TREND MICRO™

1.1

# TREND MICRO™ Safe Lock

## Administrator's Guide

A powerful lockdown solution for fixed-function computers

Endpoint Security

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

http://docs.trendmicro.com



Document Part No.: SLEM15951_130506

Release Date: May 2013

The documentation for Trend Micro Safe Lock describes the main features of the software and installation instructions for your production environment. Read through it before installing or using the software.

Detailed information about how to use specific features are available in the online Knowledge Base at the Trend Micro website.

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*.

Please evaluate this document at the following site:

http://www.trendmicro.com/download/documentation/rating.asp

# Table of Contents

## Preface



## Chapter 1: Introduction



## Chapter 2: Configuring Main Console Settings

## Chapter 3: Using the Command Line Interpreter



## Chapter 4: Troubleshooting

## Chapter 5: Getting Help



## Index

# Preface

This Administrator's Guide introduces Trend Micro Safe Lock and guides administrators through installation and deployment.

Topics in this chapter include:

# What's New in This Version

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

## Trend Micro Safe Lock 1.1 Features and Enhancements

Trend Micro Safe Lock 1.1 includes the following new features and enhancements

| Feature | Description |
|---|---|
| DLL/Driver Lockdown | Prevents unapproved DLL or drivers from being loaded into memory |
| Script Lockdown | Prevents unapproved script files from being run |
| Predefined Trusted Updater List | Allows installers or updaters to be run without the need for a user to run the Trusted Updater |

# Safe Lock Documentation

Trend Micro Safe Lock documentation includes the following:

**Table 1. Trend Micro Safe Lock Documentation**

| Documentation | Description |
|---|---|
| Installation Guide | A PDF document that discusses requirements and procedures for installing Safe Lock. |
| Administrator's Guide | A PDF document that discusses getting started information and Safe Lock usage and management. |
| Readme file | Contains a list of known issues and basic installation steps. It may also contain late-breaking product information not found in the printed documentation. |

| Documentation | Description |
|---|---|
| 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:<br><br>http://esupport.trendmicro.com |

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

http://docs.trendmicro.com

# Audience

Trend Micro Safe Lock documentation is intended for administrators responsible for Safe Lock management, including installation. These administrators are expected to have advanced computer management knowledge.

# Document Conventions

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

**Table 2. Document Conventions**

| Convention | Description |
|---|---|
| UPPER CASE | Acronyms, abbreviations, and names of certain commands and keys on the keyboard |
| **Bold** | Menus and menu commands, command buttons, tabs, and options |
| *Italics* | References to other documents |
| `Monospace` | Sample command lines, program code, web URLs, file names, and program output |

| CONVENTION | DESCRIPTION |
|---|---|
| **Navigation** > **Path** | The navigation path to reach a particular screen<br>For example, **File** > **Save** means, click **File** and then click **Save** on the interface |
|  **Note** | Configuration notes |
|  **Tip** | Recommendations or suggestions |
|  **Important** | Information regarding required or default configuration settings and product limitations |
|  **WARNING!** | Critical actions and configuration options |

# Terminology

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

**TABLE 3. Safe Lock Terminology**

| TERMINOLOGY | DESCRIPTION |
|---|---|
| ASLR | Address Space Layout Randomization/memory randomization |
| Administrator | The person responsible for installing and/or managing Safe Lock. |
| CLI | Command line interpreter. |
| Console | The user interface for configuring and managing Safe Lock. |

# Chapter 1

# Introduction

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

Topics in this chapter include:

# About Trend Micro Safe Lock

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

# Features and Benefits

Trend Micro Safe Lock includes the following features and benefits.

## Application Lockdown

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

## Exploit Protection

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 computer, and execution prevention, which helps prevent threats from spreading to the computer or from running.

## Easy Management

When software needs to be installed or updated, the Trusted Updater and Pre-approved Trusted Updater List provide an easy way to make changes to the computer 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 separate Administrator and Restricted User accounts, 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 easily use the Windows main console, while system administrators can take advantage of the command line interface 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 onto the computer, without the need to update the Approved List or unlock the computer.

## Process 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 though either the main console or the command line interpreter (CLI), while system updates can be applied without unlocking the computer through the Pre-approved Trusted Updater List or by using the Trusted Updater.

Consider this typical use case scenario:

1. Set up the Approved List and lock the computer so that unapproved applications cannot be run.

2. Use the Trusted Updater to update or install software whose installer is not on the Pre-approved Trusted Updater list.

3. Configure and enable the Restricted User account for later maintenance.

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

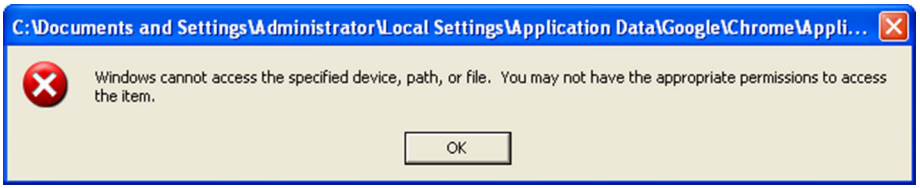



**FIGURE 1-1. Trend Micro Safe Lock blocking message**

# 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, administrators can specify the features available to the Restricted Users account.

**TABLE 1-1. Safe Lock Accounts**

| ACCOUNT | DETAILS |
|---|---|
| Administrator | • Default account<br>• Full access to Safe Lock functions<br>• Can use both the main console and command line interface |

| ACCOUNT | DETAILS |
|---|---|
| Restricted User | • Secondary maintenance account<br>• Limited access to Safe Lock functions<br>• Can only use the main console |

To enable the Restricted User account, see *Working with Passwords on page 2-16*. To sign in with a specific account, specify the password for that account. To change which features the Restricted User can access, see *Working with the Configuration File on page 3-10*.

# Chapter 2

# Configuring Main Console Settings

This chapter describes how to configure Trend Micro Safe Lock Windows using the main console.

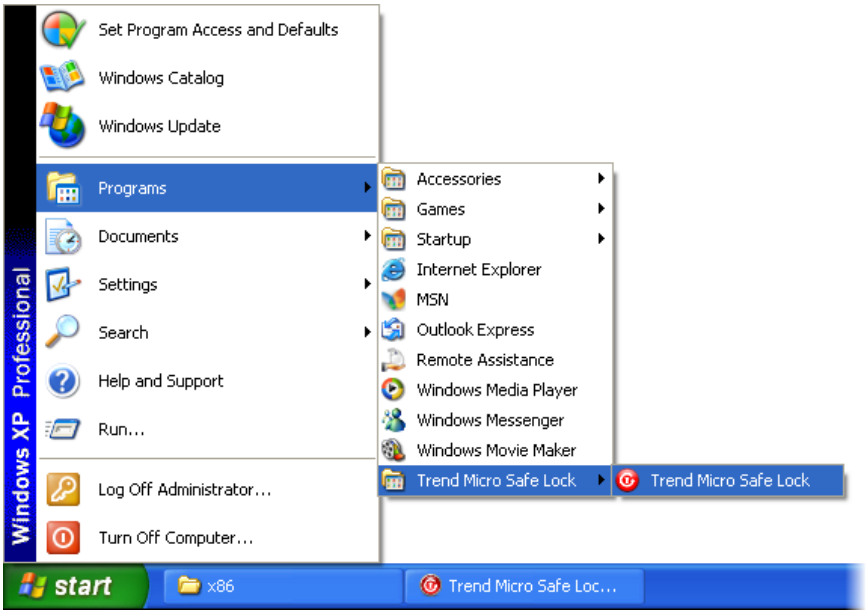
Topics in this chapter include:

# Setting Up the Approved List

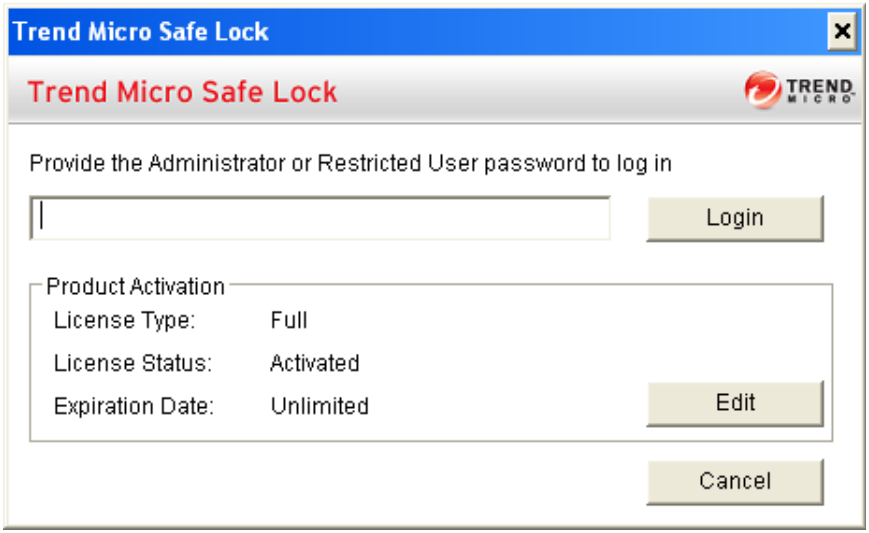
Before Trend Micro Safe Lock can protect the computer, it must check the computer for existing applications and installers necessary for the system to run correctly.

**Procedure**

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

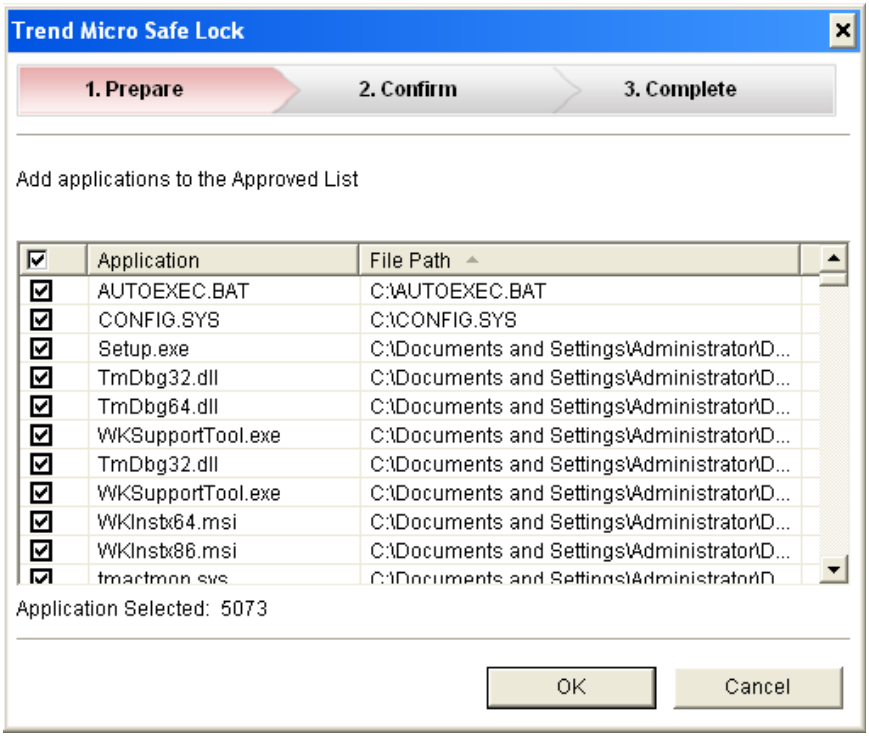



2. Provide the password and click **Login**.




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

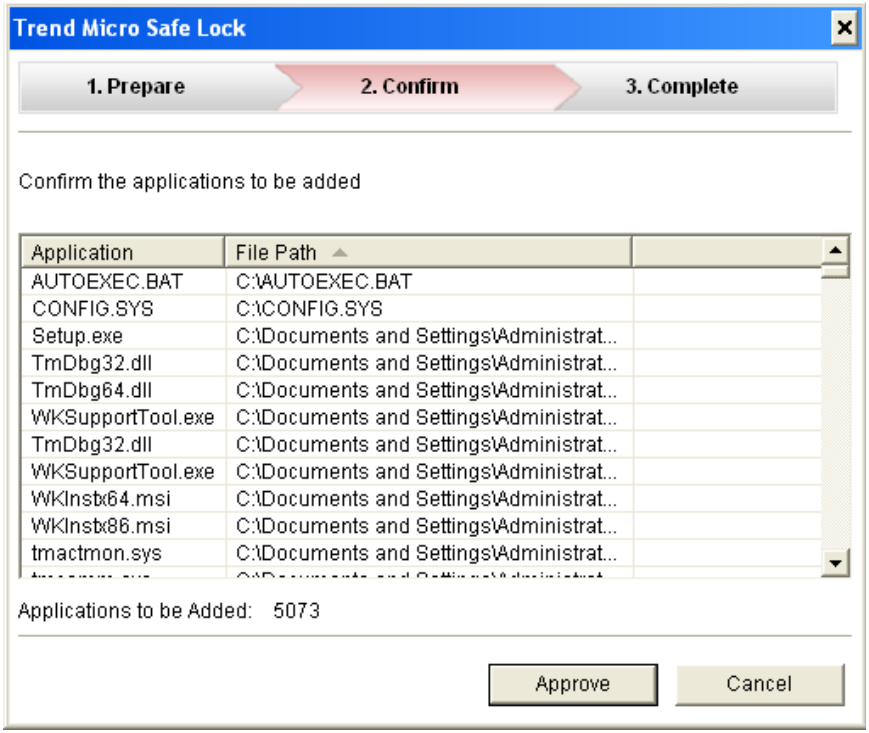

4. When the check is complete, Safe Lock provides a list of applications currently on the computer. Deselect any applications that should not be added to the Approved List, and click **OK**.



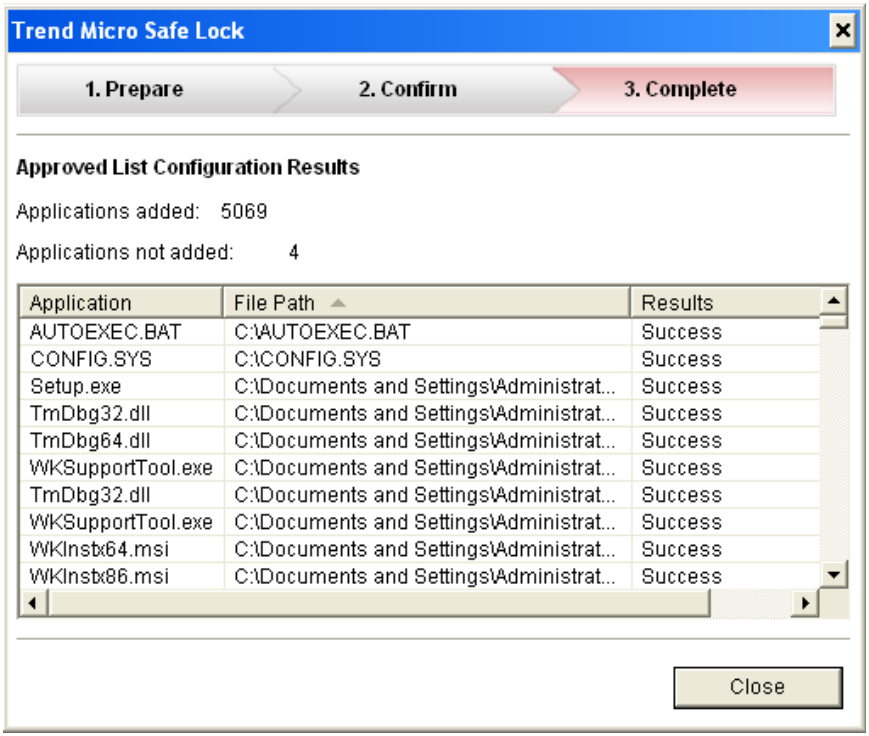

**Note**

When Trend Micro Safe Lock is locked, any applications that are not added to the Approved List will no longer be able to run.

5. Confirm the listed applications to be added to the Approved List, and click **Approve**.




6. Once the applications have been added, click **Close**.




# Understanding the Main Console

The main console provides easy access to commonly used features in Trend Micro Safe Lock. To configure which features the Restricted User account can access, see *Working with the Configuration File on page 3-10*.

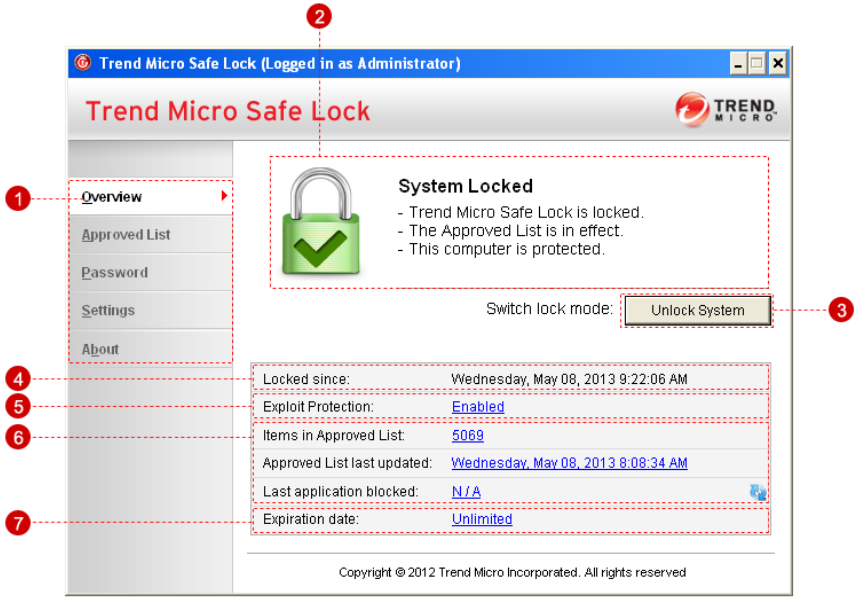



**FIGURE 2-1. The Safe Lock main console**

The following table describes the features available on the main console.

**TABLE 2-1. Main Console Feature Descriptions**

| # | ITEM | DESCRIPTION |
|---|---|---|
| 1 | Left-hand navigation | • **Overview**: displays the software status<br>• **Approved List**: displays applications allowed to run and lets users manage the list<br>• **Password**: changes the Administrator Restricted User passwords (only available to administrators)<br>• **Settings**: enables or disables vulnerability protection settings and export or import the system configuration<br>• **About**: displays the product and component version numbers |
| 2 | Status information | Displays the current status of the software. |
| 3 | **Lock System/Unlock System** | Locking the system prevents applications not on the Approved List from running. |
| 4 | **Locked since/Unlocked Since** | Displays the date when the software was last locked or unlocked. |
| 5 | **Exploit Protection** | • **Enabled**: all Exploit Protection features are enabled<br>• **Enabled (Partly)**: some Exploit Protection features are enabled<br>• **Disabled**: no Exploit Protection features are enabled<br>Click the status to open the Settings page. |
| 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 | **Expiration date** | Displays when the software expires. Click the date to provide a new Activation Code. |

## Status Icons

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

**Note**

System Tray icons display if they were enabled during installation.

**TABLE 2-2. Status Icon Descriptions**

| MAIN 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. |

# Understanding the Approved List

Use the Approved List to display the files that Safe Lock allows to run or make changes to the computer. To configure which features are available to the Restricted User account, see *Working with the Configuration File on page 3-10*.

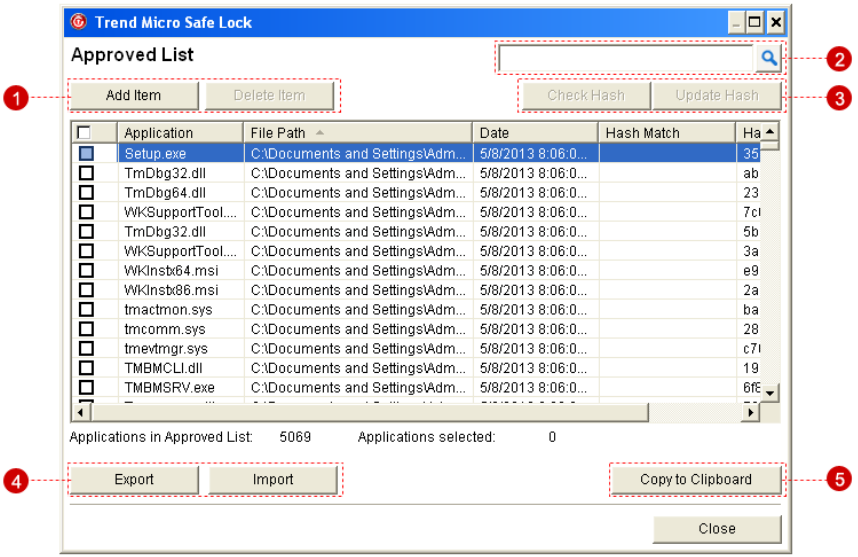



**FIGURE 2-2. The Safe Lock Approved List**

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

**TABLE 2-3. Approved List Item Descriptions**

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

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

# Configuring the Approved List

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

**TABLE 2-4. Methods for Adding Applications to the Approved List**

| OPTION | WHEN TO USE |
|---|---|
| **Add existing files and folders** | Choose this option when the software already exists on the computer and is up-to-date. Adding a file grants permission to run the file, but does not alter the file or the system.<br><br>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. |
| **Run an installer or updater** (Trusted Updater) | Choose this option to open the Trusted Updater when updating the computer or installing new software.<br><br>For example, if Mozilla Firefox needs to be installed or updated, use the Trusted Updater. Trend Micro Safe Lock adds or updates any files modified by an installer to the Approved List. |

## Adding or Removing Files

**Procedure**

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

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

   To add an item:

   a. Click **Add Item**, select **Add existing files and folders**, 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 application or folder to add, and click **Open**.

   d. In the window that opens, 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 **Run an installer or updater**, 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` and `.msi` files can be added to the Trusted Updater.

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

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


**FIGURE 2-3. The Safe Lock Trusted Updater**

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

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

## Exporting or Importing the Approved List

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

**Procedure**

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

   To export the Approved List:

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

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

   To import an Approved List:

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

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

# Understanding Hashes

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

The following table describes the hash check status icons.

**TABLE 2-5. Hash Check Status Icons**

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

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

# Configuring Passwords

While the Administrator and Restricted User passwords can be changed from the main console, only the Administrator can change passwords. To log on with the Administrator account, provide the Administrator password.

**Important**

The 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 password and click **Login**.
3. Click the **Password** menu item to display the Administrator password page.

   To change the Administrator password:

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

**WARNING!**

The only way to recover the Administrator password is by reinstalling the operating system.

To create a Restricted User password:

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

# Configuring Settings

Administrators can enable or disable specific Exploit Protection features depending on the needs of their organization. However, not all settings are available through the main console. See *Working with the Configuration File on page 3-10* for information about advanced configuration.

## Exploit Protection Settings

Safe Lock offers the following protection features.

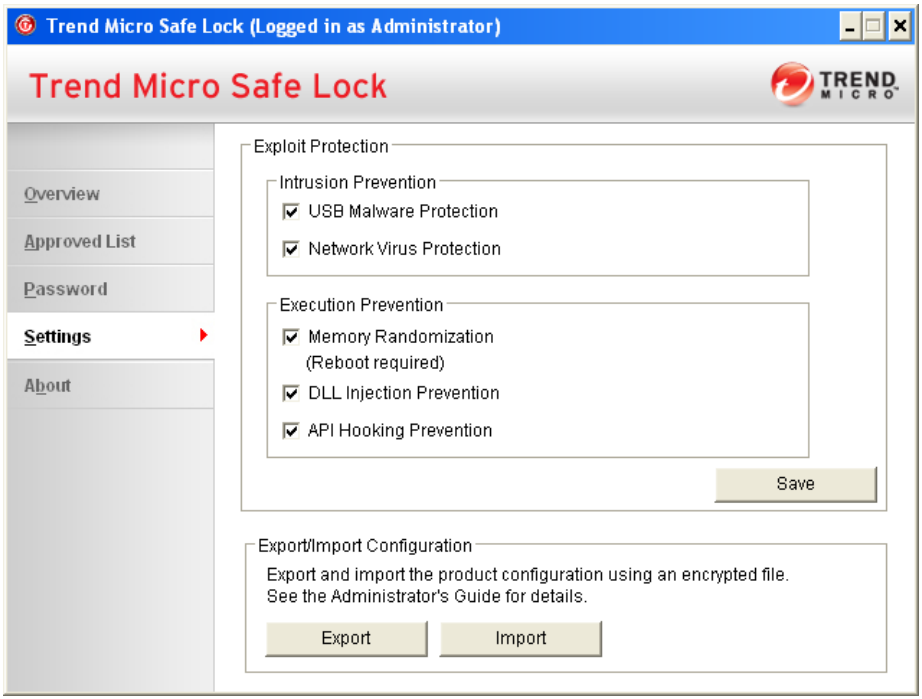



**FIGURE 2-4. Safe Lock settings screen**

**TABLE 2-6. Intrusion Prevention Mechanisms**

| SETTING | DESCRIPTION |
|---|---|
| USB Malware Protection | USB Malware Protection prevents threats on USB or remote drives from infecting the local computer. Just viewing the contents of the drive may be enough to pass along an infection.<br><br>Enable this feature to prevent files on USB devices from infecting the computer. |

| Setting | Description |
|---|---|
| Network Virus Protection | Network Virus Protection scans incoming and outgoing network traffic, blocking threats from infected computers or other devices on the network.<br><br>Enable this feature to prevent threats on the network from infecting the computer. |

**Table 2-7. Execution Prevention Mechanisms**

| Setting | Description |
|---|---|
| Memory Randomization | Address Space Layout Randomization (ASLR) helps prevent shellcode injection by randomly assigning memory locations for important functions, forcing an attacker to guess the memory location of specific processes.<br><br>Enable this feature on older operating systems such as Windows XP or Windows Server 2003, which may lack or offer limited ASLR support.<br><br>  **Note**<br>The computer 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.<br><br>Never disable this feature except in troubleshooting situations since it protects the system from a wide variety of serious threats. |
| API Hooking Prevention | API Hooking Prevention detects and blocks malicious software that tries to intercept and alter messages used in critical processes within the operating system.<br><br>Never disable this feature except in troubleshooting situations since it protects the system from a wide variety of serious threats. |

## Enabling or Disabling Exploit Protection Settings

**Note**

By default, Trend Micro Safe Lock enables all Exploit Protection 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 Protection settings.
4. Enable or disable the desired features.
5. Click **Save**.

## Exporting or Importing a Configuration File

Trend Micro Safe Lock encrypts the configuration file before export. Users must be decrypt the configuration file before modifying the contents. See *Working with the Command Line Interpreter on page 3-2* for information about decrypting the file. See *Working with the Configuration File on page 3-10* for information about modifying the system configuration.

**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.

# Chapter 3

# Using the Command Line Interpreter

This chapter describes how to configure and use Trend Micro Safe Lock using the command line interpreter.

Topics in this chapter include:

# Working with the Command Line Interpreter

Administrators can work with Trend Micro Safe Lock directly from the command line using the command interpreter `SLCmd.exe`, located in the Trend Micro Safe Lock installation folder. By default, it appears here:

```
c:\Program Files\Trend Micro\Trend Micro Safe Lock\
```

**Note**

To use `SLCmd.exe`, open a command line prompt with Windows administrator privileges.

## Command Line Interpreter and Main Console Function Comparison

The following table lists the Trend Micro Safe Lock features available in each interface..

**TABLE 3-1. Command Line Interpreter and Main Console Function Comparison**

| FUNCTION | COMMAND LINE INTERPRETER | MAIN CONSOLE |
|---|---|---|
| Account Management | Yes | Yes |
| Approved List Management | Yes | Yes |
| Decrypt/Encrypt configuration file | Yes | No |
| Display the blocked log | Yes | Yes |
| Export/Import Approved List | Yes | Yes |
| Export/Import configuration | Yes | Yes |
| Install | Yes | Yes |
| Lock/Unlock | Yes | Yes |
| License Management | Yes | Yes |
| Settings | Limited | Limited |

| Function | Command Line Interpreter | Main Console |
|---|---|---|
| Start/Stop Trusted Updater | Yes | Yes |
| Start/Stop the service | Yes | No |
| Uninstall | No | No |

Not all settings are available through the command line interpreter or main console. See *Working with the Configuration File on page 3-10* for information about modifying the system configuration.

## Opening the Command Line

**Procedure**

1. Choose one of the following ways to open a command prompt with Windows administrator privileges.

   Using the Search Bar only:

   a. Open the Start menu and type `cmd.exe`.

   b. Hold down the CTRL and SHIFT keys, and press ENTER.

   c. When prompted for permission, press ENTER.

   Using the Search Bar and mouse:

   a. Open the Start menu and type `cmd.exe`.

   b. Right click cmd.exe and select **Run as administrator**.

   c. When prompted for permission, click **OK**.

   Using the Run... dialog:

   a. Hold down the Windows key and press R.

   b. In the window that opens, type `runas /user:administrator cmd.exe` and press ENTER.

c. When promoted for the Administrator password, type the Windows administrator password (not the Trend Micro Safe Lock Administrator password).

2. Navigate to the Trend Micro Safe Lock installation folder using the **CD** command.

   To reach the default location, type the following command: `cd c:\Program Files\Trend Micro\Trend Micro Safe Lock\` and press ENTER.

3. Type `SLCmd` and press ENTER to display the list of available commands.

## Command Line Interpreter Commands

To use a command, type `SLCmd` and the desired command. The following table lists the commands available using the command line interpreter, `SLCmd.exe`.

**Note**

Only the Trend Micro Safe Lock Administrator can use the command line interpreter, and `SLCmd.exe` will prompt for the Administrator password before running a command.

**TABLE 3-2. SLCmd Commands**

| COMMAND | DESCRIPTION |
|---|---|
| `-p [password]` | Authenticates the user so the command will run. |
| `start service` | Starts the Safe Lock service. |
| `stop service` | Stops the Safe Lock service. |
| `status` | Displays the current Safe Lock status. |
| `show settings` | Displays the current settings. |
| `version` | Displays version information. |
| `set lock [enable\|disable]` | Locks or unlocks Safe Lock. If no option is specified, the current status displays. |

| COMMAND | DESCRIPTION |
|---|---|
| `set dlldriverlockdown [enable\|disable]` | Enables or disables DLL/driver lockdown. If no option is specified, the current status displays. |
| `set script [enable\|disable]` | Enables or disables script lockdown. If no option is specified, the current status displays. |
| `set user [enable\|disable]` | Enables or disables the Restricted User account. If no option is specified, the current status displays. |
| `set userpassword [new password]` | Creates or changes the Restricted User password. |
| `set adminpassword [new password]` | Changes the Administrator password. |
| `add approvedlist [path]` | Adds a file or folder to the Approved List. |
| `add approvedlist -r [path]` | Adds a folder and related subfolders to the Approved List. |
| `remove approvedlist [path]` | Removes a file from the Approved List. |
| `show approvedlist` | Lists the files on the Approved List. |
| `check approvedlist` | Checks files on the Approved List, prompts to update hash mismatches, and displays simple results. |
| `check approvedlist -f` | Checks files on the Approved List, automatically updates hash mismatches, and displays detailed results. |
| `check approvedlist -q` | Checks files on the Approved List, automatically updates hash mismatches, and displays simple results. |
| `check approvedlist -v` | Checks files on the Approved List, prompts to update hash mismatches, and displays detailed results. |
| `import approvedlist [path]` | Imports the Approved List from the specified path and appends the existing list. |

| COMMAND | DESCRIPTION |
|---|---|
| `import approvedlist -o [path]` | Imports the Approved List from the specified path and overwrites the existing list. |
| `export approvedlist [path]` | Exports the Approved List to the specified path. |
| `add script [path] [interpreter 1] [interpreter2]...` | Adds a script rule. More than one script interpreter can be specified using spaces between interpreter names. |
| `remove script [path] [interpreter 1] [interpreter2]...` | Removes a script rule. More than one script interpreter can be specified using spaces between interpreter names. |
| `show script` | Displays all script rules. |
| `add predefinedtrustedupdater -e [path]` | Adds a path to the Trusted Updater exception list. |
| `add predefinedtrustedupdater -u [path]` | Adds a path and all subfolders to the Trusted Updater exception list. |
| `add predefinedtrustedupdater -t [process\|file\|folder\| folderandsub]` | Adds the following rules to the Trusted Updater exception list:<br>• `process`: process launch<br>• `file`: file access by the appropriate script interpreter or installer<br>• `folder`: process launch or file access<br>• `folderandsubfolder`: process launch or file access |
| `add predefinedtrustedupdater -p [path]` | Adds a path and parent process using backward match. If no path is specified, any parent process will match. |
| `add predefinedtrustedupdater -al [enable\|disable]` | Sets the status of the Approved List check. The default value is enable. |
| `add predefinedtrustedupdater -l [label]` | Adds a label to the specified rule. If not specified, a label is assigned automatically. |

| COMMAND | DESCRIPTION |
|---|---|
| `remove predefinedtrustedupdater -e [path]` | Removes a path from the Predefined Trusted Updater exception list. |
| `remove predefinedtrustedupdater -l [label]` | Removes a label to the specified rule. If not specified, a label is assigned automatically. |
| `show predefinedtrustedupdater` | Lists the Predefined Trusted Updater rules |
| `show predefinedtrustedupdater -e` | Lists the items of the Predefined Trusted Updater exception list. |
| `start trustedupdater [path]` | Allows installers from the specified path to run. |
| `stop trustedupdater` | Adds files created or modified by the allowed installers to the Approved List. |
| `show blockedlog` | Lists the applications that have been prevented from running. |
| `set usbmalwareprotection [enable\|disable]` | Enables or disables USB Malware Protection. |
| `set memoryrandomization [enable\|disable]` | Enables or disables Memory Randomization. |
| `set apihookingprevention [enable\|disable]` | Enables or disables API Hooking Prevention. |
| `set dllinjectionprevention [enable\|disable]` | Enables or disables DLL Injection Prevention. |
| `set networkvirusprotection [enable\|disable]` | Enables or disables Network Virus Protection. |
| `set predefinedtrustedupdater [enable\|disable]` | Enables or disables the Predefined Trusted Updater. |
| `import configuration [path]` | Imports the configuration file from the specified path. |
| `export configuration [path]` | Exports the configuration file to the specified path. |

| COMMAND | DESCRIPTION |
|---|---|
| `import predefinedtrustedupdater [path]` | Imports the Predefined Trusted Updater list to the specified path and overwrites the existing list. |
| `export predefinedtrustedupdater [path]` | Exports the Predefined Trusted Updater list to the specified path. |
| `encrypt configuration [source] [target]` | Encrypts the configuration file in the specified path. |
| `decrypt configuration [source] [target]` | Decrypts the configuration file in the specified path. |
| `encrypt predefinedtrustedupdater [source] [target]` | Encrypts the configuration file in the specified path. |
| `decrypt predefinedtrustedupdater [source] [target]` | Decrypts the configuration file in the specified path. |
| `show license` | Displays the software license information. |
| `activate [Activation Code]` | Activates the software. |
| `help` | Displays the help file. |

## Feature Abbreviations

To make using the command line interpreter easier, use these abbreviations for regular features:

**TABLE 3-3. CLI Feature Abbreviations**

| FEATURE | ABBREVIATION |
|---|---|
| `service` | `srv` |
| `user` | `us` |

| FEATURE | ABBREVIATION |
|---|---|
| userpassword | up |
| adminpassword | ap |
| approvedlist | al |
| trustedupdater | tu |
| configuration | con |
| dlldriverlockdown | dd |
| script | scr |
| predefinedtrustedupdater | ptu |
| blockedlog | bl |
| lock | lo |
| list | li |
| license | lcsrv |
| settings | set |
| usbmalwareprotection | usb |
| memoryrandomization | mr |
| dllinjectionprevention | dll |
| apihookingprevention | api |
| networkvirusprotection | net |

# Working with the 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 2-20* for more information.

## Changing Advanced Settings

Some settings can only be changed though the configuration file using the command line interpreter. See *Working with the Command Line Interpreter on page 3-2* for more information.

**Procedure**

1. Export the configuration file.
2. Decrypt the configuration file.
3. Edit the configuration file with Windows Notepad or another text editor.
4. Encrypt the edited configuration file.
5. Import the edited configuration file.

## Configuration File Syntax

The configuration file uses the XML format to specify the necessary parameters to deploy Safe Lock. 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="yes">
```

```
      <Password>Mb4mhJHBUxvDT9JfjVQOGLmGojNgdYCYMGZ5jTa7Q49
        Ia0mPWpL6sjXBcrkSfnKtGC48rKEVLc2r98jeVqzS6g==
      </Password>
    </Account>
  </AccountGroup>
  <UI>
    <SystemTaskTrayIcon Enable="no"/>
  </UI>
  <Feature>
    <ApplicationLockDown LockDownMode="2">
      <WhiteList RecentHistoryUnapprovedFilesLimit="50"/>
      <DllDriverLockdown Enable="yes"/>
      <ScriptLockdown Enable="yes">
         <Extension Id="vbe">
            <Interpreter>cscript.exe</Interpreter>
            <Interpreter>wscript.exe</Interpreter>
          </Extension>
          <Extension Id="bat">
            <Interpreter>cmd.exe</Interpreter>
          </Extension>
      <ScriptLockdown/>
      <TrustedUpdater>
        <PredefinedTrustedUpdater Enable="yes">
          <RuleSet>
            <Condition Id="AllowOnlyCertainParentProcess">
              <ParentProcess Path="WKSrv.exe"/>
              <ApprovedListCheck Enable="yes"/>
            </Condition>
            <Rule><Updater Type="Process" Path="bar.exe"/></Rule>
            <Rule><Updater Type="File" Path="foo.msi"/></Rule>
            <Rule><Updater Type="Folder" Path="C:\bar"
                ConditionRef="AllowOnlyCertainParentProcess"/></Rule>
            <Exception Path="hoge.exe"/>
          </RuleSet>
        </PredefinedTrustedUpdater>
      </TrustedUpdater>
    </ApplicationLockDown>
    <DeviceAccessControl Enable="yes" ActionMode="1"/>
    <DllInjectionPrevention Enable="yes" ActionMode="1"/>
    <ApiHookingPrevention Enable="yes" ActionMode="1"/>
    <MemoryRandomization Enable="yes"/>
    <NetworkScan Enable="yes" ActionMode="0"/>
```

```
      <Log>
        <EventLog Enable="yes">
          <BlockedAccessLog Enable="yes"/>
          <ApprovedAccessLog Enable="yes"/>
            <DllDriverLog Enable="yes">
            <TrustedUpdaterLog Enable="yes">
          </ApprovedAccessLog>
          <SystemEventLog Enable="yes"/>
          <ListLog Enable="yes"/>
          <DeviceAccessControlLog Enable="yes"/>
          <ExecutionPreventionLog Enable="yes"/>
          <NetworkScanLog Enable="yes"/>
        </EventLog>
        <DebugLog Enable="yes"/>
      </Log>
    </Feature>
  </Configuration>
  <Permission>
    <AccountRef Id="{24335D7C-1204-43d1-9CBB-332D688C85B6}">
      <UIControl Id="DetailSetting" State="yes"/>
      <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 for configuring the following information:

- The Restricted User account
- Specific Safe Lock features
- Log files
- Main console controls available to the Restricted User account

**Important**

The configuration file only supports UTF-8 encoding.

## Account Configuration Parameters

Use the account configuration parameters to configure the Restricted User account and control the display of the system tray icon.

**TABLE 3-4. Account Configuration Parameters**

| CATEGORY | PARAMETER | VALUE | DESCRIPTION |
|---|---|---|---|
| Account | id | GUID | Restricted User account GUID. |
| | Enable | yes, no | Enables or disables the Restricted User account. |
| | Password | - | The Administrator and Restricted User passwords cannot be the same. |
| SystemTaskTrayIcon | Enable | yes, no | Turns the system tray icon and notifications on or off. |

## Feature Configuration Parameters

Use the feature configuration parameters configure the main features as necessary.

Use the `ActionMode` parameter to block applications or only record events in the corresponding logs. See *Exploit Protection Settings on page 2-17* for more information on specific features.

**TABLE 3-5. Feature Configuration Parameters**

| CATEGORY | PARAMETER | VALUES | DESCRIPTION |
|---|---|---|---|
| ApplicationLockDown | LockDownMode | 1-2 | 1=locked, 2=unlocked |

| CATEGORY | PARAMETER | VALUES | DESCRIPTION |
|---|---|---|---|
| WhiteList | RecentHistoryUnapprovedFilesLimit | 0-65535 | Specifies the maximum number of items in the Blocked applications log. |
| DLLDriverLockdown | Enable | yes, no | Enables or disables DLL/Driver Lockdown. |
| ScriptLockDown | Enable | yes, no | Enables or disables Script Lockdown. |
| ScriptLockDown > **Extension** | Id | any | Specifies the file extension of the script. |
| ScriptLockDown > Extension > **Interpreter** | n/a | n/a | Specifies the file name of the interpreter. |
| TrustedUpdater | n/a | n/a | Container for PredefinedTrustedUpdater. |
| TrustedUpdater > **PredefinedTrustedUpdater** | Enable | yes, no | Enables or disables the PredefinedTrustedUpdater. |
| TrustedUpdater > PredefinedTrustedUpdater > **RuleSet** | n/a | n/a | Container for Condition. |
| TrustedUpdater > PredefinedTrustedUpdater > RuleSet > **Condition** | Id | any | Specifies a unique name for the rule set. |
| TrustedUpdater > PredefinedTrustedUpdater > RuleSet > Condition > **ApprovedListCheck** | Enable | yes, no | Enables or disables hash check for the Trusted Updaters. |
| TrustedUpdater > PredefinedTrustedUpdater > RuleSet > Condition > **ParentProcess** | Path | any | Specifies the parent process path for the added updater. |

| CATEGORY | PARAMETER | VALUES | DESCRIPTION |
|---|---|---|---|
| TrustedUpdater > PredefinedTrustedUpdater > RuleSet > **Exception** | Path | any | Specifies the process path. |
| TrustedUpdater > PredefinedTrustedUpdater > RuleSet > **Rule** | Label | any | Specifies a unique name for the rule. |
| TrustedUpdater > PredefinedTrustedUpdater > RuleSet > Rule > **Updater** | Type | Process, File, Folder, FolderAndSubFolder | Specifies the type of updater for the current rule:<br>• Process: the rule matches a process creation event<br>• File: the rule matches a file accessed by the specified interpreter or `msiexec`<br>• Folder: the rule matches any process, script, interpreter or msi within the folder<br>• FolderAndSubFolder: the rule matches any process, script, interpreter or msi within the folder or subfolders |
| | Path | any | Specifies the path to the updater. |
| | ConditionRef | any | Specifies the Condition Id to provide a more detailed rule for the updater. |
| | | | |
| UsbMalwareProtection | Enable | yes, no | Enables or disables USB Malware Protection. |
| | ActionMode | 0-1 | 0=allow, 1=block |

| Category | Parameter | Values | Description |
|---|---|---|---|
| DllInjectionPrevention | Enable | yes, no | Enables or disables DLL Injection Prevention. |
| | ActionMode | 0-1 | 0=allow, 1=block |
| ApiHookingPrevention | Enable | yes, no | Enables or disables API Hooking Prevention. |
| | ActionMode | 0-1 | 0=allow, 1=block |
| MemoryRandomization | Enable | yes, no | Enables or disables ASLR. |
| NetworkVirusProtection | Enable | yes, no | Enables or disables Network Virus Protection. |
| | ActionMode | 0-1 | 0=allow, 1=block |

## Log Configuration Parameters

Use the log configuration parameters to configure individual log types. See *Event Log Descriptions on page 4-7* for more information about the Trend Micro Safe Lock event log.

**Table 3-6. Log Configuration Parameters**

| Category | Parameter | Value | Description |
|---|---|---|---|
| EventLog | Enable | yes, no | Displays all software. |
| BlockedAccessLog | Enable | yes, no | Displays applications that were prevented from running by the software. |
| ApprovedAccessLog | Enable | yes, no | Displays applications that were allowed to run by the software. |
| ApprovedAccessLog > **DLLDriverLog** | Enable | yes, no | Enables or disables the DLL/ Driver approved access log. |

| CATEGORY | PARAMETER | VALUE | DESCRIPTION |
|---|---|---|---|
| ApprovedAccessLog > **TrustedUpdaterLog** | Enable | yes, no | Enables or disables the Trusted Updater approved access log. |
| SystemEventLog | Enable | yes, no | Displays all events related to the system. |
| ListLog | Enable | yes, no | Displays events related to the Approved list. |
| UsbMalwareProtectionLog | Enable | yes, no | Displays events where USB Malware Protection was activated. |
| ExecutionPreventionLog | Enable | yes, no | Displays events where Execution Prevention was activated. |
| NetworkVirusProtectionLog | Enable | yes, no | Displays events where Network Virus Protection was activated. |
| DebugLog | Enable | yes, no | Displays debugging information for the software. |

## Permission Configuration Parameters

Use the permission configuration parameters to determine which main console controls are available to the Restricted User account.

**TABLE 3-7. Permission Configuration Parameters**

| CATEGORY | PARAMETER | VALUE | DESCRIPTION |
|---|---|---|---|
| UIControl | Id | DetailSetting, LockUnlock, LaunchUpdater, RecentHistoryUnapprovedFIles, ImportExportList, ListManagement | Specifies the feature that is enabled or disabled. |
| | State | yes, no | yes=enable, no=disable |

**TABLE 3-8. Permission Configuration Parameter Value Descriptions**

| VALUE | DESCRIPTION |
|---|---|
| DetailSetting | Controls the availability of all features and functions on the **Settings** page:<br>• Changes Exploit Protection settings<br>• Exports or imports a configuration file |
| LockUnlock | Locks or unlocks the software on the **Overview** page. |
| LaunchUpdater | Controls the availability of the **Run an installer or updater** option when the Restricted User clicks **Add Item** on the **Approved List** page. |
| RecentHistoryUnapprovedFiles | Controls the availability to view the Blocked Access Log if the Restricted User clicks the **Last application blocked** status on the **Overview** page. |
| ImportExportList | Controls the availability of the Import List and Export List buttons. |
| ListManagement | Controls the availability of these **Approved List** page items:<br>• **Delete Item** button<br>• **Update Hash** button<br>• **Add Item** > **Add Files/Folders** |

**Note**

The **Password** page is not available to the Restricted User account.

# Chapter 4

# Troubleshooting

This chapter describes troubleshooting techniques and frequently asked questions about Trend Micro Safe Lock.

Topics in this chapter include:

# Frequently Asked Questions (FAQ)

## What if the computer becomes infected by a threat?

Use Trend Micro Portable Security to remove the threat without having to update the Approved List or unlock the computer.

## Where can I get more help with Trend Micro Safe Lock?

Get the most up-to-date information and support from the Trend Micro support website at:

http://esupport.trendmicro.com/en-us/business/

# Working with the Diagnostic Toolkit

The Trend Micro Safe Lock Diagnostic Toolkit offers administrators the ability to perform a number of diagnostic functions, including:

- Create, collect, and delete debugging logs
- Enable or disable Self Protection

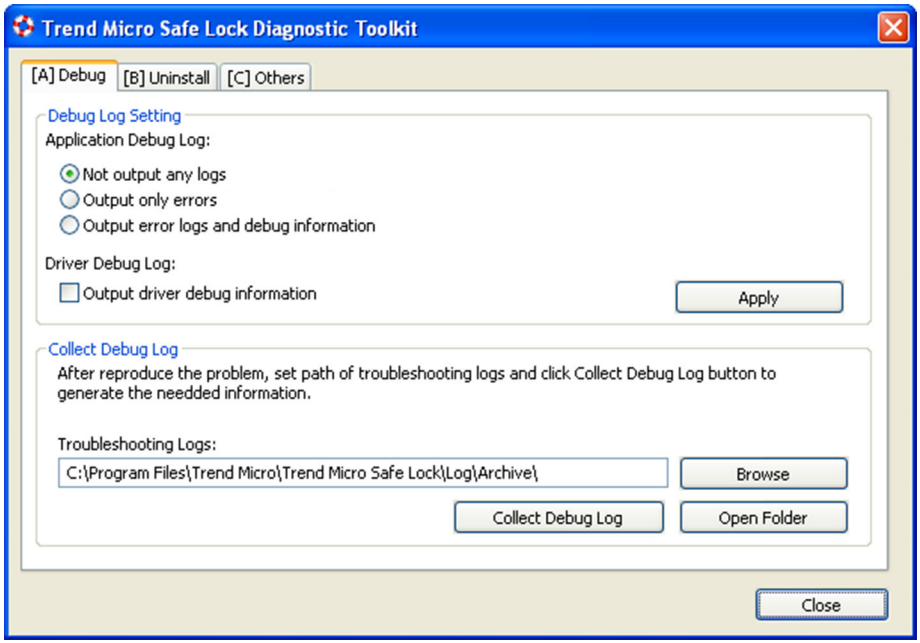



**FIGURE 4-1. The Trend Micro Safe Lock Diagnostic Toolkit Debug tab**

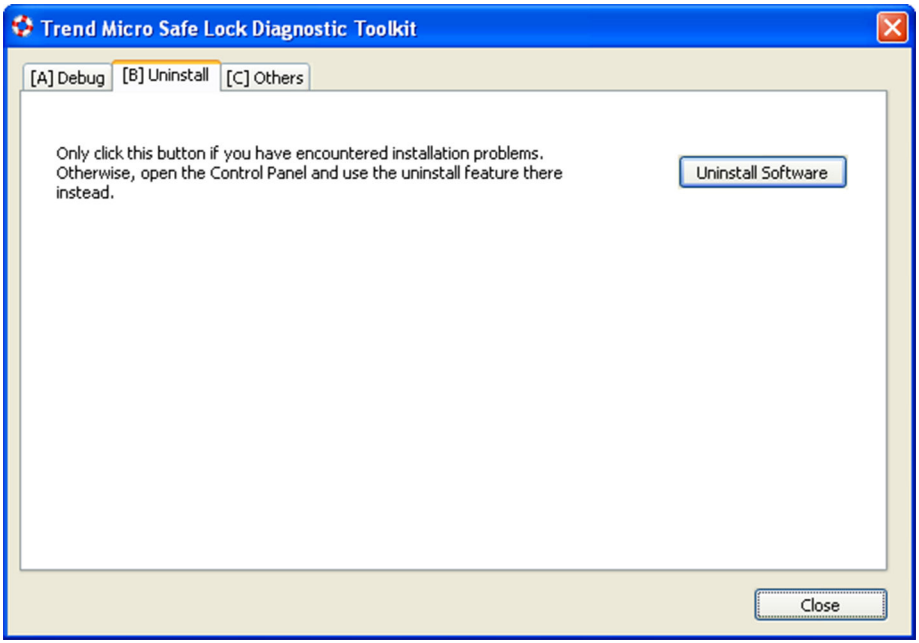



**FIGURE 4-2. The Trend Micro Safe Lock Diagnostic Uninstall tab**

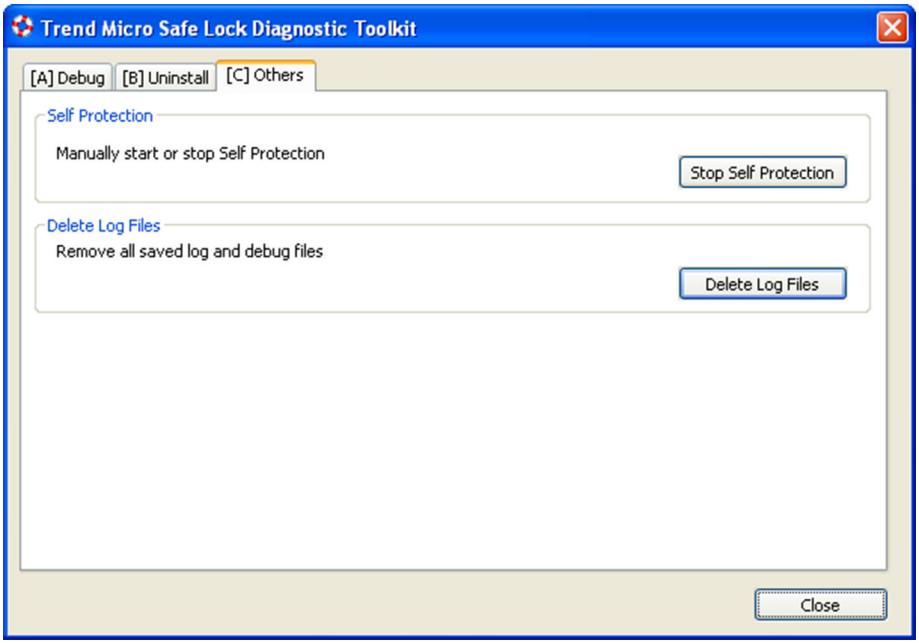



**FIGURE 4-3. The Trend Micro Safe Lock Diagnostic Toolkit Others tab**

## Logging Issues with Trend Micro Safe Lock

If Trend Micro Safe Lock experiences problems, generate a complete set of application and driver debug logs for analysis, or send them to to Trend Micro Technical Support. Both the Administrator and Restricted User accounts can collect the logs.

**Procedure**

1. Open the Diagnostic Toolkit and enable full logging:

   a. Open the Trend Micro Safe Lock installation folder and run `WKSupportTool.exe`.

**Note**

The default installation location is `C:\Program\Files\Trend Micro \Trend Micro Safe Lock\`.

b. Provide the Administrator or Restricted User password and click **OK**.

c. On the **[A] Debug** tab, select **Output error logs and debug information** and **Output driver debug information**, and click **Apply**.

2. Reproduce the problem.

3. Collect the debug logs:

a. Reopen the Diagnostic Toolkit.

b. On the **[A] Debug** tab, click **Browse** to choose the location where Trend Micro Safe Lock saves the logs.

**Note**

The default location for saved logs is: `C:\Program Files\Trend Micro \Trend Micro Safe Lock\Log\Archive\`.

c. Click **OK** when finished.

d. Click **Collect Debug Log**.

e. Once the Debug Logs have been collected, click **Open Folder** to access the zipped log files for review, or to send them to Trend Micro Technical Support.

## About Self Protection

Self Protection provides ways for Trend Micro Safe Lock to defend the processes and other resources required to function properly. Self Protection helps thwart attempts by programs or actual users to disable the software.

Self Protection blocks all attempts to terminate the following services:

- Trend Micro Safe Lock Service (`WkSrv.exe`)

- Trend Micro Unauthorized Change Prevention Service (`TMBMSRV.exe`)
- Trend Micro Personal Firewall (`TmPfw.exe`)

## Diagnostic Toolkit Commands

The following table lists the commands available using the Diagnostic Toolkit, `WKSupportTool.exe`.

**Note**

Only the Trend Micro Safe Lock Administrator can use the Diagnostic Toolkit, and `WKSupportTool.exe` will prompt for the Administrator password before running a command.

**TABLE 4-1. Diagnostic Toolkit Commands**

| COMMAND | DESCRIPTION |
|---|---|
| `-p [password]` | Authenticates the user so the command will run. |
| `debug [on\|off] [verbose\|normal] [-drv on] [-drv off]` | Turns the debug logs on or off, specifies the log detail level, and if driver logs are included. |
| `collect [path]` | Collects debugging information and creates a zip file to the specified path. If no path is specified, the default log location `<installation directory>\Log\Archive` is used. |
| `selfprotection [on\|off]` | Turns on or off Safe Lock self protection. |
| `deletelogs` | Deletes all Safe Lock logs. |
| `uninstall` | Uninstalls Trend Micro Safe Lock. |

# Event Log Descriptions

Trend Micro Safe Lock leverages the Windows™ Event Viewer to display the Safe Lock event log. Access the Event Viewer at **Start** > **Control Panel** > **Administrative Tools**.

**TABLE 4-2. Windows Event Log Descriptions**

| EVENT ID | TASK CATEGORY | LEVEL | DESCRIPTION |
|---|---|---|---|
| 1000 | System | Information | Service started. |
| 1001 | System | Information | Service stopped. |
| 1002 | System | Information | Locked. |
| 1003 | System | Information | Unlocked. |
| 1005 | System | Information | Administrator password changed. |
| 1006 | System | Information | Restricted User password changed. |
| 1007 | System | Information | Restricted User account enabled. |
| 1008 | System | Information | Restricted User account disabled. |
| 1009 | System | Information | Product activated. |
| 1011 | System | Information | License expired. Grace period enabled. |
| 1012 | System | Information | License expired. Grace period ended. |
| 1013 | System | Information | Product configuration import started: <file_path> |
| 1014 | System | Information | Product configuration import complete: <file_path> |
| 1015 | System | Information | Product configuration exported to: <file_path>. |

| Event ID | Task Category | Level | Description |
|---|---|---|---|
| 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 | Information | 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 feature was enabled. |
| 1023 | System | Information | Network Virus Protection feature was disabled. |

| Event ID | Task Category | Level | Description |
|---|---|---|---|
| 1024 | System | Information | Event log settings changed.<br>[Details]<br>Windows Event Log: <ON\|OFF><br>System Log: <ON\|OFF><br>List Log: <ON\|OFF><br>Approved Access Log: <ON\|OFF><br>DLL Driver Log: <ON\|OFF><br>Trusted Updater Log: <ON\|OFF><br>Blocked Access Log: <ON\|OFF><br>USB Malware Protection Log: <ON\|OFF><br>Network Virus Protection Log: <ON\|OFF><br>Debug Log: <ON\|OFF> |
| 1025 | System | Information | Memory Randomization enabled. |
| 1026 | System | Information | 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 | Information | 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 | Information | DLL Injection Prevention disabled. |
| 1035 | System | Information | Pre-defined Trusted Updater enabled. |
| 1036 | System | Information | Pre-definied Trusted Updator disabled. |
| 1037 | System | Information | DLL/Driver Lockdown enabled |
| 1038 | System | Information | DLL/Driver Lockdown disabled. |
| 1039 | System | Information | Script Lockdown enabled. |
| 1040 | System | Information | Script Lockdown disabled. |
| 1041 | System | Information | Script added.<br>[Details]<br>File extension: <extension><br>Interpreter: <interpreter> |
| 1042 | System | Information | Script removed.<br>[Details]<br>File extension: <extension><br>Interpreter: <interpreter> |

| Event ID | Task Category | Level | Description |
|---|---|---|---|
| 1500 | List | Information | Trusted Update started. |
| 1501 | List | Information | Trusted Update stopped. |
| 1502 | List | Information | Approved List import started: <file_path> |
| 1503 | List | Information | Approved List import completed: <file_path> |
| 1504 | List | Information | Approved List exported to: <file_path> |
| 1505 | List | Information | Added to Approved List: <file_path> |
| 1506 | List | Information | Added to Trusted Updater: <file_path> |
| 1507 | List | Information | Removed from Approved List: <file_path> |
| 1509 | List | Information | Approved List updated: <file_path> |
| 1511 | List | Error | Unable to add to or update Approved List: <file_path> |
| 1512 | List | Error | Unable to add to or update Trusted Updater List: <file_path> |
| 2000 | Access Approved | Information | File access allowed: <file_path><br>[Details]<br>Access Image Path: <file_path><br>Access User: <machine>\<user><br>Mode: <Locked\|Unlocked> |

| Event ID | Task Category | Level | Description |
|---|---|---|---|
| 2001 | Access Approved | Warning | File access allowed: <file_path><br>[Details]<br>Access Image Path: <file_path><br>Access User: <machine>\<user><br>Mode: Unlocked |
| 2002 | Access Approved | Error | File access allowed: <file_path><br>Unable to get the file path while checking the Approved List.<br>[Details]<br>Access Image Path: <file_path><br>Access User: <machine>\<user><br>Mode: <Locked\|Unlocked> |
| 2003 | Access Approved | Error | File access allowed: <file_path><br>Unable to calculate hash while checking the Approved List.<br>[Details]<br>Access Image Path: <file_path><br>Access User: <machine>\<user><br>Mode: <Locked\|Unlocked> |
| 2004 | Access Approved | Error | File access allowed: <file_path><br>Unable to get notifications to monitor process. |
| 2005 | Access Approved | Error | File access allowed: <file_path><br>Unable to add process to non exception list. |

| Event ID | Task Category | Level | Description |
|---|---|---|---|
| 2006 | Access Approved | Information | File access allowed: <file_path><br>[Details]<br>Access Image Path: <file_path><br>Access User: <machine>\<user><br>Mode: <Locked\|Unlocked> |
| 2500 | Access Blocked | Warning | File access blocked: <file_path><br>[Details]<br>Access Image Path: <file_path><br>Access User: <machine>\<user><br>Mode: Locked |
| 3000 | USB Malware Protection | Warning | Device access allowed: <file_path><br>[Details]<br>Access Image Path: <file_path><br>Access User: NT AUTHORITY\SYSTEM<br>Device Type: Removable Device |
| 3001 | USB Malware Protection | Warning | Device access blocked: <file_path><br>[Details]<br>Access Image Path: <file_path><br>Access User: NT AUTHORITY\SYSTEM<br>Device Type: Removable Device |

| Event ID | Task Category | Level | Description |
|---|---|---|---|
| 3500 | Network Virus Protection | Warning | Network virus allowed: <virus_name><br>[Details]<br>Protocol: <protocol_name><br>Source IP Address: <ip_address><br>Source Port: <port_number><br>Destination IP Address: <ip_address><br>Destination Port: <port_number> |
| 3501 | Network Virus Protection | Warning | Network virus blocked: <virus_name><br>[Details]<br>Protocol: <protocol_name><br>Source IP Address: <ip_address><br>Source Port: <port_number><br>Destination IP Address: <ip_address><br>Destination Port: <port_number> |
| 4000 | Process Protection Event | Warning | API Hooking/DLL Injection allowed: <file_path><br>[Details]<br>Threat Image Path: <file_path><br>Threat User: <machine>\<user> |
| 4001 | Process Protection Event | Warning | API Hooking/DLL Injection blocked: <file_path><br>[Details]<br>Threat Image Path: <file_path><br>Threat User: <machine>\<user> |

# Error Code Descriptions

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

**TABLE 4-3. Trend Micro Safe Lock Error Code Descriptions**

| CODE | DESCRIPTION |
|---|---|
| 0x00040200 | Operation successful. |
| 0x80040201 | Operation unsuccessful. |
| 0x80040202 | Operation unsuccessful. |
| 0x00040202 | Operation partially successful. |
| 0x00040203 | Requested function not installed. |
| 0x80040203 | Requested function not supported. |
| 0x80040204 | Invalid argument. |
| 0x80040205 | Invalid status. |
| 0x80040206 | Out of memory. |
| 0x80040207 | Busy. Request ignored. |
| 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. |

| Code | Description |
|---|---|
| 0x8004020e | Reboot required for unexpected reason. |
| 0x0004020f | Allowed to perform task. |
| 0x8004020f | Permission denied. |
| 0x00040210 | System Reserved. (Not used) |
| 0x80040210 | Invalid or unexpected service mode. |
| 0x00040211 | System Reserved. (Not used) |
| 0x80040211 | Requested task not permitted in current status. Check license. |
| 0x00040212 | System Reserved. (Not used) |
| 0x00040213 | System Reserved. (Not used) |
| 0x80040213 | Passwords do not match. |
| 0x00040214 | System Reserved. (Not used) |
| 0x80040214 | System Reserved. (Not used) |
| 0x00040215 | Not found. |
| 0x80040215 | "Expected, but not found." |
| 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). |

| Code | Description |
|---|---|
| 0x80040224 | System Reserved. (Not used) |
| 0x80040225 | System Reserved. (Not used) |
| 0x80040240 | Library not found. |
| 0x80040241 | Invalid library status or unexpected error in library function. |
| 0x80040260 | System Reserved. (Not used) |
| 0x80040261 | System Reserved. (Not used) |
| 0x80040262 | System Reserved. (Not used) |
| 0x80040263 | System Reserved. (Not used) |
| 0x80040264 | System Reserved. (Not used) |
| 0x00040265 | System Reserved. (Not used) |
| 0x80040265 | System Reserved. (Not used) |
| 0x80040270 | System Reserved. (Not used) |
| 0x80040271 | System Reserved. (Not used) |
| 0x80040272 | System Reserved. (Not used) |
| 0x80040273 | System Reserved. (Not used) |
| 0x80040274 | System Reserved. (Not used) |
| 0x80040275 | System Reserved. (Not used) |
| 0x80040280 | Invalid Activation Code. |
| 0x80040281 | Incorrect Activation Code format. |

# Chapter 5

# Getting Help

This chapter describes how to contact support.

Topics in this chapter include:

# Technical Support

Activating and registering Trend Micro Safe Lock qualifies you to receive a variety of support services.

The Trend Micro support website provides the latest information on security threats. Please visit it if you have found a security threat, or if you would like to learn more about the support services available.

http://esupport.trendmicro.com

The content of support services is subject to change without notice. Please contact Trend Micro if you have any questions. You can reach the support center by telephone, FAX, or email. The Trend Micro website lists contact numbers for different regions worldwide.

Support is available for a period of one year once you have completely finished activating your software, although this policy may differ for some licenses.

## Multi-Year Contracts

Even if you pay for multi-year contracts (by paying more than one year of support fees in advance), Trend Micro sets the period during which support for a product shall be provided without regard to your contract term.

Please note that multi-year contracts do not guarantee product support during the applicable contract period, nor do they guarantee upgrades if the product support period has concluded.

# Index


**TREND MICRO INCORPORATED**

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

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

www.trendmicro.com

Item Code: SLEM15951/130506