Windows 7 Enterprise (Ultimate) No-SP/SP1 (32-bit and 64-bit) • Windows 8 Enterprise No-SP (32-bit and 64-bit) • Windows 8.1 Enterprise No-SP (32-bit and 64-bit) • Windows Server 2003 No-SP/SP1/SP2 (32-bit and 64-bit) • Windows Server 2003 R2 No-SP/SP2 (32-bit and 64-bit) • 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)
Web browser (for Safe Lock Intelligent Manager web console access)	<ul style="list-style-type: none"> • Microsoft Internet Explorer 7 or later • The latest version of Google Chrome • The latest version of Mozilla Firefox

TABLE 1-3. Required Hardware for Safe Lock Intelligent Manager (without Safe Lock agent)

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

TABLE 1-4. Required Hardware for Safe Lock Intelligent Manager (with Safe Lock agent)

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

TABLE 1-5. 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"> • 4GB minimum • 8GB or more recommended
Processor	<ul style="list-style-type: none"> • 1 CPU core minimum • 2 CPU cores or more recommended
Available disk space	<ul style="list-style-type: none"> • 30GB minimum • 50GB or more recommended


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

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

Server Accounts Overview

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

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

	TASK	ACCOUNT PRIVILEGE REQUIRED
1	Add Safe Lock Intelligent Manager accounts.	<ul style="list-style-type: none"> admin
2	Use remote deployment tools (<code>SLrst.exe</code>) to centrally deploy agents from the server.	<ul style="list-style-type: none"> N/A <hr/>  Note 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"> admin Full Control
4	Monitor Server Event logs.	<ul style="list-style-type: none"> admin Full Control
5	Monitor Agent Event logs.	<ul style="list-style-type: none"> admin Full Control Read Only

About Trend Micro Safe Lock

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

What's New in This Version

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

Trend Micro Safe Lock 2.0 Features and Enhancements

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

TABLE 1-7. New Features

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

Agent Features and Benefits

Trend Micro Safe Lock includes the following features and benefits.

Application Lockdown

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

Exploit Prevention

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

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

Easy Management

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

Small Footprint

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

Role Based Administration

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

Graphical and Command Line Interfaces

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

Trend Micro Portable Security Compatible

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

Safe Lock Agent Requirements

This section introduces Safe Lock system requirements and upgrade limitations.

Agent Requirements

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

TABLE 1-8. Required Hardware for Safe Lock

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



Important

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

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

Agent Operating Systems



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








Note



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

TABLE 1-9. List of Supported Operating Systems

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

WINDOWS VERSION TYPE	WINDOWS VERSION NAME
Windows Server	Windows 2000 Server SP4* (32-bit)
	 Note *Without Update Rollup, this version of Windows does not support DLL/Driver Lockdown, Integrity Monitoring, and the Predefined Trusted Updater.
	Windows Server 2003 SP1/SP2 (32-bit)
	 Note Safe Lock does not support a custom action of “quarantine” on Windows XP or Windows 2003.
	Windows Server 2003 R2 No-SP/SP2 (32-bit)
	 Note Safe Lock does not support a custom action of “quarantine” on Windows XP or Windows 2003.
	Windows Server 2008 SP1/SP2 (32-bit and 64-bit)
	Windows Server 2008 R2 No-SP/SP1 (64-bit)
Windows Server 2012 No-SP (64-bit)	
Windows Server 2012 R2 No-SP (64-bit)	

WINDOWS VERSION TYPE	WINDOWS VERSION NAME
Windows Embedded Standard	Windows (Standard) XP Embedded SP1*/SP2 (32-bit) <hr/>  Note *This version of Windows does not support DLL/Driver Lockdown, Integrity Monitoring, and the Predefined Trusted Updater. Safe Lock does not support a custom action of "quarantine" on Windows XP or Windows 2003. <hr/>
	Windows Embedded Standard 2009 (32-bit)
	Windows Embedded Standard 7 (32-bit and 64-bit)
	Windows Embedded Standard 8 (32-bit and 64-bit)
	Windows Embedded Standard 8.1 (32-bit and 64-bit)
Windows Embedded POSReady	Windows Embedded POSReady (32-bit)
	Windows Embedded POSReady 2009 (32-bit)
	Windows Embedded POSReady 7 (32-bit and 64-bit)
Windows Embedded Enterprise	Windows Embedded Enterprise XP SP1*/SP2/SP3 (32-bit) <hr/>  Note *This version of Windows does not support DLL/Driver Lockdown, Integrity Monitoring, and the Predefined Trusted Updater. Safe Lock does not support a custom action of "quarantine" on Windows XP or Windows 2003. <hr/>
	Windows Embedded Enterprise Vista (32-bit)
	Windows Embedded Enterprise 7 (32-bit and 64-bit)

WINDOWS VERSION TYPE	WINDOWS VERSION NAME
Windows Embedded Server	Windows Embedded Server 2003 SP1/SP2 (32-bit)
	 Note Safe Lock does not support a custom action of “quarantine” on Windows XP or Windows 2003.
	Windows Embedded Server 2003 R2 (32-bit)
	 Note Safe Lock does not support a custom action of “quarantine” on Windows XP or Windows 2003.
	Windows Embedded Server 2008 (32-bit and 64-bit)
	Windows Embedded Server 2008 R2 (64-bit)
	Windows Embedded Server 2012 (64-bit)
Windows Embedded Server 2012 R2 (64-bit)	

Agent Upgrade Preparation



WARNING!

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

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

TABLE 1-10. 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	1.0	Manually uninstall	No settings retained
	1.1	Manually uninstall	No settings retained
	2.0 or later	Manually uninstall	No settings retained

Agent Use Overview

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

Consider this typical use case scenario:

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

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

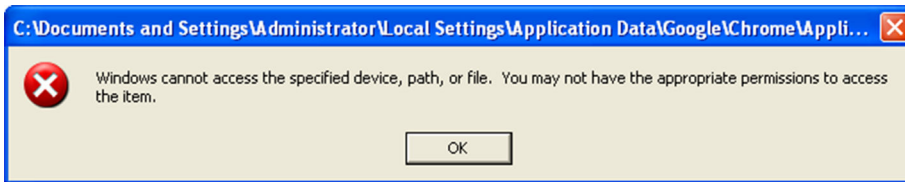


FIGURE 1-1. Trend Micro Safe Lock blocking message

Chapter 2

Working with Agents

This chapter introduces Trend Micro Safe Lock Intelligent Manager web console screen for agent management.

Topics in this chapter include:

- *[About the Agents Screen on page 2-2](#)*
- *[Remotely Changing Application Lockdown Status on page 2-6](#)*

About the Agents 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.

**Note**

To refine the list of displayed agents, see [Querying Agents on page 2-2](#).

To display the status of each Safe Lock setting for a selected agent, see [Displaying Agent Status Details on page 2-3](#).

The following table lists the available tasks on the **Agent Management** screen after selecting at least one agent endpoint.

FUNCTION	DESCRIPTION
Edit Tags	Edit tags to help you identify and search for agents.
Clear Tags	Clear existing tags for the selected endpoints.
Collect Logs & Status	Collect logs and status to update the Safe Lock Intelligent Manager database with the latest information from the selected agents.
Export	Save data about selected endpoints as a CSV file.
Remove	Remove agents from the list that Safe Lock Intelligent Manager no longer monitors.

Querying Agents

Procedure

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

The **Agent Management** screen appears.

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



Tip

Safe Lock Intelligent Manager supports partial string matching.

OPTION	DESCRIPTION
All Agents	Select to display all agents.
Endpoint	Type the host name of the endpoint.
Tags	Type the tag name.
IP Address	Type the IPv4 address.
IP Range	Type the IPv4 address.
Operating System	Select an operating system.
Application Lockdown State	Select the Application Lockdown state: Application Lockdown On or Application Lockdown Off .
Status Collected On	Select from the default time ranges or Custom and specify your own range.
Logs Collected On	Select from the default time ranges or Custom and specify your own range.

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

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

Displaying Agent Status Details

The **Agent Status** screen displays information about the selected agent, such as Application Lockdown status, program version number, and last log collection time. This screen also displays the status of specific Safe Lock features for the selected agent.

Procedure

1. Go to **Agents** in the navigation at the top of the web console.
The **Agent Management** screen appears.
 2. Click the endpoint name to display agent status details.
The **Agent Status** screen appears.
-

Editing Tags

Edit tags to help you identify and search for 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 **Edit Tags**.
 4. Type or modify the agent tags.
-



Tip

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

5. Click **Save**.
-

Collecting Logs and Status

Logs and status contain information about agent activity. Collecting logs and status 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 **Collect Logs & Status**.

Safe Lock Intelligent Manager updates the date and time displayed in the **Last Status Collected On** and **Last Logs Collected On** columns after each Safe Lock agent successfully sends logs and status to Safe Lock Intelligent Manager.

Exporting Agent Data

Safe Lock Intelligent Manager allows you to save data about selected agents as a CSV file.

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 **Export**.
 4. Save the file.
-

Removing Agents

Remove agents from the list that Safe Lock Intelligent Manager no longer manages.

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 in the list that you want to remove.
3. Click **Remove**.
4. Confirm that you want to remove the selected agents.

Safe Lock Intelligent Manager removes the agents from the list.



Important

Agents removed from the list of monitored agents that you did not remove from the network will continue to report to the server. If a removed agent reports to the server, Safe Lock Intelligent Manager adds the agent back to the list of monitored agents.

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. Click the endpoint name to display agent status details.

The **Agent Status** screen appears.

3. Click the button to change the Application Lockdown status.
 - **Turn Application Lockdown On**
 - **Turn Application Lockdown Off**
-

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 3-8*
- *About the Server Events Screen on page 3-13*
- *Maintaining Logs on page 3-14*

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

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 Endpoints Triggering Blocked Events	Displays the endpoints that triggered the most blocked events.
Blocked Event History	Displays blocked events during the specified time period.
Top Blocked Files	Displays the files that are blocked the most.
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.

WIDGET	DESCRIPTION
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.

- Click **Add Widgets** to populate the tab with widgets.
-

Configuring Tab Settings

Procedure

- Go to **Dashboard** in the navigation at the top of the web console.
 - Click **Tab Settings**.
The **Tab Settings** screen appears.
 - In the **Title** field, type a meaningful title for the tab.
 - Select a layout for the tab.
 - Configure slide show and auto-fit settings.
-

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.
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.

WIDGET	CATEGORY	DESCRIPTION
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> Tip The layout for a tab determines where you can move a widget. As you drag, a red, dotted border appears when the widget is able to move to an area.</p>

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

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 > 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 > Agent Events** in the navigation at the top of the web console.
The **Agent Events** screen appears.
2. Click the drop-down list under **Agent Events**.
A list of criteria to search by appears.
3. Select the type of criteria to search by.
Appropriate search fields appear for the selected criteria.
4. Follow the appropriate steps depending on the selected criteria:

OPTION	DESCRIPTION
All Events	Displays all events logged by agents

OPTION	DESCRIPTION
Time Period	Do one of the following: <ul style="list-style-type: none"> • Select a listed time range. • Specify a custom time range. <ol style="list-style-type: none"> a. Go to Custom in the list. b. Specify your custom time range. c. Click Search.
Level	Select an event level.
Source	Select an event source.
Event	Select a specific event.
Endpoint	Type the beginning or all of an endpoint host name and click Search .
Tags	Type all or part of the tag and click Search .
IP Address	Type the IPv4 address and click Search .
IP Range	Type the IPv4 address range and click Search .
Blocked File Name	Type all or part of a file name and click Search .
Blocked File Hash	Type a file hash and click Search .
Marked	Select Open or Closed .
Integrity Monitoring	<ol style="list-style-type: none"> a. Select one of the following: <ul style="list-style-type: none"> • File or folder • Registry key or value b. Type the search criteria and click Search.

Your search results appear in the list of events.

Exporting Agent Events

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

Procedure

1. Go to **Logs > Agent Events** in the navigation at the top of the web console.
The **Agent Events** screen appears.
 2. Select the events in the list that you want to export information for.
 3. Click **Export**.
 4. 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 `tms11log.db` file by default.

Procedure

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

The **Server Events** screen appears.

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

A list of search criteria.

3. Select the type of search criteria.

Appropriate search fields appear for the selected criteria.

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

OPTION	DESCRIPTION
Time Period	Do one of the following: <ul style="list-style-type: none"> • Select a listed time range. • Specify a custom time range.

OPTION	DESCRIPTION
	<ol style="list-style-type: none">a. Go to Custom in the list.b. Specify your custom time range.c. Click Search.
User Name	Type the beginning or all of a Safe Lock Intelligent Manager account user name.
Event	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 > 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.
 3. Click **Export**.
 4. Save the file.
-

Maintaining Logs

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

Procedure

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

The **Log Maintenance** screen appears.

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

**Note**

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

4. Under **Purge server auditing log entries older than**, specify the maximum age of server event log entries that will be preserved.
5. 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 the folder if not already present**.
6. 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 3-14*.

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 4-8*
- *Configuring Proxy Settings on page 4-11*
- *About the License Management Screen on page 4-12*

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
Update	Manually update the components you select.
Schedule Updates	Configure the update schedule. Enable or disable scheduled updates for each component.
Download Agent Installer Package	Download an up-to-date agent installer package.

Manually Updating Components

Procedure

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

The **Component Updates** screen appears.

2. Click **Update**.
3. Select the components you want to update.
4. Click **Update**.

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

Scheduling Component Updates

Procedure

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

The **Component Updates** screen appears.

2. Click **Scheduled Updates**.
3. Enable the components you want to update on a schedule.
4. In the **Update Schedule** section, select the schedule you want to use.



Important

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

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.

- 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**

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

Configuring Notification Settings

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

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

Trend Micro Safe Lock Intelligent Manager Notification

Trend Micro Safe Lock has detected a warning event that requires immediate action:

Action

Action required. The following file was blocked on 2014-03-26 07:25:35. Visit <https://10.1.128.149:443/UI/EventDetail.html##%7B%22Loid%22%3A%220%7D> to take immediate action.

Event Information

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

Trend Micro Safe Lock Intelligent Manager Notification

More than 5 warning events received in 5 minutes at 2014-03-25 19:07:25. For more details, or to check the server console, visit <https://10.1.128.149:443/UI/EventManager.html>

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

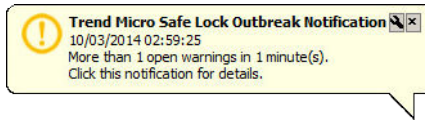
Procedure

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.
 - 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**.
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**.



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	Safe Lock: Outbreak notification
Action Required	Blocked file	Safe Lock: [Action required] File access blocked on <computer_name> (<file_name>)
Scan Result	Malware detection	Safe Lock: [Scan Result] Malware detected on <computer_name> (<file_name>)
Warning	Unauthorized change	Safe Lock: [Warning] Unauthorized change of File/Folder allowed on <computer_name>
Warning	Application Lockdown status change	Safe Lock: [Warning] Application Lockdown Turned Off on <computer_name>
Warning	Device access blocked	Safe Lock: [Warning] Device access blocked on <computer_name>

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 and permissions:

PRIVILEGES	PERMISSIONS
Administrator	<ul style="list-style-type: none"> • Add, edit, enable, disable, or delete Safe Lock Intelligent Manager web console accounts from the Account Management screen. • Modify their own account description, email address, and password • Specify actions to take on files blocked by agents • View the Safe Lock Intelligent Manager web console Logs > Server Events screen
Full Control	<ul style="list-style-type: none"> • Modify their own account description, email address, and password • Specify actions to take on files blocked by agents • View the Safe Lock Intelligent Manager web console Logs > Server Events screen
Read Only	<ul style="list-style-type: none"> • Modify their own account description, email address, and password



Note

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

Adding Accounts

Procedure

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

The **Account Management** screen appears.

3. Click **Add**.

The **Add User** screen appears.

4. Specify the privileges for the account.

See *About the Account Management Screen on page 4-8*.

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
Activation Code	Displays the Activation Code
License	Displays "Full" or "Trial"
Status	Displays "Activated", "Not Activated" or "Expired"
Expiration date	Displays the date when features and support end

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

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 5-5*
- *About the Approved List on page 5-8*
- *Account Types on page 5-15*
- *About Feature Settings on page 5-17*

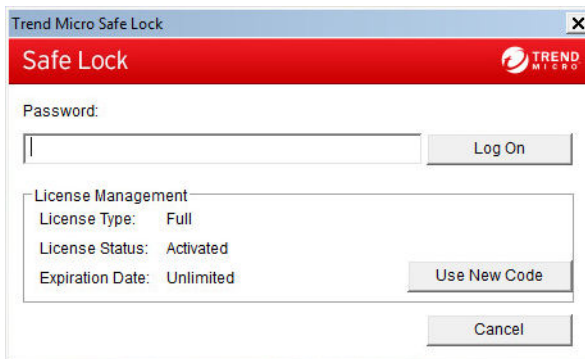
Setting Up the Approved List

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

Procedure

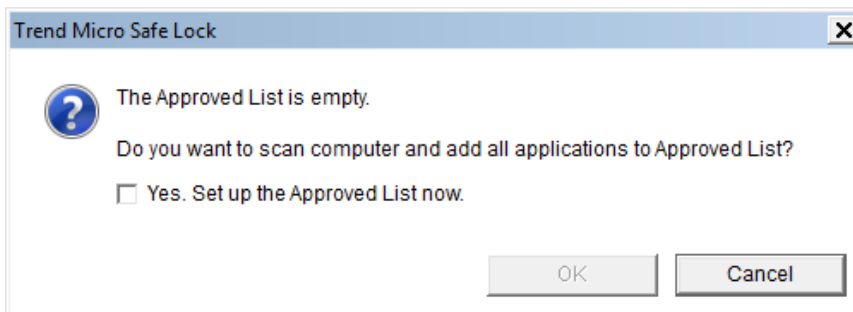
1. Open the Safe Lock console.

The Safe Lock log on screen appears.



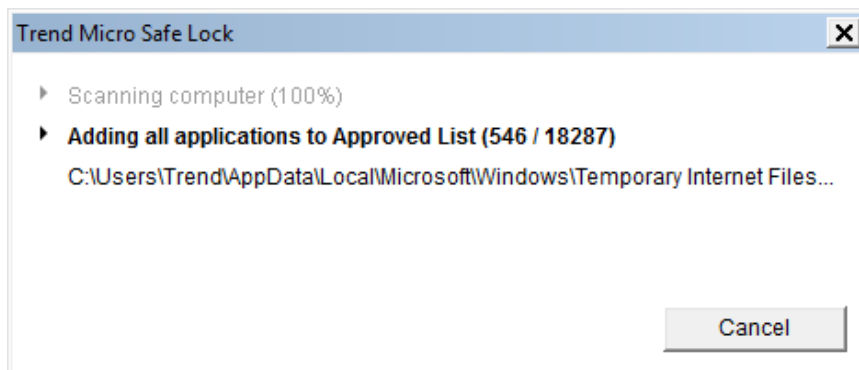
2. Provide the password and click **Login**.

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

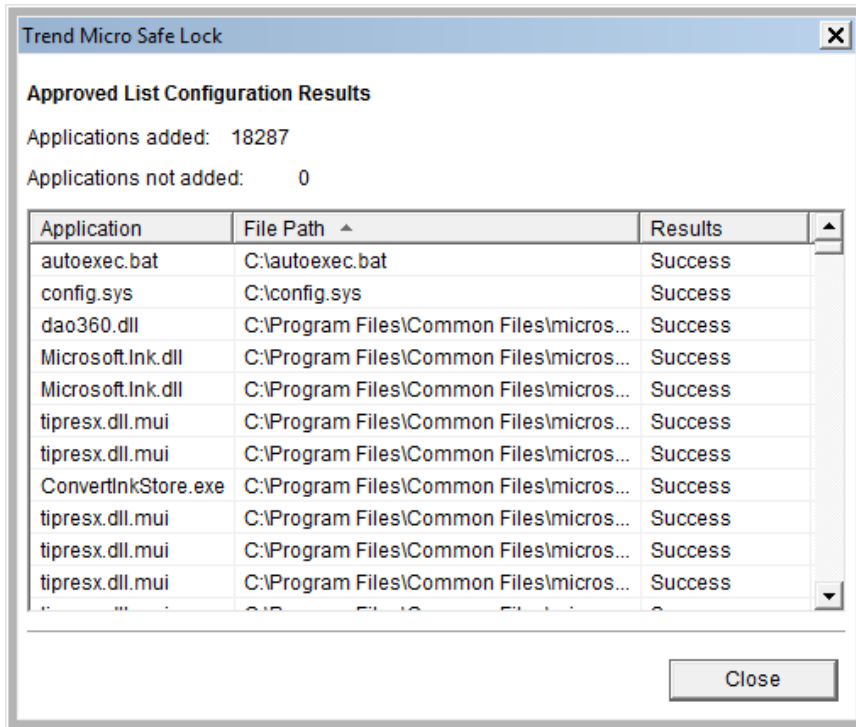


3. At the notification window, select **Yes. Set up the Approved List now** and click **OK**.

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



Safe Lock displays the Approved List Configuration Results.



Note

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

4. Click **Close**.

About the Agent Console

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

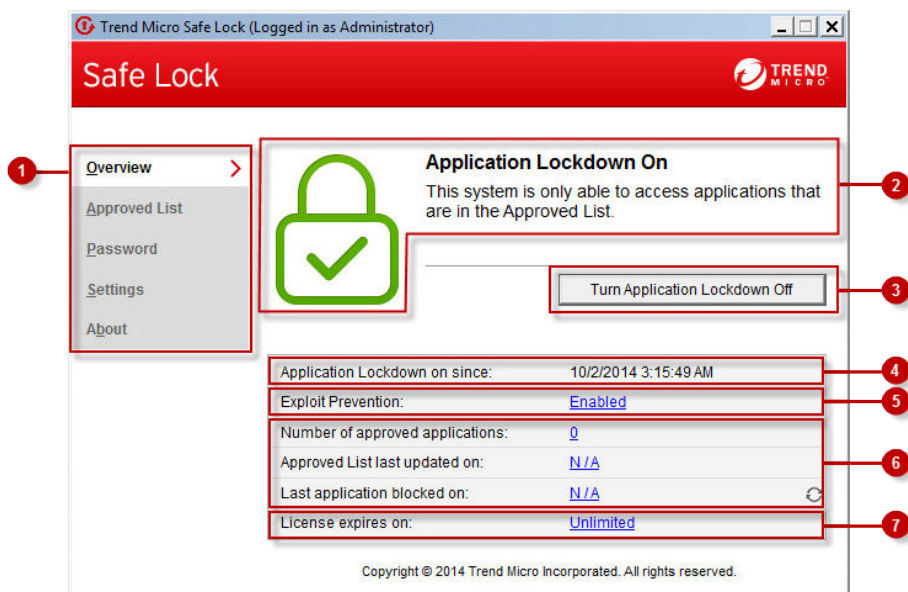



FIGURE 5-1. The Safe Lock console

The following table describes the features available on the console:

TABLE 5-1. Console Feature Descriptions

#	ITEM	DESCRIPTION
1	Overview	Display the software status
	Approved List	Display applications allowed to run and let users manage the list
	Password	Change the Safe Lock administrator or Restricted User passwords (only available to administrators)
	Settings	Enable or disable vulnerability protection settings and export or import the system configuration
	About	Display the product and component version numbers
2	Status information	The current status of the software
3	Turn Application Lockdown On	Lock down the system, blocking applications not on the Approved List from running
	Turn Application Lockdown Off	Release the system from lock down, allowing applications not on the Approved List to run <div style="border: 1px solid black; padding: 5px;">  Note After disabling Lockdown mode, Safe Lock Intelligent Manager switches to a “monitor” mode. Safe Lock Intelligent Manager does not block any applications from running, but logs when applications that are not in the Approved List run. You can use these logs to assess if the Approved List contains all the applications required on the endpoint. </div>
4	Application Lockdown on since	The date and time that Application Lockdown was last turned on
	Application Lockdown off since	The date and time that Application Lockdown was last turned off

#	ITEM	DESCRIPTION
5	Exploit Prevention	Enabled: All Exploit Prevention features are enabled Click the status to open the settings screen.
		Enabled (Partly): Some Exploit Prevention features are enabled Click the status to open the settings screen.
		Disabled: No Exploit Prevention features are enabled Click the status to open the settings screen.
6	Approved List status	Click the number of Approved List items or last updated date to open the Approved List. Click the last application blocked date to open the Blocked Application Event Log.
7	License expires on	The time and date that the software expires Click the date to provide a new Activation Code.

About Status Icons






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



Note

System Tray icons display if they were enabled during installation.

TABLE 5-2. Status Icon Descriptions

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

About the Approved List

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

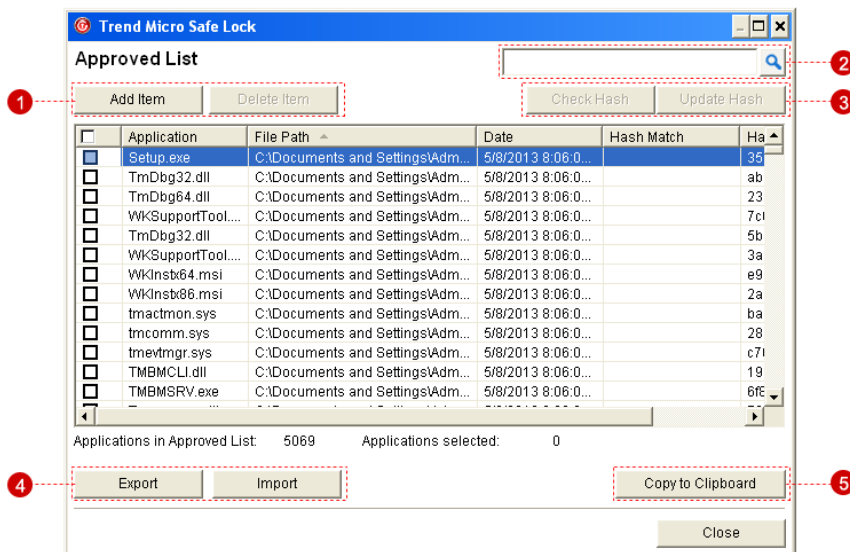


FIGURE 5-2. The Safe Lock Approved List

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

TABLE 5-3. Approved List Item Descriptions

#	ITEM	DESCRIPTION
1	Add Item/Delete Item	Adds or removes selected items to or from the Approved List.
2	Search bar	Searches the Application and File Path columns.
3	Check Hash/Update Hash	Checks or updates the hash values for applications in the Approved List.
4	Export/Import	Exports or imports the Approved List using a SQL database (.db) file.




#	ITEM	DESCRIPTION
5	Copy to Clipboard	Copies the Approved List to the clipboard in the comma separated values (CSV) format for easy review or reporting.

About Hashes

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

The following table describes the hash check status icons.

TABLE 5-4. Hash Check Status Icons

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

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

Checking or Updating Hashes

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

Procedure

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

To check the file hash values:

- a. Select the files to check. To check all files, select the check box at the top of the Approved List.
- b. Click **Check Hash**.

To update the file hash values:

- a. Select the files to update.
- b. Click **Update Hash**.



Important

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

Configuring the Approved List

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

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

OPTION	WHEN TO USE
Manually browse and select files	<p>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.</p> <p>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.</p>
Automatically add files created or modified by the selected application installer (Trusted Updater)	<p>Choose this option to open the Trusted Updater when updating the endpoint or installing new software.</p> <p>For example, if Mozilla Firefox needs to be installed or updated, use the Trusted Updater. Trend Micro Safe Lock Intelligent Manager adds or updates any files modified by an installer to the Approved List.</p>

Adding or Removing Files

Procedure

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

To add an item:

- a. Click **Add Item**, select **Manually browse and select files**, and click **Next**.
- b. In the window that opens, choose **Specific applications**, **All applications in folders and subfolders**, or **All applications in a folder** from the drop-down list.

A selection window appears.

- c. Select the desired application or folder to add, and click **Open** or **OK**.
- d. Click **OK**. Confirm the items to be added, and click **Approve**.

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

To remove an item:

- a. Search the Approved List for the application to remove.
- b. Select the check box next to the file name to be removed, and click **Delete Item**.
- c. When asked to remove the item, click **OK**.
- d. Click **OK** again to close the confirmation window.

Updating or Installing Using the Trusted Updater

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

Procedure

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



Note

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

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

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



FIGURE 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.

Procedure

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

To export the Approved List:

- a. Click **Export**, and choose where to save the file.
- b. Provide a filename, and click **Save**.

To import an Approved List:

- a. Click **Import**, and locate the database file.
 - b. Select the file, and click **Open**.
-

Account Types

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

TABLE 5-6. Safe Lock Accounts

ACCOUNT	DETAILS
Administrator	<ul style="list-style-type: none"> • Default account • Full access to Safe Lock functions • Can use both the console and command line interface (CLI)
Restricted User	<ul style="list-style-type: none"> • Secondary maintenance account • Limited access to Safe Lock functions • Can only use the console

To enable the Restricted User account, see *Configuring Passwords on page 5-16*. To sign in with a specific account, specify the password for that account.

Configuring Passwords

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



Important

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

Procedure

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

To change the Safe Lock administrator password:

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

**WARNING!**

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

To create a Restricted User password:

- a. Click **Restricted User** at the top of the console.
- b. Select the **Use Restricted User** check box.
- c. Specify and confirm the password, and click **Save**.

To change an existing Restricted User password:

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

About Feature Settings

Safe Lock offers the following protection features.

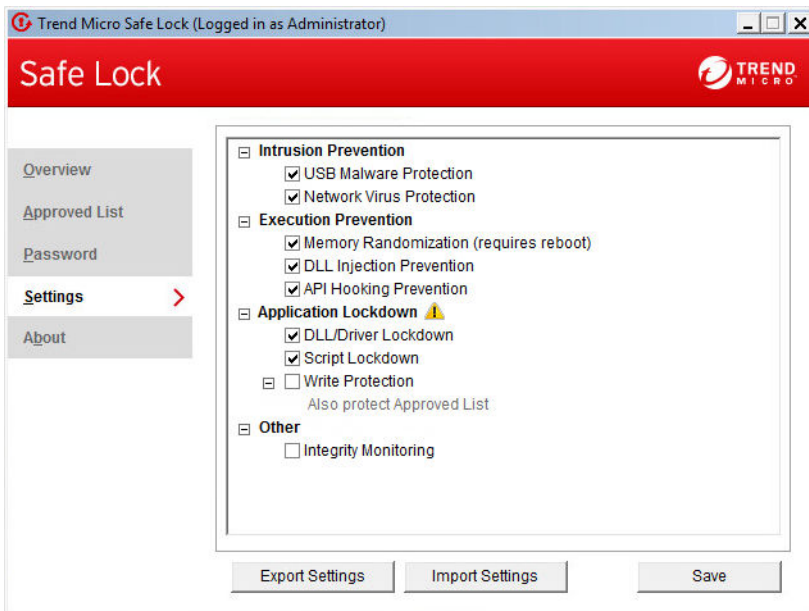


FIGURE 5-4. Safe Lock settings screen

TABLE 5-7. Intrusion Prevention

SETTING	DESCRIPTION
USB Malware Protection	<p>USB Malware Protection prevents threats on USB or remote drives from infecting the endpoint. Just viewing the contents of the drive may be enough to pass along an infection.</p> <p>Enable this feature to prevent files on USB devices from 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 5-8. 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> Note The endpoint must be restarted to enable or disable Memory Randomization.</p>
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>
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 5-9. Application Lockdown

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

SETTING	DESCRIPTION
Write Protection	Write Protection prevents write access to objects (files, folders, and registry entries) in the Write Protection List and optionally prevents write access to files in the Approved List.

TABLE 5-10. Other

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

Enabling or Disabling Feature Settings



Note

By default, Trend Micro Safe Lock enables all Exploit Prevention settings. If Network Virus Protection was not included in the initial installation, it cannot be selected. Reinstall Trend Micro Safe Lock if Network Virus Protection is not available.

Procedure

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

Chapter 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 at the command line.

Procedure

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

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

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

3. Type **SLCmd.exe**.
-

SLCmd Program and Console Function Comparison

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

TABLE 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

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

Not all settings are available through the command line interface (CLI) or console. See [Working with the Agent Configuration File on page 9-2](#) for information about modifying the system configuration.

SLC_{MD} Program Commands

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



Note

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

The following is a full list of commands available using the **SLC_{MD}** 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	VALUE	DESCRIPTION
help			Display a list of Safe Lock commands For example, type: <code>SILCmd.exe help</code>
activate		<activation_code>	Activate the Safe Lock program using the specified Activation Code For example, type: <code>SILCmd.exe activate XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX</code>

COMMAND	PARAMETER	VALUE	DESCRIPTION
set	adminpassword	<new_password>	Change the currently logged on administrator password to the newly specified password For example, type: <code>SLCmd.exe -p <admin_password> set adminpassword P@ssw0rd</code>
			Prompt the currently logged on administrator to specify a new password For example, type: <code>SLCmd.exe -p <admin_password> set adminpassword</code>
set	lock	enable	Turn on Application Lockdown For example, type: <code>SLCmd.exe -p <admin_password> set lock enable</code>
		disable	Turn off Application Lockdown For example, type: <code>SLCmd.exe -p <admin_password> set lock disable</code>
			Display the current Safe Lock Application Lockdown status For example, type: <code>SLCmd.exe -p <admin_password> set lock</code>
show	blockedlog		Display a list of applications blocked by Safe Lock For example, type:

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

COMMAND	PARAMETER	VALUE	DESCRIPTION
			<code>SLCmd.exe -p <admin_password> 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	VALUE	DESCRIPTION
decrypt	managedmodeconfiguration	<path_of_encrypted_file> <path_of_decrypted_output_file>	Decrypt the configuration file used by Managed Mode
encrypt	managedmodeconfiguration	<path_of_file> <path_of_encrypted	Encrypt the configuration file used by Managed Mode

COMMAND	PARAMETER	VALUE	DESCRIPTION
		_output_file>	
export	managedmodeconfiguration	<path_of_encrypted_output>	Export the encrypted configuration file used by Managed Mode
	servercertification	<path_of_certification_file>	Export the encrypted Safe Lock Intelligent Manager SSL communication certificate file
import	managedmodeconfiguration	<path_of_encrypted_input>	Import the encrypted configuration file used by Managed Mode
	servercertification	<path_of_certification_file>	Import the encrypted Safe Lock Intelligent Manager SSL communication certificate file
set	managedmode	enable [-cfg <path_of_encrypted_file>] [-sc <path_of_certification_file>]	Enable Managed Mode <hr/>  Note Using the optional <code>-cfg</code> value specifies the path of the configuration file. Using the optional <code>-sc</code> value specifies the path of the certificate file.
set	managedmode		Display the current Managed Mode status
show	managedmodeconfiguration		Display the configuration used by Managed Mode
test	managedmode		Connect a test Managed Mode session with Safe Lock Intelligent Manager

Optional Feature Commands

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

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

The following table lists the available abbreviated forms of parameters.

TABLE 6-6. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
usbmalwareprotection	usb	Manage USB Malware Protection
networkvirusprotection	net	Manage Network Virus Protection
memoryrandomization	mr	Manage Memory Randomization
dllinjectionprevention	dll	Manage DLL Injection Prevention
apihookingprevention	api	Manage API Hooking Prevention
dlldriverlockdown	dd	Manage DLL/Driver Lockdown
script	scr	Manage Script Lockdown
writeprotection	wp	Manage Write Protection
writeprotection-includes-approvedlist	wpal	Manage Write Protection includes Approved List
integritymonitoring	in	Manage Integrity Monitoring
customaction	ca	Manage actions taken when Safe Lock blocks specific types of events
exceptionpath	ep	Manage exceptions to Application Lockdown

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

TABLE 6-7. Optional Feature Commands


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

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

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

COMMAND	PARAMETER	VALUE	DESCRIPTION
			<code>SLCmd.exe -p <admin_password> set dllldrivlockdown</code>
set	script	enable	Enable Script Lockdown For example, type: <code>SLCmd.exe -p <admin_password> set script enable</code>
		disable	Disable Script Lockdown For example, type: <code>SLCmd.exe -p <admin_password> set script disable</code>
			Display the current status of Script Lockdown For example, type: <code>SLCmd.exe -p <admin_password> set script</code>
set	writeprotection	enable	Enable Write Protection For example, type: <code>SLCmd.exe -p <admin_password> set writeprotection enable</code>
		disable	Disable Write Protection For example, type: <code>SLCmd.exe -p <admin_password> set writeprotection disable</code>
			Display the current status of Write Protection For example, type: <code>SLCmd.exe -p <admin_password> set writeprotection</code>

COMMAND	PARAMETER	VALUE	DESCRIPTION
set	writeprotection- includes- approvedlist	enable	Enable protection of the Approved List (in addition to the Write Protection List) when Write Protection is enabled For example, type: <code>SLCmd.exe -p <admin_password> set writeprotection- includes- approvedlist enable</code>
		disable	Disable protection of the Approved List (in addition to the Write Protection List) when Write Protection is enabled For example, type: <code>SLCmd.exe -p <admin_password> set writeprotection- includes- approvedlist disable</code>
			Display the current status of Write Protection includes Approved List For example, type: <code>SLCmd.exe -p <admin_password> set writeprotection- includes- approvedlist</code>
set	integritymonitoring	enable	Enable Integrity Monitoring For example, type: <code>SLCmd.exe -p <admin_password> set integritymonitoring enable</code>
		disable	Disable Integrity Monitoring For example, type: <code>SLCmd.exe -p <admin_password> set integritymonitoring disable</code>

COMMAND	PARAMETER	VALUE	DESCRIPTION
			<p>Display the current status of Integrity Monitoring</p> <p>For example, type:</p> <pre>SLCmd.exe -p <admin_password> set integritymonitoring</pre>
set	customaction	ignore	<p>Ignore blocked files or processes when Application Lockdown blocks any of the following events:</p> <ul style="list-style-type: none"> • Process launch • DLL loading • Script file access
		quarantine	<p>Quarantine blocked files or processes when Application Lockdown blocks any of the following events:</p> <ul style="list-style-type: none"> • Process launch • DLL loading • Script file access <hr/> <p> Note Safe Lock does not support a custom action of "quarantine" on Windows XP or Windows 2003.</p> <hr/>
		ask	<p>Ask what to do for blocked files or processes when Application Lockdown blocks any of the following events:</p> <ul style="list-style-type: none"> • Process launch • DLL loading

COMMAND	PARAMETER	VALUE	DESCRIPTION
			<ul style="list-style-type: none"> Script file access
			Display the current setting for actions taken when Safe Lock blocks specific types of events
set	exceptionpath	enable	Enable exceptions to Application Lockdown
		disable	Disable exceptions to Application Lockdown
			Display current setting for using exceptions to Application Lockdown

Restricted User Account Commands

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

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

The following table lists the available abbreviated forms of parameters.

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

COMMAND	PARAMETER	VALUE	DESCRIPTION
			<p>SLCmd.exe -p <admin_password> set user enable</p>
		disable	<p>Disable the Restricted User account</p> <p>For example, type:</p> <p>SLCmd.exe -p <admin_password> set user disable</p>
			<p>Display the the Restricted User account status</p> <p>For example, type:</p> <p>SLCmd.exe -p <admin_password> set user</p>
set	userpassword	<new_password>	<p>Change the Restricted User account password to the newly specified password</p> <p>For example, type:</p> <p>SLCmd.exe -p <admin_password> set userpassword P@ssW0Rd</p>
			<p>Prompt the currently logged on administrator to specify a new Restricted User account password</p> <p>For example, type:</p> <p>SLCmd.exe -p <admin_password> set userpassword</p>

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

COMMAND	PARAMETER	VALUE	DESCRIPTION
			 Note If you do not specify any interpreter, the command removes all interpreters related to the script extension. If you specify interpreters, the command only removes the interpreters specified from the script extension rule.
<code>show</code>	<code>script</code>		Display all script rules For example, type: <pre>SLCmd.exe -p <admin_password> show script</pre>

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
<code>approvedlist</code>	<code>al</code>	Manage files in the Approved List
<code>list</code>	<code>li</code>	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	VALUE	DESCRIPTION
add	approvedlist	[-r] <file_or_folder_path>	<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 <admin_password> add approvedlist -r "C:\Program Files\Microsoft Office"</pre> <hr/> <p> Note Using the optional <code>-r</code> value includes the specified folder and related subfolders.</p>
remove	approvedlist	<file_path> >	<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 <admin_password> remove approvedlist C:\Windows\notepad.exe</pre>
show	approvedlist		<p>Display the files in the Approved List</p> <p>For example, type:</p> <pre>SLCmd.exe -p <admin_password> show approvedlist</pre>
check	approvedlist	-f	<p>Update the hash values in the Approved List and displays detailed results</p> <p>For example, type:</p>

COMMAND	PARAMETER	VALUE	DESCRIPTION
			<p><code>SLCmd.exe -p <admin_password> check approvedlist -f</code></p>
		-q	<p>Update the hash values in the Approved List and displays summarized results</p> <p>For example, type:</p> <pre>SLCmd.exe -p <admin_password> 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 <admin_password> check approvedlist -v</pre>
export	list	<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 <admin_password> export list c:\approvedlist \ap.db</pre> <hr/> <p> Note The output file type must be DB format.</p>
import	list	[-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 <admin_password> import list c:\approvedlist \ap.db</pre>

COMMAND	PARAMETER	VALUE	DESCRIPTION
			 Note 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:

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

The following table lists the available abbreviated forms of parameters.



TABLE 6-14. Abbreviations and Uses


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

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

TABLE 6-15. Application Lockdown Commands

COMMAND	PARAMETER	VALUE	DESCRIPTION
show	quarantinedfile		Display a list of quarantined files
restore	quarantinedfile	<id> [-a1] [-f]	Restore the specified file from quarantine Using the optional <code>-a1</code> value also adds the restored file to Approved List.

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

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

Write Protection Commands

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

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

The following table lists the available abbreviated forms of parameters.

TABLE 6-16. Abbreviations and Uses


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



PARAMETER	ABBREVIATION	USE
writeprotection-folder-exception	wpfoe	Manage folders in the Write Protection Exception List
writeprotection-regvalue-exception	wprve	Manage registry values and associated registry keys in the Write Protection Exception List
writeprotection-regkey-exception	wprke	Manage registry keys in the Write Protection Exception List



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


TABLE 6-17. Write Protection List “File” Commands



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



COMMAND	PARAMETER	VALUE	DESCRIPTION
	writeprotection- folder-exception		<p>Display the folders in the Write Protection Exception List</p> <p>For example, type:</p> <pre>SLCmd.exe -p <admin_password> 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 <admin_password> add writeprotection-file archive.txt</pre> <hr/> <p> Note</p> <p>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>.</p> <hr/>
	writeprotection- file-exception	-t <file_path > -p <process_ path>	<p>Add the specified file and a specific process path for that file to the Write Protection Exception List</p> <p>For example, to add write access by a process named <code>notepad.exe</code> to a file named <code>userfile.txt</code>, type:</p> <pre>SLCmd.exe -p <admin_password> add writeprotection-file- exception -t userfile.txt -p notepad.exe</pre>



COMMAND	PARAMETER	VALUE	DESCRIPTION
			<p> Note</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</code> <code><file_path></code> <code>></code></p> <p>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>SLCmd.exe -p <admin_password> add writeprotection-file-exception -t userfile.txt</pre> <hr/> <p> Note</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><process_path></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 <admin_password> add writeprotection-file-exception -p notepad.exe</pre>



COMMAND	PARAMETER	VALUE	DESCRIPTION
			 Note 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>writeprotection-folder</code>	<code>[-r] <folder_path></code>	Add the specified folder(s) to the Write Protection List For example, type: <pre>SLCmd.exe -p <admin_password> add writeprotection-folder -r userfolder</pre> <hr/>  Note Using the optional <code>-r</code> value includes the specified folder and related subfolders. The <code><folder_path></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 <folder_path> -p <process_path></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

COMMAND	PARAMETER	VALUE	DESCRIPTION
			<p>folder and related subfolders at <code>c:\Windows\System32\Temp</code>, type:</p> <pre>SLCmd.exe -p <admin_password> add writeprotection-folder-exception -r -t c:\Windows\System32\Temp -p notepad.exe</pre> <hr/> <p> Note</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 <folder_path></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 <admin_password> add writeprotection-folder-exception -r -t userfolder</pre>

COMMAND	PARAMETER	VALUE	DESCRIPTION
			<p> Note</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> <process_path></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 <admin_password> add writeprotection-folder-exception -p c:\Windows\notepad.exe</pre> <hr/> <p> Note</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>
remove	writeprotection-file	<file_path>	<p>Remove the specified file from the Write Protection List</p> <p>For example, type:</p>

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

COMMAND	PARAMETER	VALUE	DESCRIPTION
			 Note 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> .
		<code>-p</code> <code><process_path></code>	Remove the specified process path from the Write Protection Exception List For example, type: <pre>SLCmd.exe -p <admin_password> remove writeprotection-file-exception -p notepad.exe</pre> <hr/>  Note 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>writeprotection-folder</code>	<code>[-r]</code> <code><folder_path></code>	Remove the specified folder(s) from the Write Protection List For example, type: <pre>SLCmd.exe -p <admin_password> remove writeprotection-folder -r c:\Windows</pre>

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











COMMAND	PARAMETER	VALUE	DESCRIPTION
			<p> Note</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> <process_path></p> <p>Remove the specified process path from the Write Protection Exception List</p> <p>For example, type:</p> <pre>SLCmd.exe -p <admin_password> remove writeprotection-folder-exception -p c:\Windows\System32</pre> <hr/> <p> Note</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>



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




COMMAND	PARAMETER	VALUE	DESCRIPTION
show	writeprotection		Display the entire Write Protection List
	writeprotection-regvalue		Display the registry values in the Write Protection List
	writeprotection-regvalue-exception		Display the registry values in the Write Protection Exception List
	writeprotection-regkey		Display the registry keys in the Write Protection List
	writeprotection-regkey-exception		Display the registry keys in the Write Protection Exception List
add	writeprotection-regvalue	<path_of_registry_key> <registry_value>	Add the specified registry value and its related registry key to the Write Protection List For example, to add the registry value of “testvalue” in the “HKEY\test” registry key to the Write Protection List, type: SLCmd.exe -p <admin_password> add writeprotection-regvalue HKEY\test testvalue
	writeprotection-regvalue-exception	-t <path_of_registry_key> <registry_value> -p <process_path>	Add the specified registry value and its related registry key and a specific process path for that value to the Write Protection Exception List


COMMAND	PARAMETER	VALUE	DESCRIPTION
			 Note This command allows write access by the specified process to the specified registry values. The <code>-p</code> value pattern matches from the end of the path toward the beginning of the path.
		<code>-t</code> <code><path_of_registry_key></code> <code><registry_value></code>	Add the specified registry value and its related registry key to the Write Protection Exception List  Note This command allows write access by any process to the specified registry value.
		<code>-p</code> <code><process_path></code>	Add the specified process to the Write Protection Exception List  Note This command allows write access by the specified process to any registry values. The <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]</code> <code><path_of_registry_key></code>	Add the specified registry key to the Write Protection List

COMMAND	PARAMETER	VALUE	DESCRIPTION
			 Note Using the optional <code>-r</code> value includes the specified registry key and related subkeys.
	writeprotection-regkey-exception	<code>[-r] -t <path_of_registry_key> -p <process_path></code>	Add the specified registry key and processes run from the specified path to the Write Protection Exception List  Note This command allows write access by the specified process to the specified registry keys. Using the optional <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 <path_of_registry_key></code>	Add the specified registry key to the Write Protection Exception List  Note This command allows write access by any process to the specified registry keys. Using the optional <code>-r</code> value includes the specified registry key and related subkeys.

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

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

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

COMMAND	PARAMETER	VALUE	DESCRIPTION
		-p <process_path>	Remove the specified process path from the Write Protection Exception List <div style="border: 1px solid black; padding: 5px;">  Note The -p value pattern matches from the end of the path toward the beginning of the path. </div>

Trusted Certification Commands

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

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

The following table lists the available abbreviated forms of parameters.

TABLE 6-19. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
trustedcertification	tc	Manage Trusted Certifications

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

TABLE 6-20. Trusted Certificate Commands

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

COMMAND	PARAMETER	VALUE	DESCRIPTION
show	trustedcertificatio n	[-v]	Display the certificate files in the Trusted Certifications List Using the optional -v value displays detailed information.
add	trustedcertificatio n	-c <file_path > [-l <label>] [- u]	Add the specified certificate file to the Trusted Certifications List Using the optional -l value specifies the unique label for this certificate file. Using the optional -u value treats the file signed by this certificate file as a Trusted Updater.
remove	trustedcertificatio n	-l <label>	Remove a certificate file from the Trusted Certifications List by specifying its label

Trusted Updater Commands

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

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



The following table lists the available abbreviated forms of parameters.

TABLE 6-21. Abbreviations and Uses

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

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

TABLE 6-22. Trusted Updater Commands

COMMAND	PARAMETER	VALUE	DESCRIPTION
start	<code>trustedupdater</code>	<code>[-r]</code> <code><path_of_installer></code>	<p>Start the Trusted Updater and add the installation packages (<code>EXE</code> and <code>MSI</code> file types) in the specified folder to the Approved List</p> <hr/> <p> Note 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 subfolders, type:</p> <pre>SLCmd.exe -p <admin_password> start trustedupdater -r C:\Installers</pre>
stop	<code>trustedupdater</code>	<code>[-f]</code>	<p>Stop the Trusted Updater function</p> <hr/> <p> Note 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	VALUE	DESCRIPTION
			<code>SLCmd.exe -p <admin_password> 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 6-47*.

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

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

The following table lists the available abbreviated forms of parameters.


TABLE 6-23. Abbreviations and Uses

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

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

TABLE 6-24. Predefined Trusted Updater Commands

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

COMMAND	PARAMETER	VALUE	DESCRIPTION
			<p> Important</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 this list. For details on adding files to the Predefined Trusted Updater List (not the Predefined Trusted Updater Exception List), see Predefined Trusted Updater "Add" Command on page 6-47.</p> <hr/> <p>For example, to add <code>notepad.exe</code> to the Predefined Trusted Updater Exception List, type:</p> <pre>SICmd.exe -p <admin_password> add predefinedtrustedupdater - e C:\Windows\notepad.exe</pre>
<code>decrypt</code>	<code>predefinedtrustedupdater</code>	<code><path_of_encrypted_file></code> <code><path_of_decrypted_output_file></code>	<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>SICmd.exe -p <admin_password> decrypt predefinedtrustedupdater C: \notepad.xen C:\Editors \notepad.exe</pre>
<code>encrypt</code>	<code>predefinedtrustedupdater</code>	<code><path_of_file></code> <code><path_of_encrypted file></code>	<p>Encrypt a file to the specified location</p> <p>For example, to encrypt <code>C:\notepad.exe</code> to <code>C:\Editors\notepad.xen</code>, type:</p>

COMMAND	PARAMETER	VALUE	DESCRIPTION
		<code>_output_file></code>	<pre>SLCmd.exe -p <admin_password> encrypt predefinedtrustedupdater C: \Editors\notepad.exe C: \Notepad.xen</pre>
export	<code>predefinedtrustedupdater</code>	<code><path_of_encrypted_output></code>	<p>Export the Predefined Trusted Updater List to the specified encrypted file</p> <p>For example, type:</p> <pre>SLCmd.exe -p <admin_password> export predefinedtrustedupdater C: \Lists\ptu_list.xen</pre>
import	<code>predefinedtrustedupdater</code>	<code><path_of_encrypted_input></code>	<p>Import a Predefined Trusted Updater List from the specified encrypted file</p> <p>For example, type:</p> <pre>SLCmd.exe -p <admin_password> import predefinedtrustedupdater C: \Lists\ptu_list.xen</pre>
remove	<code>predefinedtrustedupdater</code>	<code>-l <label_name></code>	<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 <admin_password> remove predefinedtrustedupdater -l Notepad</pre>
		<code>-e <folder_or_file_exception></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>

COMMAND	PARAMETER	VALUE	DESCRIPTION
			<code>SLCmd.exe -p <admin_password> remove predefinedtrustedupdater -e C:\Windows\notepad.exe</code>
set	predefinedtrustedupdater	enable	Enable the Predefined Trusted Updater List
		disable	Disable the Predefined Trusted Updater List
show	predefinedtrustedupdater		Display the files in the Predefined Trusted Updater List For example, type: <code>SLCmd.exe -p <admin_password> show predefinedtrustedupdater</code>
		-e	Display the files in the Predefined Trusted Updater Exception List For example, type: <code>SLCmd.exe -p <admin_password> 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 6-25. Predefined Trusted Updater “Add” Command

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

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

TABLE 6-26. Predefined Trusted Updater “Add” Additional Values

VALUE	REQUIRED / OPTIONAL	DESCRIPTION	EXAMPLE		
-u <folder_or_file>	Required	Add the specified file or folder to the Predefined Trusted Updater List	<p>N/A</p> <hr/> <p> Note This parameter requires the use of the -t <type_of_object> value.</p>		
-t <type_of_object>	Required	<p>Specify the type of object to add to the Predefined Trusted Updater List located in -u <folder_or_file></p> <p>Available objects types are as follows:</p> <table border="1"> <tr> <td>process</td> <td>Indicates only EXE file types</td> </tr> </table>	process	Indicates only EXE file types	<pre>SLCmd.exe -p <admin_password> add predefinedtrustedupdater -u C:\Windows\notepad.exe -t process</pre>
process	Indicates only EXE file types				

VALUE	REQUIRE D / OPTI ONAL	DESCRIPTION		EXAMPLE
		file	Indicates only <code>MSI</code> and <code>BAT</code> file types	
		folder	Indicates all <code>EXE</code> , <code>MSI</code> , and <code>BAT</code> files in the specified folder	
		folderands ub	Indicates all <code>EXE</code> , <code>MSI</code> , and <code>BAT</code> files in the specified folder and related subfolders	
<code>-p</code> <parent_pr ocess>	Opti onal	Add the full file path to the specified parent process used to invoke the file(s) specified in <code>-u</code> <folder_or_file>		<code>SLCmd.exe -p</code> <admin_password> add predefinedtrustedupdater -u C:\Windows\notepad.exe -t process -p C:\batch files\note.bat
<code>-l</code> <label_name>	Opti onal	Specify a label name for the file(s) specified in <code>-u</code> <folder_or_file>		<code>SLCmd.exe -p</code> <admin_password> add predefinedtrustedupdater -u C:\Windows\notepad.exe -t process -l EDITOR
		 Note When left blank, Safe Lock assigns an arbitrary label name.		
<code>-al</code> enable	Opti onal	Compare the hash values in the Approved List with the hash values calculated from the actual files		<code>SLCmd.exe -p</code> <admin_password> add predefinedtrustedupdater -u C:\Windows\notepad.exe -t process -al enable
		 Note Enabled by default even when <code>-al</code> is not specified.		

VALUE	REQUIRED / OPTIONAL	DESCRIPTION	EXAMPLE
-al disable	Optional	Do not compare the hash values in the Approved List with the hash values calculated from the actual files	<code>SLCmd.exe -p <admin_password> add predefinedtrustedupda ter -u C:\Windows \notepad.exe -t process -al disable</code>

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 6-27. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
configuration	con	Manage the configuration file

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

TABLE 6-28. Configuration File Commands

COMMAND	PARAMETER	VALUE	DESCRIPTION
decrypt	configuration	<path_of_encrypted_file> <path_of_decrypted_output_file>	Decrypts a configuration file to the specified location For example, to decrypt C:\config.xen to C:\config.xml, type:

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

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 7-14*

The Remote Setup Tool (SLrst)

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

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

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

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

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

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

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



Important

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




Tip

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

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

TABLE 7-1. SLrst Remote Agent Setup Parameters

PARAMETER	FUNCTION
--install	Deploys and installs the Safe Lock agent on the endpoint See Remote Installation Considerations on page 7-3 .
--patch	Patches the Safe Lock agent
--reboot	Restarts the endpoint (required if you want to reinstall the Safe Lock agent) Restarting Agents Remotely on page 7-13
	<hr/>  Note 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. <hr/>
--uninstall	Uninstalls the Safe Lock agent from the endpoint Uninstalling Agents Remotely on page 7-12

Remote Installation Considerations

Before you remotely install Safe Lock Intelligent Manager 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 1-14](#).

- 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 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 7-6](#).

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 7-5.

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
10.1.199.199 10.1.199.201 192.168.1.20

NOT VALID
10.1.199.199,10.1.199.201
"10.1.199.199" "10.1.199.201" "192.168.1.20"



Tip

The targets file can be reused. Therefore, you can use the same targets file to deploy, patch, and uninstall a batch of target endpoints. Check the log information and make backups of any critical information each time you run the **SLrst** program. **SLrst** ignores and overwrites any log information in the file each time it is run.

Endpoint Info File Specifications

The “endpoint info” file used during remote agent installation contains the IP address, user name, and password of a local account on each target endpoint with access to the default share `admin$`.



Tip

Trend Micro recommends using the local administrator account on each target endpoint for deployment.

The endpoint info file uses CSV format. The filename must be `endpoint_info.csv`.

**Note**

To create the “endpoint info” CSV file, divide the records into fields for IP address, user name, and password. Use one line per record. Separate these fields using a comma. Use of spaces, quotation marks, or other delimiters is not supported.

For example:

VALID
10.1.199.199,Administrator,password1
10.1.199.200,Administrator,password2
10.1.199.201,Administrator,password3
192.168.1.20,Daniel,his_pwd
192.168.1.21,Sophia,her_pwd

NOT VALID
10.1.199.201,Administrator,password3,192.168.1.20,Daniel,his_pwd
"10.1.199.199", "Administrator", "password1"
"10.1.199.200" "Administrator", "password2"
"10.1.199.201", "Administrator", "password3"
"192.168.1.20", "Daniel", "his_pwd"
"192.168.1.21", "Sophia", "her_pwd"

Microsoft Excel will save a chart as a CSV using valid formatting.

Downloading an Up-to-Date Agent Installer Package

Procedure

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

The **Component Updates** screen appears.

2. Click **Download Agent Installer Package**.
3. Select the language the installation package.

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

**Note**

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

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

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

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

**Important**

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 7-4](#).

- 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.
-

Applying Patches and Hot Fixes 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 7-4*.

Use the **SLrst.exe** program at the command line interface (CLI) to apply patches or hot fixes to one or more Safe Lock agents connected to the network.

Procedure

1. Download an agent patch or hot fix using the Trend Micro Technical Support Download Center website:

<http://downloadcenter.trendmicro.com/>

2. Copy the downloaded agent patch or hot fix 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 hot fix 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

3. 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\"
```

4. To remotely patch or hot fix 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 hot fix agents in batches. Run the remote setup tool separately for each CSV batch file.

5. At the prompt, provide the password used to access the Safe Lock agent program.
6. Monitor the progress of the remote patch or hot fix. 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 7-4](#).

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 7-4](#).

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\nRemoteAgentSetupTool\"
```

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, and query the status of agents using a command line interface (CLI).

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).

Sending Remote Tasks

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 to the Safe Lock Intelligent Manager server by typing the following command:

```
SLtasks.exe --logon
```

4. Type your Safe Lock Intelligent Manager credentials.

The CLI confirms a successful log on to the server.

5. Query agent statuses by typing the following command:


```
SItasks.exe --query
```

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. Perform the necessary tasks using the following syntax:

```
SItasks.exe <task_parameter>
```

TABLE 7-2. SItasks Task Parameters

PARAMETER	TASK
--init	Initialize the Approved List
--lockdown	Turn Application Lockdown on
--match	Match agent licenses with 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.



Tip

To send tasks to a specific agent, append `--targetPC` to the command and type the computer name.

For example:

```
SItasks.exe <task_parameter> --targetPC <computer_name>
```

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.

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
-

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\"
```

- Log on the Safe Lock Intelligent Manager server by typing the following command:

```
SLtasks.exe --logon
```

- Type your Safe Lock Intelligent Manager credentials.

The CLI confirms a successful log on to the server.

- Query message time groups by typing the following command:

```
SLtasks.exe --querygroup
```


The results of the query are saved in `group_info.csv`.



Important

Applying message time groups requires querying message time groups, editing the results as needed, and then applying the configured message time groups to agents. A warning message appears if the query results are out-of-date when attempting to apply message time groups to agents.

- Edit the `group_info.csv` to configure the following message time group controls:

COLUMN NAME	CONTROL DESCRIPTION
TotalGroupNum	Divide agents into any number of groups  Tip Set this value to 1 to turn the feature off
OwnGroupIndex	Set which group an agent belongs to
TimePeriod	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:

SItasks.exe --applygroups



Important

- The logged on account must have “admin” or “Full Control” privilege to apply message time groups to agents.
 - Only agents listed in `group_info.csv` receive the command.
-

8. Log off the Safe Lock Intelligent Manager server by typing the following command:

SItasks.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 8-2*
- *Setting Up the Approved List on page 5-2*
- *Installation Using the Command Line on page 8-11*

Local Installation Overview

Trend Micro Safe Lock can be installed using either the Windows Installer or the command line interface (CLI) installer.



WARNING!

Depending on the installation method you select, Safe Lock versions require different preparation before upgrading. See [Agent Upgrade Preparation on page 1-14](#) for more information.

TABLE 8-1. Safe Lock Local Installation Methods

INSTALLATION METHOD	BENEFITS
Windows Installer	The Windows Installer provides simplified step-by-step installation wizard for first-time or single installation. Also suitable for preparing for mass deployment for cloned computer systems.
Command line interface installer	The command line interface (CLI) installer provides silent installation and can be integrated into a batch file for mass deployment.

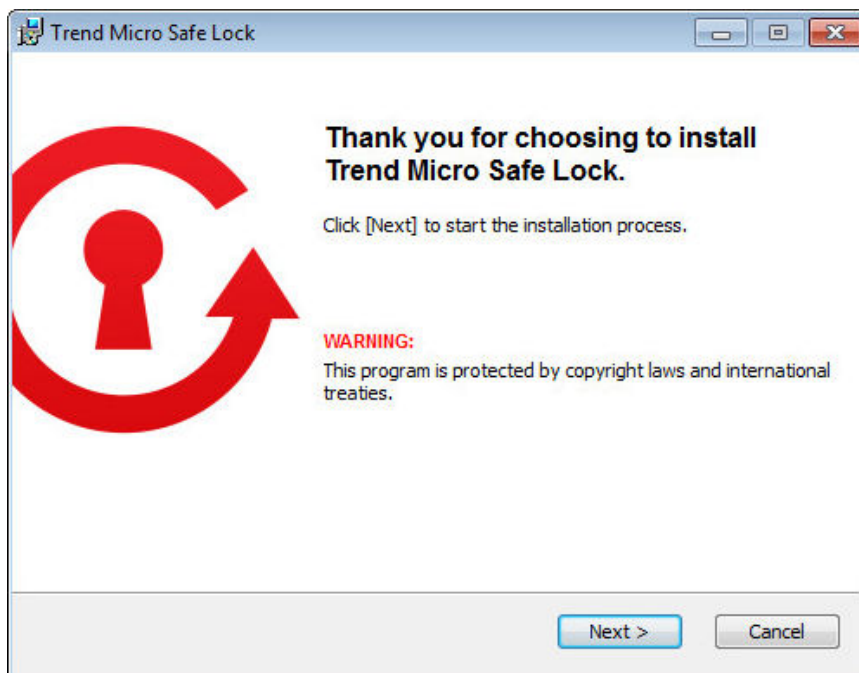
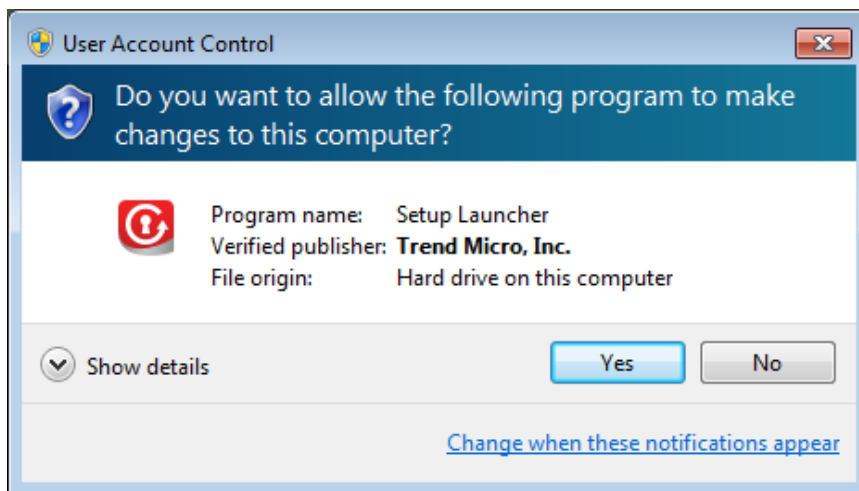
Installing from Windows

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

Procedure

1. Double-click `Setup.exe`.

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

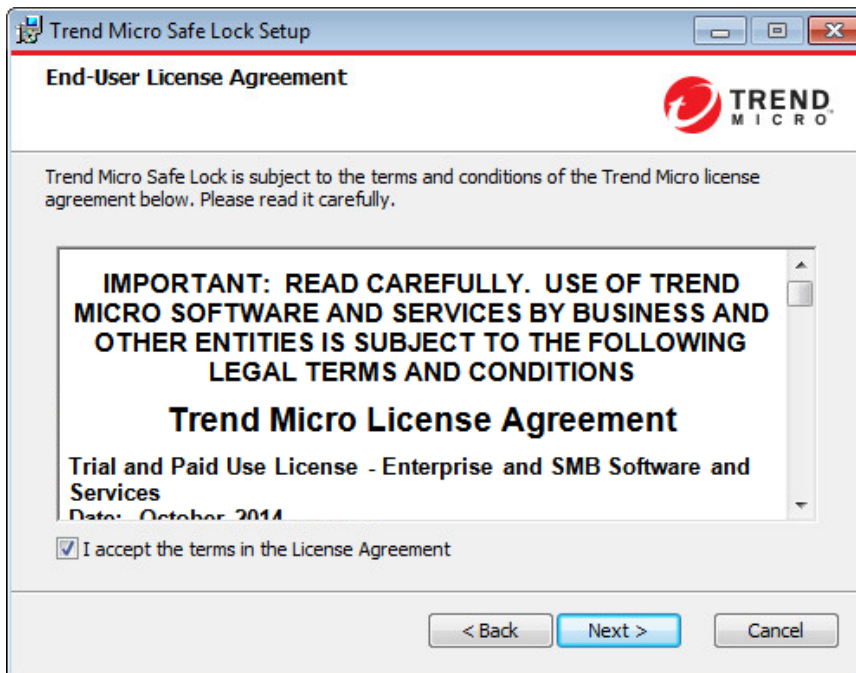


2. When the installation wizard opens, click **Next**.



If there is another version of Safe Lock on the endpoint, the installer will remove it before installing the latest version.

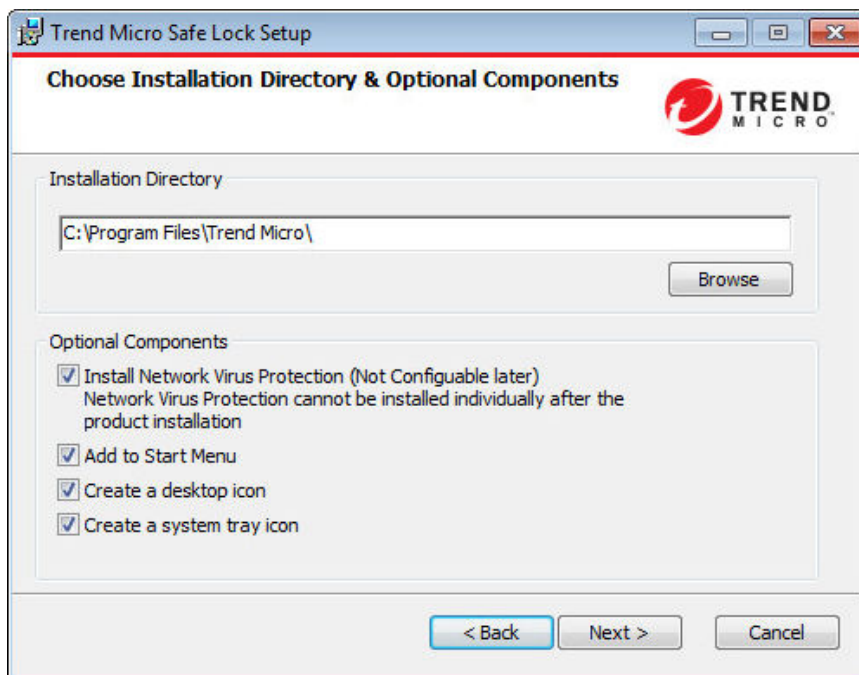
3. Read the license agreement, select **I accept the terms in the License Agreement**, and click **Next**.



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



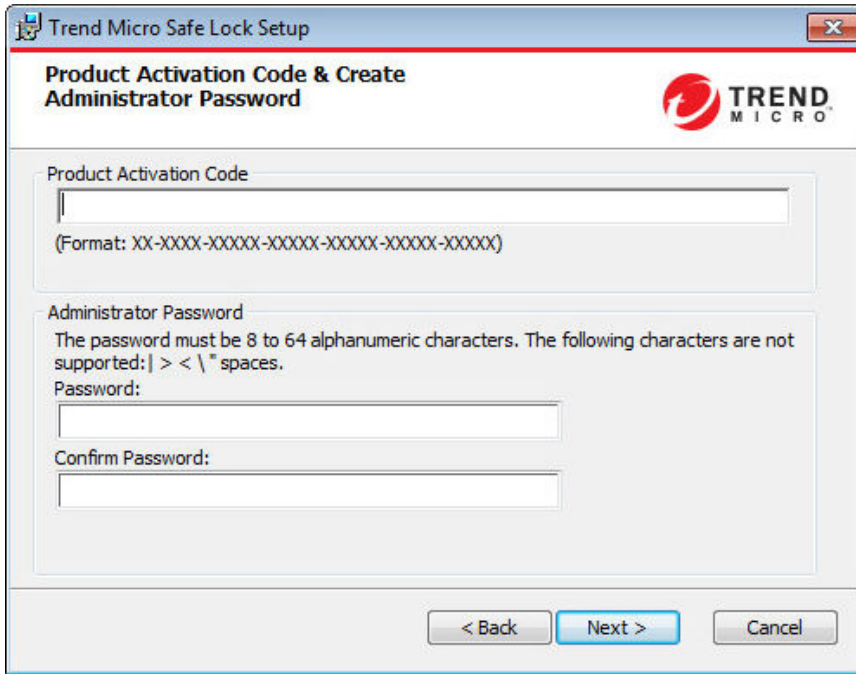
Network Virus Protection can only be installed during the initial program installation and can be disabled after installation if necessary. See *Exploit Prevention Settings* in the Administrator's Guide for more information.



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.



The screenshot shows a Windows-style dialog box titled "Trend Micro Safe Lock Setup". The main heading is "Product Activation Code & Create Administrator Password". In the top right corner, there is the Trend Micro logo. The dialog is divided into two main sections. The first section, "Product Activation Code", contains a text input field and a note: "(Format: XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX)". The second section, "Administrator Password", includes a warning: "The password must be 8 to 64 alphanumeric characters. The following characters are not supported: | > < \ " spaces." Below this are two text input fields labeled "Password:" and "Confirm Password:". At the bottom of the dialog, there are three buttons: "< Back", "Next >" (highlighted in blue), and "Cancel".

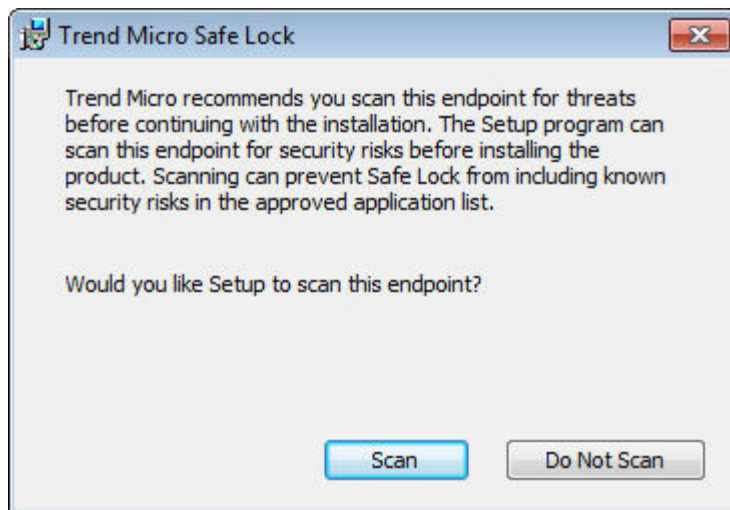


WARNING!

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.



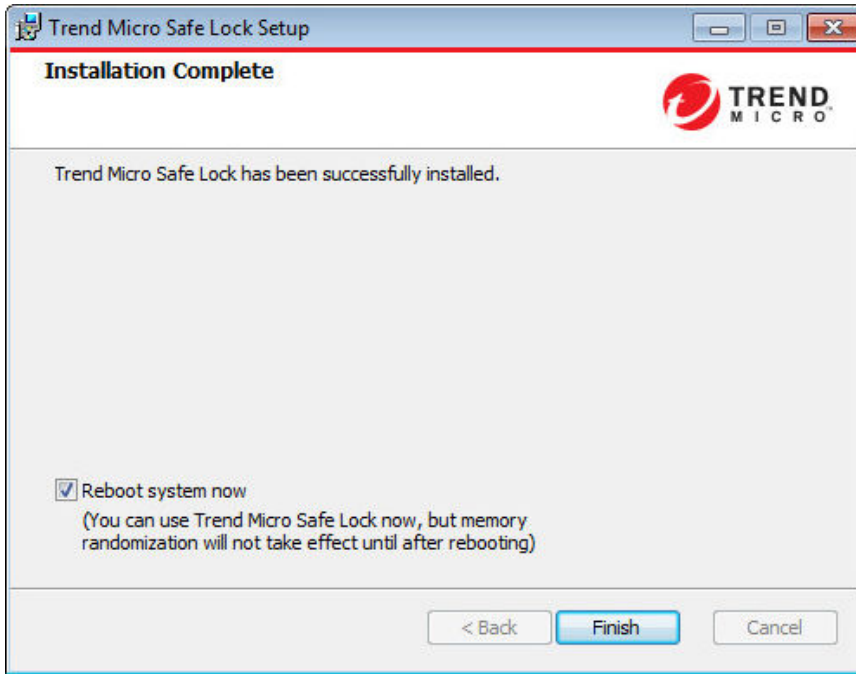
7. Optionally, scan the endpoint for threats before continuing with the installation. Trend Micro recommends you perform this scan.

- 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.

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

8. When the **Installation Complete** window displays, click **Finish**.

**Note**

While restarting the endpoint after installation is not necessary, memory randomization will not be enabled until the endpoint is restarted. See *Exploit Prevention Settings* in the Administrator's Guide for more information.

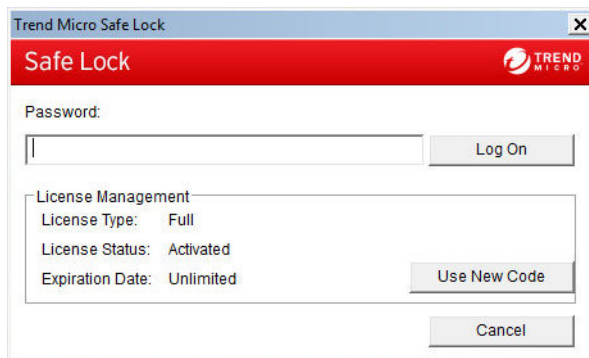
Setting Up the Approved List

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

Procedure

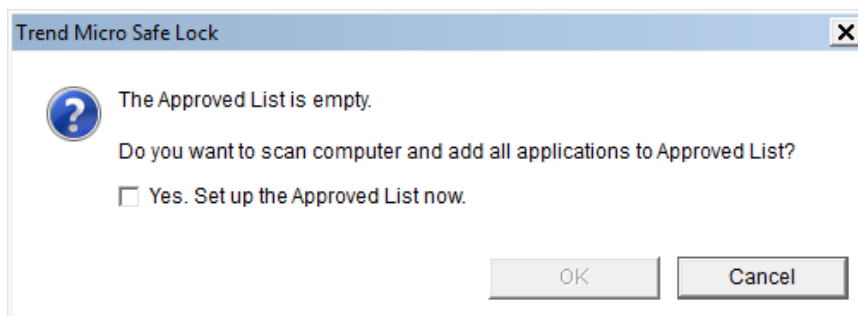
1. Open the Safe Lock console.

The Safe Lock log on screen appears.



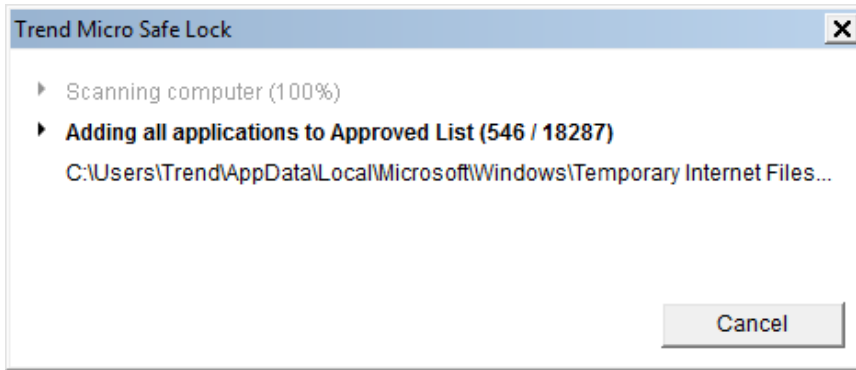
2. Provide the password and click **Log On**.

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

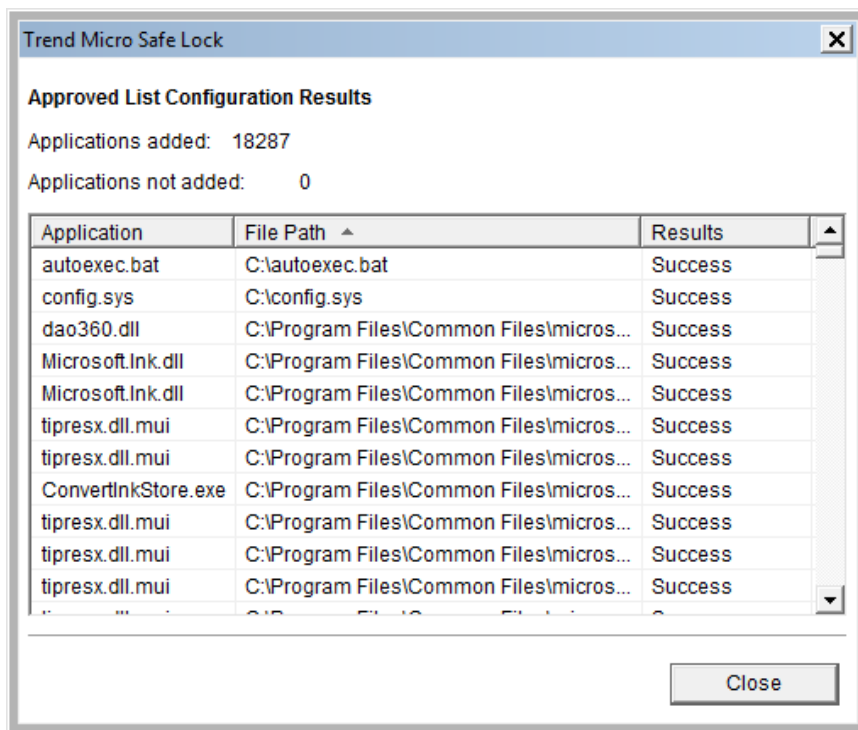


3. At the notification window, select **Yes. Set up the Approved List now** and click **OK**.

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.

Installer Command Line Interface Parameters

The following table lists the commands available for `Setup.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
-d	<path>	Specify the installation path
-ac	<activation_code>	Specify the activation code
-nd		Do not create a desktop shortcut
-ns		Do not add a shortcut to the Start menu
-ni		Hide the task tray icon
-nfw		Disable the network antivirus function
-cp	<path>	Specify the Safe Lock configuration file
		<hr/>  Note The Safe Lock configuration file can be exported after installing Safe Lock. <hr/>

PARAMETER	VALUE	DESCRIPTION
-lp	<path>	Specify the Approved List  Note After installing Safe Lock and creating the Approved List, the list can be exported.
-qp	<path>	Specify the folder path for quarantined files when custom action is set to “quarantine” mode.
-nrca		Disable the Root Cause Analysis (RCA) report
-nps		Do not execute Prescan
-ips		Do not cancel installation when Prescan detects threats

An example command line interface (CLI) install would look like this:

```
setup.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.

Installation Customization

To change the default installation parameters, create a text file called `setup.ini` in the same folder as `setup.exe`. 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.



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 `setup.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.

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"> • 1: Do not create shortcut • 0: Create shortcut 	0	No
NO_STARTMENU	Create a shortcut in the Start menu	<ul style="list-style-type: none"> • 1: Do not create shortcut • 0: Create shortcut 	0	No
NO_SYSTRAY	Display the system tray icon and Windows notifications	<ul style="list-style-type: none"> • 1: Do not create system tray icon • 0: Create system tray icon 	0	No
NO_NSC	Install firewall	<ul style="list-style-type: none"> • 1: Do not create firewall • 0: Create firewall 	0	No
CONFIG_PATH	Configuration file path	<path>	<empty>	No
LIST_PATH	Approved List path for import	<path>	<empty>	No
APPLICATIONFOLDER	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"> • 0: Standalone mode • 1: Managed mode 	0	No
PASSWORD	Password which is used for <code>SLCmd.exe</code> and	<password>	<empty>	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
	Safe Lock console			
CUSTOM_ACTION	Custom action for blocked events	<ul style="list-style-type: none"> 0: Ignore 1: Quarantine 2: Ask server 	0	No
QUARANTINE_FOLDER_PATH	Quarantine path for agent program	<path>	<empty>	No
ROOT_CAUSE_ANALYSIS	Enable Root Cause Analysis reporting	<ul style="list-style-type: none"> 0: Disable Other value: Enable 	1	No
INTEGRITY_MONITOR	Enable Integrity Monitor	<ul style="list-style-type: none"> 0: Disable Other value: Enable 	0	No
PRESKAN	Prescan the endpoint before installing Safe Lock	<ul style="list-style-type: none"> 1: Prescan the endpoint 0: Do not prescan the endpoint 	1	No
MAX_EVENT_DB_SIZE	Maximum database file size (MB)	Positive integer	1024	No
WEL_SIZE	Windows Event Log size (KB)	Positive integer	1024	No
WEL_RETENTION	Windows Event Log option when maximum event log size is reached on Windows Event Log.	For Windows XP or earlier platforms: <ul style="list-style-type: none"> 0: Overwrite events as needed 1 - 365: Overwrite events older than (1-365) days 	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPT-ED
		<ul style="list-style-type: none"> -1: Do not overwrite events (Clear logs manually) <p>For Windows Vista or later platforms:</p> <ul style="list-style-type: none"> 0: Overwrite events as needed (oldest events first) 1: Archive the log when full, do not overwrite events -1: Do not overwrite events (Clear logs manually) 		
WEL_IN_SIZE	Windows Event Log size for Integrity Monitor events (KB)	Positive integer	1024	No
WEL_IN_RETENTION	Windows Event Log option when maximum event log size for Integrity Monitor events is reached on Windows Event Log.	<p>For Windows XP or earlier platforms:</p> <ul style="list-style-type: none"> 0: Overwrite events as needed 1 - 365: Overwrite events older than (1-365) days -1: Do not overwrite events (Clear logs manually) <p>For Windows Vista or later platforms:</p>	0	No


KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		<ul style="list-style-type: none"> 0: Overwrite events as needed (oldest events first) 1: Archive the log when full, do not overwrite events -1: Do not overwrite events (Clear logs manually) 		
SILENT_INSTALL	Execute installation in silent mode	<ul style="list-style-type: none"> 1: Use silent mode 0: Do not use silent mode 	0	No
	 Important To use silent mode, you must also specify the ACTIVATION_CODE and PASSWORD keys and values. For example: <pre>[PROPERTY] ACTIVATION_CODE=XX-XXXX-XXX XX-XXXX-XXXX-XXXX-XXXX PASSWORD=P@ssW0Rd SILENT_INSTALL=1</pre>			

TABLE 8-4. Setup.ini File [Server] Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
HOSTNAME	Server host name	<host_name>	<empty>	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
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

TABLE 8-5. 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"> • 0: Protect against BEAST attacks • <other_value>: Do not implement any security workarounds for BEAST vulnerabilities 	1	No

TABLE 8-6. Setup.ini File [Message] Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
REGISTER_TRIGGER	Register message trigger	<ul style="list-style-type: none"> • 1: Immediately • 2: On demand 	1	No
UNREGISTER_TRIGGER	Unregister message trigger	<ul style="list-style-type: none"> • 1: Immediately • 2: On demand 	1	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
UPDATESTATUS_TRIGGER	Update status message trigger	<ul style="list-style-type: none"> • 1: Immediately • 2: On demand 	1	No
UPLOADBLOCKEDEVENT_TRIGGER	Upload blocked event message trigger	<ul style="list-style-type: none"> • 1: Immediately • 2: On demand 	1	No
CHECKFILEHASH_TRIGGER	Check file hash message trigger	<ul style="list-style-type: none"> • 1: Immediately • 2: On demand 	1	No
QUICKSCANFILE_TRIGGER	Quick scan file message trigger	<ul style="list-style-type: none"> • 1: Immediately • 2: On demand 	1	No

TABLE 8-7. Setup.ini File [MessageRandomization] Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
TOTAL_GROUP_NUM	Number of groups controlled by the server controls	0 - 2147483647	0	No
OWN_GROUP_INDEX	Index of group which this agent belongs to	0 - 2147483647	0	No
TIME_PERIOD	Maximum amount of time agents have to upload data (in seconds)	0 - 2147483647	0	No




Note


Safe Lock agents respond as soon as possible to direct requests from Safe Lock Intelligent Manager.

TABLE 8-8. Setup.ini File [Proxy] Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
MODE	Proxy mode	<ul style="list-style-type: none"> 0: No proxy used 1: Proxy used with manual settings 2: Proxy used with settings retrieved from Internet Explorer automatically 	0	No
HOSTNAME	Proxy host name	<host_name>	<empty>	No
PORT	Proxy port	1 - 65535	<empty>	No
USERNAME	Proxy user name	<user_name>	<empty>	No
PASSWORD	Proxy password	<password>	<empty>	No

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

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
IGNORE_THREAT	Cancel installation after detecting malware threat during prescan  Note Only valid during silent installations.	<ul style="list-style-type: none"> 0: Cancel 1: Continue installation after detecting malware threat during prescan 	0	No
REPORT_FOLDER	An absolute folder path	<ul style="list-style-type: none"> <folder_path> 	<empty>	No

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

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		<ul style="list-style-type: none"> Temp folder For example, c:\Users \Trend \AppData \Local\Temp Desktop folder including sub folders and files For example, c:\Users \Trend \Desktop Specific: Scan folders specified with SPECIFIC_FOLDER entries 		
COMPRESS_LAYER	The number of compressed layers to scan when a compressed file is scanned.	1 - 20	2	No
SCAN_REMOVABLE_DRIVE	Scan removable drives	<ul style="list-style-type: none"> 1: Scan removable drives <other_value>: Do not scan removable drives 	0	No
SPECIFIC_FOLDER	An absolute folder path to scan when the	<folder_path> Multiple folders can be specified by creating	<empty>	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
	scan type is [Specific]	<p>new entries whose name starting with SPECIFIC_FOLDER.</p> <p>Every entry name needs to be unique.</p> <p>For example:</p> <p>SPECIFIC_FOLDER=c:\folder1</p> <p>SPECIFIC_FOLDER2=c:\folder2</p> <p>SPECIFIC_FOLDER3=c:\folder3</p>		
EXCLUDED_FILE	An absolute file path to exclude from scanning	<p><file_path></p> <p>Multiple files can be specified by creating new entries whose name starting with EXCLUDED_FILE. Every entry name needs to be unique.</p> <p>For example:</p> <p>EXCLUDED_FILE=c:\file1.exe</p> <p>EXCLUDED_FILE2=c:\file2.exe</p> <p>EXCLUDED_FILE3=c:\file3.exe</p>	<empty>	No
EXCLUDED_FOLDER	An absolute folder path to exclude from scanning	<p><folder_path></p> <p>Multiple folders can be specified by creating new entries whose name starting with EXCLUDED_FOLDER.</p>	<empty>	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		<p>Every entry name needs to be unique.</p> <p>For example:</p> <p>EXCLUDED_FOLDER=c:\file1.exe</p> <p>EXCLUDED_FOLDER2=c:\file2.exe</p> <p>EXCLUDED_FOLDER3=c:\file3.exe</p>		
EXCLUDED_EXTENSION	A file extension to exclude from scanning	<p><file_extension></p> <p>Multiple extensions can be specified by creating new entries whose name starting with EXCLUDED_EXTENSION.</p> <p>Every entry name needs to be unique.</p> <p>For example:</p> <p>EXCLUDED_EXTENSION=bmp</p> <p>EXCLUDED_EXTENSION2=png</p>	<empty>	No

Example Setup.ini File

The following is an example of setup.ini file syntax:

```
[Property]
ACTIVATION_CODE=XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
NO_SYSTRAY=1
LIST_PATH=c:\temp\list.db
```

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 9-2](#) 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.
 4. Encrypt the edited configuration file.
 5. Import the edited configuration file.
-

Exporting or Importing a Configuration File

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

Procedure

1. Open the Trend Micro Safe Lock console using the desktop icon (if available) or the **Start** menu by clicking **All Programs > Trend Micro Safe Lock**.
2. Provide the password and click **Login**.
3. Click the **Settings** menu item to access the **Export/Import Configuration** section.

To export the configuration file as a database (.xen) file:

- a. Click **Export**, and choose the location to save the file.
- b. Provide a filename, and click **Save**.

To import the configuration file as a database (.xen) file:

- a. Click **Import**, and locate the database file.
- b. Select the file, and click **Open**.

Trend Micro Safe Lock overwrites the existing configuration settings with the settings in the database file.

Configuration File Syntax

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



Important

The configuration file only supports UTF-8 encoding.

Refer to the following example of the configuration file:

```
<?xml version="1.0" encoding="UTF-8"?>
<Configurations version="1.00.000"
  xmlns:xsi="http://www.w3.org/2001/
  XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="WKConfig.xsd">
  <Configuration>
    <AccountGroup>
      <Account
        ID="{24335D7C-1204-43d1-9CBB-332D688C85B6}"
        Enable="no">
        <Password/>
      </Account>
    </AccountGroup>
  <UI>
    <SystemTaskTrayIcon Enable="yes"/>
  </Configuration>
</Configurations>
```

```
</UI>
<Feature>
  <ApplicationLockDown LockDownMode="2">
    <WhiteList
      RecentHistoryUnapprovedFilesLimit="50"/>
    <ScriptLockdown Enable="yes">
      <Extension ID="bat">
        <Interpreter>cmd.exe</Interpreter>
      </Extension>
      <Extension ID="cmd">
        <Interpreter>cmd.exe</Interpreter>
      </Extension>
      <Extension ID="com">
        <Interpreter>ntvdm.exe</Interpreter>
      </Extension>
      <Extension ID="dll">
        <Interpreter>ntvdm.exe</Interpreter>
      </Extension>
      <Extension ID="drv">
        <Interpreter>ntvdm.exe</Interpreter>
      </Extension>
      <Extension ID="exe">
        <Interpreter>ntvdm.exe</Interpreter>
      </Extension>
      <Extension ID="js">
        <Interpreter>cscript.exe</Interpreter>
        <Interpreter>wscript.exe</Interpreter>
      </Extension>
      <Extension ID="msi">
        <Interpreter>msiexec.exe</Interpreter>
      </Extension>
      <Extension ID="pif">
        <Interpreter>ntvdm.exe</Interpreter>
      </Extension>
      <Extension ID="ps1">
        <Interpreter>powershell.exe
      </Interpreter>
      </Extension>
      <Extension ID="sys">
        <Interpreter>ntvdm.exe</Interpreter>
      </Extension>
      <Extension ID="vbe">
```



```

        <Interpreter>cscript.exe</Interpreter>
        <Interpreter>wscript.exe</Interpreter>
    </Extension>
    <Extension ID="vbs">
        <Interpreter>cscript.exe</Interpreter>
        <Interpreter>wscript.exe</Interpreter>
    </Extension>
</ScriptLockdown>
<TrustedUpdater>
    <PredefinedTrustedUpdater Enable="no">
        <RuleSet/>
    </PredefinedTrustedUpdater>
</TrustedUpdater>
<DllDriverLockDown Enable="yes"/>
<ExceptionPath Enable="no">
    <ExceptionPathList/>
</ExceptionPath>
<TrustedCertification Enable="yes"/>
<WriteProtection Enable="yes" ActionMode="1"
ProtectApprovedList="yes"/>
<CustomAction ActionMode="0"/>
</ApplicationLockDown>
<UsbMalwareProtection Enable="yes" ActionMode="1"/>
<DllInjectionPrevention Enable="yes"
ActionMode="1"/>
<ApiHookingPrevention Enable="yes" ActionMode="1"/>
<MemoryRandomization Enable="yes"/>
<NetworkVirusProtection Enable="yes"
ActionMode="1"/>
<IntegrityMonitoring Enable="yes"/>
<Log>
    <EventLog Enable="yes">
        <BlockedAccessLog Enable="yes"/>
        <ApprovedAccessLog Enable="yes">
            <TrustedUpdaterLog Enable="yes"/>
            <DllDriverLog Enable="yes"/>
            <ExceptionPathLog Enable="yes"/>
            <TrustedCertLog Enable="yes"/>
            <WriteProtectionLog Enable="yes"/>
        </ApprovedAccessLog>
        <SystemEventLog Enable="yes">
            <ExceptionPathLog Enable="yes"/>
        </SystemEventLog>
    </EventLog>
</Log>

```

```
        <WriteProtectionLog Enable="yes"/>
    </SystemEventLog>
    <ListLog Enable="yes"/>
    <UsbMalwareProtectionLog Enable="yes"/>
    <ExecutionPreventionLog Enable="yes"/>
    <NetworkVirusProtectionLog Enable="yes"/>
    <IntegrityMonitoringLog>
        <FileCreatedLog Enable="yes"/>
        <FileModifiedLog Enable="yes"/>
        <FileDeletedLog Enable="yes"/>
        <FileRenamedLog Enable="yes"/>
        <RegValueModifiedLog Enable="yes"/>
        <RegValueDeletedLog Enable="yes"/>
        <RegKeyCreatedLog Enable="yes"/>
        <RegKeyDeletedLog Enable="yes"/>
        <RegKeyRenamedLog Enable="yes"/>
    </IntegrityMonitoringLog>
</EventLog>
<DebugLog Enable="no"/>
</Log>
</Feature>
<ManagedMode Enable="yes">
    <Agent>
        <Port/>
        <SslAllowBeast>1</SslAllowBeast>
    </Agent>
    <Server>
        <HostName/>
        <FastPort/>
        <SlowPort/>
        <ApiKey/>
    </Server>
    <Message>
        <Register Trigger="1"/>
        <Unregister Trigger="1"/>
        <UpdateStatus Trigger="1"/>
        <UploadBlockedEvent Trigger="1"/>
        <CheckFileHash Trigger="1"/>
        <QuickScanFile Trigger="1"/>
    </Message>
    <MessageRandomization TotalGroupNum="1"
    OwnGroupIndex="0"
```

```

        TimePeriod="0"/>
    <Proxy Mode="0">
        <HostName/>
        <Port/>
        <UserName/>
        <Password/>
    </Proxy>
</ManagedMode>
</Configuration>
<Permission>
    <AccountRef
        ID="{24335D7C-1204-43d1-9CBB-332D688C85B6}">
        <UIControl ID="DetailSetting" State="no"/>
        <UIControl ID="LockUnlock" State="yes"/>
        <UIControl ID="LaunchUpdater" State="yes"/>
        <UIControl ID="RecentHistoryUnapprovedFiles"
            State="yes"/>
        <UIControl ID="ImportExportList" State="yes"/>
        <UIControl ID="ListManagement" State="yes"/>
    </AccountRef>
</Permission>
</Configurations>

```

Configuration File Parameters

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

TABLE 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 AccountGroup Section on page 9-9 . See Account Types on page 5-15 .

SECTION		DESCRIPTION	ADDITIONAL INFORMATION
	UI	Parameters to configure the display of the system tray icon	See UI Section on page 9-10 .
	Feature	Container for the Feature section	
	ApplicationLockDown	Parameters to configure Safe Lock features and functions	See Feature Section on page 9-10 . See About Feature Settings on page 5-17 .
	UsbMalwareProtection		
	DllInjectionPrevention		
	ApiHookingPrevention		
	MemoryRandomization		
	NetworkVirusProtection		
	IntegrityMonitoring		
	Log	Parameters to configure individual log types	See Log Section on page 9-20 . See Agent Event Log Descriptions on page 13-4 .
	ManagedMode	Parameters to configure Centralized Management functions	See ManagedMode Section on page 9-24 .
	Permission	Container for the Permission section	

SECTION		DESCRIPTION	ADDITIONAL INFORMATION
	AccountRef	Parameters to configure the Safe Lock console controls available to the Restricted User account	See AccountRef Section on page 9-27 . See Account Types on page 5-15 .


AccountGroup Section

Parameters to configure the Restricted User account

See [Account Types on page 5-15](#).

TABLE 9-2. AccountGroup Section Parameters

PARAMETER	SETTING	VALUE	DESCRIPTION
Configuration			Container for the Configuration section
AccountGroup			Container for the AccountGroup section
Account	ID	<GUID>	Restricted User account GUID
	Enable	yes	Enable the Restricted User account
		no	Disable the Restricted User account
	Password	<Safe_Lock_password>	Password for the Restricted User account to access the Safe Lock console

PARAMETER			SETTING	VALUE	DESCRIPTION
					 Note The Safe Lock administrator and Restricted User passwords cannot be the same.

UI Section

Parameters to configure the display of the system tray icon

TABLE 9-3. UI Section Parameters

PARAMETER			SETTING	VALUE	DESCRIPTION
Configuration					Container for the Configuration section
	UI				Container for the UI section
		SystemTask TrayIcon	Enable	yes	Display the system tray icon and Windows notifications
				no	Hide the system tray icon and Windows notifications

Feature Section

Parameters to configure Safe Lock features and functions

See [About Feature Settings on page 5-17](#).

TABLE 9-4. Feature Section Parameters

PARAMETER			SETTING	VALUE	DESCRIPTION
Configuration					Container for the Configuration section

PARAMETER	SETTING	VALUE	DESCRIPTION
Feature			Container for the Feature section
ApplicationLockDown	LockDown Mode	1	Turn on Application Lockdown
		2	Turn off Application Lockdown
WhiteList	RecentHistoryUnapprovedFilesLimit	0 - 65535	Maximum number of entries in the Blocked Files log
ScriptLockDown	Enable	yes	Enable Script Lockdown
		no	Disable Script Lockdown
Extension	ID	<file_extension>	File extension for Script Lockdown to block For example, specify a value of <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.
TrustedUpdater			Container for the TrustedUpdater section
PredefinedTrustedUpdater	Enable	yes	Enable Trusted Updater
		no	Disable Trusted Updater
RuleSet			Container for RuleSet conditions

PARAMETER				SETTING	VALUE	DESCRIPTION
			Condition	ID	<unique_ruleset_name>	Unique name for the set of rules
			ApprovedListCheck	Enable	yes	Enable hash checks for Trusted Updaters
					no	Disable hash checks for Trusted Updaters
			ParentProcess	Path	<process_path>	Path of the parent process to add to the Trusted Updater List
			Exception	Path	<process_path>	Path to exclude from the Trusted Updater List
			Rule	Label	<unique_rule_name>	Unique name for this rule
			Updater	Type	process	Use the specified EXE file
					file	Use the specified MSI or BAT file
					folder	Use the EXE, MSI or BAT files in the specified folder
					folderandsub	Use the EXE, MSI or BAT files in the specified folder and its subfolders
				Path	<updater_path>	Updater path
				ConditionRef	<condition_ID>	Condition ID to provide a more detailed rule for the updater
			DLLDriverLockdown	Enable	yes	Enable DLL/Driver Lockdown

PARAMETER	SETTING	VALUE	DESCRIPTION
		no	Disable DLL/Driver Lockdown
ExceptionPath	Enable	yes	Enable exception paths
		no	Disable exception paths
ExceptionPathList			Container for the Exception List
ExceptionPath	Path	<exception_path>	Exception path
	Type	file	Use only the specified file
		folder	Use the files in the specified folder
		folderandsub	Use the files in the specified folder and its subfolders
TrustedCertification	Enable	yes	Enable using Trusted Certifications
		no	Disable using Trusted Certifications
PredefinedTrustedCertification	Type	updater	File signed by this certificate is treated as a Trusted Updater
		lockdown	File signed by this certificate is not treated as a Trusted Updater
	Hash	<SHA-1_hash_value>	SHA1-hash value of this certificate
	Label	<label>	Description of this certificate
	Subject	<subject>	Subject of this certificate

PARAMETER	SETTING	VALUE	DESCRIPTION
	Issuer	<issuer>	Issuer of this certificate
WriteProtection	Enable	yes	Enable Write Protection
		no	Disable Write Protection
	ActionMode	0	Allow actions such as edit, rename, and delete
		1	Block actions such as edit, rename, and delete
	ProtectApprovedList	yes	Enable protection of the Approved List (in addition to the Write Protection List) when Write Protection is enabled
		no	Disable protection of the Approved List (in addition to the Write Protection List) when Write Protection is enabled
List			Container for the Write Protection List
File	Path	<file_path>	File path
	Folder	Path	<folder_path>
	Includesubfolder	yes	Use the files in the specified folder and its subfolders
		no	Use the files in the specified folder
RegistryKey	Key	<reg_key>	Registry key <reg_key> can be abbreviated or expanded as shown below:

PARAMETER					SETTING	VALUE	DESCRIPTION
							<ul style="list-style-type: none"> • HKEY_LOCAL_MACHINE\test HKLM\test • HKEY_CURRENT_CONFIG\test HKCC\test • HKEY_CLASSES_ROOT\test HKCR\test • HKEY_CURRENT_USER\test HKCU\test • HKEY_USERS\test HKU\test
				Includes subkey	yes	Include any subkeys	
					no	Do not include any subkeys	
			RegistryValue	Key	<reg_key>	<p>Registry key</p> <p><reg_key> can be abbreviated or expanded as shown below:</p> <ul style="list-style-type: none"> • HKEY_LOCAL_MACHINE\test HKLM\test • HKEY_CURRENT_CONFIG\test HKCC\test • HKEY_CLASSES_ROOT\test HKCR\test 	

PARAMETER				SETTING	VALUE	DESCRIPTION
						<ul style="list-style-type: none"> HKEY_CURRENT_USER\test HKCU\test HKEY_USERS\test HKU\test
				Name	<reg_value_name>	Registry value name
			ExceptionList			Container for the Write Protection Exception List
			Process	Path	<process_path>	Path of the process
			File	Path	<file_path>	File path
			Folder	Path	<folder_path>	Folder path
				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"> HKEY_LOCAL_MACHINE\test HKLM\test HKEY_CURRENT_CONFIG\test HKCC\test

PARAMETER					SETTING	VALUE	DESCRIPTION
							<ul style="list-style-type: none"> • HKEY_CLASSES_ROOT\test • HKCR\test • HKEY_CURRENT_USER\test • HKCU\test • HKEY_USERS\test • HKU\test
					Includes subkey	yes	Include any subkeys
						no	Do not include any subkeys
			RegistryValue	Key	<reg_key>		<p>Registry key</p> <p><reg_key> can be abbreviated or expanded as shown below:</p> <ul style="list-style-type: none"> • HKEY_LOCAL_MACHINE\test • HKLM\test • HKEY_CURRENT_CONFIG\test • HKCC\test • HKEY_CLASSES_ROOT\test • HKCR\test • HKEY_CURRENT_USER\test • HKCU\test • HKEY_USERS\test • HKU\test

PARAMETER				SETTING	VALUE	DESCRIPTION
				Name	<reg_value_name>	Registry value name
			CustomAction	ActionMode	0	Ignore blocked files or processes when Application Lockdown blocks any of the following events: <ul style="list-style-type: none"> Process launch DLL loading Script file access
					1	Quarantine blocked files or processes when Application Lockdown blocks any of the following events: <ul style="list-style-type: none"> Process launch DLL loading Script file access
					2	Ask what to do for blocked files or processes when Application Lockdown blocks any of the following events: <ul style="list-style-type: none"> Process launch DLL loading Script file access
			UsbMalwareProtection	Enable	yes	Enable USB Malware Protection
					no	Disable USB Malware Protection
				ActionMode	0	Allow action by detected malware

PARAMETER	SETTING	VALUE	DESCRIPTION
		1	Block action by detected malware
DllInjectionPrevention	Enable	yes	Enable DLL Injection Prevention
		no	Disable DLL Injection Prevention
	ActionMode	0	Allows DLL injections
		1	Blocks DLL injections
ApiHookingPrevention	Enable	yes	Enable API Hooking Prevention
		no	Disable API Hooking Prevention
	ActionMode	0	Allow API hooking
		1	Block API hooking
MemoryRandomization	Enable	yes	Enable Memory Randomization
		no	Disable Memory Randomization
NetworkVirusProtection	Enable	yes	Enable Network Virus Protection
		no	Disable Network Virus Protection
	ActionMode	0	Allow action by detected network viruses
		1	Block action by detected network viruses
IntegrityMonitoring	Enable	yes	Enable Integrity Monitoring
		no	Disable Integrity Monitoring

PARAMETER		SETTING	VALUE	DESCRIPTION
	Log			Container for configuring logs See Log Section on page 9-20 .

Log Section

Parameters to configure individual log types

See [Agent Event Log Descriptions on page 13-4](#).

TABLE 9-5. Log Configuration Parameters

PARAMETER		SETTING	VALUE	DESCRIPTION
Configuration				Container for the Configuration section
Feature				Container for the Feature section
Log				Container for configuring logs
	EventLog	Enable	yes	Log the Safe Lock events specified in the following elements
			no	Do not the Safe Lock events specified in the following elements
	BlockedAccessLog	Enable	yes	Log files blocked by Safe Lock
			no	Do not log files blocked by Safe Lock
	ApprovedAccessLog	Enable	yes	Log files approved by Safe Lock
			no	Do not log files approved by Safe Lock

PARAMETER		SETTING	VALUE	DESCRIPTION
	TrustedUpdaterLog	Enable	yes	Enable the Trusted Updater approved access log
			no	Disable the Trusted Updater approved access log
	DLLDriverLog	Enable	yes	Enable the DLL/Driver approved access log
			no	Disable the DLL/Driver approved access log
	ExceptionPathLog	Enable	yes	Enable the Application Lockdown exception path approved access log
			no	Disable the Application Lockdown exception path approved access log
	TrustedCertLog	Enable	yes	Enable the Trusted Certifications approved access log
			no	Disable the Trusted Certifications approved access log
	WriteProtectionLog	Enable	yes	Enable the Write Protection approved access log
			no	Disable the Write Protection approved access log
	SystemEventLog	Enable	yes	Log events related to the system
			no	Do not log events related to the system
	ExceptionPathLog	Enable	yes	Enable exceptions to Application Lockdown

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

PARAMETER				SETTING	VALUE	DESCRIPTION
					no	Do not log file modified events
			FileDeletedLog	Enable	yes	Log file and folder deleted events
					no	Do not log file and folder deleted events
			FileRenamedLog	Enable	yes	Log file and folder renamed events
					no	Do not log file and folder renamed events
			RegValueModifiedLog	Enable	yes	Log registry value modified events
					no	Do not log registry value modified events
			RegValueDeletedLog	Enable	yes	Log registry value deleted events
					no	Do not log registry value deleted events
			RegKeyCreatedLog	Enable	yes	Log registry key created events
					no	Do not log registry key created events
			RegKeyDeletedLog	Enable	yes	Log registry key deleted events
					no	Do not log registry key deleted events
			RegKeyRenamedLog	Enable	yes	Log registry key renamed events
					no	Do not log registry key renamed events
			EventLog	Enable	yes	Log debugging information

PARAMETER	SETTING	VALUE	DESCRIPTION
		no	Do not log debugging information



ManagedMode Section

Parameters to configure Centralized Management functions

TABLE 9-6. ManagedMode Section Parameters

PARAMETER	SETTING	VALUE	DESCRIPTION
Configuration			Container for the Configuration section
ManagedMode	Enable	yes	Enable managed mode
		no	Disable managed mode
Agent			Container for configuring Safe Lock agents
Port		<server_messages_port >	Specify the secure port for server communications (formerly the agent listening port)
SslAllowBest		0	Allow upload of large files (>10MB) on Windows Server 2008 platforms
		1	Prevent the unsuccessful upload of large files (>10MB) on Windows Server 2008 platforms (default value)
Server			Container for configuring Safe Lock Intelligent Manager
HostName		<hostname >	Specify the host name of the Intelligent Manager server

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

PARAMETER		SETTING	VALUE	DESCRIPTION
	QuickScanFile	Trigger	1	Send as soon as possible after the event occurs
			2	Do not send unless requested to by Intelligent Manager
MessageRandomization		TotalGroupNum	Positive Integer (≥ 1)	Specify the total number of message time groups
 Note Safe Lock agents respond as soon as possible to direct requests from Safe Lock Intelligent Manager.		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 messages to Intelligent Manager when this group's message-sending cycle is active  Note Message time groups do not become active if their duration is set to zero (0).
Proxy		Mode	0	Do not use a proxy (direct access)
			1	Use a proxy (manual setting)
			2	Synchronize proxy settings with Internet Explorer
	HostName		<proxy_hostname>	Specify the proxy host name


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

AccountRef Section

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

See [Account Types on page 5-15](#).

TABLE 9-7. AccountRef Section Parameters

PARAMETER			SETTING	VALUE	DESCRIPTION
Configuration					Container for the Configuration section
Permission					Container for the Permission section
AccountRef					Container for the AccountRef section
		UIControl	ID	DetailSetting	<p>Access the features and functions on the Safe Lock console Settings page</p> <hr/> <p> Note The Password page is not available to the Restricted User account.</p>

PARAMETER				SETTING	VALUE	DESCRIPTION
					LockUnlock	Access the Application Lockdown setting on the Overview screen
					LaunchUpdater	Access the Automatically add files created or modified by the selected application installer option when a Restricted User clicks Add Item on the Approved List screen
					RecentHistoryUnapprovedFiles	Access the Block logs if a Restricted User clicks Last application blocked on the Overview screen
					ImportExportList	Access the Import List and Export List buttons
					ListManagement	Access the following items on the Approved List screen: <ul style="list-style-type: none"> • The Delete Item button • The Update Hash button • The Add Item > Add Files/Folders menu
				State	yes	Enable the permission specified by ID
					no	Disable the permission specified by ID

Chapter 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
If you use one of the following operating systems: <ul style="list-style-type: none"> • Windows Server 2012 • Windows Server 2008 • Windows 8 • Windows 7 • Windows Vista 	<ol style="list-style-type: none"> a. Go to Start > Control Panel > Uninstall a program. b. In the list, double-click Trend Micro Safe Lock.
If you use one of the following operating systems: <ul style="list-style-type: none"> • Windows Server 2003 • Windows XP • Windows 2000 	<ol style="list-style-type: none"> a. Go to Start > Control Panel > Add or Remove Programs. b. In the list, select Trend Micro Safe Lock. c. Click Remove.

Safe Lock Setup opens in uninstaller mode.

2. After Safe Lock Setup opens, click **Next**.
3. Provide the Safe Lock administrator password, and click **Next**.

4. After the software is finished uninstalling, click **Finish**.
-

Chapter 11

Troubleshooting & FAQs

This chapter provides a list of resources you can use to troubleshoot Trend MicroSafe 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.

Chapter 12

Technical Support

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

Topics include:

- *Troubleshooting Resources on page 12-2*
- *Contacting Trend Micro on page 12-3*
- *Other Resources on page 12-4*
- *About Trend Micro 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 a product or service from the appropriate drop-down list and specify any other related information.

The **Technical Support** product page appears.

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

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

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

Trend Community

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

<http://community.trendmicro.com/>

Contacting Trend Micro

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

Address	Trend Micro, Inc. 10101 North De Anza Blvd., Cupertino, CA 95014
Phone	Toll free: +1 (800) 228-5651 (sales) Voice: +1 (408) 257-1500 (main)
Fax	+1 (408) 257-2003
Website	http://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:
<http://www.trendmicro.com/us/about-us/contact/index.html>
- Trend Micro product documentation:
<http://docs.trendmicro.com>

Related information

↳ *Speeding Up the Support Call*

Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional hardware connected to the endpoint
- Amount of memory and free hard disk space
- Operating system and service pack version
- Endpoint agent version

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

Other Resources

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

Related information

- ↳ [TrendEdge](#)
- ↳ [Download Center](#)
- ↳ [TrendLabs](#)

TrendEdge

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

See the latest information added to TrendEdge at:

<http://trendedge.trendmicro.com/>

Download Center

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

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

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

TrendLabs

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

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

Learn more about TrendLabs at:

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

About Trend Micro

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

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

<http://www.trendmicro.com>

Trend Micro and the Trend Micro t-ball logo are trademarks of Trend Micro Incorporated and are registered in some jurisdictions. All other marks are the trademarks or registered trademarks of their respective companies.

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 13-25*

Enabling Local Administrator Accounts

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

Procedure

1. Open **Computer Management**.

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

The **Computer Management** window appears.

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

The list of local Windows user accounts displays.

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

The **Administrator Properties** window appears.

4. In the **General** tab, clear **Account is disabled**.

5. Click **OK**.

The **Computer Management** window reappears, displaying the list of local Windows user accounts.

6. Right-click **Administrator**, then go to **Set Password...**

A message displays instructions for setting the password.

7. Set the password.

8. Exit **Computer Management**.

Enabling Local Accounts for Default Shares

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



Tip

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

Procedure

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

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows  
\CurrentVersion\Policies\System
```
3. Locate the `LocalAccountTokenFilterPolicy` registry entry.

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

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

7. Exit **Registry Editor**.

Agent Event Log Descriptions

Trend Micro Safe Lock 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**.

TABLE 13-1. Windows Event Log Descriptions

EVENT ID	TASK CATEGORY	LEVEL	DESCRIPTION
1000	System	Information	Service started.
1001	System	Warning	Service stopped.
1002	System	Information	Application Lockdown Turned On.
1003	System	Warning	Application Lockdown Turned Off.
1004	System	Information	Disabled.
1005	System	Information	Administrator password changed.
1006	System	Information	Restricted User password changed.
1007	System	Information	Restricted User account enabled.
1008	System	Information	Restricted User account disabled.
1009	System	Information	Product activated.
1010	System	Information	Product deactivated.
1011	System	Warning	License Expired. Grace period enabled.
1012	System	Warning	License Expired. Grace period ended.
1013	System	Information	Product configuration import started: <full_path>

EVENT ID	TASK CATEGORY	LEVEL	DESCRIPTION
1014	System	Information	Product configuration import complete: <full_path>
1015	System	Information	Product configuration exported to: <full_path>
1016	System	Information	USB Malware Protection set to Allow.
1017	System	Information	USB Malware Protection set to Block.
1018	System	Information	USB Malware Protection enabled.
1019	System	Warning	USB Malware Protection disabled.
1020	System	Information	Network Virus Protection set to Allow.
1021	System	Information	Network Virus Protection set to Block.
1022	System	Information	Network Virus Protection enabled.
1023	System	Warning	Network Virus Protection disabled.
1025	System	Information	Memory Randomization enabled.
1026	System	Warning	Memory Randomization disabled.
1027	System	Information	API Hooking Prevention set to Allow.
1028	System	Information	API Hooking Prevention set to Block.
1029	System	Information	API Hooking Prevention enabled.
1030	System	Warning	API Hooking Prevention disabled.
1031	System	Information	DLL Injection Prevention set to Allow.
1032	System	Information	DLL Injection Prevention set to Block.
1033	System	Information	DLL Injection Prevention enabled.
1034	System	Warning	DLL Injection Prevention disabled.
1035	System	Information	Auto Trusted Update enabled.
1036	System	Information	Auto Trusted Update disabled.

EVENT ID	TASK CATEGORY	LEVEL	DESCRIPTION
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.

EVENT ID	TASK CATEGORY	LEVEL	DESCRIPTION
1046	System	Information	<p>Event Log settings changed.</p> <p>[Details]</p> <p>Windows Event 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: <ON off></p> <p>DLL Driver 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>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 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> <p>RegKey Renamed Log: <ON off></p> <p>Debug Log: <on OFF></p>

EVENT ID	TASK CATEGORY	LEVEL	DESCRIPTION
1047	System	Information	Trusted certificate enabled.
1048	System	Information	Trusted certificate disabled.
1049	System	Information	Write Protection enabled.
1050	System	Warning	Write Protection disabled.
1051	System	Information	Write Protection set to Allow.
1052	System	Information	Write Protection set to Block.
1055	System	Information	Added file to Write Protection List. Path: <full_path>
1056	System	Information	Removed file from Write Protection List. Path: <full_path>
1057	System	Information	Added file to Write Protection Exception List Path: <full_path> Process: <process>
1058	System	Information	Removed file from Write Protection Exception List. Path: <full_path> Process: <process>
1059	System	Information	Added folder to Write Protection List. Path: <full_path> Scope: Folder
1060	System	Information	Removed folder from Write Protection List. Path: <full_path> Scope: Folder

EVENT ID	TASK CATEGORY	LEVEL	DESCRIPTION
1061	System	Information	Added folder to Write Protection Exception List. Path: <full_path> Scope: Folder Process: <process>
1062	System	Information	Removed folder from Write Protection Exception List. Path: <full_path> Scope: Folder Process: <process>
1063	System	Information	Added registry value to Write Protection List. Registry Key: <reg_key> Registry Value Name: <reg_value>
1064	System	Information	Removed registry value from Write Protection List. Registry Key: <reg_key> Registry Value Name: <reg_value>
1065	System	Information	Added registry value to Write Protection Exception List. Registry Key: <reg_key> Registry Value Name: <reg_value> Process: <process>
1066	System	Information	Removed registry value from Write Protection Exception List. Registry Key: <reg_key> Registry Value Name: <reg_value> Process: <process>

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

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

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

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

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

EVENT ID	TASK CATEGORY	LEVEL	DESCRIPTION
2006	Access Approved	Information	File access allowed: <full_path> [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode>
2007	Access Approved	Warning	File access allowed: <full_path> An error occurred while checking the Exception Path List. [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode>
2008	Access Approved	Warning	File access allowed: <full_path> An error occurred while checking the Trusted Certificate List. [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode>

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

EVENT ID	TASK CATEGORY	LEVEL	DESCRIPTION
2015	Access Approved	Information	Change of Registry Value allowed by Exception List. Registry Key: <reg_key> Registry Value Name: <reg_value> [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode>
2016	Access Approved	Information	Change of Registry Key allowed by Exception List. Registry Key: <reg_key> [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode>
2017	Access Approved	Warning	Change of File/Folder allowed: <full_path> [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode>

EVENT ID	TASK CATEGORY	LEVEL	DESCRIPTION
2019	Access Approved	Warning	Change of Registry Value allowed. Registry Key: <reg_key> Registry Value Name: <reg_value> [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode>
2020	Access Approved	Warning	Change of Registry Key allowed. Registry Key: <reg_key> [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode>
2503	Access Blocked	Warning	Change of File/Folder blocked: <full_path> [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode>

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

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

EVENT ID	TASK CATEGORY	LEVEL	DESCRIPTION
3001	USB Malware Protection	Warning	Device access blocked: <full_path> [Details] Access Image Path: <full_path> Access User: <user_name> Device Type: <type>
3500	Network Virus Protection	Warning	Network virus allowed: <name> [Details] Protocol: TCP Source IP Address: <ip_address> Source Port: <port> Destination IP Address: <ip_address> Destination Port: <port>
3501	Network Virus Protection	Warning	Network virus blocked: <name> [Details] Protocol: TCP Source IP Address: <ip_address> Source Port: <port> Destination IP Address: <ip_address> Destination Port: <port>
4002	Process Protection Event	Warning	API Hooking allowed: <full_path> [Details] Threat Image Path: <full_path> Threat User: <user_name>

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

EVENT ID	TASK CATEGORY	LEVEL	DESCRIPTION
4502	Changes in System	Information	File/Folder deleted: <full_path> [Details] Access Image Path: <full_path> Access Process ID: <proc_id> Access User: <user_name>
4503	Changes in System	Information	File/Folder renamed: <full_path> New path: <full_path> [Details] Access Image Path: <full_path> Access Process ID: <proc_id> Access User: <user_name>
4504	Changes in System	Information	Registry Value modified. Registry Key: <reg_key> Registry Value Name: <reg_value> Registry Value Type: <reg_value_type> [Details] Access Image Path: <full_path> Access Process ID: <proc_id> Access User: <user_name>

EVENT ID	TASK CATEGORY	LEVEL	DESCRIPTION
4505	Changes in System	Information	Registry Value deleted. Registry Key: <reg_key> Registry Value Name: <reg_value> [Details] Access Image Path: <full_path> Access Process ID: <proc_id> Access User: <user_name>
4506	Changes in System	Information	Registry Key created. Registry Key: <reg_key> [Details] Access Image Path: <full_path> Access Process ID: <proc_id> Access User: <user_name>
4507	Changes in System	Information	Registry Key deleted. Registry Key: <reg_key> [Details] Access Image Path: <full_path> Access Process ID: <proc_id> Access User: <user_name>

EVENT ID	TASK CATEGORY	LEVEL	DESCRIPTION
4508	Changes in System	Information	Registry Key renamed. Registry Key: <reg_key> New Registry Key: <reg_key> [Details] Access Image Path: <full_path> Access Process ID: <proc_id> Access User: <user_name>

Agent Error Code Descriptions

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

TABLE 13-2. Trend Micro Safe Lock Intelligent Manager 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.

CODE	DESCRIPTION
0x80040207	Busy. Request ignored.
0x00040208	Retry. (Usually the result of a task taking too long)
0x80040208	System Reserved. (Not used)
0x80040209	The file path is too long.
0x0004020a	System Reserved. (Not used)
0x8004020b	System Reserved. (Not used)
0x0004020c	System Reserved. (Not used)
0x0004020d	System Reserved. (Not used)
0x8004020d	System Reserved. (Not used)
0x0004020e	Reboot required.
0x8004020e	Reboot required for unexpected reason.
0x0004020f	Allowed to perform task.
0x8004020f	Permission denied.
0x00040210	System Reserved. (Not used)
0x80040210	Invalid or unexpected service mode.
0x00040211	System Reserved. (Not used)
0x80040211	Requested task not permitted in current status. Check license.
0x00040212	System Reserved. (Not used)
0x00040213	System Reserved. (Not used)
0x80040213	Passwords do not match.
0x00040214	System Reserved. (Not used)
0x80040214	System Reserved. (Not used)
0x00040215	Not found.

CODE	DESCRIPTION
0x80040215	"Expected, but not found."
0x80040216	Authentication is locked.
0x80040217	Invalid password length.
0x80040218	Invalid characters in password.
0x00040219	Duplicate password. Administrator and Restricted User passwords cannot match.
0x80040220	System Reserved. (Not used)
0x80040221	System Reserved. (Not used)
0x80040222	System Reserved. (Not used)
0x80040223	File not found (as expected, and not an error).
0x80040224	System Reserved. (Not used)
0x80040225	System Reserved. (Not used)
0x80040240	Library not found.
0x80040241	Invalid library status or unexpected error in library function.
0x80040260	System Reserved. (Not used)
0x80040261	System Reserved. (Not used)
0x80040262	System Reserved. (Not used)
0x80040263	System Reserved. (Not used)
0x80040264	System Reserved. (Not used)
0x00040265	System Reserved. (Not used)
0x80040265	System Reserved. (Not used)
0x80040270	System Reserved. (Not used)
0x80040271	System Reserved. (Not used)

CODE	DESCRIPTION
0x80040272	System Reserved. (Not used)
0x80040273	System Reserved. (Not used)
0x80040274	System Reserved. (Not used)
0x80040275	System Reserved. (Not used)
0x80040280	Invalid Activation Code.
0x80040281	Incorrect Activation Code format.

Index

A

accounts. *See* web console accounts

agent configuration file, 9-2, 9-7

 editing, 9-2

 exporting or importing, 9-2

 syntax, 9-3

agent events

 exporting, 3-11

 importing, 3-11

 log maintenance, 3-14

 notifications, 4-5

 querying logs, 3-9

 tracking, 3-8

agent installer

 approved list, 5-2, 8-8

 command line interface, 8-11, 8-12

 downloading, 4-3, 7-7

 modified packages, 4-4

 overview, 8-2

 Setup.ini, 8-24

 Setup.ini arguments, 8-13

 upgrade preparation, 1-14

 Windows Installer, 8-2

agents, 1-7

 account passwords, 5-16

 accounts, 1-9, 5-15

 changing lockdown, 2-6

 collecting logs, 2-4

 collecting status, 2-4

 component update locations, 4-5

 console, 5-5

 displaying details, 2-3

 editing tags, 2-4

 error codes, 13-25

 event ID codes, 13-4

 exporting data, 2-5

 features and benefits, 1-8

 manual component updates, 4-2

 operating systems, 1-10

 querying, 2-2

 remote setup, 7-2

 removing from list, 2-5

 scheduled component updates, 4-3

 settings, 5-17, 5-20

 status icons, 5-7

 system requirements, 1-9

 uninstallation, 10-2

 use overview, 1-15

Application Lockdown, 1-8

Approved List, 5-8

 adding or removing files, 5-12

 checking or updating hashes, 5-10

 configuring, 5-11

 exporting or importing, 5-15

 hashes, 5-10

 installing or updating files, 5-13

 setting up, 5-2, 8-8

C

configuration file. *See* agent configuration file

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. *See* widgets
default shares, 13-3
documentation, v

E

error codes. *See* agents, error codes
event ID codes. *See* agents, event ID codes
events. *See* agent events; server events
Exploit Prevention, 1-8

H

hashes, 5-10

I

installation
 customization, 8-13
 methods, 8-2
installer. *See* agent installer

L

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

N

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

O

operating systems. *See* agents, operating systems; server, operating systems

P

passwords. *See* agents, account passwords

R

remote tasks. *See* SLrst Program; SLtasks Program

requirements. *See* agents, system requirements; server, system requirements
Restricted User account
 enabling, 5-17

S

Safe Lock. *See* agents; server
Safe Lock Intelligent Manager. *See* server
server, 1-2

 accounts, 1-6
 features and benefits, 1-2
 message time groups, 7-16
 notifications, 4-8
 operating systems, 1-3
 remote tasks, 7-2, 7-14
 system requirements, 1-3
server console. *See* web console
server events
 exporting, 3-14
 log maintenance, 3-14
 querying logs, 3-13
 tracking, 3-13

SLCmd Commands

 For Application Lockdown, 6-22
 For Approved List, 6-19
 For Central Management, 6-7
 For Configuration File, 6-50
 For General Actions, 6-4
 For Optional Features, 6-9
 For Predefined Trusted Updater, 6-44
 For Predefined Trusted Updater
 "Add", 6-47
 For Restricted User Accounts, 6-16
 For Scripts, 6-17
 For Trusted Certifications, 6-41
 For Trusted Updater, 6-42
 For Write Protection, 6-24

- SLCmd Program, 6-3
 - commands. *See* SLCmd Commands
 - comparison to console functions, 6-2
 - using, 6-2
 - SLrst Program, 7-2
 - agent target files, 7-4–7-6
 - downloading installers, 4-3, 7-7
 - remote installation considerations, 7-3
 - remotely hot fixing agents, 7-10
 - remotely installing agents, 7-9
 - remotely patching agents, 7-10
 - remotely restarting agents, 7-13
 - remotely uninstalling agents, 7-12
 - SLtasks Program, 7-14
 - message time groups, 7-16
 - sending tasks, 7-14
 - system requirements. *See* agents, system requirements; server, system requirements
- T**
- tabs. *See* dashboard
 - tab widgets. *See* widgets
 - technical support, 12-1
 - terminology, vii
 - Trend Micro, 12-5
 - Trend Micro Portable Security, 1-9
 - Trusted Updater, 5-13
- U**
- uninstallation. *See* agents, uninstallation
 - upgrading. *See* agent installer, upgrade preparation
- W**
- web console
 - accounts. *See* web console accounts
 - activation codes, 4-13
 - agent details, 2-3
 - changing lockdown, 2-6
 - collecting logs, 2-4
 - component updates, 4-2
 - dashboard. *See* dashboard
 - editing agent tags, 2-4
 - exporting agent data, 2-5
 - exporting agent events, 3-11
 - exporting server events, 3-14
 - importing agent events, 3-11
 - license management, 4-12, 4-13
 - log maintenance, 3-14
 - marking events, 3-12
 - proxy settings, 4-11
 - querying agent events, 3-9
 - querying agents, 2-2
 - querying server events, 3-13
 - removing agents, 2-5
 - widgets. *See* widgets
 - web console accounts, 4-8
 - adding, 4-9
 - editing, 4-10
 - widgets, 3-5. *See also* dashboard
 - adding, 3-7
 - using, 3-6



TREND MICRO INCORPORATED

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

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

www.trendmicro.com

Item Code: SLEM26724/141016