TREND MICRO™

2.0

Trend Micro Safe Lock™ with Intelligent Manager

Service Pack 1

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

Document Part No.: SLEM27315/160128

Release Date: April 2016

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

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

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

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

Evaluate this documentation on the following site:

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

Table of Contents

Preface

Chapter 1: Introduction

Chapter 2: Working with Agents

Chapter 3: Monitoring Safe Lock

Chapter 4: Configuring Administration Settings

Chapter 5: Using the Agent Console

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

Chapter 7: Managing Agents Remotely

Chapter 8: Local Agent Installation

Chapter 9: Working with the Agent Configuration File

Chapter 10: Local Agent Uninstallation

Chapter 11: Troubleshooting & FAQs

Chapter 12: Technical Support

Chapter 13: Appendix: Reference

Index

Preface

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

Topics in this chapter include:

- *About the Documentation on page vii*
- *Audience on page viii*
- *Document Conventions on page viii*
- *Terminology on page ix*

About the Documentation

Trend Micro Safe Lock Intelligent Manager documentation includes the following:

TABLE 1. Trend Micro Safe Lock Intelligent Manager Documentation

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

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

http://docs.trendmicro.com

Audience

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

Document Conventions

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

TABLE 2. Document Conventions

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

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

Terminology

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

Table 3. Safe Lock Intelligent Manager Terminology

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

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

Chapter 1

Introduction

Trend Micro Safe Lock Intelligent Manager 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 1-8*

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, create initial agent Approved Lists, and change agent Application Lockdown states. Additionally, Safe Lock Intelligent Manager performs malware scans and administrators can view root cause information on files blocked from running by Safe Lock agents, reducing the time and effort needed to verify events and allowing quick responses to incidents.

What's New in This Version

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

Trend Micro Safe Lock Intelligent Manager 2.0 SP1 Features and Enhancements

Trend Micro Safe Lock Intelligent Manager 2.0 SP1 includes the following new features and enhancements.

Table 1-1. New Features

Feature	Description
Support for NAT agents	Support agents that are built under NAT-enabled routers.
Remote deployment of trusted applications	Deploy trusted applications remotely from the Safe Lock Intelligent Manager to multiple target endpoints using the hash values.
Remote patching with firewall settings enabled	Deploy patch to agents with the agent firewall settings enabled using the Remote Task Tool.

Feature	Description
Agent grouping	• Organize agents into groups and subgroups on the Agent Management console. • Configure Application Lockdown status or add files to the Approved List of the agents in user-selected groups.

Server Features and Benefits

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

Table 1-2. Features and Benefits

Feature	Benefit
Dashboard	The web console dashboard provides summarized information about monitored Safe Lock agents. Administrators can check deployed Safe Lock agent status easily, and can generate security reports related to Safe Lock agent activity for specified periods.
Quick Scan	Trend Micro Intelligent Manager provides malware scans of files blocked by application protection and sets actions for the affected files, such as delete, quarantine, or add to Approved List.
Centralized Agent Management	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 1-3. Required Software for Safe Lock Intelligent Manager

REQUIRED SOFTWARE	SPECIFICATIONS
Operating systems	• Windows XP SP2/SP3 (32-bit) • Windows 7 No-SP/SP1 (32-bit and 64-bit) • Windows 8 No-SP (32-bit and 64-bit) • Windows 8.1 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)	• Microsoft Internet Explorer 7 or later • The latest version of Google Chrome • The latest version of Mozilla Firefox

Note

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

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

REQUIRED HARDWARE	SPECIFICATION
RAM	• 2GB minimum • 4GB or more recommended
Processor	• 1 CPU core minimum • 1 CPU core or more recommended

Required Hardware	Specification
Available disk space	• 10GB minimum • 20GB or more recommended

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

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

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

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

Table 1-7. Required Hardware for Safe Lock Intelligent Manager (with or without Safe Lock agent) + SQL Server

Required Hardware	Specification
RAM	• 32GB or more required

Required Hardware	Specification
Processor	• 2 CPU cores minimum • 4 CPU cores or more recommended
Available disk space	• 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.	• admin
2	Use remote deployment tools (`SLrst.exe`) to centrally deploy agents from the server.	• N/A **Note** Using the `SLrst.exe` tool does not require specific account privileges, but does require the Safe Lock agent password to deploy tasks.
3	Use the Safe Lock Intelligent Manager console and remote deployment tools (`SLtasks.exe`) to manage the Approved List and Write Protection List on Safe Lock agents.	• admin • Full Control

	Task	Account Privilege Required
4	Monitor Server Event logs.	• admin • Full Control
5	Monitor Agent Event logs.	• admin • Full Control • Read Only
6	Download Trend Micro Safe Lock agent installer image.	• 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 SP1 Features and Enhancements

Trend Micro Safe Lock 2.0 SP1 includes the following new features and enhancements.

TABLE 1-8. New Features

FEATURE	DESCRIPTION
Support for NAT agents	Allows agents built under NAT-enabled routers to be identified and connect to the Intelligent Manager at a user-configurable frequency using the Setup.ini file.
Prescan	Allows Safe Lock to skip scanning compressed files and files that are larger than a specified size.
Approved List	Allows for adding applications from multiple folders to the Approved List in one operation.
Support for Windows Update	Allows Windows Update to run on endpoints where Application Lockdown is enabled by enabling this function through command line interface or the Setup.ini file.
Partial import of the configuration file	Import only the modified settings of a configuration file to update shared settings on multiple agents

Agent Features and Benefits

Trend Micro Safe Lock includes the following features and benefits.

Application Lockdown

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

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

Exploit Prevention

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

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

Easy Management

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

Small Footprint

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

Role Based Administration

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

Graphical and Command Line Interfaces

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

Trend Micro Portable Security Compatible

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

Safe Lock Requirements

This section introduces Safe Lock system requirements and upgrade limitations.

Hardware Requirements

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

Table 1-9. Required Hardware for Safe Lock

Hardware/Software	Description
Available disk space	200MB minimum 300MB recommended
Monitor resolution	640x480

Important

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

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

Operating Systems

Note

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

Table 1-10. 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 No-SP (32-bit and 64-bit)
	Windows 8.1 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 and 64-bit) **Note** Safe Lock does not support a custom action of “quarantine” on Windows XP or Windows 2003.
	Windows Server 2008 SP1/SP2 (32-bit and 64-bit)
	Windows Server 2008 R2 No-SP/SP1 (64-bit)
	Windows Server 2012 No-SP (64-bit)
	Windows Server 2012 R2 No-SP (64-bit)

Windows Version Type	Windows Version Name
Windows Embedded Standard	Windows (Standard) XP Embedded SP1*/SP2 (32-bit) **Note** *This version of Windows does not support DLL/Driver Lockdown, Integrity Monitoring, and the Predefined Trusted Updater. Safe Lock does not support a custom action of “quarantine” on Windows XP or Windows 2003.
	Windows Embedded Standard 2009 (32-bit)
	Windows Embedded Standard 7 (32-bit and 64-bit)
	Windows Embedded Standard 8 (32-bit and 64-bit)
	Windows Embedded Standard 8.1 (32-bit and 64-bit)
Windows Embedded POSReady	Windows Embedded POSReady (32-bit)
	Windows Embedded POSReady 2009 (32-bit)
	Windows Embedded POSReady 7 (32-bit and 64-bit)
Windows Embedded Enterprise	Windows Embedded Enterprise XP SP1*/SP2/SP3 (32-bit) **Note** *This version of Windows does not support DLL/Driver Lockdown, Integrity Monitoring, and the Predefined Trusted Updater. Safe Lock does not support a custom action of “quarantine” on Windows XP or Windows 2003.
	Windows Embedded Enterprise Vista (32-bit)
	Windows Embedded Enterprise 7 (32-bit and 64-bit)

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

Note

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

Agent Upgrade Preparation

WARNING!

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

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

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

Table 1-11. 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 **Note** Remote Safe Lock installations are possible with Safe Lock Intelligent Manager.	1.0	Manually uninstall	No settings retained
	1.1	Manually uninstall	No settings retained
	2.0 or later	Manually uninstall	No settings retained

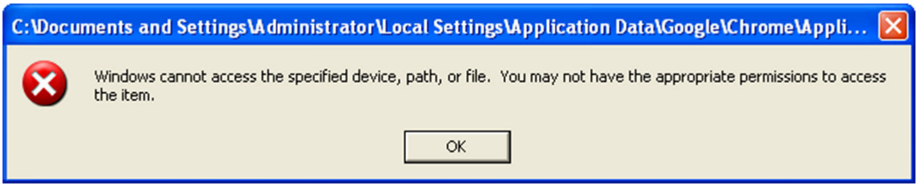
Agent Use Overview

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

Consider this typical use case scenario:

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

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



C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome\Appli...

Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item.

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*
- *Collecting Logs and Status on page 2-7*
- *Remotely Changing Application Lockdown Status on page 2-8*
- *Remotely Adding Trusted Applications and Files on page 2-8*

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 2-3*.

To display the status of each Safe Lock setting for a selected agent, see *Displaying Agent Status Details on page 2-4*.

To group agents, see *Grouping Agents on page 2-4*.

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

FUNCTION	DESCRIPTION
Group Agents	Group agents according to location, type, or purpose for more efficient management.
Remove	Remove groups, ungroup agents, or unregister agents from the Safe Lock Intelligent Manager server.
Send Command	Remotely collect logs and status, configure the Application Lockdown status, and add trusted files to the selected agents.
Collect Logs & Status	Collect logs and status to update the Safe Lock Intelligent Manager database with the latest information from the selected agents.
Configure Application Lockdown	Change the Application Lockdown status of agents.
Add Trusted Files	Allow trusted files to run on target agents.
Move	Move agents and groups to a selected location.

FUNCTION	DESCRIPTION
Edit Tags	Edit tags to help you identify and search for agents.
Clear Tags	Clear existing tags for the selected endpoints.
Export	Save data about selected endpoints as a CSV file.

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
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.

OPTION	DESCRIPTION
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, last log collection time, and pending commands for NAT agents. This screen also displays the status of specific Safe Lock features for the selected agent.

Important

Remote commands for managed NAT agents are only deployed at the specified connection frequency. To configure this setting, see *Installation Customization using a Setup.ini File on page 8-14*.

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.

Grouping Agents

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

Procedure

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

   The **Agent Management** screen appears.

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

   Note

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

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

   Tip

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

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**.

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 and Groups

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

Agents unregister from Safe Lock Intelligent Manager during uninstallation. However, if you are unable to uninstall an agent before removing it from the environment, the agent may continue to appear on the **Agent Management** screen. To remove the endpoints that Safe Lock Intelligent Manager no longer manages from the list of monitored agents, use the **Remove** feature to "unregister" the agents.

Note

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

Procedure

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

   The **Agent Management** screen appears.

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

3. Click **Remove**.

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

   Safe Lock Intelligent Manager removes the agents from the list.

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 **Send Command** and select **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.

Remotely Changing Application Lockdown Status

Note

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

Procedure

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

2. For a single agent, click the endpoint name to display agent status details, and then click the button to change the Application Lockdown status.

   - **Turn Application Lockdown On**

   - **Turn Application Lockdown Off**

3. For multiple agents and groups, select these items from the **Agent Management** table, click **Send Command**, select **Configure Application Lockdown**, and click the button to change the Application Lockdown status.

   - **Turn On**

   - **Turn Off**

Remotely Adding Trusted Applications and Files

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

Procedure

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

   The **Agent Management** screen appears.

2. Select one or more agents and groups.

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

   The **Add Trusted Files** screen appears.

4. Click **Download File Hash Generator** to download the tool for calculating hash values. For detailed steps, see *Calculating the Hash Values on page 2-9*.

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

6. Mark application installers in the Installer column.

   Note

   This allows the files created or modified by these installers to be automatically added to the Approved List on the selected endpoints.

Calculating the Hash Values

Use File Hash Generator to calculate hash values. To download this tool, see *Remotely Adding Trusted Applications and Files on page 2-8*.

Procedure

1. Execute WKFileHashGen.exe from the downloaded folder.

   The Trend Micro File Hash Generator screen appears.

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

   Note

   - To ensure that all necessary files are calculated for hash values, Trend Micro recommends adding the root folder of the wanted application to the File Hash Generator for calculation.

   - The **Add Folder** button will only calculate installer files, script files, and files in the Portable Executable format.

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

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

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

Chapter 3

Monitoring Safe Lock

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

Topics in this chapter include:

About the Dashboard

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

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

About Web Console Accounts and the Dashboard

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

Note

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

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

About Dashboard Tabs

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

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

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

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

Tip

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

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

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

Tip

Navigating to a different tab also stops the slide show.

About Default Tabs

The dashboard provides the following default tabs:

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

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

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

Widget	Description
Application Lockdown State	Displays the Application Lockdown status for agents.

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.

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

Configuring Tab Settings

Procedure

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

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

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	Move widgets on tabs by clicking and holding on the title bar at the top of the widget and dragging to various locations on a tab. **Tip** The layout for a tab determines where you can move a widget. As you drag, a red, dotted border appears when the widget is able to move to an area.

TASK	STEPS
Resize a widget	Horizontally resize a widget on a multi-column tab by doing the following: 1. Hover the pointer at the edge of a widget. A vertical, gray bar appears. 2. Drag the pointer left or right. Vertically resize widgets on a multi-column tab by enabling **Auto-fit** in the **Tab Settings**. This automatically adjusts widgets to be the same height as the widgets beside them.
Refresh widget data	Click the **Refresh** icon at the top of the widget.
Specify automatic refresh settings	1. Click the **More Options** icon at the top of the widget. 2. Select **Refresh Settings**. The **Refresh Settings** screen appears. 3. To enable automatic refresh for this widget, do the following: a. Select **Automatically refresh the widget**. b. Specify a frequency.
Rename a widget	1. Click the **More Options** icon at the top of the widget. 2. Select **Widget Settings**. The **Widget Settings** screen appears. 3. Type a meaningful title for the widget.
Close a widget	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: • Select a listed time range. • Specify a custom time range. a. Go to **Custom** in the list. b. Specify your custom time range. c. Click **Search**.
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	a. Select one of the following: • **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 `tmsllog.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: • Select a listed time range. • Specify a custom time range.

Option	Description
	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

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.

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`

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.

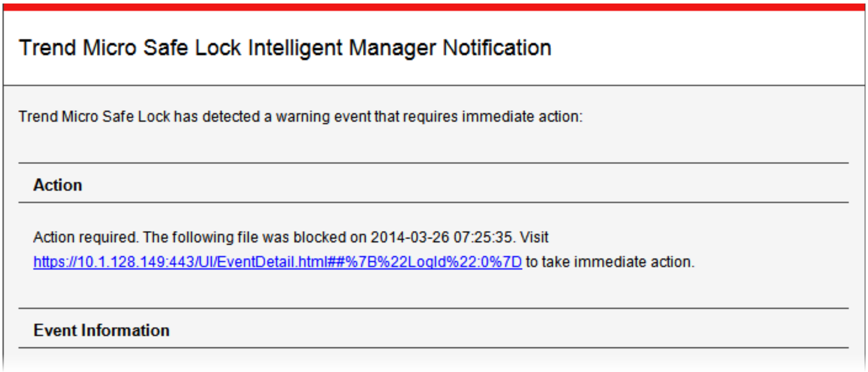
2. Select the appropriate download location for your environment:

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

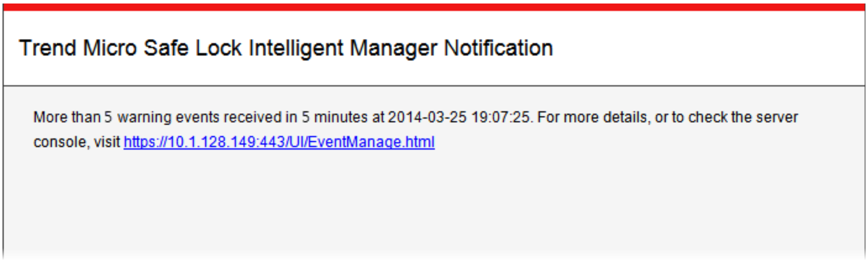
Trend Micro Safe Lock has detected a warning event that requires immediate action:

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%22LogId%22:0%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/EventManage.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:

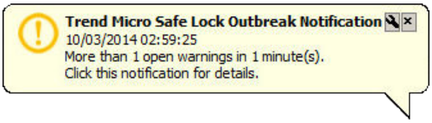
   a. Go to the **Outbreak** tab.

   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 on the physical Trend Micro Safe Lock Intelligent Manager server**.



Trend Micro Safe Lock Outbreak Notification
10/03/2014 02:59:25
More than 1 open warnings in 1 minute(s).
Click this notification for details.

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	• 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	• 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	• 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.

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

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

7. Optionally, type an account description.

   > Note
   >
   > The following characters are not supported:
   >
   > > < & " '

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

9. Specify the password.

   > Note
   >
   > The password must be 8 to 64 alphanumeric characters. The following characters are not supported:
   >
   > | > " : < \ spaces

Editing Accounts

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

Procedure

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

   The **Account Management** screen appears.

2. Click the user name of the account.

   The **Edit User** screen appears.

3. Modify settings.

Configuring Proxy Settings

Procedure

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

   The **Proxy Settings** screen appears.

2. To configure proxy settings for updates:

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

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

   c. Specify the port.

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

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

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

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

c. Specify the port.

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

Tip

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

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

About the License Management Screen

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

The following details appear on this screen:

ITEM	DESCRIPTION
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:

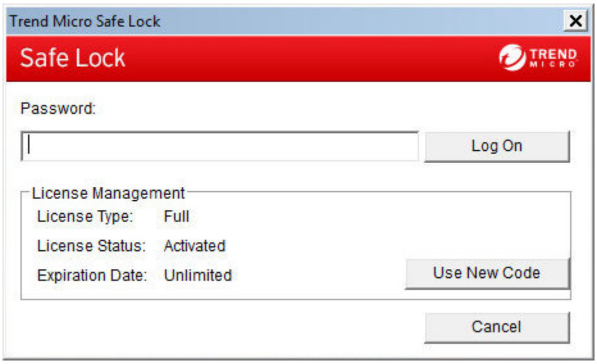
Setting Up the Approved List

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.



Trend Micro Safe Lock

Safe Lock

Password:

License Management

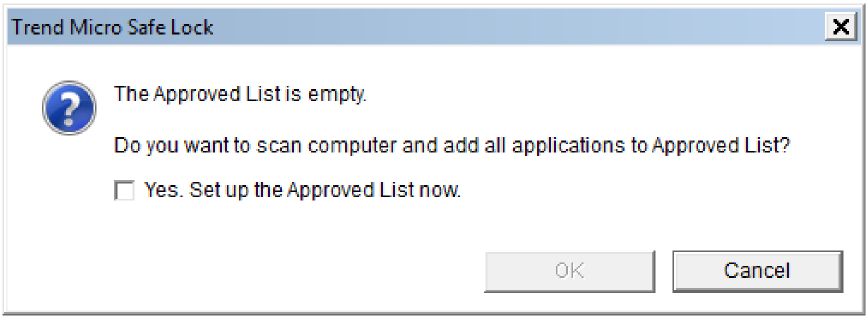
License Type: Full

License Status: Activated

Expiration Date: Unlimited

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

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



Trend Micro Safe Lock

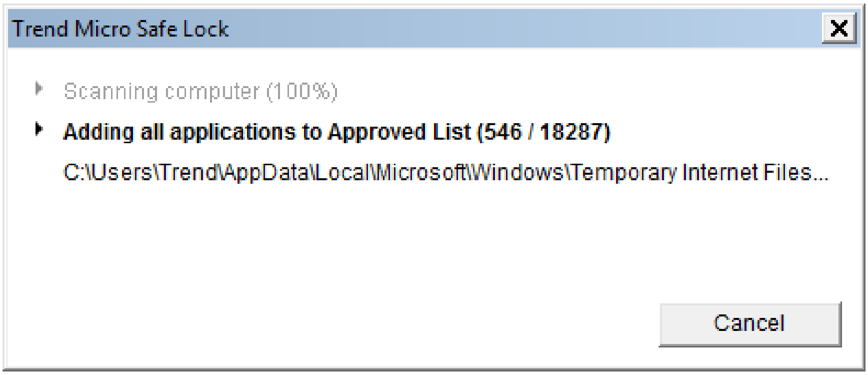
The Approved List is empty.

Do you want to scan computer and add all applications to Approved List?

□ Yes. 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.



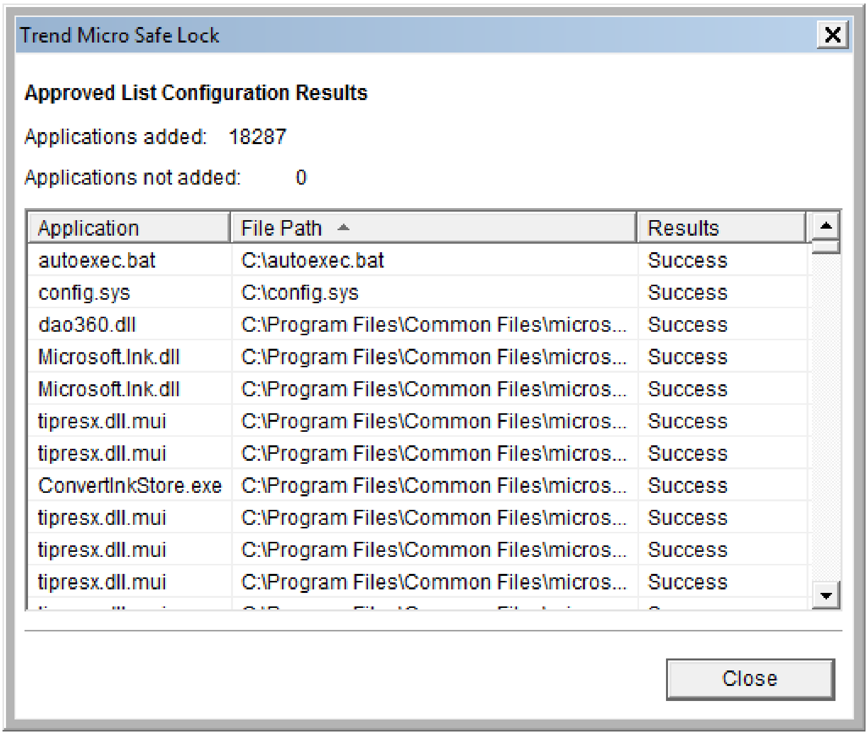
Trend Micro Safe Lock

Scanning computer (100%)

Adding all applications to Approved List (546 / 18287)

C:\Users\Trend\AppData\Local\Microsoft\Windows\Temporary Internet Files...

Safe Lock displays the Approved List Configuration Results.



Approved List Configuration Results

Applications added: 18287

Applications not added: 0

Application	File Path	Results
autoexec.bat	C:\autoexec.bat	Success
config.sys	C:\config.sys	Success
dao360.dll	C:\Program Files\Common Files\micros...	Success
Microsoft.Ink.dll	C:\Program Files\Common Files\micros...	Success
Microsoft.Ink.dll	C:\Program Files\Common Files\micros...	Success
tipresx.dll.mui	C:\Program Files\Common Files\micros...	Success
tipresx.dll.mui	C:\Program Files\Common Files\micros...	Success
ConvertInkStore.exe	C:\Program Files\Common Files\micros...	Success
tipresx.dll.mui	C:\Program Files\Common Files\micros...	Success
tipresx.dll.mui	C:\Program Files\Common Files\micros...	Success
tipresx.dll.mui	C:\Program Files\Common Files\micros...	Success

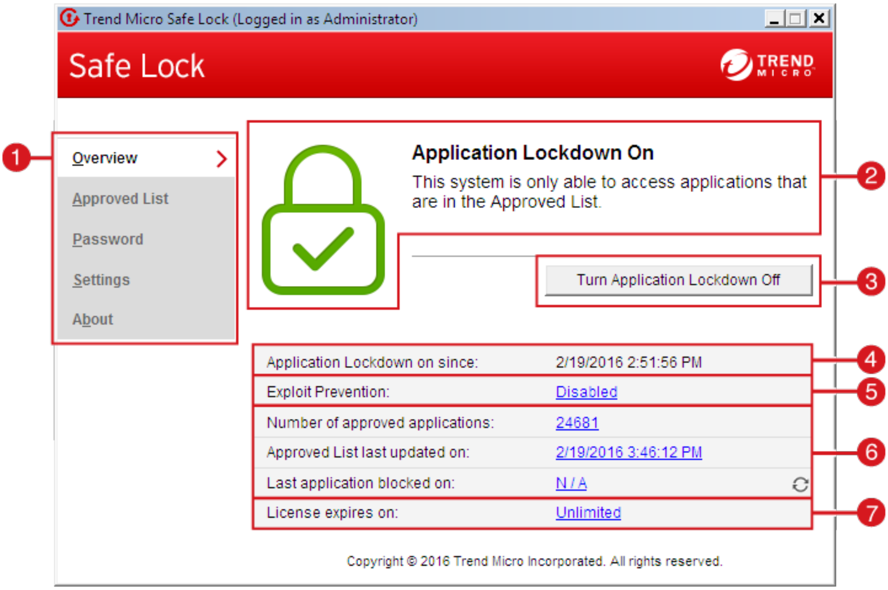
Note

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.


Trend Micro Safe Lock (Logged in as Administrator)
Safe Lock
TREND MICRO
Overview
Approved List
Password
Settings
About
Turn Application Lockdown Off
1
2
3
4
5
6
7

Application Lockdown On

This system is only able to access applications that are in the Approved List.

Application Lockdown on since:	2/19/2016 2:51:56 PM
Exploit Prevention:	Disabled
Number of approved applications:	24681
Approved List last updated on:	2/19/2016 3:46:12 PM
Last application blocked on:	N / A
License expires on:	Unlimited

Copyright © 2016 Trend Micro Incorporated. All rights reserved.

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 **Note** After disabling Lockdown mode, Safe Lock Intelligent Manager switches to a “monitor” mode. Safe Lock Intelligent Manager does not block any applications from running, but logs when applications that are not in the Approved List run. You can use these logs to assess if the Approved List contains all the applications required on the endpoint.
4	**Application Lockdown on since**	The date and time that Application Lockdown was last turned on
	Application Lockdown off since	The date and time that Application Lockdown was last turned off

#	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.

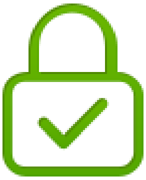
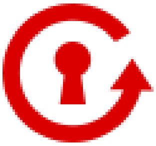
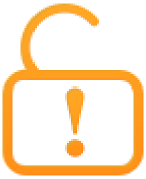
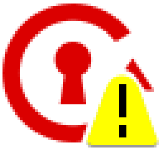
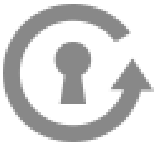
About Status Icons

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

Note

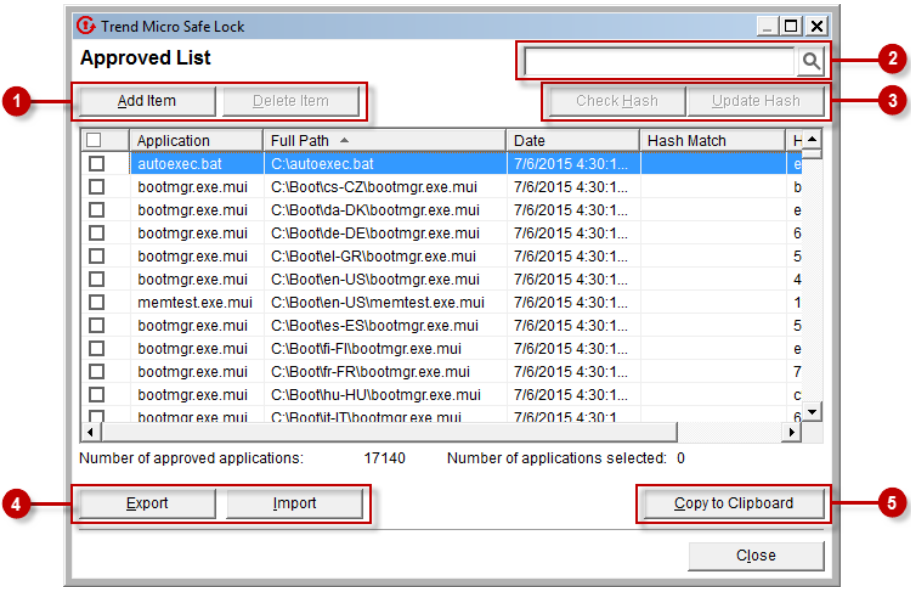
System Tray icons display if they were enabled during installation.

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.



□	Application	Full Path	Date	Hash Match	H
□	autoexec.bat	C:\autoexec.bat	7/6/2015 4:30:1...		e
□	bootmgr.exe.mui	C:\Boot\cs-CZ\bootmgr.exe.mui	7/6/2015 4:30:1...		b
□	bootmgr.exe.mui	C:\Boot\da-DK\bootmgr.exe.mui	7/6/2015 4:30:1...		e
□	bootmgr.exe.mui	C:\Boot\de-DE\bootmgr.exe.mui	7/6/2015 4:30:1...		6
□	bootmgr.exe.mui	C:\Boot\el-GR\bootmgr.exe.mui	7/6/2015 4:30:1...		5
□	bootmgr.exe.mui	C:\Boot\en-US\bootmgr.exe.mui	7/6/2015 4:30:1...		4
□	memtest.exe.mui	C:\Boot\en-US\memtest.exe.mui	7/6/2015 4:30:1...		1
□	bootmgr.exe.mui	C:\Boot\es-ES\bootmgr.exe.mui	7/6/2015 4:30:1...		5
□	bootmgr.exe.mui	C:\Boot\fi-FI\bootmgr.exe.mui	7/6/2015 4:30:1...		e
□	bootmgr.exe.mui	C:\Boot\fr-FR\bootmgr.exe.mui	7/6/2015 4:30:1...		7
□	bootmgr.exe.mui	C:\Boot\hu-HU\bootmgr.exe.mui	7/6/2015 4:30:1...		c
□	bootmgr.exe.mui	C:\Boot\it-IT\bootmgr.exe.mui	7/6/2015 4:30:1		6

Number of approved applications: 17140 Number of applications selected: 0

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.
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	Choose this option when the software already exists on the endpoint and is up-to-date. Adding a file grants permission to run the file, but does not alter the file or the system. For example, if Windows Media Player (`wmplayer.exe`) is not in the Approved List after initial setup, users can add it to the list using the console.
Automatically add files created or modified by the selected application installer (Trusted Updater)	Choose this option to open the Trusted Updater when updating the endpoint or installing new software. For example, if Mozilla Firefox needs to be installed or updated, use the Trusted Updater. Trend Micro Safe Lock Intelligent Manager adds or updates any files modified by an installer to the Approved List.

Adding or Removing Files

Procedure

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

   To add an item:

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

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

      A selection window appears.

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

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

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

   To remove an item:

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

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

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

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

Updating or Installing Using the Trusted Updater

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

Procedure

1. Open the Trend Micro Safe Lock console using the desktop icon (if available) or the **Start** menu by clicking **All Programs** > **Trend Micro Safe Lock**.
2. Provide the password and click **Login**.
3. Click the **Approved List** menu item to open the list.
4. To install or update an application, select the installer that the Trusted Updater should temporarily allow to run:

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

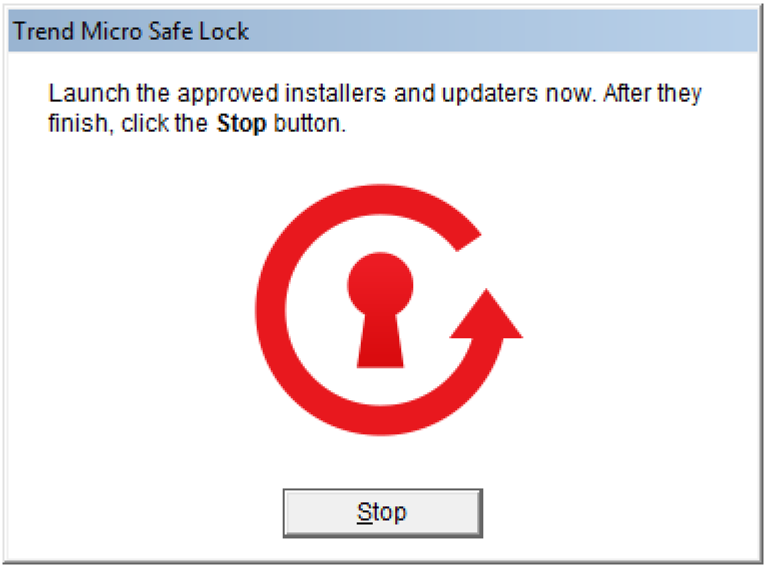
    b. In the window that opens, choose **File**, **Folder**, or **Folder and sub folders** from the drop-down list.

    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.



Trend Micro Safe Lock

Launch the approved installers and updaters now. After they finish, click the **Stop** button.

FIGURE 5-3. The Safe Lock Trusted Updater

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

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

Exporting or Importing the Approved List

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

WARNING!

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

Procedure

1. Open the Trend Micro Safe Lock console using the desktop icon (if available) or the **Start** menu by clicking **All Programs** > **Trend Micro Safe Lock**.

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

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

   To export the Approved List:

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

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

   To import an Approved List:

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

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

Account Types

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

ACCOUNT	DETAILS
Restricted User	• Secondary maintenance account • Limited access to Safe Lock functions • Can only use the console

To enable the Restricted User account, see *Configuring Passwords on page 5-16* . 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.

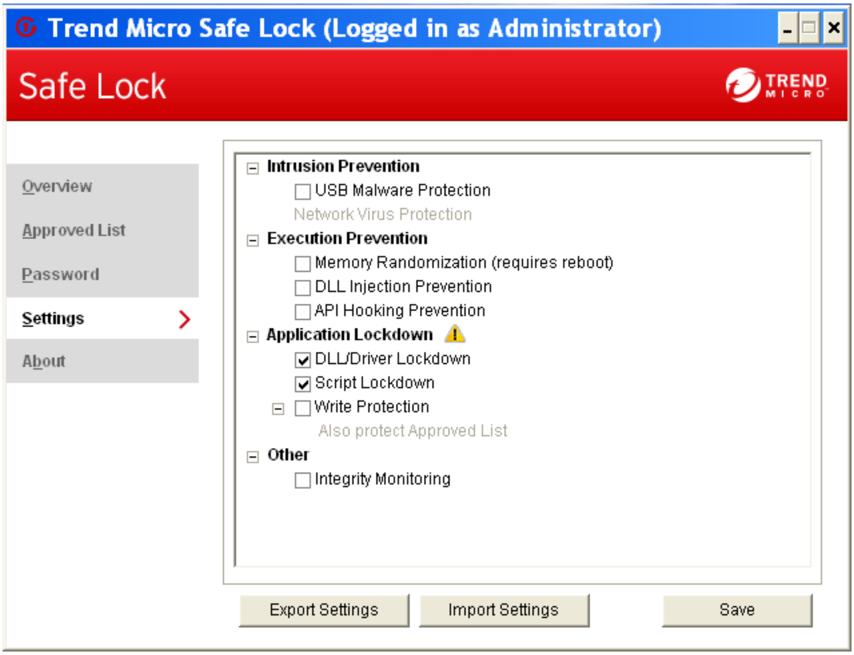
c. Specify and confirm the password, and click **Save**.

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.



⊟ **Intrusion Prevention**
- □ USB Malware Protection
- Network Virus Protection

⊟ **Execution Prevention**
- □ Memory Randomization (requires reboot)
- □ DLL Injection Prevention
- □ API Hooking Prevention

⊟ **Application Lockdown** ⚠
- ☑ DLL/Driver Lockdown
- ☑ Script Lockdown
- ⊟ □ Write Protection
  - Also protect Approved List

⊟ **Other**
- □ Integrity Monitoring

FIGURE 5-4. Safe Lock settings screen

TABLE 5-7. Intrusion Prevention

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

TABLE 5-8. Execution Prevention

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

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

TABLE 5-9. 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.
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 the **DLL/Driver Lockdown** and **Script Lockdown** features of the Exploit Prevention settings. If Network Virus Protection was not included in the initial installation, it cannot be selected. Reinstall Trend Micro Safe Lock if Network Virus Protection is not available.

Procedure

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

Chapter 6

Using the Agent Command Line Interface (CLI)

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

Topics in this chapter include:

Using SLCmd at the Command Line Interface (CLI)

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	SLCmd Program at the Command Line Interface (CLI)	Console
Export/Import Approved List	Yes	Yes
Export/Import configuration	Yes	Yes
Install	Yes	Yes
Windows Update Support	Yes	No
Application Lockdown	Yes	Yes
Write Protection	Yes	Yes
Write Protection Exceptions	Yes	No
Integrity Monitoring	Yes	Yes
Exception Paths	Yes	No
License Management	Yes	Yes
Settings	Limited	Limited
Start/Stop Trusted Updater	Yes	Yes
Trusted Hash List	Yes	No
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.

SLCmd Program Commands

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

Note

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

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

General Commands

Perform general actions using the Command Line Interface.

The following table lists the available abbreviated forms of parameters.

Table 6-2. Abbreviations and Uses

Parameter	Abbreviation	Use
`adminpassword`	`ap`	Manage the Safe Lock admistrator password
`lock`	`lo`	Manage Application Lockdown status
`blockedlog`	`bl`	Manage the applications blocked by Safe Lock
`license`	`lc`	Manage the Safe Lock license
`settings`	`set`	Manage the Safe Lock settings
`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: `SLCmd.exe help`
`activate`		<activation_code>	Activate the Safe Lock program using the specified Activation Code For example, type: `SLCmd.exe activate XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX`
`set`	`adminpassword`	<new_password>	Change the currently logged on administrator password to the newly specified password For example, type: `SLCmd.exe -p <admin_password> set adminpassword P@ssW0Rd`
			Prompt the currently logged on administrator to specify a new password For example, type: `SLCmd.exe -p <admin_password> set adminpassword`
`set`	`lock`	`enable`	Turn on Application Lockdown For example, type: `SLCmd.exe -p <admin_password> set lock enable`
		`disable`	Turn off Application Lockdown For example, type:

COMMAND	PARAMETER	VALUE	DESCRIPTION
			`SLCmd.exe -p <admin_password> set lock disable`
			Display the current Safe Lock Application Lockdown status For example, type: **`SLCmd.exe -p <admin_password> set lock`**
`show`	`blockedlog`		Display a list of applications blocked by Safe Lock For example, type: **`SLCmd.exe -p <admin_password> show blockedlog`**
`show`	`license`		Display the current Safe Lock license information For example, type: **`SLCmd.exe show license`**
`show`	`settings`		Display the current status of the vulnerability attack prevention features For example, type: **`SLCmd.exe -p <admin_password> show settings`**
`start`	`service`		Start the Safe Lock service For example, type: **`SLCmd.exe start service`**
`status`			Display the current status of Application Lockdown and the auto update function of the Approved List For example, type:

Command	Parameter	Value	Description
			SLCmd.exe -p <admin_password> status
stop	service		Stop the Safe Lock service For example, type: **SLCmd.exe -p <admin_password> stop service**
version			Display the current versions of Safe Lock components For example, type: **SLCmd.exe -p <admin_password> version**

Central Management Commands

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

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

The following table lists the available abbreviated forms of parameters.

Table 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_output_file>	Encrypt the configuration file used by Managed Mode
export	managedmodeconfiguration	<path_of_encrypted_output>	Export the encrypted configuration file used by Managed Mode
	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

Command	Parameter	Value	Description
			Note Using the optional `-cfg` value specifies the path of the configuration file. Using the optional `-sc` value specifies the path of the certificate file.
`set`	`managedmode`		Display the current Managed Mode status
`show`	`managedmodeconfiguration`		Display the configuration used by Managed Mode
`test`	`managedmode`		Connect a test Managed Mode session with Safe Lock Intelligent Manager

Optional Feature Commands

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

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

The following table lists the available abbreviated forms of parameters.

Table 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

Parameter	Abbreviation	Use
`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: **`SLCmd.exe -p <admin_password> set usbmalwareprotection enable`**
		`disable`	Disable USB Malware Protection For example, type: **`SLCmd.exe -p <admin_password> set usbmalwareprotection disable`**
			Display the current status of USB Malware Protection

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

Command	Parameter	Value	Description
			For example, type: `SLCmd.exe -p <admin_password> set memoryrandomization`
set	dllinjectionprevention	enable	Enable DLL Injection Prevention For example, type: `SLCmd.exe -p <admin_password> set dllinjectionprevention enable`
		disable	Disable DLL Injection Prevention For example, type: `SLCmd.exe -p <admin_password> set dllinjectionprevention disable`
			Display the current status of DLL Injection Prevention For example, type: `SLCmd.exe -p <admin_password> set dllinjectionprevention`
set	apihookingprevention	enable	Enable API Hooking Prevention For example, type: `SLCmd.exe -p <admin_password> set apihookingprevention enable`
		disable	Disable API Hooking Prevention For example, type: `SLCmd.exe -p <admin_password> set apihookingprevention disable`
			Display the current status of API Hooking Prevention

Command	Parameter	Value	Description
			For example, type: **SLCmd.exe -p <admin_password> set apihookingprevention**
set	dlldriverlockdown	enable	Enable DLL/Driver Lockdown For example, type: **SLCmd.exe -p <admin_password> set dlldriverlockdown enable**
		disable	Disable DLL/Driver Lockdown For example, type: **SLCmd.exe -p <admin_password> set dlldriverlockdown disable**
			Display the current status of DLL/ Driver Lockdown For example, type: **SLCmd.exe -p <admin_password> set dlldriverlockdown**
set	script	enable	Enable Script Lockdown For example, type: **SLCmd.exe -p <admin_password> set script enable**
		disable	Disable Script Lockdown For example, type: **SLCmd.exe -p <admin_password> set script disable**
			Display the current status of Script Lockdown For example, type:

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

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

Command	Parameter	Value	Description
			• Process launch • DLL loading • Script file access **Note** Safe Lock does not support a custom action of “quarantine” on Windows XP or Windows 2003.
		`ask`	Ask what to do for blocked files or processes when Application Lockdown blocks any of the following events: • Process launch • DLL loading • 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: **`SLCmd.exe -p <admin_password> set user enable`**
		`disable`	Disable the Restricted User account For example, type: **`SLCmd.exe -p <admin_password> set user disable`**
			Display the the Restricted User account status For example, type: **`SLCmd.exe -p <admin_password> set user`**
`set`	`userpassword`	<new_password>	Change the Restricted User account password to the newly specified password For example, type: **`SLCmd.exe -p <admin_password> set userpassword P@ssW0Rd`**

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

Script Commands

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

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

The following table lists the available abbreviated forms of parameters.

TABLE 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 `JSP` with the interpreter file `jscript.js`, type:

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

Approved List Commands

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

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

The following table lists the available abbreviated forms of parameters.

Table 6-12. Abbreviations and Uses

Parameter	Abbreviation	Use
`approvedlist`	`al`	Manage files in the Approved List
`list`	`li`	Manage the Approved List import and export functions

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

Table 6-13. Approved List Commands

Command	Parameter	Value	Description
`add`	`approvedlist`	[`-r`] <file_or_folder_path>	Add the specified file to the Approved List For example, to add all Microsoft Office files to the Approved List, type: **`SLCmd.exe -p <admin_password> add approvedlist -r "C:\Program Files\Microsoft Office"`** **Note** Using the optional `-r` value includes the specified folder and related subfolders.
`remove`	`approvedlist`	<file_path>	Remove the specified file from the Approved List For example, to remove `notepad.exe` from the Approved List, type: **`SLCmd.exe -p <admin_password> remove approvedlist C:\Windows\notepad.exe`**

Command	Parameter	Value	Description
show	approvedlist		Display the files in the Approved List For example, type: **SLCmd.exe -p <admin_password> show approvedlist**
check	approvedlist	-f	Update the hash values in the Approved List and displays detailed results For example, type: **SLCmd.exe -p <admin_password> check approvedlist -f**
		-q	Update the hash values in the Approved List and displays summarized results For example, type: **SLCmd.exe -p <admin_password> check approvedlist -q**
		-v	Compare the hash values in the Approved List with the hash values calculated from the actual files and prompts the user after detecting mismatched values For example, type: **SLCmd.exe -p <admin_password> check approvedlist -v**
export	list	<output_file>	Export the Approved List to the file path and file name specified For example, type: **SLCmd.exe -p <admin_password> export list c:\approvedlist\ap.db**

Command	Parameter	Value	Description
			Note The output file type must be `DB` format.
`import`	`list`	[-o] <input_file>	Import an Approved List from the file path and file name specified For example, type: **`SLCmd.exe -p <admin_password> import list c:\approvedlist\ap.db`** **Note** The input file type must be `DB` format. Using the optional `-o` value overwrites the existing list.

Application Lockdown Commands

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

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

The following table lists the available abbreviated forms of parameters.

Table 6-14. Abbreviations and Uses

Parameter	Abbreviation	Use
`quarantinedfile`	`qf`	Manage quarantined files
`exceptionpath`	`ep`	Manage exceptions to Application Lockdown

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

Table 6-15. Application Lockdown Commands

Command	Parameter	Value	Description
`show`	`quarantinedfile`		Display a list of quarantined files
`restore`	`quarantinedfile`	<id> [`-al`] [`-f`]	Restore the specified file from quarantine Using the optional `-al` value also adds the restored file to Approved List. Using the optional `-f` value forces the restore.
`remove`	`quarantinedfile`	<id>	Delete the specified file
`show`	`exceptionpath`		Display current exceptions to Application Lockdown
`add`	`exceptionpath`	`-e` <file_path>`-t file`	Add an exception for the specified file
		`-e` <folder_path>`-t folder`	Add an exception for the specified folder
		`-e` <folder_path>`-t folderandsub`	Add an exception for the specified folder and related subfolders
`remove`	`exceptionpath`	`-e` <file_path>`-t file`	Remove an exception for the specified file **Note** Specify the exact <file_path> originally specified in the corresponding add command.

Command	Parameter	Value	Description
		-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.
		-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

Parameter	Abbreviation	Use
`writeprotection-folder`	`wpfo`	Manage folders in the Write Protection List
`writeprotection-regvalue`	`wprv`	Manage registry values and associated registry keys in the Write Protection List
`writeprotection-regkey`	`wprk`	Manage registry keys in the Write Protection List
`writeprotection-file-exception`	`wpfie`	Manage files in the Write Protection Exception List
`writeprotection-folder-exception`	`wpfoe`	Manage folders in the Write Protection Exception List
`writeprotection-regvalue-exception`	`wprve`	Manage registry values and associated registry keys in the Write Protection Exception List
`writeprotection-regkey-exception`	`wprke`	Manage registry keys in the Write Protection Exception List

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

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

Command	Parameter	Value	Description
`show`	`writeprotection`		Display the entire Write Protection List
	`writeprotection-file`		Display the files in the Write Protection List For example, type: **`SLCmd.exe -p <admin_password> show writeprotection-file`**
	`writeprotection-file-exception`		Display the files in the Write Protection Exception List For example, type:

Command	Parameter	Value	Description
			`SLCmd.exe -p <admin_password> show writeprotection-file-exception`
	`writeprotection-folder`		Display the folders in the Write Protection List For example, type: **`SLCmd.exe -p <admin_password> show writeprotection-folder`**
	`writeprotection-folder-exception`		Display the folders in the Write Protection Exception List For example, type: **`SLCmd.exe -p <admin_password> show writeprotection-folder-exception`**
`add`	`writeprotection-file`	<file_path>	Add the specified file to the Write Protection List For example, type: **`SLCmd.exe -p <admin_password> add writeprotection-file archive.txt`** **Note** The <file_path> value pattern matches from the end of the path toward the beginning of the path. For example, specifying `userfile.txt` matches `c:\Windows\userfile.txt` and `c:\Temp\userfile.txt`.
	`writeprotection-file-exception`	`-t` <file_path> `-p`	Add the specified file and a specific process path for that file to the Write Protection Exception List

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

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

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

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

Command	Parameter	Value	Description
		`-p` <process_path>	Add processes run from the specified paths to the Write Protection Exception List For example, to add write access by a process named `notepad.exe` to any folder, type: **`SLCmd.exe -p <admin_password> add writeprotection-folder-exception -p c:\Windows\notepad.exe`** **Note** The `-p` value pattern matches from the end of the process path toward the beginning of the path. For example, specifying `notepad.exe` matches `c:\Windows\notepad.exe` and `c:\Temp\notepad.exe`.
`remove`	`writeprotection-file`	<file_path>	Remove the specified file from the Write Protection List For example, type: **`SLCmd.exe -p <admin_password> remove writeprotection-file archive.txt`** **Note** Specify the exact <file_path> originally specified in the corresponding add command.
	`writeprotection-file-exception`	`-t` <file_path> `-p`	Remove the specified file and process path from the Write Protection Exception List

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

Command	Parameter	Value	Description
			Note The -p value pattern matches from the end of the process path toward the beginning of the path. For example, specifying `notepad.exe` matches `c:\Windows\notepad.exe` and `c:\Temp\notepad.exe`.
	`writeprotection-folder`	[-r] <folder_path>	Remove the specified folder(s) from the Write Protection List For example, type: **`SLCmd.exe -p <admin_password> remove writeprotection-folder -r c:\Windows`** **Note** Using the optional -r value includes the specified folder and related subfolders. Specify the exact <folder_path> and -r value originally specified in the corresponding add command.
	`writeprotection-folder-exception`	[-r] -t <folder_path> -p <process_path>	Remove the specified folder and process path from the Write Protection Exception List For example, type: **`SLCmd.exe -p <admin_password> remove writeprotection-folder-exception -r -t c:\Windows\System32\Temp -p c:\Windows\notepad.exe`**

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

Command	Parameter	Value	Description
			`exception -p c:\Windows\System32` **Note** The `-p` value pattern matches from the end of the process path toward the beginning of the path. For example, specifying `notepad.exe` matches `c:\Windows\notepad.exe` and `c:\Temp\notepad.exe`.

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

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

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

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

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

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

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

Command	Parameter	Value	Description
		`-p <process_path>`	Remove the specified process path from the Write Protection Exception List **Note** The `-p` value pattern matches from the end of the path toward the beginning of the path.

Trusted Certification Commands

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

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

The following table lists the available abbreviated forms of parameters.

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

Trusted Hash List Commands

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

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

The following table lists the available abbreviated forms of parameters.

Table 6-21. Abbreviations and Uses

Parameter	Abbreviation	Use
trustedhash	th	Manage trusted hash values (files) added by the Safe Lock Intelligent Manager administrator.

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

TABLE 6-22. Trusted Hash List Commands

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

Command	Parameter	Value	Description
			Using the optional `-t` value specifies a file path to check for the hash value **Note** The `-t` value pattern matches from the end of the path toward the beginning of the path. For example, specifying `userfile.txt` matches `c:\Windows\userfile.txt` and `c:\Temp\userfile.txt`. Using the optional `-n` value adds a note for the file hash
`remove`	`trustedhash`	`-l` <label>	Remove a file from the Trusted Hash List by specifying its label
`remove`	`trustedhash`	`-a`	Remove all the hash values in the Trusted Hash List

Trusted Updater Commands

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 6-23. Abbreviations and Uses

Parameter	Abbreviation	Use
`trustedupdater`	`tu`	Manage the Predefined Trusted Updater tool process

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

Table 6-24. Trusted Updater Commands

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

Command	Parameter	Value	Description
			`SLCmd.exe -p <admin_password> stop trustedupdater -f`

Predefined Trusted Updater Commands

Important

The `add` command for adding files to the Predefined Trusted Updater List follows a different format than the general commands specified in the Predefined Trusted Updater Commands table. For details on adding files to the Predefined Trusted Updater List, see *Predefined Trusted Updater "Add" Command on page 6-49*.

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 6-25. Abbreviations and Uses

Parameter	Abbreviation	Use
`predefinedtrustedupdater`	`ptu`	Manage files in the Predefined Trusted Updater Lists

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

Table 6-26. Predefined Trusted Updater Commands

Command	Parameter	Value	Description
add	`predefinedtrustedupdater`	`-e` <folder_or_file_exception>	Add the specified file or folder to the Predefined Trusted Updater Exception List

COMMAND	PARAMETER	VALUE	DESCRIPTION
			Important The `add` command for adding files to the Predefined Trusted Updater List follows a different format than the other commands specified in the this list. For details on adding files to the Predefined Trusted Updater List (not the Predefined Trusted Updater Exception List), see *Predefined Trusted Updater "Add" Command on page 6-49*. For example, to add `notepad.exe` to the Predefined Trusted Updater Exception List, type: **`SLCmd.exe -p <admin_password> add predefinedtrustedupdater -e C:\Windows\notepad.exe`**
`decrypt`	`predefinedtrustedupdater`	<path_of_encrypted_file> <path_of_decrypted_output_file>	Decrypt a file to the specified location For example, to decrypt `C:\Notepad.xen` to `C:\Editors\notepad.exe`, type: **`SLCmd.exe -p <admin_password> decrypt predefinedtrustedupdater C:\Notepad.xen C:\Editors\notepad.exe`**
`encrypt`	`predefinedtrustedupdater`	<path_of_file> <path_of_encrypted	Encrypt a file to the specified location For example, to encrypt `C:\notepad.exe` to `C:\Editors\Notepad.xen`, type:

Command	Parameter	Value	Description
		_output_file>	**`SLCmd.exe -p <admin_password> encrypt predefinedtrustedupdater C:\Editors\notepad.exe C:\Notepad.xen`**
`export`	`predefinedtrustedupdater`	<path_of_encrypted_output>	Export the Predefined Trusted Updater List to the specified encrypted file For example, type: **`SLCmd.exe -p <admin_password> export predefinedtrustedupdater C:\Lists\ptu_list.xen`**
`import`	`predefinedtrustedupdater`	<path_of_encrypted_input>	Import a Predefined Trusted Updater List from the specified encrypted file For example, type: **`SLCmd.exe -p <admin_password> import predefinedtrustedupdater C:\Lists\ptu_list.xen`**
`remove`	`predefinedtrustedupdater`	`-l` <label_name>	Remove the specified labeled rule from the Predefined Trusted Updater List For example, to remove the “Notepad” rule, type: **`SLCmd.exe -p <admin_password> remove predefinedtrustedupdater -l Notepad`**
		`-e` <folder_or_file_exception>	Remove the specified exception from the Predefined Trusted Updater Exception List For example, to remove the `notepad.exe` exception, type:

Command	Parameter	Value	Description
			SLCmd.exe -p <admin_password> remove predefinedtrustedupdater -e C:\Windows\notepad.exe
set	predefinedtrustedupdater	enable	Enable the Predefined Trusted Updater List
		disable	Disable the Predefined Trusted Updater List
show	predefinedtrustedupdater		Display the files in the Predefined Trusted Updater List For example, type: **SLCmd.exe -p <admin_password> show predefinedtrustedupdater**
		-e	Display the files in the Predefined Trusted Updater Exception List For example, type: **SLCmd.exe -p <admin_password> show predefinedtrustedupdater -e**

Predefined Trusted Updater "Add" Command

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

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

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

TABLE 6-27. Predefined Trusted Updater "Add" Command

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

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

TABLE 6-28. Predefined Trusted Updater "Add" Additional Values

<table>
<tr><th>VALUE</th><th>REQUIRED / OPTIONAL</th><th colspan="2">DESCRIPTION</th><th>EXAMPLE</th></tr>
<tr><td><code>-u</code> &lt;folder_or_file&gt;</td><td>Required</td><td colspan="2">Add the specified file or folder to the Predefined Trusted Updater List</td><td>N/A
<b>Note</b>
This parameter requires the use of the <code>-t</code> &lt;type_of_object> value.</td></tr>
<tr><td rowspan="3"><code>-t</code> &lt;type_of_object&gt;</td><td rowspan="3">Required</td><td colspan="2">Specify the type of object to add to the Predefined Trusted Updater List located in <code>-u</code> &lt;folder_or_file>
Available objects types are as follows:</td><td rowspan="3"><b><code>SLCmd.exe -p <admin_password> add predefinedtrustedupdater -u C:\Windows\notepad.exe -t process</code></b></td></tr>
<tr><td>process</td><td>Indicates only <code>EXE</code> file types</td></tr>
<tr><td>file</td><td>Indicates only <code>MSI</code> and <code>BAT</code> file types</td></tr>
</table>

Value	Required / Optional	Description	Example
		folder: Indicates all EXE, MSI, and BAT files in the specified folder folderandsub: Indicates all EXE, MSI, and BAT files in the specified folder and related subfolders	
-p <parent_process>	Optional	Add the full file path to the specified parent process used to invoke the file(s) specified in -u <folder_or_file>	**SLCmd.exe -p <admin_password> add predefinedtrustedupdater -u C:\Windows\notepad.exe -t process -p C:\batch files\note.bat**
-l <label_name>	Optional	Specify a label name for the file(s) specified in -u <folder_or_file> **Note** When left blank, Safe Lock assigns an arbitrary label name.	**SLCmd.exe -p <admin_password> add predefinedtrustedupdater -u C:\Windows\notepad.exe -t process -l EDITOR**
-al enable	Optional	Compare the hash values in the Approved List with the hash values calculated from the actual files **Note** Enabled by default even when -al is not specified.	**SLCmd.exe -p <admin_password> add predefinedtrustedupdater -u C:\Windows\notepad.exe -t process -al enable**
-al disable	Optional	Do not compare the hash values in the Approved List with the hash	**SLCmd.exe -p <admin_password> add**

Value	Required / Optional	Description	Example
		values calculated from the actual files	**predefinedtrustedupdater -u C:\Windows \notepad.exe -t process -al disable**

Windows Update Support

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

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

The following table lists the available abbreviated forms of parameters.

Table 6-29. Abbreviations and Uses

Parameter	Abbreviation	Use
windowsupdatesupport	wus	Allow Windows Update to run on the agent with the Application Lockdown on.

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

Table 6-30. Windows Update Support Commands

Command	Parameter	Value	Description
set	windowsupdatesupport	enable	Enable Windows Update Support
		disable	Disable Windows Update Support
			Display current setting for Windows Update Support

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 6-31. Abbreviations and Uses

Parameter	Abbreviation	Use
`configuration`	`con`	Manage the configuration file

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

Table 6-32. 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: **`SLCmd.exe -p <admin_password> decrypt configuration C:\config.xen C:\config.xml`**
`encrypt`	`configuration`	<path_of_file> <path_of_encrypted_output_file>	Encrypts a configuration file to the specified location For example, to encrypt `C:\config.xml` to `C:\config.xen`, type: **`SLCmd.exe -p <admin_password> encrypt configuration C:\config.xml C:\config.xen`**

Command	Parameter	Value	Description
`export`	`configuration`	<path_of_encrypted_output>	Export the configuration file to the specified location For example, type: **`SLCmd.exe -p <admin_password> export configuration C:\config.xen`**
`import`	`configuration`	<path_of_encrypted_input>	Import a configuration file from the specified location For example, type: **`SLCmd.exe -p <admin_password> import configuration C:\config.xen`**

Chapter 7

Managing Agents Remotely

This chapter describes remote Trend Micro Safe Lock agent management.

Topics in this chapter include:

The Remote Setup Tool (SLrst)

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

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

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

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

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

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

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

Important

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

Tip

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

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

TABLE 7-1. SLrst Remote Agent Setup Parameters

PARAMETER	FUNCTION
`--install`	Deploys and installs the Safe Lock agent on the endpoint See *Remote Installation Considerations on page 7-3*.
`--patch`	Patches the Safe Lock agent
`--reboot`	Restarts the endpoint (required if you want to reinstall the Safe Lock agent) *Restarting Agents Remotely on page 7-18* **Note** The `reboot` function is not compatible on systems running Windows 2000 platforms. Manually restart endpoints running Windows 2000 platforms if you want to reinstall the Safe Lock agent.
`--uninstall`	Uninstalls the Safe Lock agent from the endpoint *Uninstalling Agents Remotely on page 7-17*

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 1-15*.
- 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.

> **Note**
>
> To keep firewall settings enabled on Windows-based endpoints, use the Remote Task Tool command `--applyupdate`. For details, see *Sending Remote Tasks on page 7-19*.

- Target endpoints are not running Windows Installer sessions. Specifically, confirm that Windows Update is not updating the endpoint in the background.

Preparing Windows Server 2003 for Remote Installations

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

- Windows Server 2003

- Windows Server 2003 R2

Procedure

1. Turn off Windows Firewall.

2. Turn on File and Printer Sharing for Microsoft Networks.

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

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

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

Preparing Windows Server 2008 for Remote Installations

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

- Windows Server 2008
- Windows Server 2008 R2

Procedure

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

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

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

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

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

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

       ii. Select **DWORD Value**.

       iii. Type `LocalAccountTokenFilterPolicy` and then press ENTER.

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

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

    f. Click **OK**.

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

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

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

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

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

Preparing Windows 7 for Remote Installations

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

- Windows 7

Procedure

1. Turn off Windows Firewall.

   See http://windows.microsoft.com/en-us/windows/turn-windows-firewall-on-off#turn-windows-firewall-on-off=windows-7.

2. Turn off User Account Control by editing the registry.

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

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

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

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

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

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

      ii. Select **DWORD Value**.

      iii. Type `LocalAccountTokenFilterPolicy` and then press ENTER.

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

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

   f. Click **OK**.

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

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

   See http://windows.microsoft.com/en-us/windows/enable-disable-network-discovery#1TC=windows-7.

Preparing Windows 8 for Remote Installations

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

- Windows 8
- Windows 8.1

Procedure

1. Turn off Windows Firewall.

   See http://windows.microsoft.com/en-US/windows-8/Windows-Firewall-from-start-to-finish.

2. Turn off User Account Control by editing the registry.

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

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

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

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

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

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

ii. Select **DWORD Value**.

iii. Type `LocalAccountTokenFilterPolicy` and then press ENTER.

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

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

f. Click **OK**.

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

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

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

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

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

Preparing Windows XP for Remote Installations

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

- Windows XP

Procedure

1. Turn off Windows Firewall.

   See http://support.microsoft.com/kb/283673/en.

2. Turn on File and Printer Sharing for Microsoft Networks.

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

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

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

3. Disable Simple File Sharing.

   See http://support.microsoft.com/kb/307874/en.

Preparing the Agent Target Files

The Remote Setup Tool utilizes two files when processing commands.

- `endpoint_info.csv`: Stores relevant connection information for agent endpoints
- `targets.csv`: Targets specific endpoints for the current deployment

Important

To edit `endpoint_info.csv` or `targets.csv` files that are in the Program Files folder, copy them to a path with file write priveleges, edit them, then copy them back to the suggested path below.

Procedure

1. Prepare the “endpoint info” file and save it as `endpoint_info.csv` in the following path:

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

   See *Endpoint Info File Specifications on page 7-11*.

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 7-10*.

Targets File Specifications

The “targets” file used during remote agent installation contains the IP address of target endpoints. The targets file uses CSV format and has the file name `targets.csv` by default.

Tip

Remote agent setup using the **`SLrst`** command line program can be done in batches using more than one targets file and the same endpoint info file. The endpoint info file can contain information for endpoints outside the scope of the target endpoints listed in the targets file.

To create customized “targets” CSV files, specify the IP address of each target endpoint. Use one line per record. Use of spaces, quotation marks, or other delimiters is not supported.

For example:

VALID

```
Targeted IP
10.1.199.199
10.1.199.201
192.168.1.20
```

NOT VALID

```
10.1.199.199,10.1.199.201
```

```
"10.1.199.199"
"10.1.199.201"
"192.168.1.20"
```

Tip

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

Endpoint Info File Specifications

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

Tip

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

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

Note

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

For example:

Valid

```
IP,Username,Password
10.1.199.199,Administrator,password1
10.1.199.200,Administrator,password2
10.1.199.201,Administrator,password3
192.168.1.20,Daniel,his_pwd
192.168.1.21,Sophia,her_pwd
```

Not Valid

```
10.1.199.201,Administrator,password3,192.168.1.20,Daniel,his_pwd
```

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

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

Downloading an Up-to-Date Agent Installer Package

Procedure

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

   The **Component Updates** screen appears.

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

3. Select the language the installation package.

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

   > Note
   >
   > The agent installer package is considered up-to-date by Safe Lock Intelligent Manager based on the component versions displayed on the **Component Updates** screen. If the cached agent installer package is not up-to-date, Safe Lock Intelligent Manager prepares and caches an up-to-date package before starting the download.
   >
   > Preparing an up-to-date agent installer package is system-intensive. Depending on the hardware running Safe Lock Intelligent Manager, preparing an up-to-date agent installer package can take a while.

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

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

Important

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 7-9*.

- Before remotely installing Safe Lock agents, download an up-to-date agent installer package.

  See *Downloading an Up-to-Date Agent Installer Package on page 4-3*.

Use the **`SLrst.exe`** program at the command line interface (CLI) to install one or more Safe Lock agents connected to the network.

Procedure

1. Open a command prompt window with Windows administrator privileges.
2. Navigate to the Trend Micro Safe Lock Intelligent Manager "Safe Lock Remote Setup Tool" program folder using the **`cd`** command.

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

   `cd` `/d` "c:\Program Files\Trend Micro\Safe Lock Intelligent Manager\CmdTools \RemoteAgentSetupTool\"

3. To remotely install agents using the default targets file `targets.csv`, type the following at the command prompt:

   ```
   SLrst.exe targets.csv --install.
   ```

   The remote setup tool looks for targets in the `targets.csv` file. For large production environments, Trend Micro recommends that you install agents in batches. Run the remote setup tool separately for each CSV batch file.

4. At the prompt, provide a password used to access the Safe Lock agent program and then confirm the password.

5. Select the target language.

6. Select to perform a prescan for malware on the target endpoints before installing the Safe Lock agent.

7. Select to enable root cause analysis on the target endpoints.

8. Monitor the progress of the remote installation process. Safe Lock writes log information directly in the CSV file (by default, `targets.csv`) specified in the command line argument.

Customizing Agent Installation Remotely Using a Setup.ini File

Procedure

1. Navigate to the “package” folder of the Trend Micro Safe Lock Intelligent Manager installation folder.

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

   "C:\Program Files\Trend Micro\Safe Lock Intelligent Manager\CmdTools \RemoteAgentSetupTool\package"

2. Unzip the `TMSL2.0_EN` file.

3. In the unzipped file, open the `Setup.ini` file and make changes to installation parameters as required. For details on installation parameters and their possible values, see *Setup.ini File Arguments on page 8-15*.

4. Zip the `TMSL2.0_EN` file and make sure it is saved to the installed path.

5. Install agents remotely. For details, see *Installing Agents Remotely on page 7-13*.

Applying Patches and Hotfixes to Agents Remotely

Important

- Before remotely managing Safe Lock agents using the Remote Setup Tool, prepare the "endpoint info" and "targets" files.

  See *Preparing the Agent Target Files on page 7-9*.

- Before remotely updating Safe Lock agents, download the latest agent patch or hotfix file using the Trend Micro Technical Support Download Center website: http://downloadcenter.trendmicro.com/

Use the **`SLrst.exe`** program at the command line interface (CLI) to install one or more Safe Lock agents connected to the network.

Procedure

1. Copy the downloaded agent patch or hotfix to the path used by **`SLrst`**.

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

Important

The patch or hot fix file name must follow the format: `TMSL2.0_Hotfix_<language_abbreviation>.zip`

For example:

`TMSL2.0_Hotfix_EN.zip`	`TMSL2.0_Hotfix_EN (1).zip`
`TMSL2.0_Hotfix_JA.zip`	`TMSL2.0_Hotfix_EN_1.zip`

2. Navigate to the Trend Micro 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 patch or hotfix agents using the default targets file `targets.csv`, type the following at the command prompt:

   SLrst.exe `targets.csv --patch`.

   The remote setup tool looks for targets in the `targets.csv` file. For large production environments, Trend Micro recommends that you patch or hotfix agents in batches. Run the remote setup tool separately for each CSV batch file.

4. At the prompt, provide the password used to access the Safe Lock agent program.

5. Monitor the progress of the remote patch or hotfix. Safe Lock writes log information directly in the CSV file (by default, `targets.csv`) specified in the command line argument.

Uninstalling Agents Remotely

> **Important**
>
> Before remotely managing Safe Lock agents using the Remote Setup Tool, prepare the "endpoint info" and "targets" files.
>
> See *Preparing the Agent Target Files on page 7-9*.

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 7-9*.

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

Procedure

1. Open a command prompt window with Windows administrator privileges.

2. Navigate to the Trend Micro Safe Lock Intelligent Manager "Safe Lock Remote Setup Tool" folder inside the installation folder using the **cd** command.

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

   ```
   cd /d "c:\Program Files\Trend Micro\Safe Lock Intelligent Manager\CmdTools
   \RemoteAgentSetupTool\"
   ```

3. To remotely install agents using the default targets file `targets.csv`, type the following at the command prompt:

   ```
   SLrst.exe targets.csv --reboot.
   ```

   The remote setup tool looks for targets in the `targets.csv` file. For large production environments, Trend Micro recommends that you restart agents in batches. Run the remote setup tool separately for each CSV batch file.

4. Monitor the progress of the remote restart process. Safe Lock writes log information directly in the CSV file (by default, `targets.csv`) specified in the command line argument.

   Endpoints restart automatically after receiving the command.

The Remote Tasks Tool (SLtasks)

You can use the Remote Tasks Tool to initialize agent Approved Lists, lockdown agents, match licenses, deploy patch or hotfixes without disabling firewall settings on agents, and query the status of agents using a command line interface (CLI).

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

```
<Safe_Lock_Intelligent_Manager_installation_folder>\CmdTools
\RemoteAgentTasksTool\
```

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

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

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

4. Type your Safe Lock Intelligent Manager credentials.

   The CLI confirms a successful log on to the server.

Important

- The logged on account must have “admin” or “Full Control” privilege to send tasks to agents.
- To reduce network and endpoint impact, Safe Lock Intelligent Manager queries target agents for their configurations and then sends only tasks it determines are needed.

5. Query agent statuses. To limit the query to agents before or after a specific version, append `--minversion` and `--maxversion` to the command and type the agent version.

    - **`SLtasks.exe`** `--query --minversion <agent_version>`
    - **`SLtasks.exe`** `--query --maxversion <agent_version>`

    Important

    The `<agent_version>` must be in the form of `x.x.xxxx`. For example, `2.0.5000`.

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

    Tip

    Trend Micro recommends querying agent statuses before deploying any tasks. A warning message appears if the query results are out-of-date when attempting to deploy tasks.

6. Perform the necessary tasks using the following syntax:

    `SLtasks.exe` `<task_parameter>`

    Table 7-2. SLtasks Task Parameters

Parameter	Task
`--init`	Initialize the Approved List
`--lockdown`	Turn Application Lockdown on

PARAMETER	TASK
`--match`	Match agent licenses with the server
`--applyupdate`	Apply patches and hotfixes

Tip

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

  For example:

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

- To ensure efficiency when updating multiple agents, append `--concurrentdownload` to limit the number of agents allowed for downloading the patch or hotfix at the same time.

  For example:

  `SLtasks.exe` `--applyupdate` <update_files> `--concurrentdownload 2`

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.

Deploying Patches and Hotfixes to Agents Remotely

Procedure

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

   http://downloadcenter.trendmicro.com/

2. Copy the downloaded agent patch or hotfix to the patch used by **`SLtasks`**.

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

3. Open a command prompt window with Windows administrator privileges.

4. Navigate to the Trend Micro Safe Lock Intelligent Manager “Safe Lock Remote Tasks Tool” folder inside the installation folder using the **cd** command.

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

   ```
   cd /d "c:\Program Files\Trend Micro\Safe Lock Intelligent Manager\CmdTools\RemoteAgentTasksTool\"
   ```

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

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

6. Query agent statuses. To limit the query to agents before or after a specific version, append `--minversion` and `--maxversion` to the command and type the agent version.

   - `SLtasks.exe --query --minversion <agent_version>`
   - `SLtasks.exe --query --maxversion <agent_version>`

   Important

   The `<agent_version>` must be in the form of `x.x.xxxx`. For example, `2.0.5000`.

7. Apply the hotfix by typing the following command and specify the file name:

   ```
   SLtasks.exe --applyupdate <hotfix_file_name_with_extension>
   ```

Applying Message Time Groups

Message time groups use message-sending cycles to add additional bandwidth control to automated messages sent from Safe Lock agents to the Safe Lock Intelligent Manager.

During a message-sending cycle, agents in the active group send automated messages, which include log and status as well as quarantined files to be scanned, to Safe Lock Intelligent Manager. When a message-sending cycle ends, the next group of agents becomes active and sends automated messages.

Agents outside the active group do not send automated messages. However, agents in all groups respond as soon as possible to direct requests from Safe Lock Intelligent Manager. For example, a request to send logs and status from the web console will be replied to by the target agent as soon as network connectivity allows.

Note

The following conditions apply to automated messages:

By default, Safe Lock Intelligent Manager puts all agents into one "always on" group.

During a message-sending cycle, messages are sent in the following order:

- Higher priority first
- Oldest (least recent) first

Applying Message Time Groups Using the Remote Tasks Tool

Use **SLtasks.exe** to apply message time groups to agents.

Procedure

1. Open a command prompt window with Windows administrator privileges.
2. Navigate to the Trend Micro Safe Lock Intelligent Manager “Safe Lock Remote Tasks Tool” folder inside the installation folder using the **cd** command.

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

   cd /d "c:\Program Files\Trend Micro\Safe Lock Intelligent Manager\CmdTools\RemoteAgentTasksTool\"
3. Log on the Safe Lock Intelligent Manager server by typing the following command:

   SLtasks.exe --logon

4. Type your Safe Lock Intelligent Manager credentials.

   The CLI confirms a successful log on to the server.

5. Query message time groups by typing the following command:

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

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

   Important

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

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

Column Name	Control Description
TotalGroupNum	Divide agents into any number of groups **Tip** Set this value to 1 to turn the feature off
OwnGroupIndex	Set the message group ID number of this Safe Lock Intelligent Manager agent
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

7. Apply message time groups to agents using the configured `group_info.csv` file by typing the following command:

   ```
   SLtasks.exe --applygroups
   ```

Important

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

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

   ```
   SLtasks.exe --logoff
   ```

   The CLI confirms a successful log off from the server.

Applying Message Time Groups Using the Configuration File

Procedure

1. Access the **Export/Import Configuration** section from the Trend Micro Safe Lock console.

   a. Open the Trend Micro Safe Lock console using the desktop icon (if available) or the **Start** menu by clicking **All Programs** > **Trend Micro Safe Lock**.

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

   c. Click the **Settings** menu item.

2. Export the configuration file as a database `.xen` file.

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

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

3. Decrypt the configuration file.

4. From Windows Notepad or another text editor, edit the `MessageRandomization` parameter in the `ManagedMode` section:

Column Name	Control Description
TotalGroupNum	Divide agents into any number of groups
OwnGroupIndex	Set the message group ID number of this Safe Lock Intelligent Manager agent
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

5. From the **Export/Import Configuration** section of the Trend Micro Safe Lock console, import the configuration file as a database (`.xen`) file.

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

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

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

Applying Message Time Groups Using the Setup.ini File

Procedure

1. Edit the `MESSAGERANDOMIZATION` arguments in the `Setup.ini` file.

    a. From the Trend Micro Safe Lock Intelligent Manager folder, double-click `Setup.ini`.

    b. Edit the following arguments in the `MESSAGERANDOMIZATION` section:

Column Name	Control Description
`TOTAL_GROUP_NUM`	Divide agents into any number of groups
`OWN_GROUP_INDEX`	Set the message group ID number of this Safe Lock Intelligent Manager agent

Column Name	Control Description
`TIME_PERIOD`	Set a duration for how long each group is allowed to send messages to Safe Lock Intelligent Manager when that group's message-sending cycle is active

2. Install the Safe Lock Intelligent Manager using Windows Installer or the command line interface (CLI) installer. For details, see *Installing from Windows* and *Installation Using the Command Line* from the Trend Micro Safe Lock Intelligent Manager Installation Guide.

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

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 1-15* 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.

To customize installations using either the Windows Installer or the command line interface (CLI) installer, modify the Setup.ini file. See *Installation Customization using a Setup.ini File on page 8-14*.

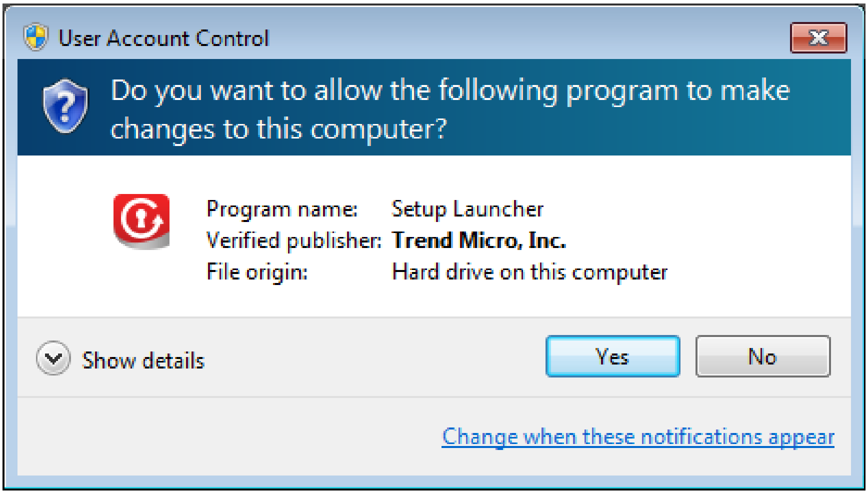
Installing from Windows

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

Procedure

1. Double-click `SL_Install.exe`.

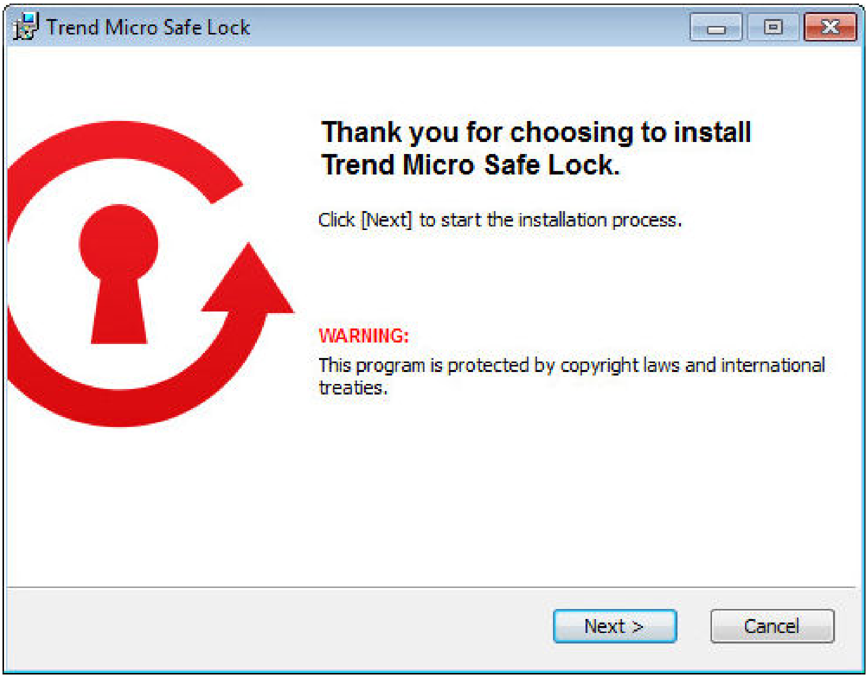
   If a **User Account Control** warning from Windows appears, click **Yes**.



User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: Setup Launcher
Verified publisher: **Trend Micro, Inc.**
File origin: Hard drive on this computer



Trend Micro Safe Lock

Thank you for choosing to install Trend Micro Safe Lock.

Click [Next] to start the installation process.

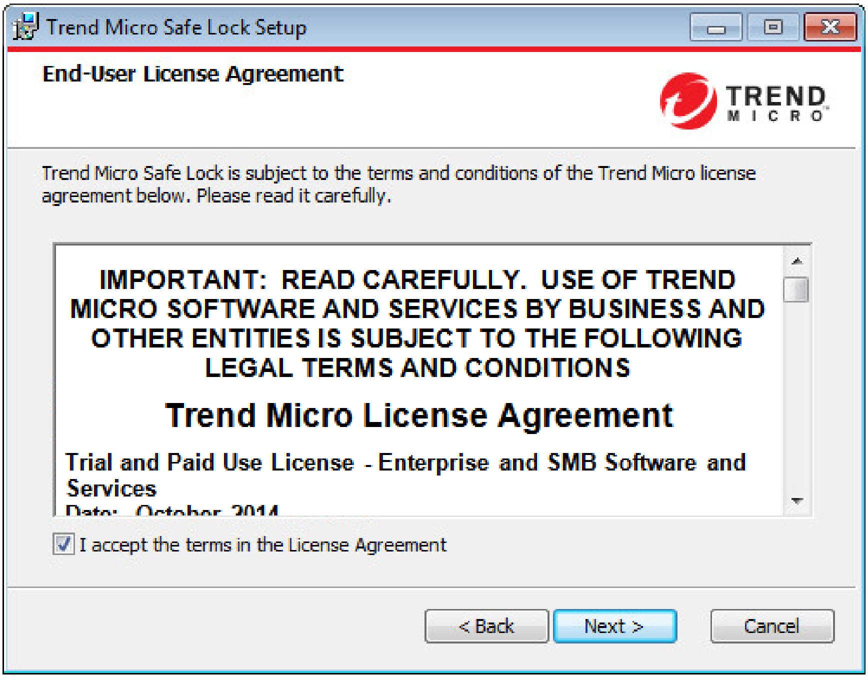
WARNING:
This program is protected by copyright laws and international treaties.

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

Note

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

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



Trend Micro Safe Lock Setup

End-User License Agreement

Trend Micro Safe Lock is subject to the terms and conditions of the Trend Micro license agreement below. Please read it carefully.

IMPORTANT: READ CAREFULLY. USE OF TREND MICRO SOFTWARE AND SERVICES BY BUSINESS AND OTHER ENTITIES IS SUBJECT TO THE FOLLOWING LEGAL TERMS AND CONDITIONS

Trend Micro License Agreement

Trial and Paid Use License - Enterprise and SMB Software and Services

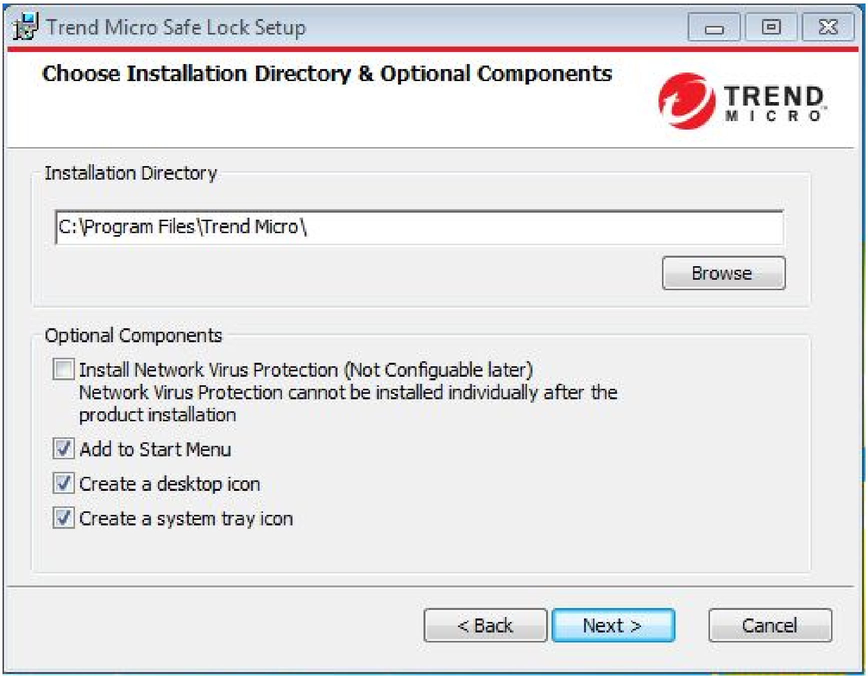
Date: October 2014

☑ I accept the terms in the License Agreement

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

Important

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



Trend Micro Safe Lock Setup

Choose Installation Directory & Optional Components

Installation Directory

C:\Program Files\Trend Micro\

Optional Components

□ Install Network Virus Protection (Not Configuable later)
Network Virus Protection cannot be installed individually after the product installation

☑ Add to Start Menu

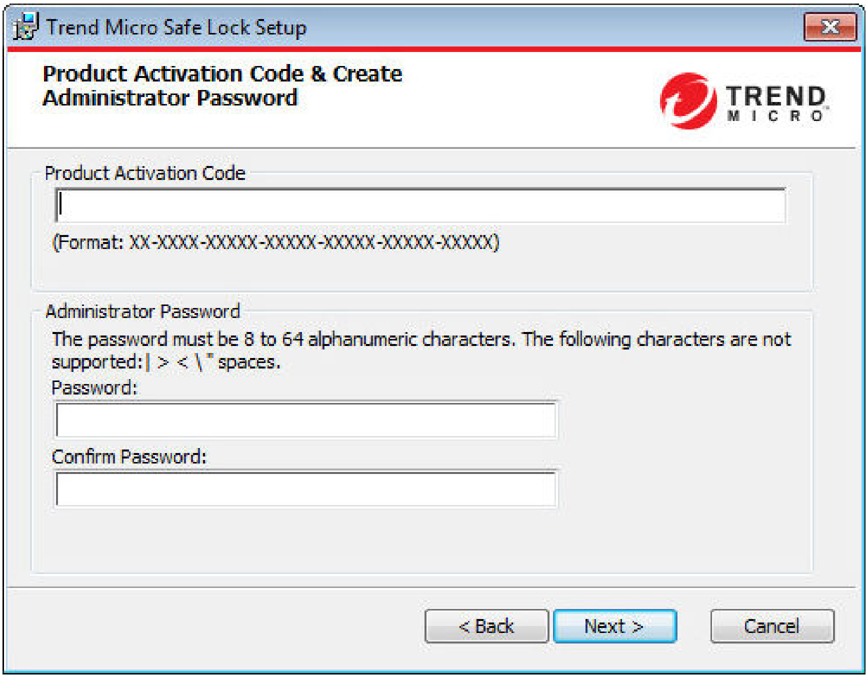
☑ Create a desktop icon

☑ Create a system tray icon

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.



Trend Micro Safe Lock Setup

Product Activation Code & Create Administrator Password

Product Activation Code

(Format: XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX)

Administrator Password

The password must be 8 to 64 alphanumeric characters. The following characters are not supported:| > < \ " spaces.

Password:

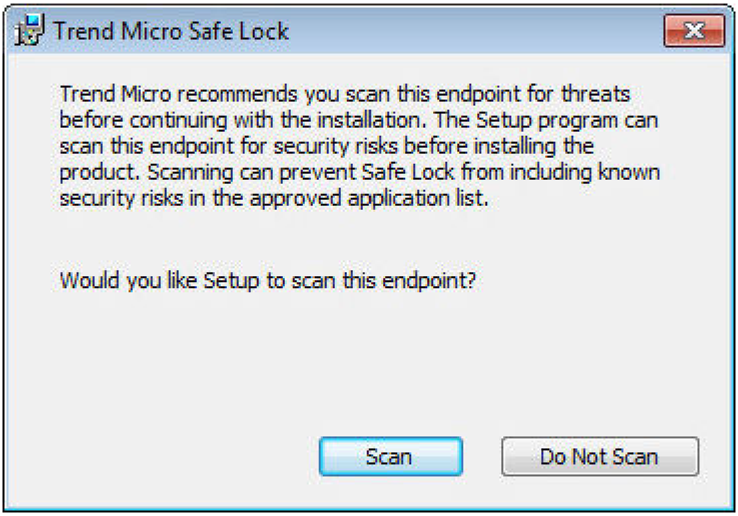
Confirm Password:

WARNING!

Do not forget the Safe Lock administrator password. The only way to recover after losing the Safe Lock administrator password is by reinstalling the operating system.

6. Click **Next**.

A message appears asking if you would like to scan the endpoint for threats before continuing with the installation.



Trend Micro Safe Lock

Trend Micro recommends you scan this endpoint for threats before continuing with the installation. The Setup program can scan this endpoint for security risks before installing the product. Scanning can prevent Safe Lock from including known security risks in the approved application list.

Would you like Setup to scan this endpoint?

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

    - To scan the endpoint for threats, click **Scan**.

        a. The **Endpoint Prescan** window appears.

        b. To customize the scan settings, click **Edit Scan Settings**.

        c. Click **Scan Now**.

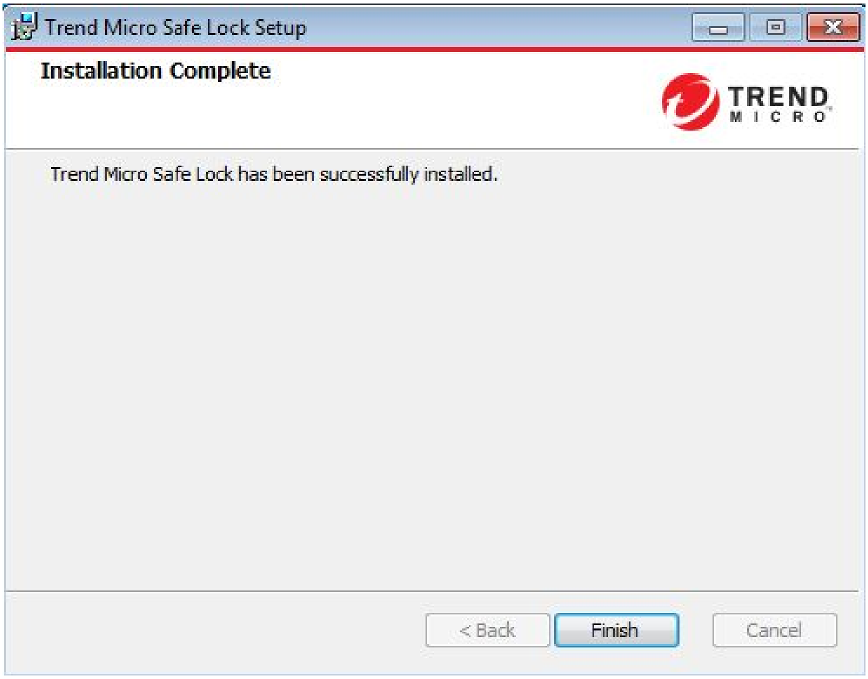
        If Endpoint Prescan detects security risks, Trend Micro recommends canceling the installation. Remove threats from the endpoint and try again. If critical programs are detected as threats, confirm that the endpoint is secure and that the versions of the programs installed do not contain threats. Ignore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

Tip

Trend Micro provides solutions for detecting and removing threats. For endpoints with limited or no network access, Trend Micro recommends using Trend Micro Portable Security. See *Trend Micro Portable Security Compatible on page 1-10*. For more information about this and other solutions from Trend Micro, go to http://trendmicro.com/.

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

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



Trend Micro Safe Lock Setup

Installation Complete

Trend Micro Safe Lock has been successfully installed.

Note

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

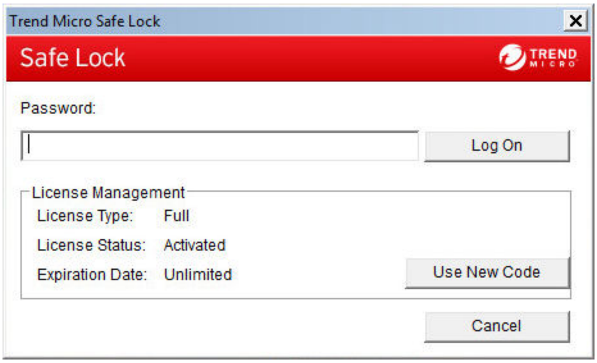
Setting Up the Approved List

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

Procedure

1. Open the Safe Lock console.

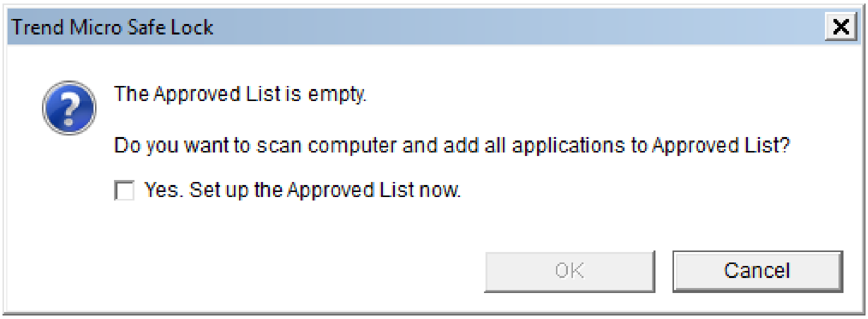
   The Safe Lock log on screen appears.



License Management
License Type: Full
License Status: Activated
Expiration Date: Unlimited

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

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



Trend Micro Safe Lock

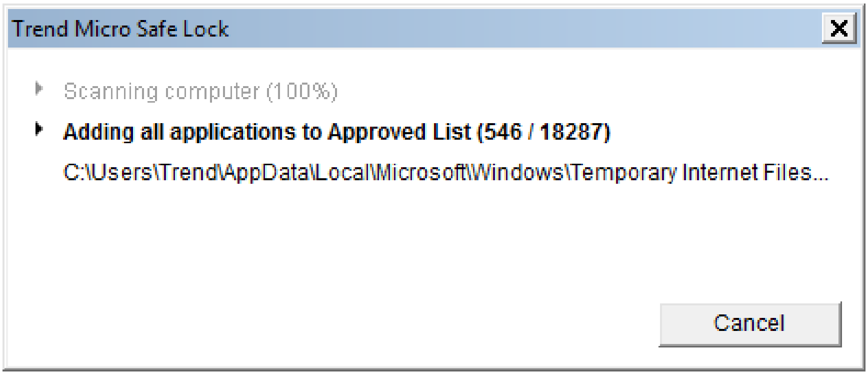
The Approved List is empty.

Do you want to scan computer and add all applications to Approved List?

□ Yes. 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.



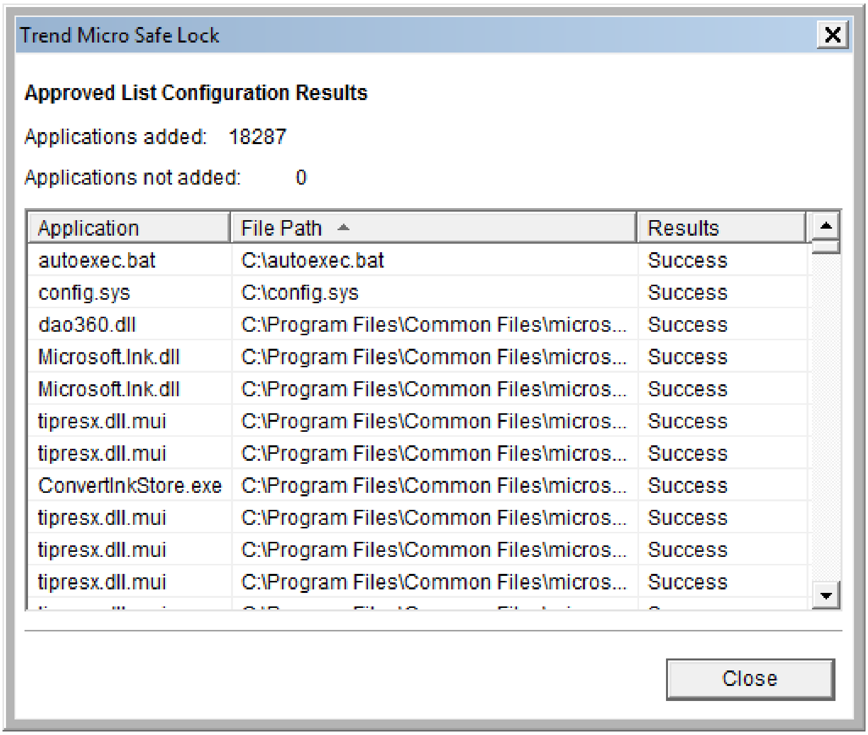
Trend Micro Safe Lock

Scanning computer (100%)

Adding all applications to Approved List (546 / 18287)

C:\Users\Trend\AppData\Local\Microsoft\Windows\Temporary Internet Files...

Safe Lock displays the Approved List Configuration Results.



Trend Micro Safe Lock

Approved List Configuration Results

Applications added: 18287

Applications not added: 0

Application	File Path	Results
autoexec.bat	C:\autoexec.bat	Success
config.sys	C:\config.sys	Success
dao360.dll	C:\Program Files\Common Files\micros...	Success
Microsoft.Ink.dll	C:\Program Files\Common Files\micros...	Success
Microsoft.Ink.dll	C:\Program Files\Common Files\micros...	Success
tipresx.dll.mui	C:\Program Files\Common Files\micros...	Success
tipresx.dll.mui	C:\Program Files\Common Files\micros...	Success
ConvertInkStore.exe	C:\Program Files\Common Files\micros...	Success
tipresx.dll.mui	C:\Program Files\Common Files\micros...	Success
tipresx.dll.mui	C:\Program Files\Common Files\micros...	Success
tipresx.dll.mui	C:\Program Files\Common Files\micros...	Success

Note

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

4. Click **Close**.

Installation Using the Command Line

Administrators can install Safe Lock from the command line interface (CLI) or using a batch file, allowing for silent installation and mass deployment. For mass deployment, Trend Micro recommends first installing Safe Lock on a test computer since a customized installation may require a valid configuration file and Approved List. See the Trend Micro Safe Lock Administrator's Guide for more information about the Approved List and configuration file.

WARNING!

Do not forget the Safe Lock administrator password. The only way to recover after losing the Safe Lock administrator password is by reinstalling the operating system.

Important

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

Note

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

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

Installer Command Line Interface Parameters

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

Table 8-2. Safe Lock Intelligent Manager Installer Command Line Options

Parameter	Value	Description
`-q`		Run the installer silently
`-p`	<administrator_ password>	Specify the administrator password

PARAMETER	VALUE	DESCRIPTION
`-d`	<path>	Specify the installation path
`-ac`	<activation_code>	Specify the activation code
`-nd`		Do not create a desktop shortcut
`-fw`		Enable Network Virus Protection
`-ns`		Do not add a shortcut to the Start menu
`-ni`		Hide the task tray icon
`-cp`	<path>	Specify the Safe Lock configuration file **Note** The Safe Lock configuration file can be exported after installing Safe Lock.
`-lp`	<path>	Specify the Approved List **Note** After installing Safe Lock and creating the Approved List, the list can be exported.
`-qp`	<path>	Specify the folder path for quarantined files when custom action is set to “quarantine” mode.
`-nrca`		Disable the Root Cause Analysis (RCA) report
`-nps`		Do not execute Prescan
`-ips`		Do not cancel installation when Prescan detects threats

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

```
SL_Install.exe -q -ac XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX -p
P@ssW0Rd -nd
```

Important

An administrator password and Activation Code must be specified for the installation to continue.

Installation Customization using a Setup.ini File

Note

Arguments specified at the command line interface (CLI) take higher priority than the setup file, which takes higher priority over the default values. For example, if the switch –nd is added to `SL_Install.exe`, and `setup.ini` contains `NO_DESKTOP=0`, the switch will take precedence, and a Safe Lock Intelligent Manager desktop shortcut will not be created.

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

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
```

Setup.ini File Arguments

Note

Arguments specified at the command line interface (CLI) take higher priority than the setup file, which takes higher priority over the default values. For example, if the switch –nd is added to SL_Install.exe, and setup.ini contains NO_DESKTOP=0, the switch will take precedence, and a Safe Lock Intelligent Manager desktop shortcut will not be created.

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

EventLog Section

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

TABLE 8-3. Setup.ini File [EVENTLOG] Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPT-ED
ENABLE	Log events related to Safe Lock	• 1: Log • 0: Do not log	1	No
LEVEL_WARNINGLOG	Log “Warning” level events related to Safe Lock	• 1: Log • 0: Do not log	1	No
LEVEL_INFORMATIONLOG	Log “Information” level events related to Safe Lock	• 1: Log • 0: Do not log	0	No
BLOCKEDACCESSLOG	Log files blocked by Safe Lock	• 1: Log • 0: Do not log	1	No

Key	Description	Possible Values	Default Value	Encrypt-ed
APPROVEDACCESSLOG	Log files approved by Safe Lock	• 1: Log • 0: Do not log	1	No
APPROVEDACCESSLOG_TRUSTEDUPDATER	Log Trusted Updater approved access	• 1: Log • 0: Do not log	1	No
APPROVEDACCESSLOG_DLLDRIVER	Log DLL/Driver approved access	• 1: Log • 0: Do not log	0	No
APPROVEDACCESSLOG_EXCEPTIONPATH	Log Application Lockdown exception path approved access	• 1: Log • 0: Do not log	1	No
APPROVEDACCESSLOG_TRUSTEDCERT	Log Trusted Certifications approved access	• 1: Log • 0: Do not log	1	No
APPROVEDACCESSLOG_WRITEPROTECTION	Log Write Protection approved access	• 1: Log • 0: Do not log	1	No
SYSTEMEVENTLOG	Log events related to the system	• 1: Log • 0: Do not log	1	No
SYSTEMEVENTLOG_EXCEPTIONPATH	Log exceptions to Application Lockdown	• 1: Log • 0: Do not log	1	No
SYSTEMEVENTLOG_WRITEPROTECTION	Log Write Protection events	• 1: Log • 0: Do not log	1	No
LISTLOG	Log events related to the Approved list	• 1: Log • 0: Do not log	1	No

Key	Description	Possible Values	Default Value	Encrypted
USBMALWAREPROTECTIONLOG	Log events that trigger USB Malware Protection	• 1: Log • 0: Do not log	1	No
EXECUTIONPREVENTIONLOG	Log events that trigger Execution Prevention	• 1: Log • 0: Do not log	1	No
NETWORKVIRUSPROTECTIONLOG	Log events that trigger Network Virus Protection	• 1: Log • 0: Do not log	1	No
INTEGRITYMONITORINGLOG_FILECREATED	Log file and folder created events	• 1: Log • 0: Do not log	1	No
INTEGRITYMONITORINGLOG_FILEMODIFIED	Log file modified events	• 1: Log • 0: Do not log	1	No
INTEGRITYMONITORINGLOG_FILEDELETED	Log file and folder deleted events	• 1: Log • 0: Do not log	1	No
INTEGRITYMONITORINGLOG_FILERENAMED	Log file and folder renamed events	• 1: Log • 0: Do not log	1	No
INTEGRITYMONITORINGLOG_REGVALUEMODIFIED	Log registry value modified events	• 1: Log • 0: Do not log	1	No
INTEGRITYMONITORINGLOG_REGVALUEDELETED	Log registry value deleted events	• 1: Log • 0: Do not log	1	No
INTEGRITYMONITORINGLOG_REGKEYCREATED	Log registry key created events	• 1: Log • 0: Do not log	1	No

Key	Description	Possible Values	Default Value	Encrypt-ed
INTEGRITYMONITORINGLOG_REGKEYDELETED	Log registry key deleted events	• 1: Log • 0: Do not log	1	No
INTEGRITYMONITORINGLOG_REGKEYRENAMED	Log registry key renamed events	• 1: Log • 0: Do not log	1	No

Property Section

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

Table 8-4. Setup.ini File [PROPERTY] Section Arguments

Key	Description	Possible Values	Default Value	Encrypt-ed
ACTIVATION_CODE	Activation Code	<activation_code>	<empty>	No
NO_DESKTOP	Create a shortcut on desktop	• 1: Do not create shortcut • 0: Create shortcut	0	No
NO_STARTMENU	Create a shortcut in the Start menu	• 1: Do not create shortcut • 0: Create shortcut	0	No
NO_SYSTRAY	Display the system tray icon and Windows notifications	• 1: Do not create system tray icon • 0: Create system tray icon	0	No
NO_NSC	Install firewall	• 1: Do not create firewall • 0: Create firewall	0	No

Key	Description	Possible Values	Default Value	Encrypt-ed
`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	• `0`: Standalone mode • `1`: Managed mode	`0`	No
`PASSWORD`	Password which is used for **`SLCmd.exe`** and Safe Lock console	<password>	<empty>	No
`CUSTOM_ACTION`	Custom action for blocked events	• `0`: Ignore • `1`: Quarantine • `2`: Ask server	`0`	No
`QUARANTINE_FOLDER_PATH`	Quarantine path for agent program	<path>	<empty>	No
`ROOT_CAUSE_ANALYSIS`	Enable root cause analysis reporting	• `0`: Disable • `Other value`: Enable	`1`	No
`INTEGRITY_MONITOR`	Enable Integrity Monitor	• `0`: Disable • `1`: Enable	`0`	No

Key	Description	Possible Values	Default Value	Encrypt-ed
PREDEFINED_TRUSTED_UPDATER	Enable Predefined Trusted Updater	• 0: Disable • 1: Enable	0	No
WINDOWS_UPDATE_SUPPORT	Enable Window Update Support	• 0: Disable • 1: Enable	0	No
PRESCAN	Prescan the endpoint before installing Safe Lock	• 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: • 0: Overwrite events as needed • 1 - 365: Overwrite events older than (1-365) days • -1: Do not overwrite events (Clear logs manually) For Windows Vista or later platforms: • 0: Overwrite events as needed (oldest events first)	0	No

Key	Description	Possible Values	Default Value	Encrypt-ed
		- 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.	For Windows XP or earlier platforms: - 0: Overwrite events as needed - 1 - 365: Overwrite events older than (1-365) days - -1: Do not overwrite events (Clear logs manually) For Windows Vista or later platforms: - 0: Overwrite events as needed (oldest events first) - 1: Archive the log when full, do not overwrite events - -1: Do not overwrite events	0	No

Key	Description	Possible Values	Default Value	Encrypted
		(Clear logs manually)		
`USR_DEBUGLOG_ENABLE`	Enable debug logging for user sessions	• `0`: Log • `1`: Do not log	`0`	No
`USR_DEBUGLOGLEVEL`	The number of debug log entries allowed for user sessions	• `273`	`273`	No
`SRV_DEBUGLOG_ENABLE`	Enable debug logging for service sessions.	• `0`: Log • `1`: Do not log	`0`	No
`SRV_DEBUGLOGLEVEL`	The number of debug log entries allowed for service sessions	• `273`	`273`	No

`SILENT_INSTALL`	Execute installation in silent mode
	Important
	To use silent mode, you must also specify the ACTIVATION_CODE and PASSWORD keys and values. For example:
	`[PROPERTY]`
	`ACTIVATION_CODE=XX-XXXX-XXX`
	`XX-XXXXX-XXXXX-XXXXX-XXXXX`
	`PASSWORD=P@ssW0Rd`
	`SILENT_INSTALL=1`
		• `1`: Use silent mode
		• `0`: Do not use silent mode
			`0`	No

Server Section

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

Table 8-5. Setup.ini File `[SERVER]` Section Arguments

Key	Description	Possible Values	Default Value	Encrypt-ed
`HOSTNAME`	Server host name	<host_name>	<empty>	No
`PORT_FAST`	Server listen port for fast lane	`1 - 65535`	<empty>	No
`PORT_SLOW`	Server listen port for slow lane	`1 - 65535`	<empty>	No
`CERT`	Certificate file name	<certificate_file_name >	<empty>	No
`API_KEY`	API key	<API_key>	<empty>	No

Agent Section

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

Table 8-6. Setup.ini File `[AGENT]` Section Arguments

Key	Description	Possible Values	Default Value	Encrypt-ed
`PORT`	Agent listening port	`1 - 65535`	<empty>	No
`SSL_ALLOW_BEAST`	Handles possible security flaws in SSL3 and TLS 1.0 protocols for BEAST attacks	• `0`: Protect against BEAST attacks • `1`: Do not implement any security	`1`	No

Key	Description	Possible Values	Default Value	Encrypted
		workarounds for BEAST vulnerabilities		
`POLL_SERVER`	Identify the agent as an NAT agent	- `0`: Non-NAT agent - `1`: NAT agent	`0`	No
`POLL_SERVER_INTERVAL`	Set the NAT connection frequency	- `1 - 64800`: Connect to the Safe Lock Intelligent Manager server every (1 - 64800) minutes	`10`	No

Message Section

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

Table 8-7. Setup.ini File `[MESSAGE]` Section Arguments

Key	Description	Possible Values	Default Value	Encrypted
`REGISTER_TRIGGER`	Register message trigger	- `1`: Immediately - `2`: On demand	`1`	No
`UNREGISTER_TRIGGER`	Unregister message trigger	- `1`: Immediately - `2`: On demand	`1`	No
`UPDATESTATUS_TRIGGER`	Update status message trigger	- `1`: Immediately - `2`: On demand	`1`	No
`UPLOADBLOCKEDEVENT_TRIGGER`	Upload blocked event message trigger	- `1`: Immediately - `2`: On demand	`1`	No

Key	Description	Possible Values	Default Value	Encrypt-ed
CHECKFILEHASH_TRIGGER	Check file hash message trigger	- 1: Immediately - 2: On demand	1	No
QUICKSCANFILE_TRIGGER	Quick scan file message trigger	- 1: Immediately - 2: On demand	1	No

MessageRandomization Section

Note

Safe Lock agents respond as soon as possible to direct requests from Safe Lock Intelligent Manager. For details, refer to Applying Message Time Groups in the Safe Lock Intelligent Manager Administrator's Guide.

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

Table 8-8. Setup.ini File [MESSAGERANDOMIZATION] Section Arguments

Key	Description	Possible Values	Default Value	Encrypt-ed
TOTAL_GROUP_NUM	Number of groups controlled by the server	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

Proxy Section

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

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

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPT-ED
`MODE`	Proxy mode	• `0`: No proxy used • `1`: Proxy used with manual settings • `2`: Proxy used with settings retrieved from Internet Explorer automatically	`0`	No
`HOSTNAME`	Proxy host name	<host_name>	<empty>	No
`PORT`	Proxy port	`1 - 65535`	<empty>	No
`USERNAME`	Proxy user name	<user_name>	<empty>	No
`PASSWORD`	Proxy password	<password>	<empty>	No

Prescan Section

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

TABLE 8-10. Setup.ini File `[PRESCAN]` Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPT-ED
`IGNORE_THREAT`	Cancel installation after detecting	• `0`: Cancel • `1`: Continue installation after detecting malware	`0`	No

Key	Description	Possible Values	Default Value	Encrypt-ed
	malware threat during prescan **Note** Only valid during silent installations.	threat during prescan		
`REPORT_FOLDER`	An absolute folder path where prescan result reports are saved.	- <folder_path> - <empty>: Defaults to `%windir%\temp\prescan\log`	<empty>	No

`SCAN_TYPE`	The type of scan executed during silent installation
	Note
	The selected value is used as the default value for a UI installation.
		- `Full`: Scan all folders on the endpoint.
		- `Quick`: Scans the following folders:
		  - Fixed root drives
		  For example:
		  `c:\`
		  `d:\`
		  - System root folder
		  For example, `c:\Windows`
		  - System folder
		  For example, `c:\Windows\System`
			`Full`	No

Key	Description	Possible Values	Default Value	Encrypt-ed
		- System32 folder For example, `c:\Windows\System32` - Driver folder For example, `c:\Windows\System32\Drivers` - 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	- `0`: Do not scan compressed files - `1` - `20`: Scan up to the specified	`2`	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPT-ED
	compressed file is scanned.	number of layers of a compressed file		
MAX_FILE_SIZE	The largest file allowed for scan	• 0: Scan files of any sizes • 1 - 9999: Only scan files equal to or smaller than the specified size (MB)	0	No
SCAN_REMOVABLE_DRIVE	Scan removable drives	• 0: Do not scan removable drives • 1: Scan removable drives	0	No

SPECIFIC_FOLDER	An absolute folder path to scan when the scan type is [Specific]	<folder_path>
		Multiple folders can be specified by creating new entries whose name starting with SPECIFIC_FOLDER. Every entry name needs to be unique.
		For example:
		SPECIFIC_FOLDER=c:\folder1
		SPECIFIC_FOLDER2=c:\folder2
		SPECIFIC_FOLDER3=c:\folder3
			<empty>	No

EXCLUDED_FILE	An absolute file path to exclude from scanning	<file_path> Multiple files can be specified by creating	<empty>	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPT-ED

		new entries whose name starting with EXCLUDED_FILE. Every entry name needs to be unique.
		For example:
		EXCLUDED_FILE=c:\file1.exe
		EXCLUDED_FILE2=c:\file2.exe
		EXCLUDED_FILE3=c:\file3.exe		

EXCLUDED_FOLDER	An absolute folder path to exclude from scanning	<folder_path>
		Multiple folders can be specified by creating new entries whose name starting with EXCLUDED_FOLDER. Every entry name needs to be unique.
		For example:
		EXCLUDED_FOLDER=c:\file1.exe
		EXCLUDED_FOLDER2=c:\file2.exe
		EXCLUDED_FOLDER3=c:\file3.exe
			<empty>	No

EXCLUDED_EXTENSION	A file extension to exclude from scanning	<file_extension> Multiple extensions can be specified by creating new entries whose name starting with	<empty>	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPT-ED

		`EXCLUDED_EXTENSION`. Every entry name needs to be unique.
		For example:
		`EXCLUDED_EXTENSION=bmp`
		`EXCLUDED_EXTENSION2=png`		

Chapter 9

Working with the Agent Configuration File

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

Topics in this chapter include:

Working with the Agent Configuration File

The configuration file allows administrators to create and deploy a single configuration across multiple machines. See *Exporting or Importing a Configuration File on page 9-2* for more information.

Changing Advanced Settings

Some settings can only be changed though the configuration file using the command line interface (CLI). See *Using SLCmd at the Command Line Interface (CLI) on page 6-2* for more information.

Procedure

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

   Important

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

   Tip

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

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

Exporting or Importing a Configuration File

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

Procedure

1. Open the Trend Micro Safe Lock console using the desktop icon (if available) or the **Start** menu by clicking **All Programs** > **Trend Micro Safe Lock**.

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

3. Click the **Settings** menu item to access the **Export/Import Configuration** section.

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

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

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

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

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

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

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

Configuration File Syntax

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

Important

The configuration file only supports UTF-8 encoding.

Refer to the following example of the configuration file:

```
<?xml version="1.0" encoding="UTF-8"?>
<Configurations version="1.00.000"
    xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="WKConfig.xsd">
    <Configuration>
        <AccountGroup>
```

```
            <Account
                ID="{24335D7C-1204-43d1-9CBB-332D688C85B6}"
                Enable="no">
                <Password/>
            </Account>
        </AccountGroup>
        <UI>
            <SystemTaskTrayIcon Enable="yes"/>
        </UI>
        <Feature>
            <ApplicationLockDown LockDownMode="2">
                <WhiteList
                RecentHistoryUnapprovedFilesLimit="50"/>
                <ScriptLockdown Enable="yes">
                    <Extension ID="bat">
                        <Interpreter>cmd.exe</Interpreter>
                    </Extension>
                    <Extension ID="cmd">
                        <Interpreter>cmd.exe</Interpreter>
                    </Extension>
                    <Extension ID="com">
                        <Interpreter>ntvdm.exe</Interpreter>
                    </Extension>
                    <Extension ID="dll">
                        <Interpreter>ntvdm.exe</Interpreter>
                    </Extension>
                    <Extension ID="drv">
                        <Interpreter>ntvdm.exe</Interpreter>
                    </Extension>
                    <Extension ID="exe">
                        <Interpreter>ntvdm.exe</Interpreter>
                    </Extension>
                    <Extension ID="js">
                        <Interpreter>cscript.exe</Interpreter>
                        <Interpreter>wscript.exe</Interpreter>
                    </Extension>
                    <Extension ID="msi">
                        <Interpreter>msiexec.exe</Interpreter>
                    </Extension>
                    <Extension ID="pif">
                        <Interpreter>ntvdm.exe</Interpreter>
                    </Extension>
                    <Extension ID="ps1">
                        <Interpreter>powershell.exe
                        </Interpreter>
                    </Extension>
                    <Extension ID="sys">
                        <Interpreter>ntvdm.exe</Interpreter>
                    </Extension>
                    <Extension ID="vbe">
                        <Interpreter>cscript.exe</Interpreter>
                        <Interpreter>wscript.exe</Interpreter>
                    </Extension>
                    <Extension ID="vbs">
                        <Interpreter>cscript.exe</Interpreter>
                        <Interpreter>wscript.exe</Interpreter>
                    </Extension>
                </ScriptLockdown>
                <TrustedUpdater>
                    <PredefinedTrustedUpdater Enable="no">
                        <RuleSet/>
                    </PredefinedTrustedUpdater>
                    <WindowsUpdateSupport Enable="yes"/>
                </TrustedUpdater>
                <DllDriverLockDown Enable="yes"/>
                <ExceptionPath Enable="no">
                    <ExceptionPathList/>
                </ExceptionPath>
                <TrustedCertification Enable="yes"/>
                <TrustedHash Enable="no"/>
                <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">
```

```
                    <Level>
                        <WarningLog Enable="yes" />
                        <InformationLog Enable="yes" />
                    </Level>
                    <BlockedAccessLog Enable="yes"/>
                    <ApprovedAccessLog Enable="yes">
                        <TrustedUpdaterLog Enable="yes"/>
                        <DllDriverLog Enable="yes"/>
                        <ExceptionPathLog Enable="yes"/>
                        <TrustedCertLog Enable="yes"/>
                        <TrustedHashLog Enable="yes"/>
                        <WriteProtectionLog Enable="yes"/>
                    </ApprovedAccessLog>
                    <SystemEventLog Enable="yes">
                        <ExceptionPathLog Enable="yes"/>
                        <WriteProtectionLog Enable="yes"/>
                    </SystemEventLog>
                    <ListLog Enable="yes"/>
                    <UsbMalwareProtectionLog Enable="yes"/>
                    <ExecutionPreventionLog Enable="yes"/>
                    <NetworkVirusProtectionLog Enable="yes"/>
                    <IntegrityMonitoringLog>
                        <FileCreatedLog Enable="yes"/>
                        <FileModifiedLog Enable="yes"/>
                        <FileDeletedLog Enable="yes"/>
                        <FileRenamedLog Enable="yes"/>
                        <RegValueModifiedLog Enable="yes"/>
                        <RegValueDeletedLog Enable="yes"/>
                        <RegKeyCreatedLog Enable="yes"/>
                        <RegKeyDeletedLog Enable="yes"/>
                        <RegKeyRenamedLog Enable="yes"/>
                    </IntegrityMonitoringLog>
                </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*.
	`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 9-21*. See *Agent Event Log Descriptions on page 13-4*.

Section	Description	Additional Information
ManagedMode	Parameters to configure Centralized Management functions	See *ManagedMode Section on page 9-25*.
Permission	Container for the Permission section	
AccountRef	Parameters to configure the Safe Lock console controls available to the Restricted User account	See *AccountRef Section on page 9-29*. 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. Configuration File `AccountGroup` Section Parameters

Parameter	Setting	Value	Description
Configuration			Container for the Configuration section
AccountGroup			Container for the AccountGroup section
Account	ID	<GUID>	Restricted User account GUID
	Enable	yes	Enable the Restricted User account
		no	Disable the Restricted User account
	Password	<Safe_Lock_password>	Password for the Restricted User account to access the Safe Lock console

Parameter	Setting	Value	Description
			Note The Safe Lock administrator and Restricted User passwords cannot be the same.

UI Section

Parameters to configure the display of the system tray icon

Table 9-3. Configuration File `UI` Section Parameters

Parameter	Setting	Value	Description
`Configuration`			Container for the Configuration section
`UI`			Container for the UI section
`SystemTaskTrayIcon`	`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. Configuration File `Feature` Section Parameters

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

PARAMETER	SETTING	VALUE	DESCRIPTION
`Feature`			Container for the Feature section
`ApplicationLockDown`	`LockDownMode`	`1`	Turn on Application Lockdown
		`2`	Turn off Application Lockdown
`WhiteList`	`RecentHistoryUnapprovedFilesLimit`	`0 - 65535`	Maximum number of entries in the Blocked Files log
`ScriptLockDown`	`Enable`	`yes`	Enable Script Lockdown
		`no`	Disable Script Lockdown
`Extension`	`ID`	<file_extension>	File extension for Script Lockdown to block For example, specify a value of `MSI` to block `.msi` files.
`Interpreter`		<file_name>	Interpreter for the specified file extension For example, specify **`msiexec.exe`** as the interpreter for `.msi` files.
`TrustedUpdater`			Container for the TrustedUpdater section
`PredefinedTrustedUpdater`	`Enable`	`yes`	Enable Trusted Updater
		`no`	Disable Trusted Updater
`RuleSet`			Container for RuleSet conditions

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

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

Parameter	Setting	Value	Description
	Issuer	<issuer>	Issuer of this certificate
TrustedHash	Enable	yes	Enable using the Trusted Hash List
		no	Disable using the Trusted Hash List
PredefinedTrustedHash	Type	updater	File matched by this hash value is treated as a Trusted Updater
		lockdown	File matched by this hash value is not treated as a Trusted Updater
	Hash	<SHA-1_hash_value>	SHA-1 hash value of this file
	Label	<label>	Description of this file
	AddToApprovedList	yes	Add the file matched by this hash value to the Approved List when it is accessed for the first time
		no	Do not add the file matched by this hash value to the Approved List
	Path	<file_path>	File path
	Note	<note>	Add a note for the file matched by this hash value
WriteProtection	Enable	yes	Enable Write Protection
		no	Disable Write Protection
	ActionMode	0	Allow actions such as edit, rename, and delete

Parameter	Setting	Value	Description
		`1`	Block actions such as edit, rename, and delete
	`ProtectApprovedList`	`yes`	Enable protection of the Approved List (in addition to the Write Protection List) when Write Protection is enabled
		`no`	Disable protection of the Approved List (in addition to the Write Protection List) when Write Protection is enabled
`List`			Container for the Write Protection List
`File`	`Path`	<file_path>	File path
`Folder`	`Path`	<folder_path>	Folder path
	`IncludeSubfolder`	`yes`	Use the files in the specified folder and its subfolders
		`no`	Use the files in the specified folder
`RegistryKey`	`Key`	<reg_key>	Registry key <reg_key> can be abbreviated or expanded as shown below: • HKEY_LOCAL_MACHINE\test HKLM\test • HKEY_CURRENT_CONFIG\test HKCC\test

Parameter	Setting	Value	Description
			• HKEY_CLASSES_ROOT\test HKCR\test • HKEY_CURRENT_USER\test HKCU\test • HKEY_USERS\test HKU\test
	IncludeSubkey	yes	Include any subkeys
		no	Do not include any subkeys
RegistryValue	Key	<reg_key>	Registry key <reg_key> can be abbreviated or expanded as shown below: • HKEY_LOCAL_MACHINE\test HKLM\test • HKEY_CURRENT_CONFIG\test HKCC\test • HKEY_CLASSES_ROOT\test HKCR\test • HKEY_CURRENT_USER\test HKCU\test • HKEY_USERS\test HKU\test

Parameter						Setting	Value	Description
						Name	<reg_value_name>	Registry value name
				ExceptionList				Container for the Write Protection Exception List
					Process	Path	<process_path>	Path of the process
					File	Path	<file_path>	File path
					Folder	Path	<folder_path>	Folder path
						IncludeSubfolder	yes	Use the files in the specified folder and its subfolders
							no	Use the files in the specified folder
					RegistryKey	Key	<reg_key>	Registry key <reg_key> can be abbreviated or expanded as shown below: • HKEY_LOCAL_MACHINE\test HKLM\test • HKEY_CURRENT_CONFIG\test HKCC\test • HKEY_CLASSES_ROOT\test HKCR\test • HKEY_CURRENT_USER\test

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

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

Parameter			Setting	Value	Description
			ActionMode	0	Allows DLL injections
				1	Blocks DLL injections
		ApiHookingPrevention	Enable	yes	Enable API Hooking Prevention
				no	Disable API Hooking Prevention
			ActionMode	0	Allow API hooking
				1	Block API hooking
		MemoryRandomization	Enable	yes	Enable Memory Randomization
				no	Disable Memory Randomization
		NetworkVirusProtection	Enable	yes	Enable Network Virus Protection
				no	Disable Network Virus Protection
			ActionMode	0	Allow action by detected network viruses
				1	Block action by detected network viruses
		IntegrityMonitoring	Enable	yes	Enable Integrity Monitoring
				no	Disable Integrity Monitoring
		Log			Container for configuring logs See *Log Section on page 9-21*.

Log Section

Parameters to configure individual log types

See *Agent Event Log Descriptions on page 13-4*.

TABLE 9-5. Configuration File `Log` Section Parameters

Parameter	Setting	Value	Description
`Configuration`			Container for the Configuration section
`Feature`			Container for the Feature section
`Log`			Container for configuring logs
`EventLog`	`Enable`	`yes`	Log the Safe Lock events specified in the following elements
		`no`	Do not log the Safe Lock events specified in the following elements
`Level`			Container for configuring log levels
`WarningLog`	`Enable`	`yes`	Log “Warning” level events related to Safe Lock
		`no`	Do not log “Warning” level events related to Safe Lock
`InformationLog`	`Enable`	`yes`	Log “Information” level events related to Safe Lock
		`no`	Do not log “Information” level events related to Safe Lock
`BlockedAccessLog`	`Enable`	`yes`	Log files blocked by Safe Lock
		`no`	Do not log files blocked by Safe Lock

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

Parameter	Setting	Value	Description
ExceptionPathLog	Enable	yes	Log exceptions to Application Lockdown
		no	Do not log exceptions to Application Lockdown
WriteProtectionLog	Enable	yes	Log Write Protection events
		no	Do not log Write Protection events
ListLog	Enable	yes	Log events related to the Approved list
		no	Do not log events related to the Approved list
USBMalwareProtectionLog	Enable	yes	Log events that trigger USB Malware Protection
		no	Do not log events that trigger USB Malware Protection
ExecutionPreventionLog	Enable	yes	Log events that trigger Execution Prevention
		no	Do not log events that trigger Execution Prevention
NetworkVirusProtectionLog	Enable	yes	Log events that trigger Network Virus Protection
		no	Do not log events that trigger Network Virus Protection
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

Parameter	Setting	Value	Description
FileModifiedLog	Enable	yes	Log file modified events
		no	Do not log file modified events
FileDeletedLog	Enable	yes	Log file and folder deleted events
		no	Do not log file and folder deleted events
FileRenamedLog	Enable	yes	Log file and folder renamed events
		no	Do not log file and folder renamed events
RegValueModifiedLog	Enable	yes	Log registry value modified events
		no	Do not log registry value modified events
RegValueDeletedLog	Enable	yes	Log registry value deleted events
		no	Do not log registry value deleted events
RegKeyCreatedLog	Enable	yes	Log registry key created events
		no	Do not log registry key created events
RegKeyDeletedLog	Enable	yes	Log registry key deleted events
		no	Do not log registry key deleted events
RegKeyRenamedLog	Enable	yes	Log registry key renamed events
		no	Do not log registry key renamed events

PARAMETER	SETTING	VALUE	DESCRIPTION
DebugLog	Enable	yes	Log debugging information
		no	Do not log debugging information

ManagedMode Section

Parameters to configure Centralized Management functions

TABLE 9-6. Configuration File `ManagedMode` Section Parameters

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

PARAMETER	SETTING	VALUE	DESCRIPTION
`Server`			Container for configuring Safe Lock Intelligent Manager
`HostName`		<hostname>	Specify the host name of the Intelligent Manager server
`FastPort`		<logs_port>	Specify secure port for collecting logs and status (formerly Fast Lane)
`SlowPort`		<files_port>	Specify secure port for collecting files for scanning (formerly Slow Lane)
`ApiKey`		<API_key>	Specify API key
`Message`			Container for configuring automated messages to Safe Lock Intelligent Manager
`Register`	`Trigger`	`1`	Send as soon as possible after the event occurs
		`2`	Do not send unless requested to by Intelligent Manager
`Unregister`	`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
UpdateStatus	Trigger	1	Send as soon as possible after the event occurs
		2	Do not send unless requested to by Intelligent Manager
UploadBlockedEvent	Trigger	1	Send as soon as possible after the event occurs
		2	Do not send unless requested to by Intelligent Manager
CheckFileHash	Trigger	1	Send as soon as possible after the event occurs
		2	Do not send unless requested to by Intelligent Manager
QuickScanFile	Trigger	1	Send as soon as possible after the event occurs
		2	Do not send unless requested to by Intelligent Manager
MessageRandomization **Note** Safe Lock agents respond as soon as possible to direct requests from Safe Lock Intelligent Manager. For details, refer to Applying Message Time Groups in the Safe Lock Intelligent Manager Administrator's Guide.			
	TotalGroupNum	Positive Integer (>= 1)	Specify the total number of message time groups

Parameter	Setting	Value	Description
	OwnGroupIndex	Zero or Positive Integer, < TotalGroupNum	Specify the message time group ID number of this Safe Lock agent
	TimePeriod	Zero or Positive Integer	Specify the duration of time in whole seconds that this message time group ID number will send automated messages to Intelligent Manager when this group's message-sending cycle is active **Note** Message time groups do not become active if their duration is set to zero (0).
Proxy	Mode	0	Do not use a proxy (direct access)
		1	Use a proxy (manual setting)
		2	Synchronize proxy settings with Internet Explorer
HostName		<proxy_hostname>	Specify the proxy host name
Port		<proxy_port>	Specify the proxy port number
UserName		<proxy_user_name>	Specify the proxy user name

Parameter	Setting	Value	Description
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. Configuration File `AccountRef` Section Parameters

Parameter	Setting	Value	Description
Configuration			Container for the Configuration section
Permission			Container for the Permission section
AccountRef			Container for the AccountRef section
UIControl	ID	DetailSetting	Access the features and functions on the Safe Lock console **Settings** page **Note** The **Password** page is not available to the Restricted User account.
		LockUnlock	Access the Application Lockdown setting on the **Overview** screen
		LaunchUpdater	Access the **Automatically add files created or modified by the selected application installer** option when a Restricted User

PARAMETER	SETTING	VALUE	DESCRIPTION
			clicks **Add Item** on the **Approved List** screen
		`RecentHistoryUnapprovedFIles`	Access the Block logs if a Restricted User clicks **Last application blocked** on the **Overview**screen
		`ImportExportList`	Access the **Import List** and **Export List** buttons
		`ListManagement`	Access the following items on the **Approved List** screen: • The **Delete Item** button • The **Update Hash** button • The **Add Item** > **Add Files/ Folders** menu
	`State`	`yes`	Enable the permission specified by `ID`
		`no`	Disable the permission specified by `ID`

Chapter 10

Local Agent Uninstallation

This chapter describes Trend Micro Safe Lock agent uninstallation procedures.

Topics in this chapter include:

Uninstalling Agents from Windows

Note

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

Procedure

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

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

OPTION	DESCRIPTION
If you use one of the following operating systems: • Windows Server 2012 • Windows Server 2008 • Windows 8 • Windows 7 • Windows Vista	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: • Windows Server 2003 • Windows XP • Windows 2000	a. Go to **Start** > **Control Panel** > **Add or Remove Programs**. b. In the list, select Trend Micro Safe Lock. c. Click **Remove**.

   Safe Lock Setup opens in uninstaller mode.

2. After Safe Lock Setup opens, click **Next**.

3. Provide the Safe Lock administrator password, and click **Next**.

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

Chapter 11

Troubleshooting & FAQs

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

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

Using the Support Portal

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

Procedure

1. Go to http://esupport.trendmicro.com.
2. Select a product or service from the appropriate drop-down list and specify any other related information.

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

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

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

Trend Community

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

http://community.trendmicro.com/

Contacting Trend Micro

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

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

- Worldwide support offices:

  http://www.trendmicro.com/us/about-us/contact/index.html

- Trend Micro product documentation:

  http://docs.trendmicro.com

Related information

➥ *Speeding Up the Support Call*

Speeding Up the Support Call

To improve problem resolution, have the following information available:

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

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

Other Resources

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

Related information

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

TrendEdge

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

See the latest information added to TrendEdge at:

http://trendedge.trendmicro.com/

Download Center

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

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

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

TrendLabs

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

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

Learn more about TrendLabs at:

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

About Trend Micro

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

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

http://www.trendmicro.com

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

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**.

Tip

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

- Before installation, modify the Setup.ini file. See *Setup.ini File Arguments > EventLog Section* in the Safe Lock Installation Guide.
- After installation, modify the configuration file. See *Configuration File Parameters > Log Section on page 9-21*.

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.

Event ID	Task Category	Level	Description
1009	System	Information	Product activated.
1010	System	Information	Product deactivated.
1011	System	Warning	License Expired. Grace period enabled.
1012	System	Warning	License Expired. Grace period ended.
1013	System	Information	Product configuration import started: <full_path>
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.

Event ID	Task Category	Level	Description
1032	System	Information	DLL Injection Prevention set to Block.
1033	System	Information	DLL Injection Prevention enabled.
1034	System	Warning	DLL Injection Prevention disabled.
1035	System	Information	Auto Trusted Update enabled.
1036	System	Information	Auto Trusted Update disabled.
1037	System	Information	DLL/Driver Lockdown enabled.
1038	System	Warning	DLL/Driver Lockdown disabled.
1039	System	Information	Script Lockdown enabled.
1040	System	Warning	Script Lockdown disabled.
1041	System	Information	Script added. [Details] File extension: <extension> Interpreter: <interpreter>
1042	System	Information	Script removed. [Details] File extension: <extension> Interpreter: <interpreter>
1044	System	Information	Exception path enabled.
1045	System	Information	Exception path disabled.

Event ID	Task Category	Level	Description
1046	System	Information	Event Log settings changed. [Details] Windows Event Log: <ON|off> System Log: <on|OFF> Exception Path Log: <ON|off> Write Protection Log: <ON|off> List Log: <ON|off> Approved Access Log: <ON|off> DLL Driver Log: <on|OFF> Trusted Updater Log: <ON|off> Exception Path Log: <ON|off> Trusted Certification Log: <ON|off> Write Protection Log: <ON|off> Blocked Access Log: <ON|off> USB Malware Protection Log: <on|OFF> Execution Prevention Log: <on|OFF> Network Virus Protection Log: <on|OFF> Integrity Monitoring Log File Created Log: <ON|off> File Modified Log: <ON|off> File Deleted Log: <ON|off> File Renamed Log: <ON|off> RegValue Modified Log: <ON|off> RegValue Deleted Log: <ON|off> RegKey Created Log: <ON|off> RegKey Deleted Log: <ON|off> RegKey Renamed Log: <ON|off> Debug Log: <on|OFF>

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

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

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

Event ID	Task Category	Level	Description
1075	System	Information	Quarantined file is deleted. [Details] Original Location: <full_path> Source: <source>
1076	System	Information	Integrity Monitoring enabled.
1077	System	Information	Integrity Monitoring disabled.
1078	System	Information	Root cause analysis report failed. [Details] Access Image Path: <full_path>
1079	System	Information	Server certificate imported: <full_path>
1080	System	Information	Server certificate exported to: <full_path>
1081	System	Information	Managed mode configuration imported: <full_path>
1082	System	Information	Managed mode configuration exported to: <full_path>
1083	System	Information	Managed mode enabled.
1084	System	Information	Managed mode disabled.
1085	System	Information	When Write Protection is enabled, it includes the Write Protection List and the Approved List.
1086	System	Warning	When Write Protection is enabled, it includes the Write Protection List only.
1087	System	Information	Event log settings changed.
1088	System	Information	Windows Update Support enabled.
1089	System	Information	Windows Update Support disabled.

Event ID	Task Category	Level	Description
1094	System	Information	Trend Micro Safe Lock updated. File applied: <file_name>
1096	System	Information	Trusted Hash List enabled.
1097	System	Information	Trusted Hash List disabled.
1098	System	Information	Event log settings changed.
1500	List	Information	Trusted Update started.
1501	List	Information	Trusted Update stopped.
1502	List	Information	Approved List import started: <full_path>
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>

Event ID	Task Category	Level	Description
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>
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>

EVENT ID	TASK CATEGORY	LEVEL	DESCRIPTION
1517	System	Information	Hash value added to the Trusted Hash List. [Details] Label: <label> Hash: <hash_value> Type: <type> Add to Approved List: <yes|no> Path: <file_path> Note: <note>
1518	System	Information	Hash value removed from the Trusted Hash List. [Details] Label: <label> Hash: <hash_value> Type: <type> Add to Approved List: <yes|no> Path: <file_path> Note: <note>
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>
2021	Access Approved	Warning	File access allowed: <full_path> An error occurred while checking the Trusted Hash List. [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode>

Event ID	Task Category	Level	Description
2503	Access Blocked	Warning	Change of File/Folder blocked: <full_path> [Details] Access Image Path: <full_path> Access User: <user_name> Mode: <mode>
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>

EVENT ID	TASK CATEGORY	LEVEL	DESCRIPTION
2508	Access Blocked	Warning	Failed to take specified action: <full_path> [Details] Action: <action> Source: <source>
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>

Event ID	Task Category	Level	Description
3000	USB Malware Protection	Warning	Device access allowed: <full_path> [Details] Access Image Path: <full_path> Access User: <user_name> Device Type: <type>
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>

Event ID	Task Category	Level	Description
3501	Network Virus Protection	Warning	Network virus blocked: <name> [Details] Protocol: TCP Source IP Address: <ip_address> Source Port: <port> Destination IP Address: <ip_address> Destination Port: <port>
4002	Process Protection Event	Warning	API Hooking allowed: <full_path> [Details] Threat Image Path: <full_path> Threat User: <user_name>
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>

Event ID	Task Category	Level	Description
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>
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>

Event ID	Task Category	Level	Description
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>
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>

Event ID	Task Category	Level	Description
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>
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.
0x80040207	Busy. Request ignored.
0x00040208	Retry. (Usually the result of a task taking too long)
0x80040208	System Reserved. (Not used)
0x80040209	The file path is too long.
0x0004020a	System Reserved. (Not used)
0x8004020b	System Reserved. (Not used)
0x0004020c	System Reserved. (Not used)
0x0004020d	System Reserved. (Not used)
0x8004020d	System Reserved. (Not used)
0x0004020e	Reboot required.
0x8004020e	Reboot required for unexpected reason.
0x0004020f	Allowed to perform task.
0x8004020f	Permission denied.

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

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

Index

TREND MICRO™

TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: SLEM27315/160128