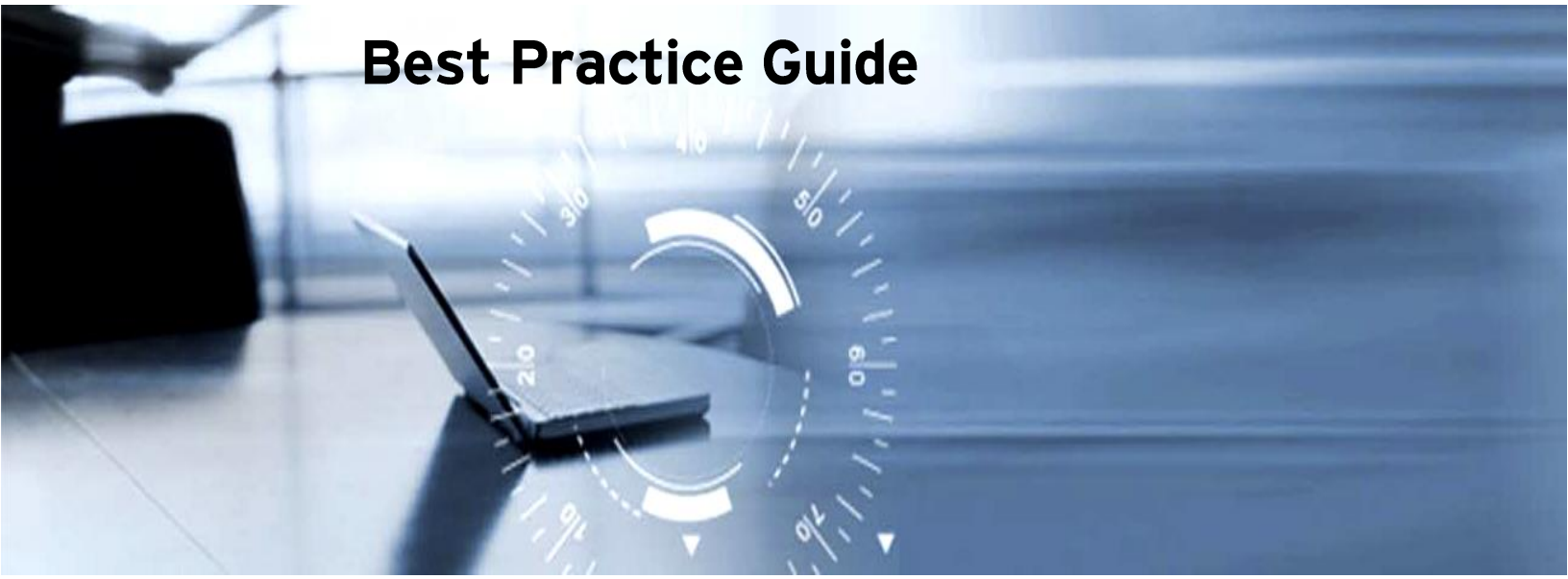
Trend Micro™ Safelock TXOne Edition

Best Practice Guide



Anti-Spyware Anti-Spam Antivirus Anti-Phishing Content & URL Filtering

Author: Jean Busante

Version: 1.**0**
Released: March 10, 2020

Table of Contents

Introduction **5**
0.1 > About Trend Micro SafeLock TXOne Edition 5
0.2 > Terminologies 5

Chapter 1: Installing TMSL Agent (Stand Alone) **6**
1 Installing TMSL Agent (Standalone) 6
1.1 Device Preparation and Planning 6
1.2 Configure Setup (setup.ini) 7
1.3 TMSL Agent Installation 8

Chapter 2: Installing TMSL Agent with Intelligent Manager **12**
2.1 Install IM 12
2.1.1 System Requirements 12
2.1.2 Sizing 12
2.1.3 Installation 15
2.2 Install TMSL Agent 16
2.2.1 Device Preparation and Planning 16
2.2.2 Configure Setup (setup.ini) 17
2.2.3 Install TMSL Agent 19

Chapter 3: Configuring Approved Lists **25**
3.1 Initialize and Build Approved List 25
3.2 Updating Approved List 26
3.2.1 Maintenance Mode 26
3.2.2 Windows Update Support 29
3.2.3 Manual Update 30
3.2.4 Trusted Updater 33
3.2.5 Predefined Trusted Updater 35
3.2.6 Trusted Hash 39
3.2.7 Trusted Digital Signature Update 42

Chapter 4: Intelligent Manager Management **45**
4.1 > Agent and IM Connection 45
4.1.1 Agent and IM Communication 45
4.1.2 Verifying IM to TMSL Agent Connection 45
4.1.3 Verifying TMSL Agent to IM Connection 46
4.2 > Event Management 46
4.3 > Log Purge Settings 49

Introduction

0.1 > About Trend Micro SafeLock TXOne Edition

Trend Micro Safe Lock TXOne Edition is an application/device trusting solution designed to protect 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.

0.2 > Terminologies

This document uses the following terminologies:

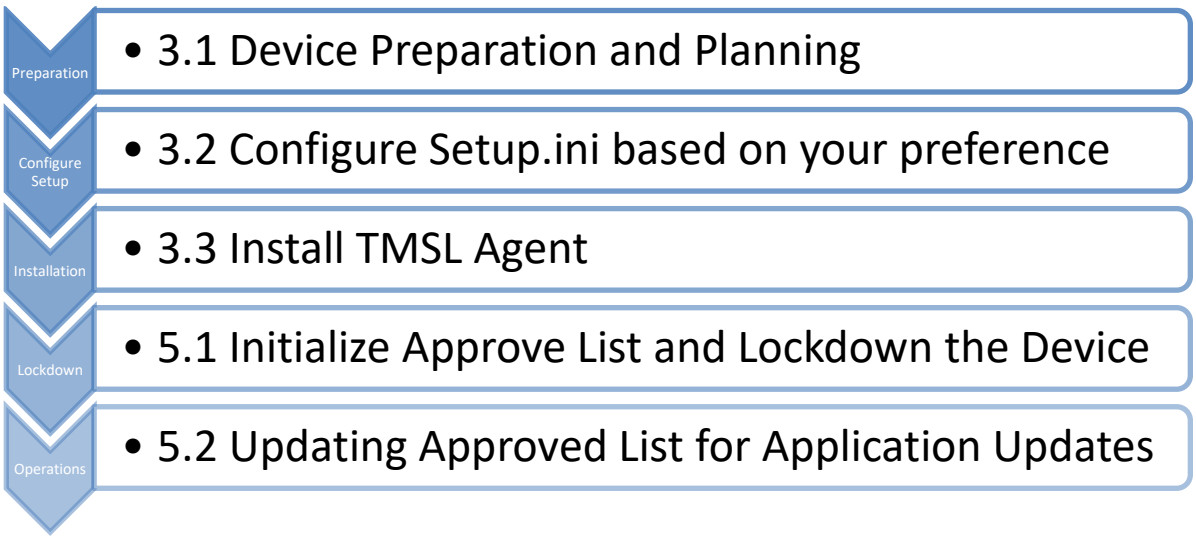
Tarminology	Meaning
TMSL	Trend Micro Safe Lock. TMSL is a security software using trusted application solution.
TMSL Agent	TMSL Agent is installed to a fixed function computer and blocks un-registered executable modules/scripts.
IM	TMSL Intelligent Manager manages TMSL Agents. IM can send alert to the administrator when TMSL Agent blocks un-registered executable modules/scripts.

Table 1 – Terminology

Chapter 1: Installing TMSL Agent (Stand Alone)

1 Installing TMSL Agent (Standalone)

Below is the standard flow of installing TMSL Agent (Standalone). To know more detail, you may refer to Trend Micro Safe Lock Agent Installation Guide



1.1 Device Preparation and Planning

1.1.1 Device Preparation

As we know, Safe Lock is primarily an application trusting solution. A device that is not properly prepared for this product may cause some inconveniences and issues. Below are the things we recommend to prepare before installing Safe Lock Agent on the device:

- Uninstall Antivirus programs
- Disable Windows Defender

- Ensure sure Windows Updates are completed and no updates are running during **5.1 Initialize Approved List and Lockdown the Device**

1.1.2 Planning

Please carefully review and plan which features you would like to use for Safe Lock Agent. Full details can be found on Administrator Guide. Additionally, the following features need to be taken into consideration as they may have impact on Agent Performance:

- Predefined Trusted Updater
- Trusted Hash
- Integrity Monitoring
- Root Cause Analysis

1.2 Setup Configuration (setup.ini)

You can configure TMSL Agent installation by modifying the setup.ini. It is also recommended to run a Pre-Scan on the device before installing TMSL Agent.

1. You can download the TMSL Agent Package from Trend Micro Download Center
2. Extract the TMSL Agent package and Open setup.ini file
3. Modify the setup.ini parameters based on your preference. Complete list of setup.ini arguments and the descriptions can be found on Setup.ini File Arguments (2-18) of Trend Micro SafeLock Agent Installation Guide
4. For additional security, you can encrypt your setup.ini file using WKSupportTool.exe included in the TMSL Agent Package. You can use the command: **WKSupportTool.exe EncryptSetupIni Setup.ini Setup.bin**

1.2.1 Pre-Scan

To initiate a scan on the device before installation. You may follow the configuration below.

NOTE The settings shown below are the default values.

```
[Property]
PRESCAN=1

[Prescan]
IGNORE_THREAT=0
REPORT_FOLDER=
```

```
SCAN_TYPE=Full
COMPRESS_LAYER=2
MAX_FILE_SIZE=0
SCAN_REMOVABLE_DRIVE=0
FORCE_PRESCAN=0
```

1.2.2 Initiate Approved List

To automatically initiate Approved List after installation, you may follow the configuration below:

```
[Property]
  INIT_LIST=1
```

1.2.3 Application Lockdown

To Turn On Application Lockdown after the installation finish

```
[Property]
  LOCKDOWN=1
```

1.2.4 Silent Install

To perform silent installation, you may follow the configuration below:

```
[Property]
  SILENT_INSTALL=1
  ACTIVATION_CODE=XX-XXXXX-XXXXX-XXXXXX-XXXX
  PASSWORD=XXXXXXXX
```

1.3 TMSL Agent Installation

There are different Installation Methods for installing TMSL Agent (Standalone).

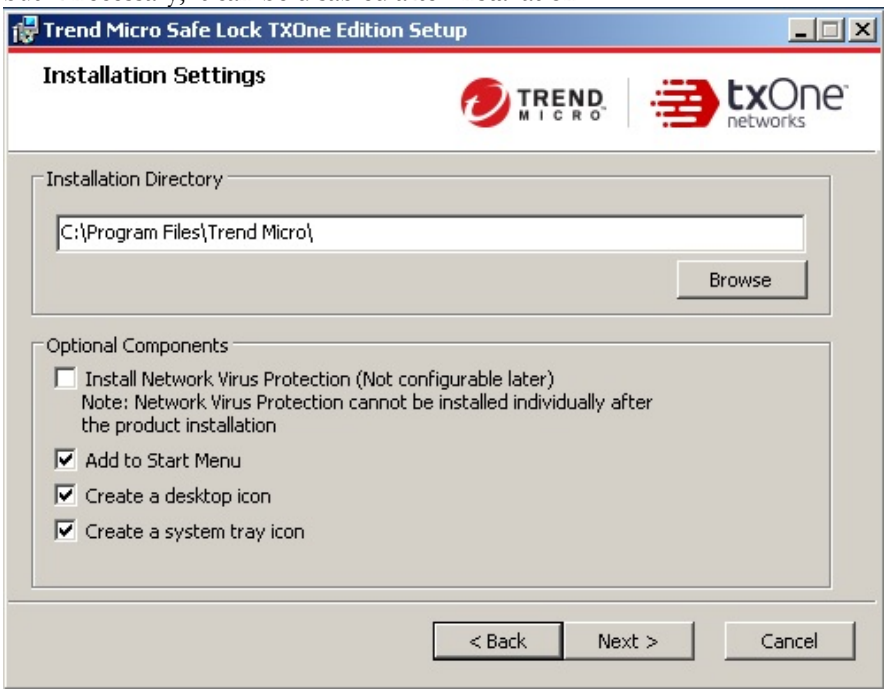
Installation Method	Description
Windows Installer	The Windows Installer provides simplified step-by-step installation wizard for first-time or single installation.
Command Line Interface Installation	This method utilizes Command Line Interface (CLI).

Table 2 - Installation Methods

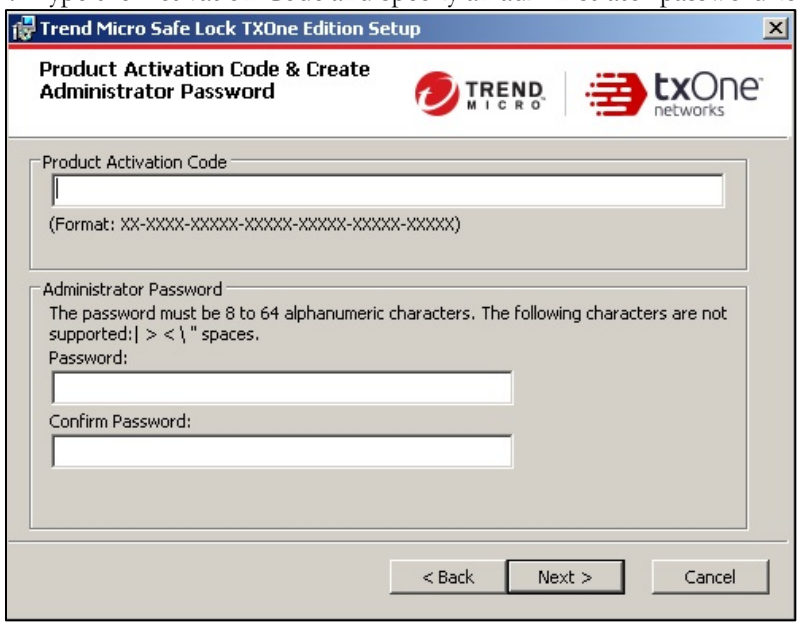
1.3.1 Windows Installer

5. 1. Run SL_Install.exe from TMSL Agent Installer Package
   2. Follow the Installation Wizard

3. In Installation Settings. select desired settings and components. Take note that for Network Virus Protection, this can only be installed during the initial program installation, but if necessary, it can be disabled after installation.



4. Type the Activation Code and specify an administrator password for TMSL Agent



Important:

-- 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

-- 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

5. You will be prompted for a Pre-Scan on the device first before installing TMSL Agent. This takes time to complete however Trend Micro recommends it for the device safety.

6. Continue through the installation till finish

1.3.2 Command Line Interface (CLI) Installation

1.3.2.1 Silent Install using Command Line Interface (CLI)

1. Open Command Prompt as Administrator
2. Navigate to the TMSL Agent Installer Path
3. Enter the following required commands: SL_install.exe -q -ac <activation_code> -p <admin_password>

List of Parameter are below

Parameter	Value	Description
-q		Run the installer silently
-p	<administrator_password>	Specify the administrator password
-d	<path>	Specify the installation path
-ac	<activation_code>	Specify the activation code
-nd		Do not create a desktop shortcut
-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**

Parameter	Value	Description
		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.
-nps		Do not execute Prescan
-ips		Do not cancel installation when Prescan detects threats

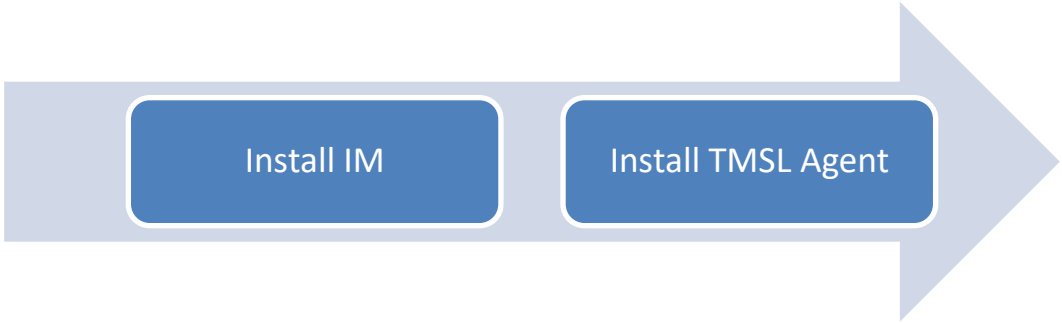
Table 3 - Silent Install Parameters

Important:

-- 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 desktop shortcut will not be created
-- 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
-- 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
-- You should create Approved List and lockdown TMSL Agent manually, if you did not set INIT_LIST and LOCKDOWN in setup.ini

Chapter 2: Installing TMSL Agent with Intelligent Manager

Below is the standard flow to install the Intelligent Manager and Agent. To see more details about the installation process, you may refer to Trend Micro Safe Lock TXOne Edition Installation Guide and Administration Guide from this link.



2.1 Install IM

2.1.1 System Requirements

Refer to **Trend Micro SafeLock TXOne Edition Intelligent Manager Installation guide** for compete details.

2.1.2 Sizing

To determine your ideal IM server spec, please refer to the following formula:

```
[A single TMSL Agent Log output numbers] X [Log store period in Days] X [Total number of
  TMSL Agent]
  [A single TMSL Agent Log output numbers]
```

The amount of logs a single TMSL Agent outputs depends on the log output setting. Here is a reference for the estimates:

Output Logs	Explanation	One TMSL Agent Logs output number / day
Block Log only (Default)	TMSL Agent outputs only block event logs	150

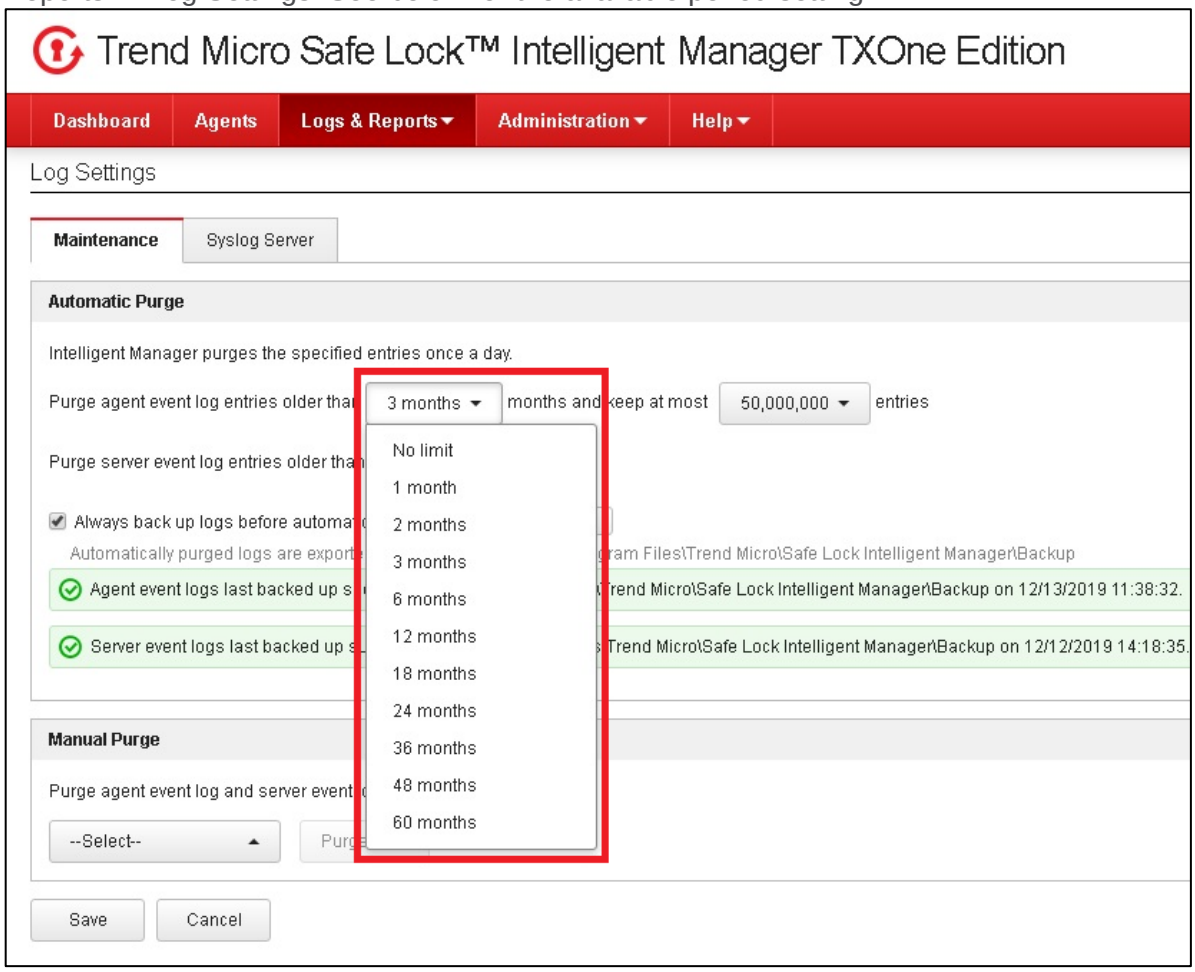
Output Logs	Explanation	One TMSL Agent Logs output number / day
Block Log + **Approved Log**	TMSL Agent outputs block event logs and allow event logs	7,150 (150 (Block Log) +7,000 (Approved Log))
Block Log + Approved Log + **Integrity Monitor Log**	TMSL Agent outputs block event logs, allow event logs and integrity logs.	57,150 (150 (Block Log) + 7,000 (Approved Log) + 50,000 (Integrity Monitor Log))

Table 4 - TMSL Outpit Logs Setting

TMSL Agent log function can be configured using setup file. For more details, refer to

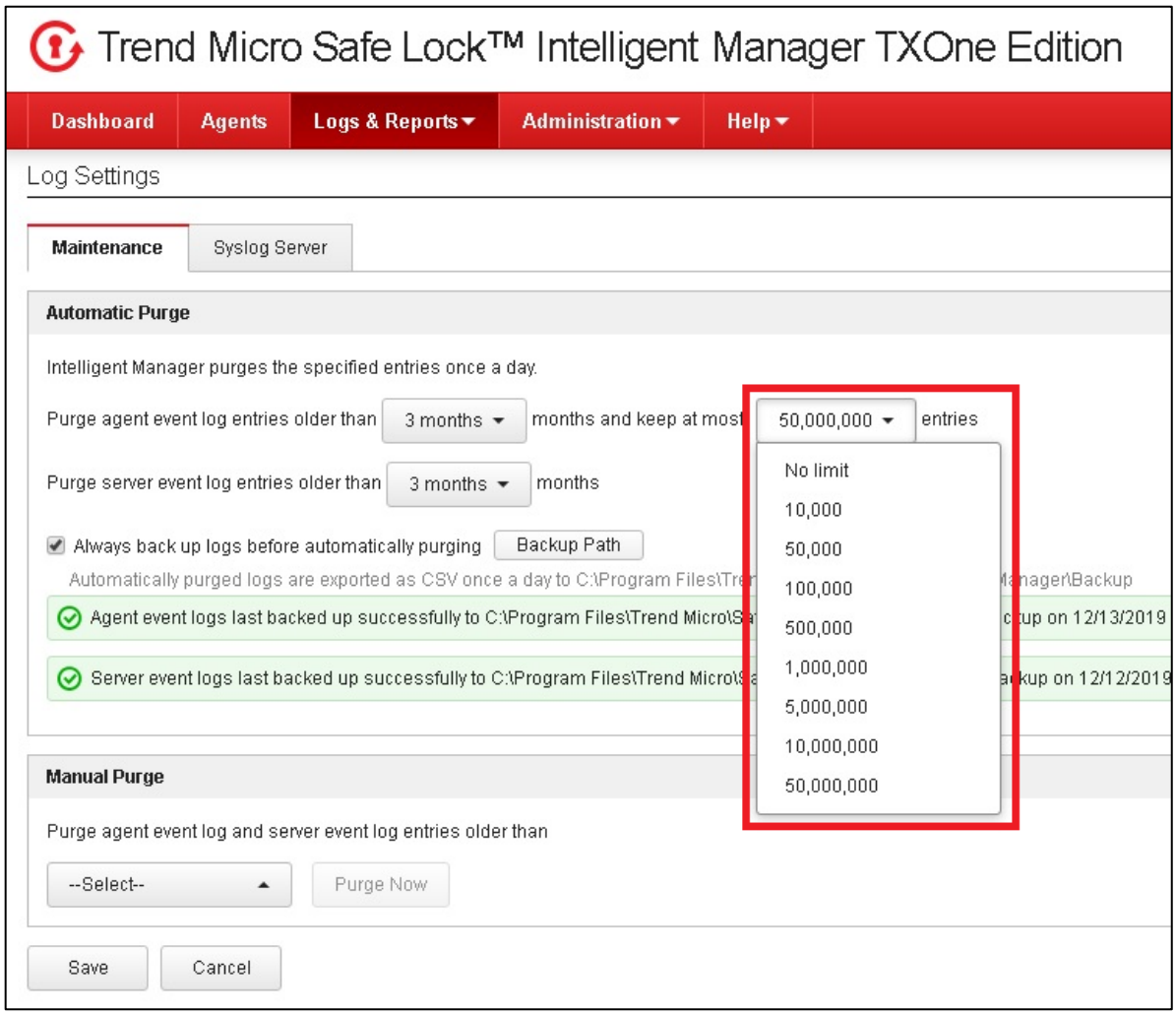
[Log store period in Days]

Below are the possible Log Store Period settings in IM. To see this, Click Logs & Reports -> Log Settings. See below for the available period setting



It is also recommended setting the maximum log number on IM to avoid occupying

disk space.



Number of TMSL Agent	HDD Space	Memory Size	CPU Core
1-1,000	50GB	4GB	2
1,001-5,000	75GB	8GB	4
5,001-10,000	100GB	8GB	4

Table 5 - IM Sizing

IM stores logs, settings, etc. in SQL server. Here's Database sizing and the amount of storable logs.

SQL Server edition	Database size	Numbers of log
Express	10GB	~400,000

SQL Server edition	Database size	Numbers of log
Standard or above	500GB	~20,000,000
Standard or above	4,000GB	~160,000,000

Table 6 - SQL Server Sizing

[Sizing Calculation Sample]

<Premise>
- TMSL Agent numbers: 100
- Log setting: Block log only
- Log store period: 1month (31 days)
- Maximum store log numbers: 100,000 logs

<Calculation>
150 logs [One TMSL Agent Log Output Number] X 31 [Log Store Period in Days] X 100 [Total no. of TMSL Agents] = 465,000 logs

<IM Server/SQL Server sizing>
IM Server:
- HDD Space: 50GB
- Memory Size: 4GB
- CPU core: 2 or above

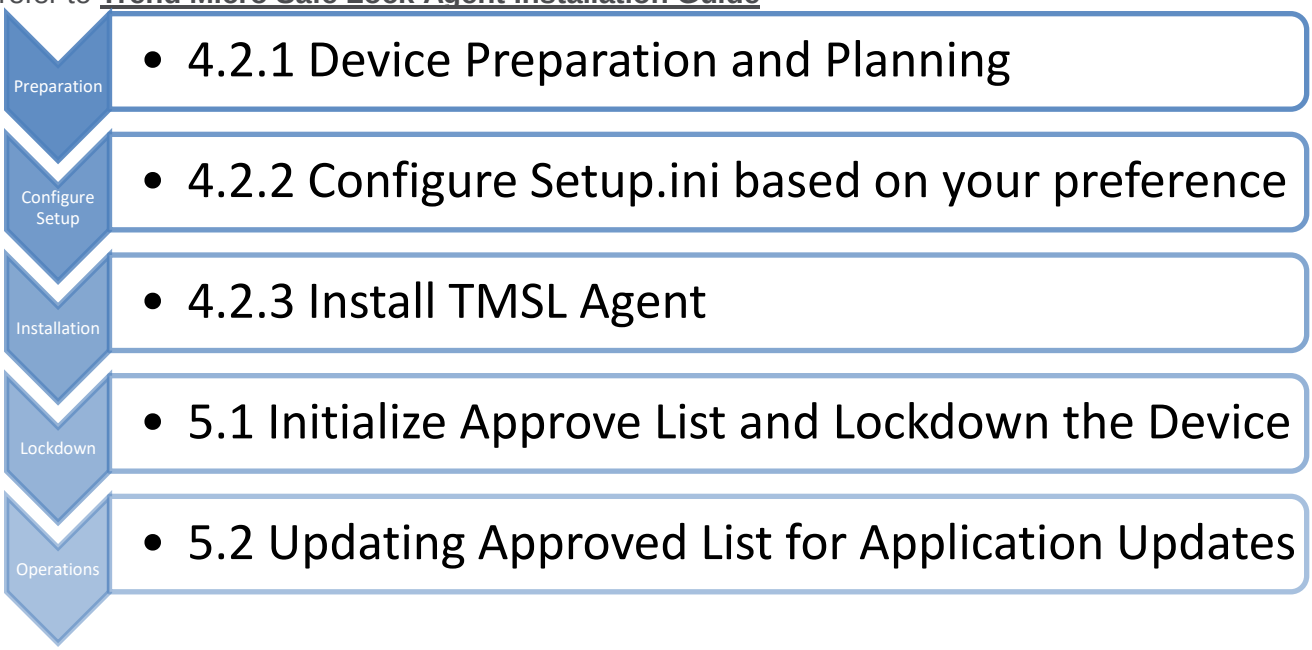
SQL Server:
- Edition: standard or above
- Database size: 500 GB

2.1.3 Installation

You can refer to Trend Micro Safe Lock Intelligent Manager Installation Guide for more details for IM Installation

2.2 Install TMSL Agent

Below is the standard flow of installing TMSL Agent. To know more detail, you may refer to **Trend Micro Safe Lock Agent Installation Guide**



2.2.1 Device Preparation and Planning

2.2.1.1 Device Preparation

As we know, Safe Lock is primarily an application trusting solution. A device that is not properly prepared for this product may cause some inconveniences and issues. Below are the recommend steps before installing Safe Lock Agent on a device:

- Uninstall Antivirus programs
- Disable Windows Defender
- Ensure Windows and Software updates are completed and no updates running during **5.1 Initialize Approved List and Lockdown the Device**

2.2.1.2Planning

Please carefully review and plan which features you would like to use for Safe Lock Agent. Full details can be found on Administrator Guide. Additionally, the following features need to be taken into consideration as they may have impact on Agent Performance::

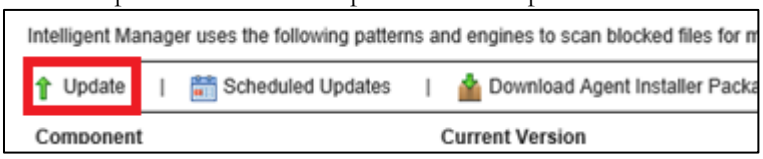
- Predefined Trusted Updater
- Trusted Hash

- Integrity Monitoring
- Root Cause Analysis

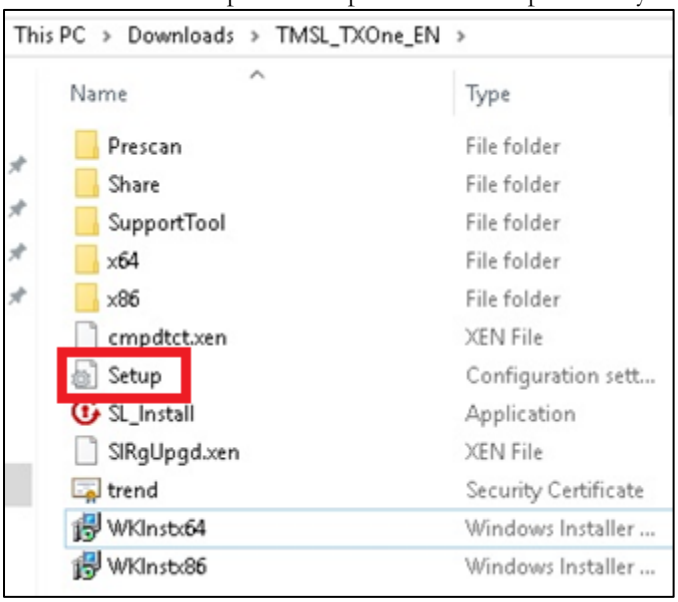
2.2.2 Setup Configuration (setup.ini)

You can modify setup.ini file to customize the installation.

1. Login to IM web console using an account with Admin privilege
2. Click Administrator -> Components -> Update
3. Click Update -> Select Components then Update



4. Click Download TMSL Agent Installer Package
5. Extract the TMSL Agent Installer Package
6. Look for the setup.ini and open it with notepad or any text editor



7. Modify the setup.ini parameters based on your preference. Complete list of setup.ini arguments and the descriptions can be found in Setup.ini File Arguments (2-18) of Trend Micro SafeLock Agent Installation Guide
8. Save the changes made on your setup.ini

9. For additional security, you can encrypt your setup.ini file using WKSupportTool.exe included in the TMSL Agent Package. You can use the command: **WKSupportTool.exe EncryptSetupIni Setup.ini Setup.bin**

10. Compress the TMSL Agent Installer. Make sure that the folder structure are the same as before and the filename of the compressed file is **TMSL_TXOne_EN.zip**

11. Save the zip file in **C:\Program Files\Trend Micro\Safe Lock Intelligent Manager\CmdTools\RemoteAgentSetupTool\package**

2.2.2.1Pre-Scan

To initiate a scan on the device before installation. You may follow the configuration below. Note that this is the default setting:

```
[Property]
PRESCAN=1

[Prescan]
IGNORE_THREAT=0
REPORT_FOLDER=
SCAN_TYPE=Full
COMPRESS_LAYER=2
MAX_FILE_SIZE=0
SCAN_REMOVABLE_DRIVE=0
FORCE_PRESCAN=0
```

2.2.2.2 Initiate Approved List

To automatically initiate Approved List after installation, you may follow the configuration below:

```
[Property]
INIT_LIST=1
```

2.2.2.3 Application Lockdown

To Turn On Application Lockdown after the installation finish

```
[Property]
LOCKDOWN=1
```

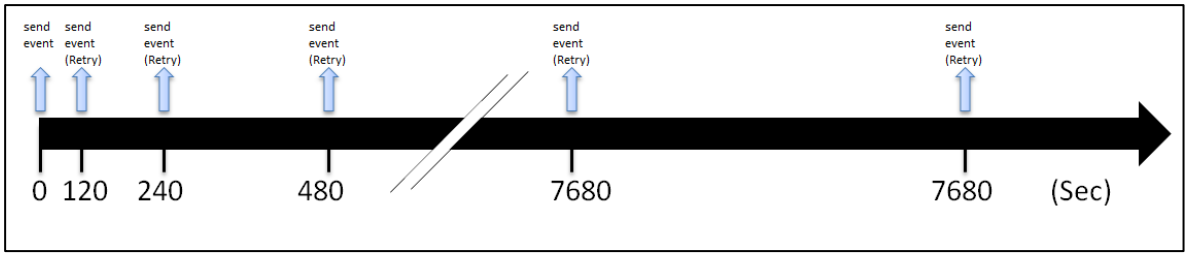
2.2.2.4 Silent Install

To perform silent installation, you may follow the configuration below:

```
[Property]
  SILENT_INSTALL=1
  ACTIVATION_CODE=XX-XXXXX-XXXXX-XXXXXX-XXXX
  PASSWORD=XXXXXXXX
```

2.2.2.5 Message Retry Interval

When TMSL Agent fails to send an event to IM, the TMSL Agent retries based on “INITIAL_RETRY_INTERVAL” and “MAX_RETRY_INTERVAL” settings, and it uses an exponential Backoff algorithm. For example, if you set as INITIAL_RETRY_INTERVAL=120 (sec) and MAX_RETRY_INTERVAL=7680 (sec), the behavior is as below:



2.2.3 Install TMSL Agent

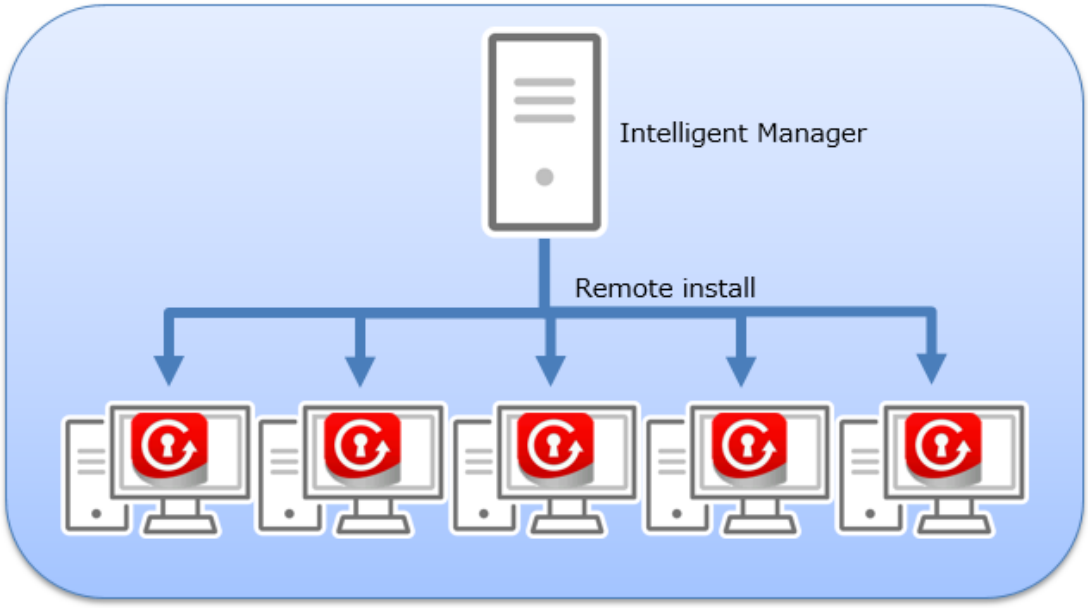
This document explains different methods of installing TMSL Agent.

Category	Description
Remote installation	● The devices already exist in factory/store/customer site and can change its OS setting (such as disable UAC) remotely or it has already changed for TMSL remote installation. Each device has a unique IP address and can be accessed from IM.
Local installation	● These devices have built-in HDD (that cannot be removed) and have not yet been sent to the customer’s factory/store/site. Tablet PC’s are good examples of such devices. ● The devices already exist in each factory/store/customer site, but cannot change the OS setting. ● Need to install TMSL Agent with the devices local maintenance timing. The device is under NAT environment
HDD copy installation	These devices have removable HDD and have not yet been sent to the customer’s factory/store/site.

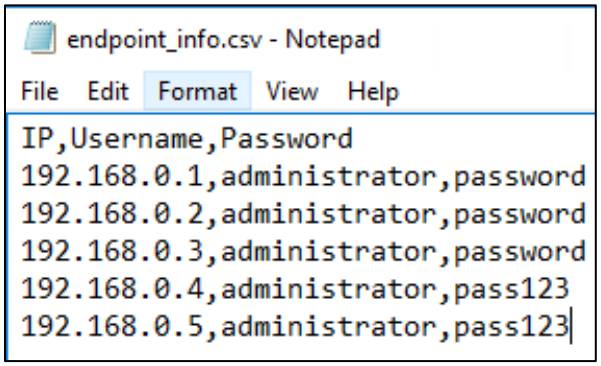
Table 7 - TMSL Agent Installation Methods

2.2.3.1Remote Installation

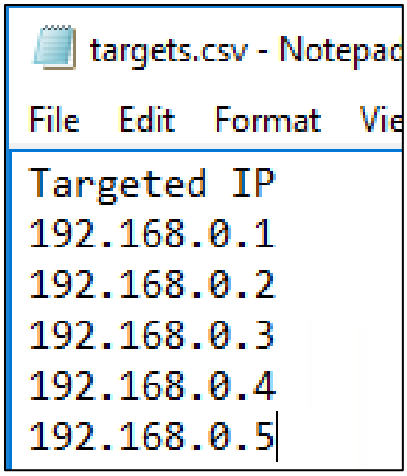
This method is used for remote installation of TMSL Agent from IM. This installation method requires some changes on the device. More information is available at **Trend Micro Safe Lock Intelligent Manager Administrator Guide**



1. Login to IM
2. Navigate to C:\Program Files\Trend Micro\Safe Lock Intelligent Manager\CmdTools\RemoteAgentSetupTool
3. Open endpoint_info.csv and add the target devices' IP Address, Administrator account , and Password



4. Open targets.csv and add the target devices' IP Addresses



5. From the Command Prompt and with Administrator Privileges, initiate the remote install by entering the "*SLrst.exe targets.csv –install*" command
6. In Create Password for Remote Safe Lock Agents prompt, Enter and Confirm TMSL Agent Password

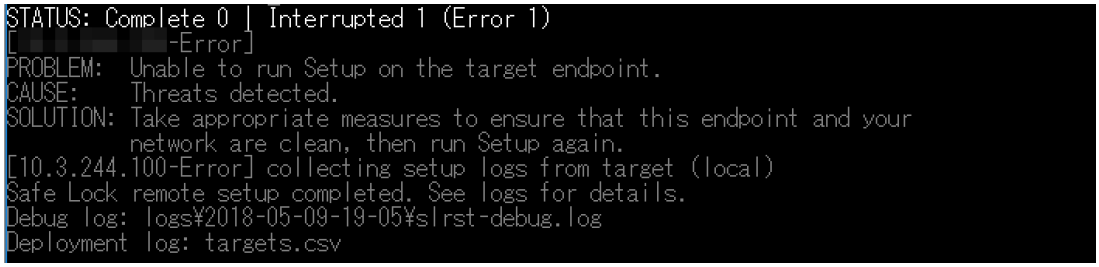
Important: -

- 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
-- 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

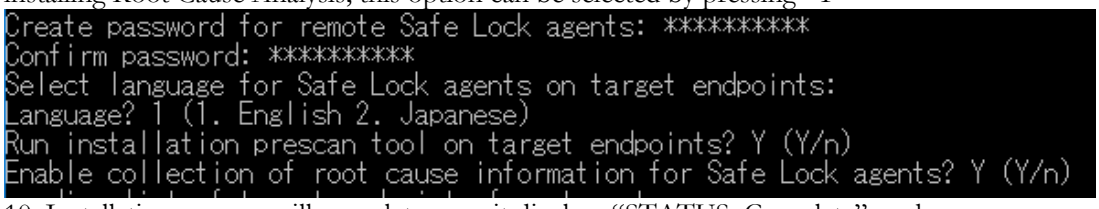
7. Select Language
8. Select Y in Run installation pre-scan tool on target endpoints to start pre-scan

Important:

-- Pre-scan may require some time to complete but it is recommended for security of the device
-- If a malware was found during pre-scan, the remote installation will be interrupted

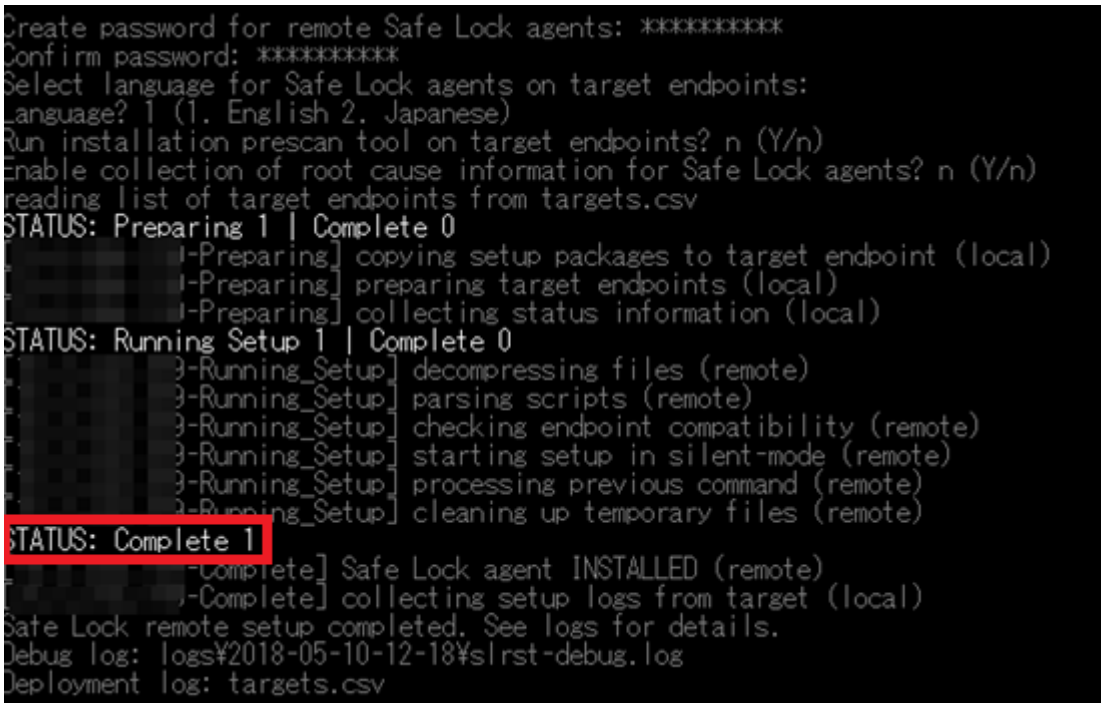


9. "Enable Collection of root cause information for Safe Lock agents" prompt is for installing Root Cause Analysis; this option can be selected by pressing "Y"

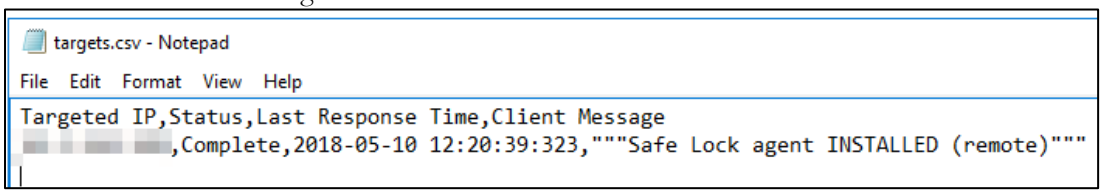


10. Installation process will complete once it displays "STATUS: Complete" as shown

below:



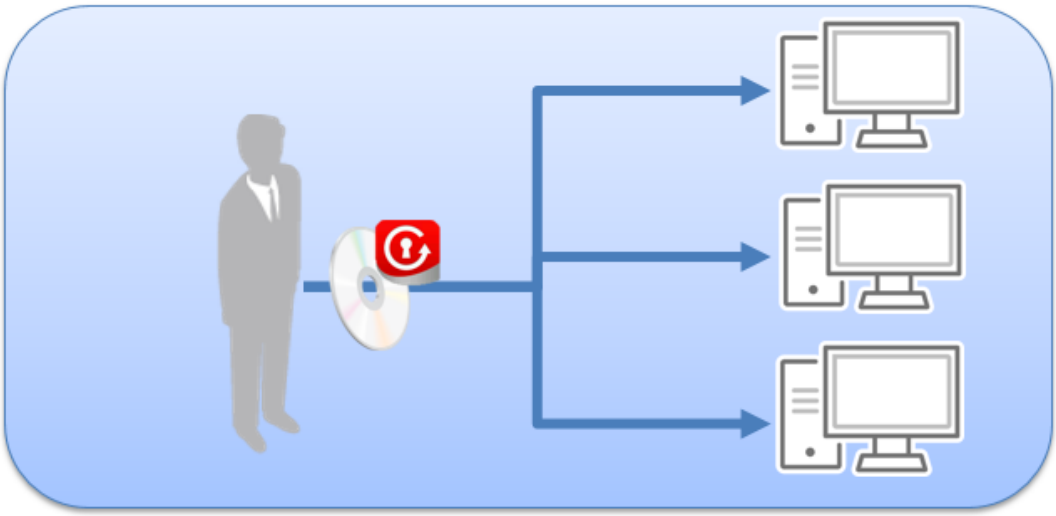
11. You can also check targets.csv for the status



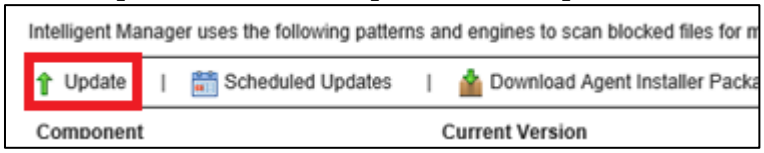
Important: *If INIT_LIST and LOCKDOWN in setup.ini is not set, Approved List and lockdown TMSL Agent should be created manually..*

2.2.3.2 Local Installation

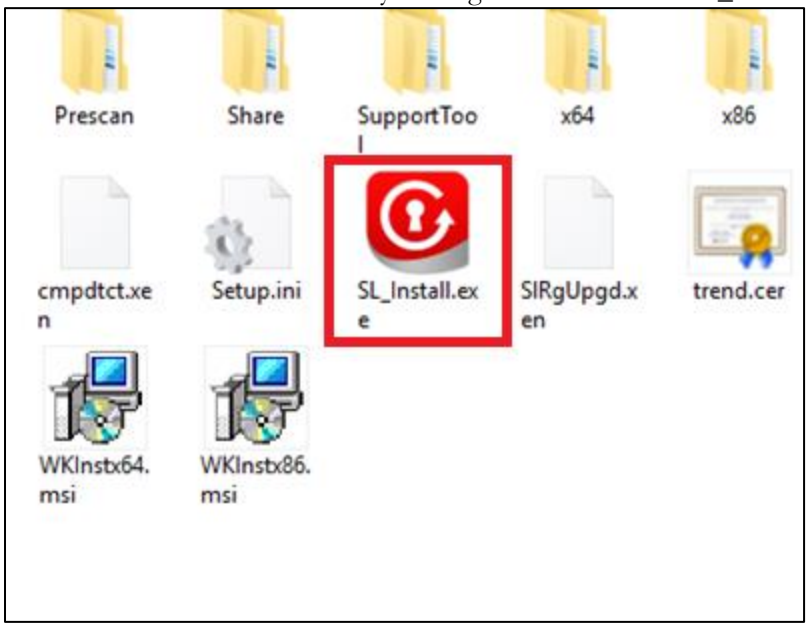
TMSL Agent can be installed for each device one by one. TMSL Agent will register to IM directly after installation process finishes



1. Login to IM web console using an account with Admin privileges
2. Click **Administrator -> Components -> Update**
3. Click **Update -> Select Components then Update**



4. Click on Download Agent Installer Package
5. Extract the Agent Installer Package and copy it into a removable media
6. Insert the removable media to your target device and run **SL_Install.exe**



7. Install TMSL Agent following the installation wizard

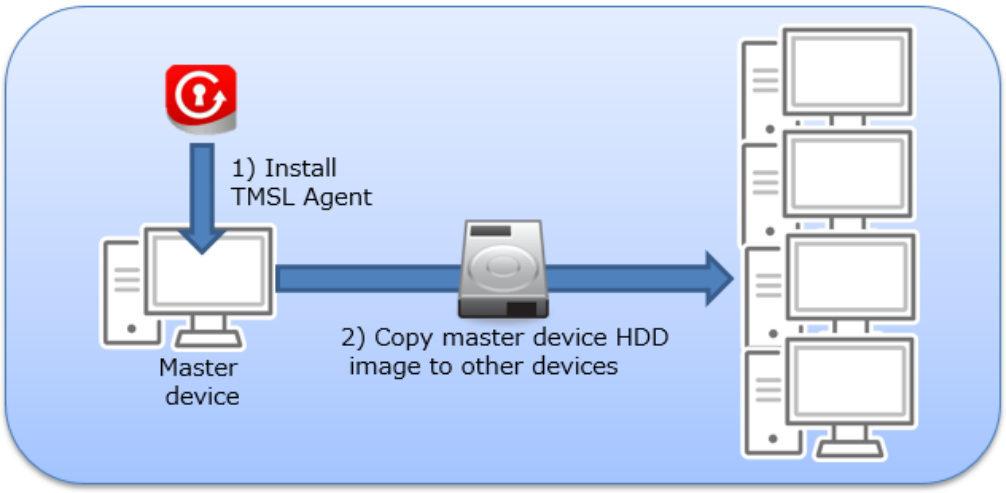
Important: *-*

- 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
-- 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
-- You should create Approved List and lockdown TMSL Agent manually, if you did not set INIT_LIST and LOCKDOWN in setup.ini.

2.2.3.3 HDD Copy Installation

This installation method is used for when you have HDD copy of your device with TMSL Agent and you want to apply this to other devices. You'll need to first prepare a Master Device configured with your desired settings and installed applications including TMSL Agent



This installation method requires special assistance which is only available for Trend Micro Premium Support (TPS) contract holders. For more details, please contact Trend Micro.

Chapter 3: Configuring Approved Lists

3.1 Initialize and Build Approved List

After TMSL Agent installation, we recommend to build and initialize the Approved List. As instructed below:

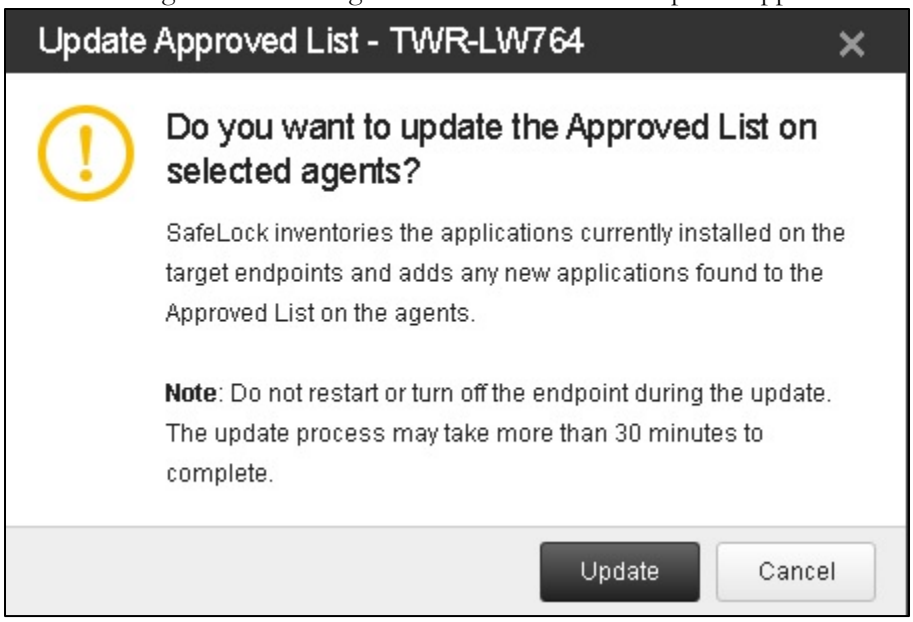
1. From TMSL Agent side, you can initialize Approved List by opening the TMSL Agent console and clicking on TMSL Agent icon; You'll be ask to initialize Approved List.

2. From TMSL Agent side, you can also initialize Approved List by using CLI command "SLCmd.exe add approvedlist –r C:\"

```
C:\Program Files\Trend Micro\Safe Lock>SLCmd.exe add approvedlist -r C:\
Password:
Scanning computer (53%)_
```

3.

4. From IM > Agents > Select Agent > Send Command > Update Approved List



3.2 Updating Approved List

3.2.1 Maintenance Mode

Maintenance Mode is a new feature that is introduced in Trend Micro Safe Lock TXOne Edition. It allows the user to a period when TMSL Agent allows all file executions, and adds all files that are created, executed or modified to the Approved List. This is especially helpful and valuable when applying a patch to software or apps on your device. This feature can also run a scan on the endpoint at the end of Maintenance Mode to make sure that threats are filtered. Given this, we **highly recommend** to use Maintenance Mode as the method of updating the Approved List.

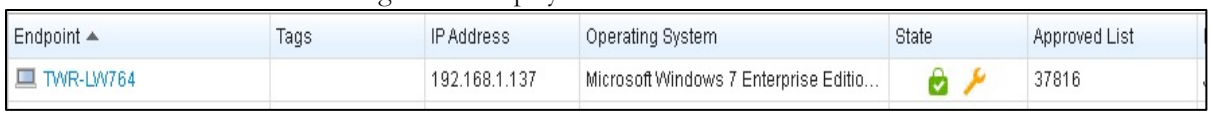
3.2.1.1 Configure Maintenance Mode via IM

You can configure scheduling of Maintenance Mode using IM.

6. From IM. Click Agents > Select Agent > Send Command > Configure Maintenance Mode > Select Enable
7. The Configure Maintenance Mode window will expand. If you see an option to Update Agent Component, click this first to apply the latest component updates to agent

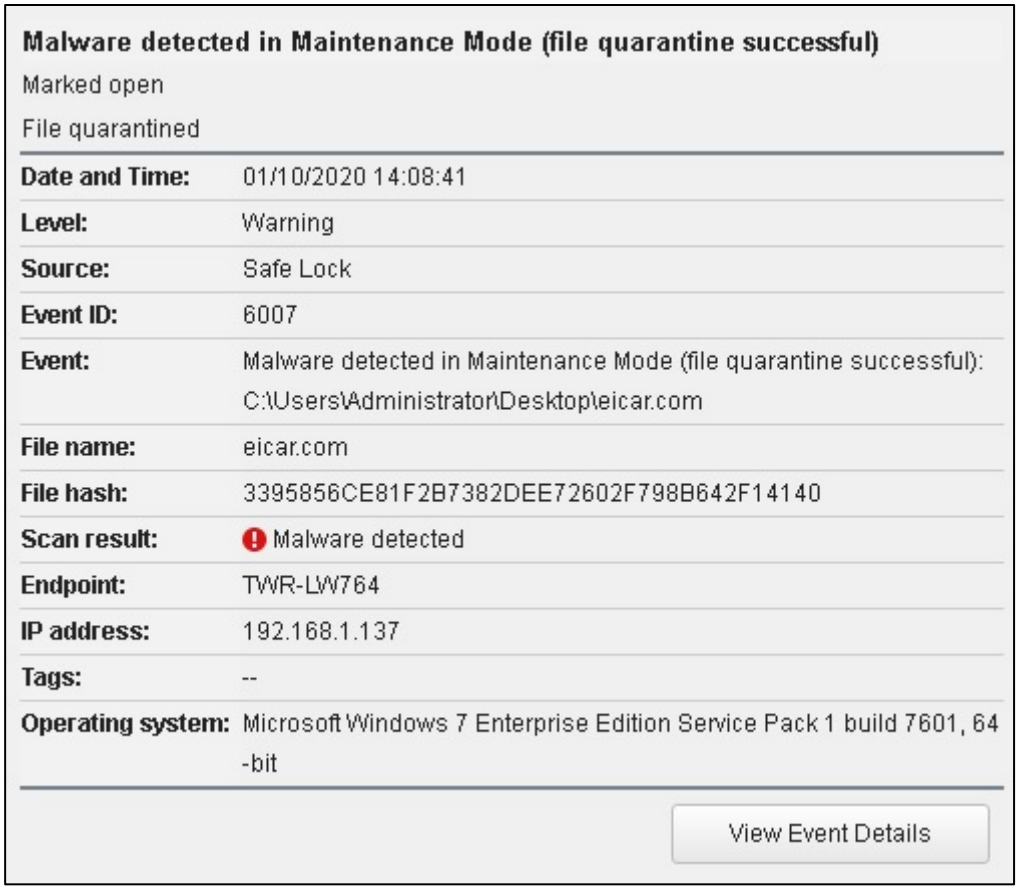
8. Select **Schedule** From and To

9. Place a check mark on Scan endpoints after Maintenance Mode is stopped. Depending on your preference, you can either select **Quarantine detected files** or **Add detected files to Approve List.**
10. Click Deploy
11. The wrench icon of the TMSL Agent will display on Maintenance Mode



12. In your TMSL Agent, you will the wrench icon see the TMSL Agent systray icon and in the Agent Console

13. At the end of Maintenance Mode, the virus scan will trigger. If it finds any threats, the Agent Events will be shown similar to below:



14. Approved List will also be updated based on the changes during Maintenance Mode

3.2.1.2Configure Maintenance Mode via TMSL Agent

You can instantly enable Maintenance Mode using the command:

```
SLCmd.exe -p <password> start maintenancemode -scan quarantine
```

```
C:\Program Files\Trend Micro\Safe Lock>SLCmd.exe -p [redacted] start maintenance
mode -scan quarantine
Maintenance Mode started.
```

Check status of Maintenance Mode using the command:

```
SLCmd.exe -p <password> show maintenancemode
```

```
C:\Program Files\Trend Micro\Safe Lock>SLCmd.exe -p [redacted] show maintenancem
ode
In Maintenance Mode.
```

Stop Maintenance Mode using the command:

```
SLCmd.exe -p <password stop maintenancemode
```

```
C:\Program Files\Trend Micro\Safe Lock>SLCmd.exe -p [redacted] stop maintenancem
ode
Maintenance Mode stopped.
```

Schedule a Maintenance Mode using the command:

```
SLCmd.exe -p <password> set maintenancemodeschedule -start YYYY-MMDDTHH:MM:SS -end YYYY-
  MMDDTHH:MM:SS
```

```
C:\Program Files\Trend Micro\Safe Lock>SLCmd.exe -p [redacted] set maintenancemo
deschedule -start 2020-01-10T14:41:00 -end 2020-01-10T14:45:00 -scan quarantine
Maintenance Mode schedule configured.
```

Check the configured Maintenance Mode schedule using the command:

```
SLCmd.exe -p <password> show maintenancemodeschedule
```

```
C:\Program Files\Trend Micro\Safe Lock>SLCmd.exe -p [redacted] show maintenancem
odeschedule
Start time: 2020-01-10T14:41:00
End time: 2020-01-10T14:45:00
Scan: Yes
Scan action: Quarantine
```

To see full details of Maintenance Mode commands. Please see Trend Micro SafeLock TXOne Edition Administrator Guide

3.2.1.3 Maintenance Mode Limitations

The following are limitations of Maintenance Mode:

15. Installation involving reboot may result in file events not being recorded by Maintenance Mode. This is because events or actions occurred prior to when TMSL service started, will not be recorded.
16. When Maintenance Mode is enabled, Safe Lock does not support Windows updates that require restarting an endpoint during the maintenance period
17. When the agent is about to leave Maintenance Mode, restarting the agent endpoint prevents Safe Lock from adding files in the queue to the Approved List.

3.2.2 Windows Update Support

For Windows Update scenario, it is recommended to use Windows Update Support feature. This feature, when enabled, automatically adds the updated files from Windows Update to the Approved Lis

This feature is capable of supporting the following scenarios:

- Online Windows Update
- Local Windows Update using *.msu KB File
- Local Windows Update using *.exe KB File
- Windows Update that includes reboot

This feature has limitations on the following scenarios:

- Windows Update with Device Drivers included
- Service Pack Installation

3.2.2.1Configure Windows Update Support using CLI

Use the following command to configure Windows Update Support: **SLCmd.exe set wus enable**

```
C:\Program Files\Trend Micro\Safe Lock>SLCmd.exe set wus enable
Password:
Windows Update Support: Enabled
```

3.2.2.2 Configure Windows Update Support using setup file (setup.ini)

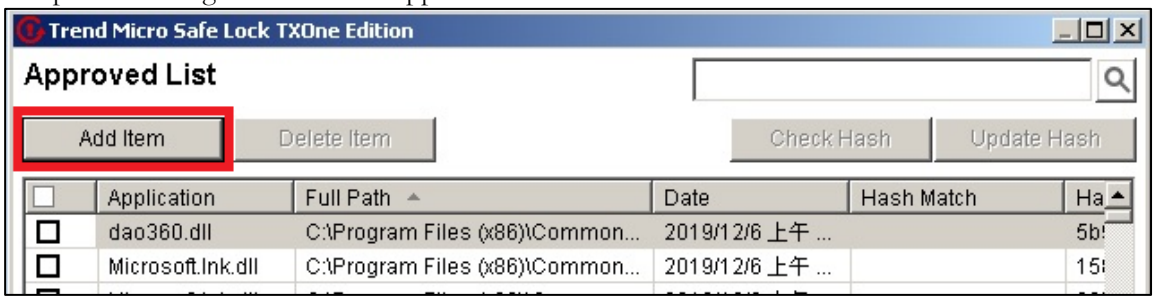
Here is how to configure Windows Update Support using setup.ini file:

```
[Property]
WINDOWS_UPDATE_SUPPORT=1
```

3.2.3 Manual Update

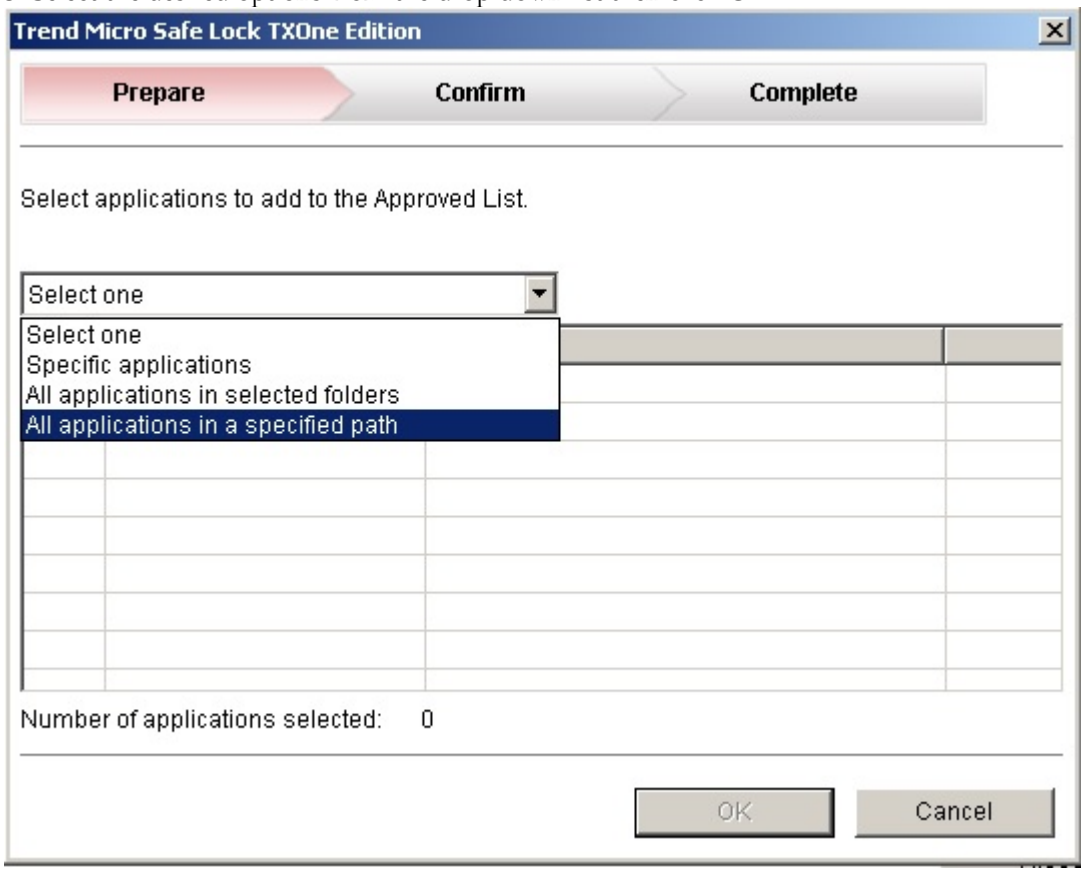
3.2.3.1Manually Update Approved List via TMSL Agent Console

1. Open TMSL Agent Console > Approved List > Add Item

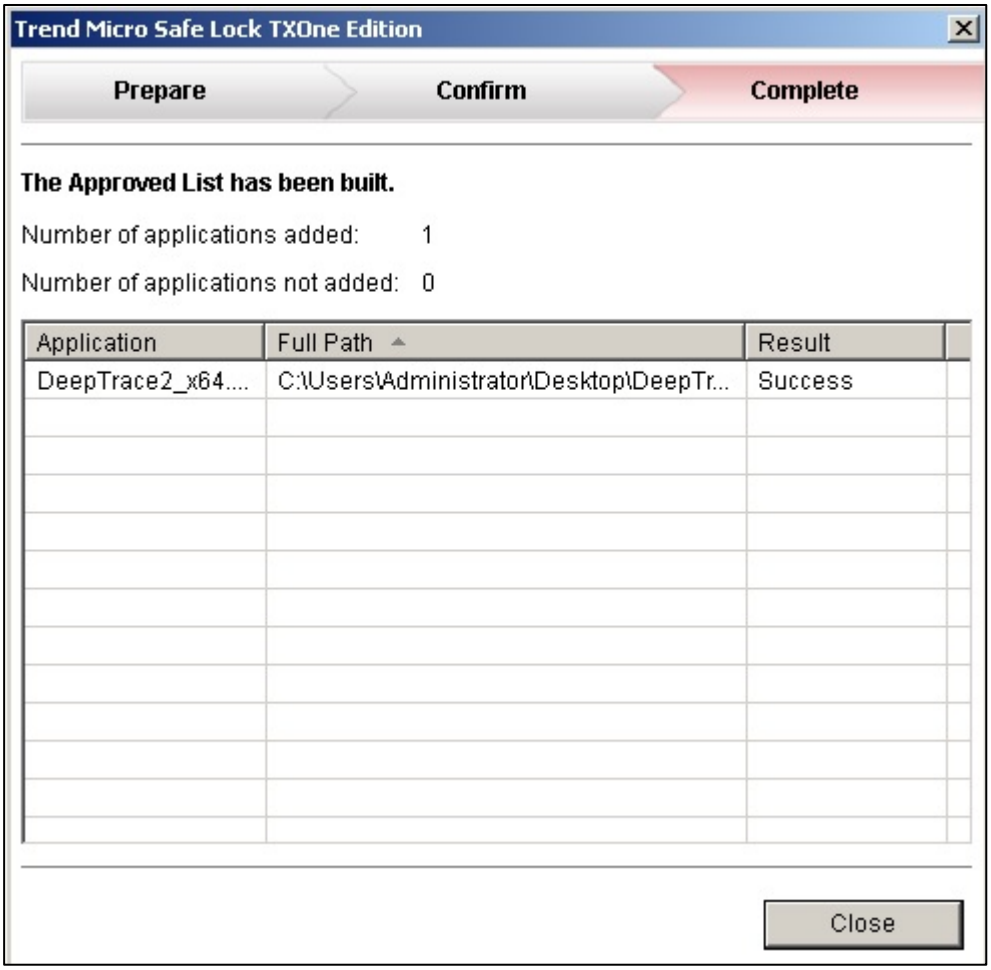


2. Select Manually Browser and Select Files then hit **Next**

3. Select the desired options from the drop down list then click Ok



4. Click **Approve** and wait till it shows **Success** in the results



5. Click **Close**

3.2.3.2 Manually Update Approved List via Command Line (CLI)

1. Open Command Prompt as Administrator
2. Navigate to C:\Program Files\Trend Micro\Safe Lock
3. Enter the command: slcmd.exe –p <password> add approvedlist <file path>

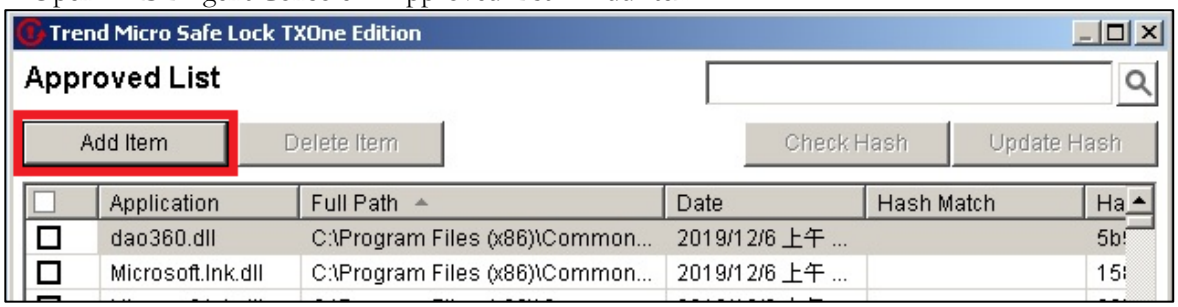
```
C:\Program Files\Trend Micro\Safe Lock>SLCmd.exe -p [redacted] add approvedlist
"C:\Documents and Settings\Administrator\Desktop\TeamViewer_Setup.exe"
Add file from specified path:
[OK] C:\Users\Administrator\Desktop\TeamViewer_Setup.exe
Finished.
Successful Items: 1
Failed Items: 0
```

4. If you want to add a folder and its sub folders, you can use the command:: **slcmd.exe –p <password> add approvedlist –r <folder path >**

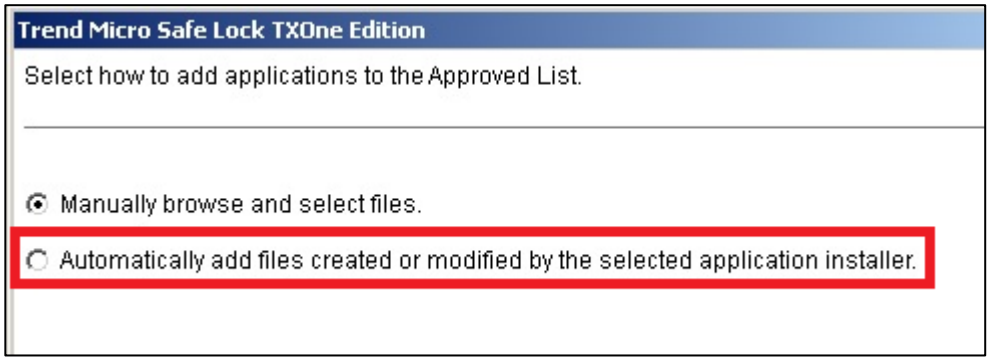
3.2.4 Trusted Updater

Trusted Updater is a method of updating Approved List in which all of its applicable scenarios are already well covered by Maintenance Mode so unless it is specifically required, we recommend to use Maintenance Mode instead. Details on how to use the Trusted Updater are as follows:

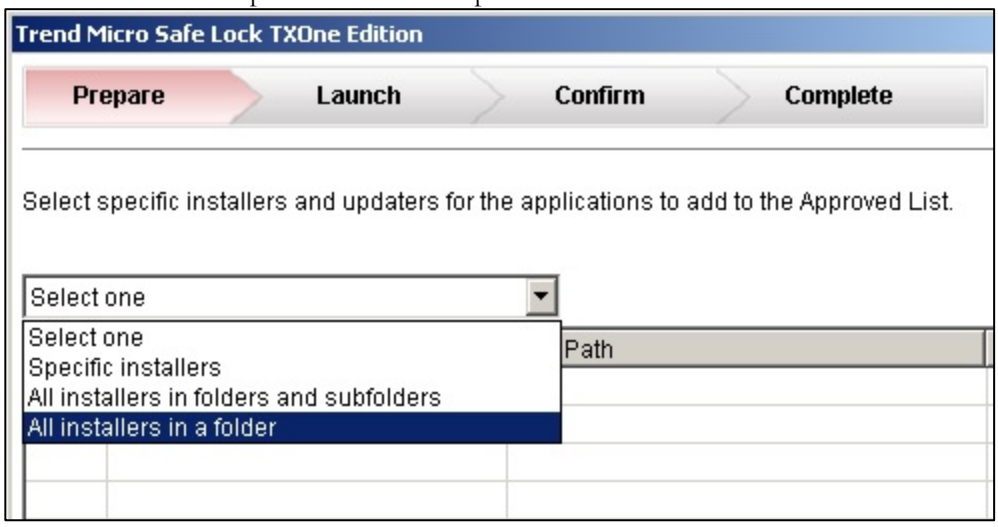
1. Open TMSL Agent Console > Approved List > Add Item



2. Select **Automatically add files created** or **modified by the selected application installer** then click **Next**

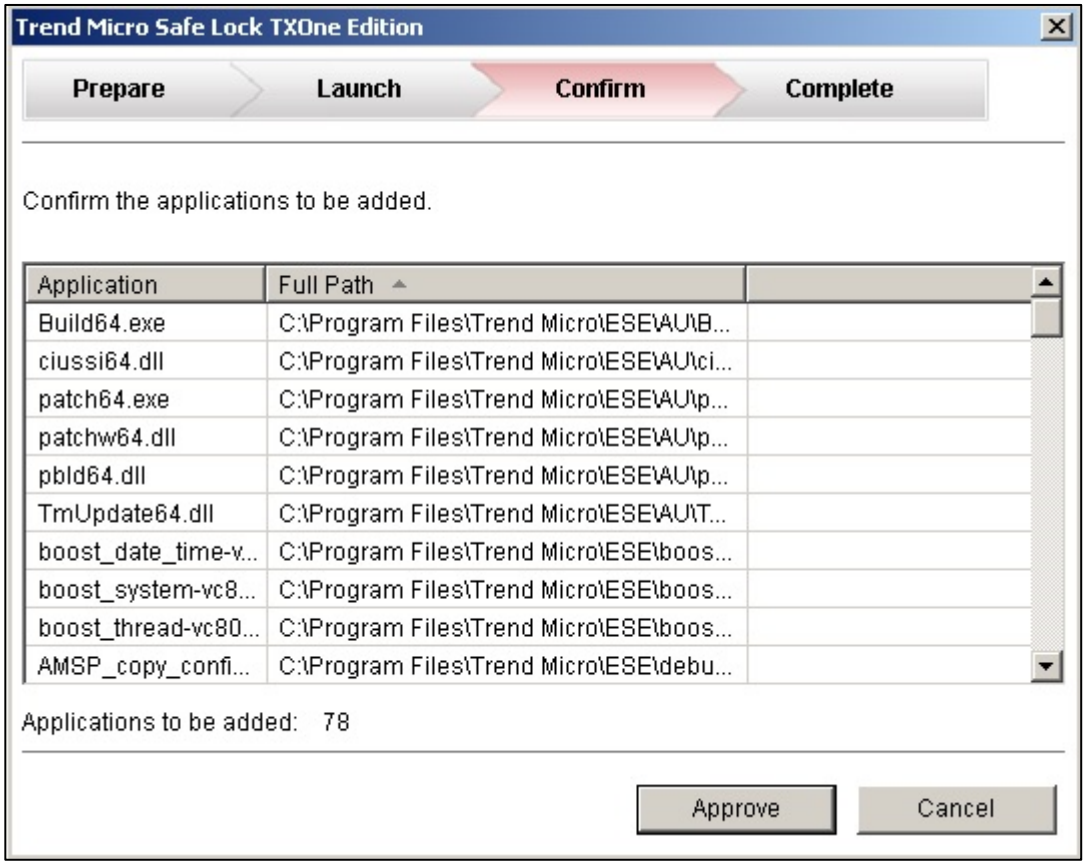


3. Select the desired options from the drop down list then click **Start**

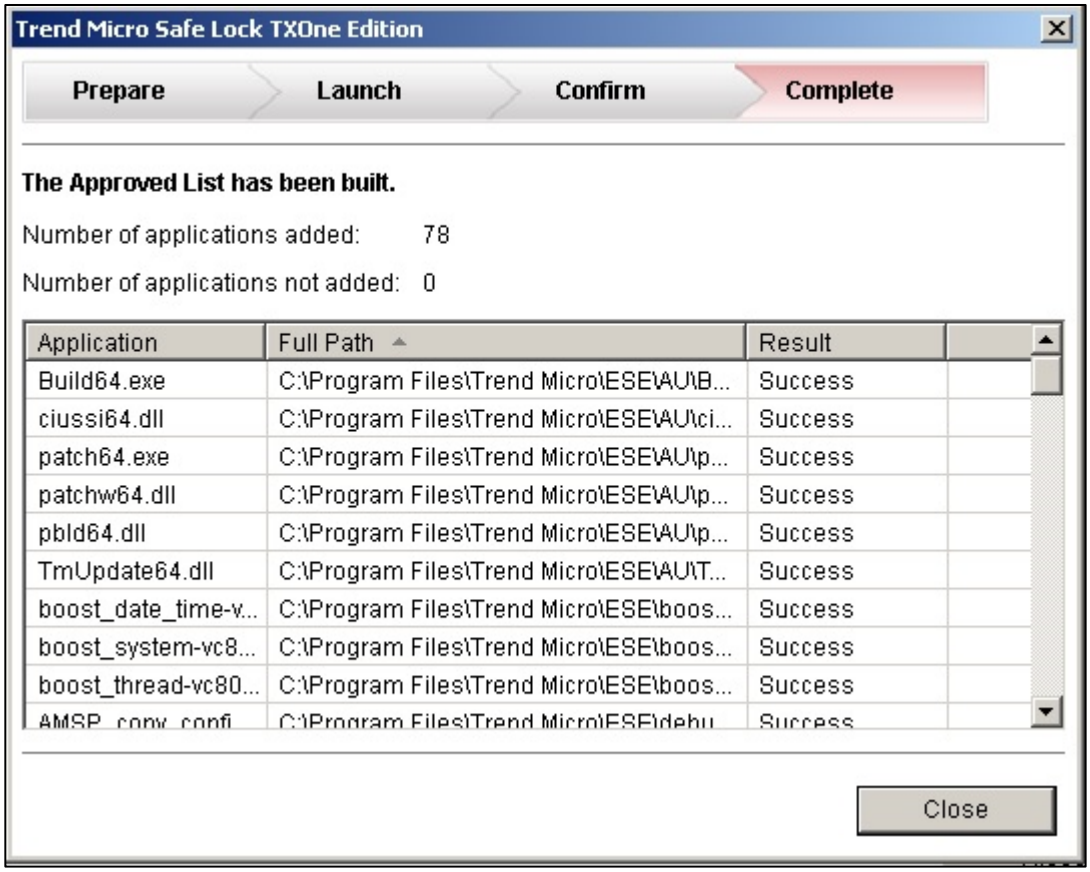


4. The following window will appear. During this time, run the installer then click Stop once the installation has finished

5. This should list out all files that were added during the installation. Click **Approve**



6. It should show results when finished



3.2.5 Predefined Trusted Updater

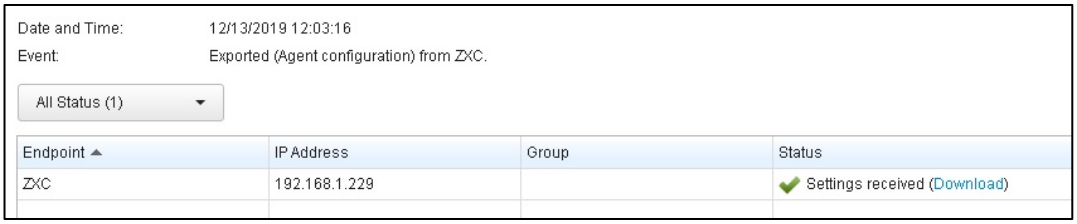
Predefined Trusted Updater is a method of updating Approved List in which all of its applicable scenarios are already well covered by Maintenance

Mode so unless it is specifically required, we recommend to use Maintenance Mode instead. Details on how to use the Predefined Trusted Updater

are as follows.

3.2.5.1Configure Predefined Trusted Updater via IM

1. Login to IM with an account with Admin privileges
2. Click **Agents -> Right click your Target Agent -> Send Command -> Export Settings -> Agent Configuration**
3. A new window will appear. Wait till export is finished and click **Download**. The file downloaded will be named as config.xml



4. Open config.xml and modify the following depending on your requirements.

```
<PredefinedTrustedUpdater Enable="yes">
        <RuleSet>
        <Condition Id="Application_Installer">
                <ApprovedListCheck Enable="no"/>
                <ParentProcess Path=""/>
        </Condition>
        <Rule Label="Trusted_Installer_1">
                        <Updater Path="c:\updater\setup.exe"
Type="Process" ConditionRef="Application_Installer"
RunonceTrace="yes"/>
        </Rule>
        </RuleSet>
```

Important: *-- Make sure to keep the encoding as **UTF-8** when saving*

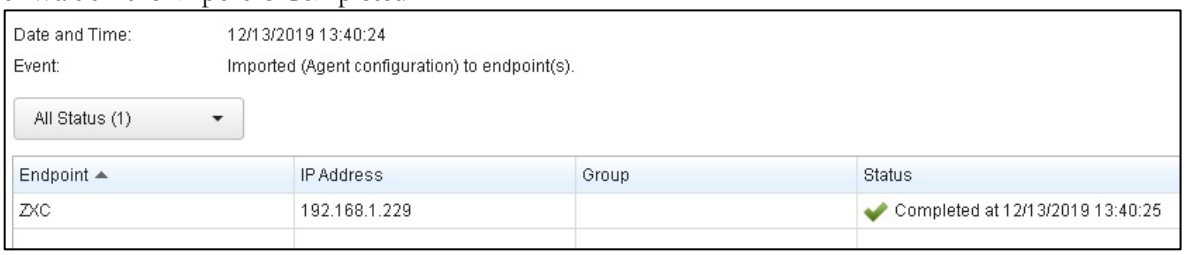
Below are the parameters for config.xml related to Predefined Trusted Updater:

Parameter	Settnig	Value	Modify / Add	Description
PredefinedTrustedupdater	Enable	Yes	Modify	Enable Predefined Trusted updater
Condition	Id	<unique_ruleset_name>	Add	Describe an installer program name. * this name should be unique in the configuration file
ApprovedListCheck	Enable	Yes	Add	Yes = Enable the installer program hash checks with Approved List. No = Disable the installer program hash checks with Approved List.

Parameter	Settnig	Value	Modify / Add	Description
Parent Process	Path	-	Add	Specify the parent process of the installer program.
Rule	Label	<unique_rule_name>	Add	Specify this rule name.
Updater	Path	<updater_path>	Add	Path of the Installer program
	Type	process	Add	If the installer program is an exe file, it set as "Process"
		file	Add	If the installer program is a bat or msi, it's set as "file"
		folder	Add	Use the exe, msi or bat files in the specified folder.
		folderandsub	Add	Use the exe, msi or bat files in the specified folder and its subfolders.
	ConditionRef	<same_as_ruleset_name>	Add	Add same Condition name
Runonce	Trace	Yes	Add	If TMSL Agent needs to trace installer program after reboot, set "yes"

Table 8 - Predefined Trusted Updater settings in Config.xml

5. Return to **IM -> Agents -> Right click your Target Agent -> Send Command -> Import Settings -> Agent Configuration -> Select the modified config.xml -> Click Import** and **Apply**
6. Wait till the Import is Completed



3.2.5.2 Configure Predefined Trusted Updater via TMSL Agent

1. Open Command Prompt as Administrator
2. Navigate to C:\Program Files\Trend Micro\Safe Lock
3. Enter the command: slcmd.exe set predefinedtrustedupdater enable

```
C:\Program Files\Trend Micro\Safe Lock>SLCmd.exe set predefinedtrustedupdater en
able
Password:
Pre-defined Trusted Updater: Enabled
```

This will enable Pre-defined Trusted Updater

Important: *If you keep getting "The program is already running. Cannot launch another instance" message, make sure to close TMSL Agent console*

Here are the parameters for predefinedtrustedupdater

Parameter	Required?	Description
-u <folder_or_file>	Required	Add the specified file or folder to the Predefined Trusted Updater List
-t <type_of_object>	Required	Specify the "type of object. Available objects types are as follows: process: Indicates only exe file. file: Indicates only msi and bat file. 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 of the installer program.
-l <label_name>	Optional	Specify a rule name.
-al enable	Optional	Compare the hash values in the Approved List with the installer program's hash values. Enabled by default even when -al is not specified
-al disable	Optional	Do not compare the hash values in the Approved List with t the installer program's hash values.

Table 9 - Predefined Trusted Updater Parameters

4. Enter the command:

```
slcmd.exe add predefinedtrustedupdater –u <file_or_folder> -t <type_of_object> -l
  <lable_name> -al disable
```

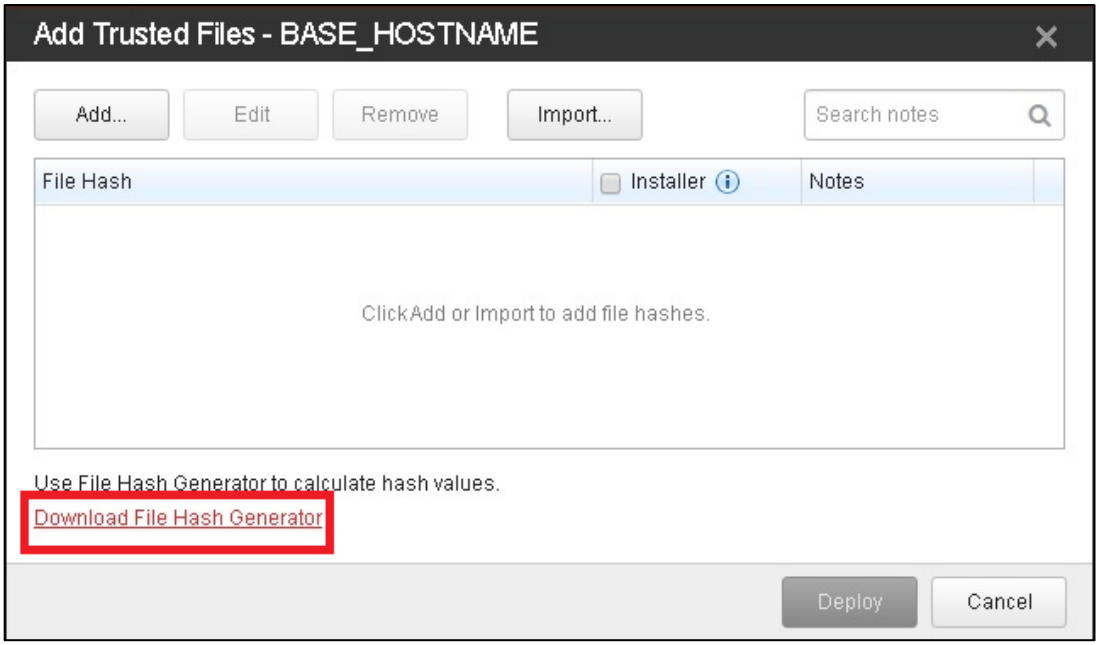
```
C:\Program Files\Trend Micro\Safe Lock>SLCmd.exe add predefinedtrustedupdater -u
 C:\aa.exe -t process -l Trusted_Installer_3 -al disable
Password:
New Predefined Trusted Updater rule added.
```

5. Run the installer in Predefined Trusted Updater

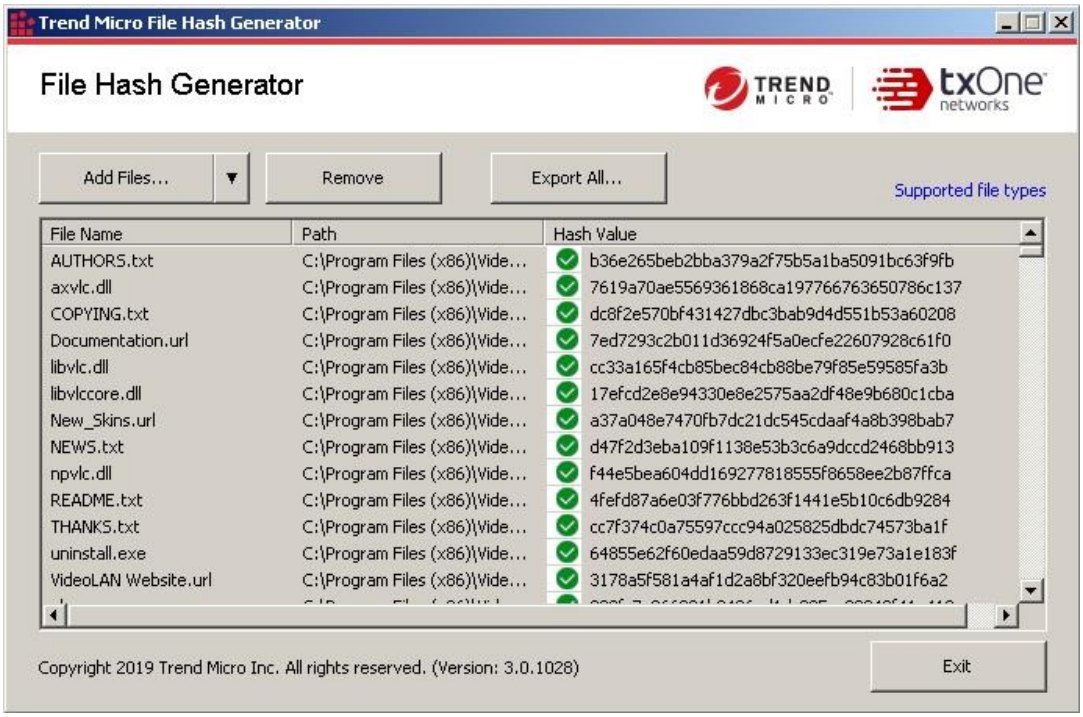
3.2.6 Trusted Hash

3.2.6.1Configure Trusted Hash via IM

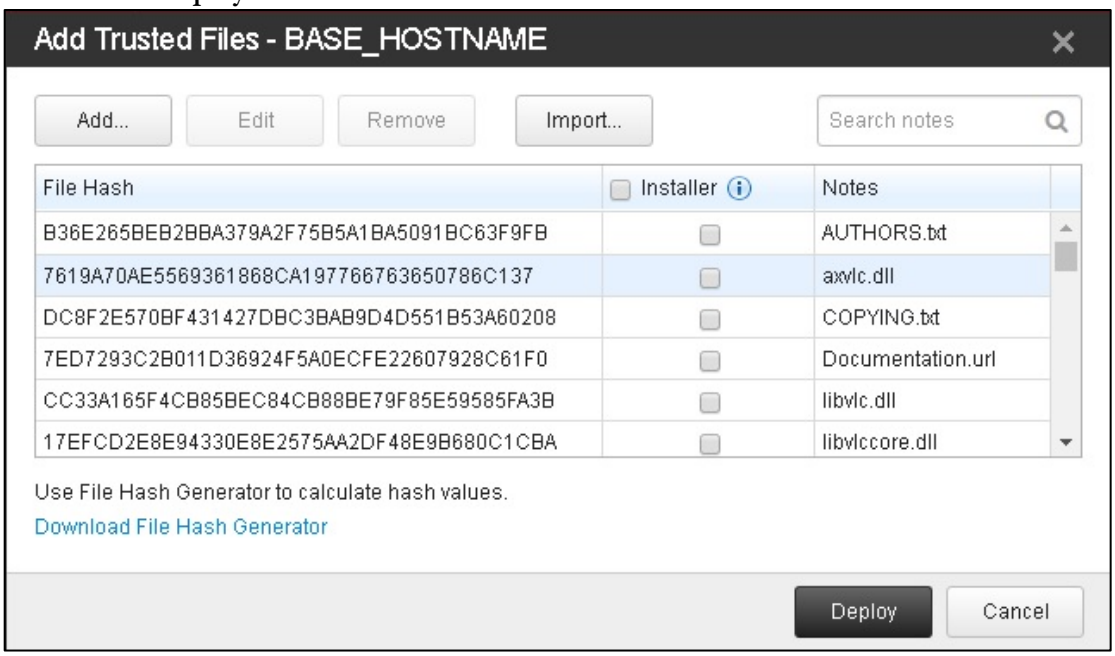
1. Login to IM with an account with Admin privilege
2. Click **Agents -> Right click your Target Agent -> Send Command -> Add Trusted Files**
3. A new window will appear. Click Download File Hash Generator to download the tool named TMSL_FileHashGen_EN



4. Copy the TMSL_FileHashGen_EN tool to your device and run it
5. Drag the files or folders you want to add to Trusted Hash. The FileHashGen should get the hash value automatically



6. Click **Export All**. It should export a text file.
7. Copy this file to IM. In the Add Trusted Files window, click on **Import** then select **the file -> Click Deploy**



8. Hashes will be added; wait till it is Completed

3.2.6.2 Configure Trusted Hash via TMSL Agent

1. Open Command Prompt as Administrator
2. Navigate to C:\Program Files\Trend Micro\Safe Lock

3. To enable the Trusted Hash and Predefined Trusted Updater, please enter the command below:

```
slcmd.exe set trustedhash enable
slcmd.exe set predefinedtrustedupdater enable
```

```
C:\Program Files\Trend Micro\Safe Lock>SLCmd.exe set trustedhash enable
Password:
Trusted Hash List: Enabled

C:\Program Files\Trend Micro\Safe Lock>SLCmd.exe set ptu enable
Password:
Pre-defined Trusted Updater: Enabled
```

4. Calculate the SHA1 value of your installer
5. Enter the following command to add the Installer's Hash Value to Trusted Hash

```
slcmd.exe add trustedhash –v <installer_hash_value> -u
```

```
C:\Program Files\Trend Micro\Safe Lock>SLCmd.exe add trustedhash –v 79a4ba5672d4
b94acf6792a1eae1d0dd7d7ceca1 –u
Password:
Hash value added to the Trusted Hash List.
```

Below are the parameters that can be used for Trusted Hash

Parameters	Required	Description
-v <file_hash>	Required	Add the specified file hash to the Trusted Hash.
-t <file_path>	Optional	The –t parameter lets you to specify the path of the file
-al	Optional	Using the optional -al value adds the file of the specified hash value to Approved List.
-l <label_name>	Optional	Specify a label name for this hash value.
-u	Optional	Using the optional -u value treats the file of the specified hash value as a Trusted Updater where TMSL Agent adds files, which created / modified from the file of the specified hash value to the Approved List. This parameter requires to enable "Predefined Trusted Updater"
-n <note>	Optional	The -n value adds a note for the file hash.

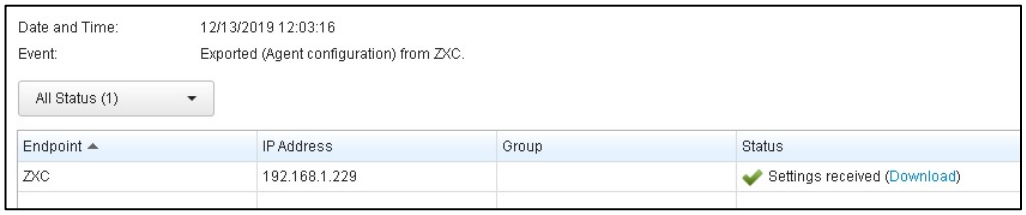
Table 10 - Trusted Hash Parameters

6. To check the added hash. You can enter **slcmd.exe show trustedhash**
7. You should be able to run the file having the hash value that you just added

3.2.7 Trusted Digital Signature Update

3.2.7.1Configure Trusted Digital Signature Update via IM

1. Login to IM with an account with Admin privilege
2. Click **Agents -> Right click your Target Agent -> Send Command -> Export Settings -> Agent Configuration**
3. A new window will appear; wait till export is finished and click Download. The file downloaded will be named as config.xml



4. Open config.xml and modify the following depending on your requirements.

```
<TrustedUpdater>
<PredefinedTrustedUpdater Enable="Yes">
<RuleSet/>
</PredefinedTrustedUpdater>
<WindowsUpdateSupport Enable="no"/>
</TrustedUpdater>
<DllDriverLockDown Enable="yes"/>
<ExceptionPath Enable="no">
<ExceptionPathList/>
</ExceptionPath>
<TrustedCertification Enable="yes">
  <PredefinedTrustedCertification Label="certification1" Type="updater"
      Issuer="TrendMicro" Subject="Trend Micro"
  Hash="6ffad4a3b15f6a2c71d43c8e551dcecab3a5183c"/>
```

Important: *Make sure to keep the encoding as UTF-8 when saving*

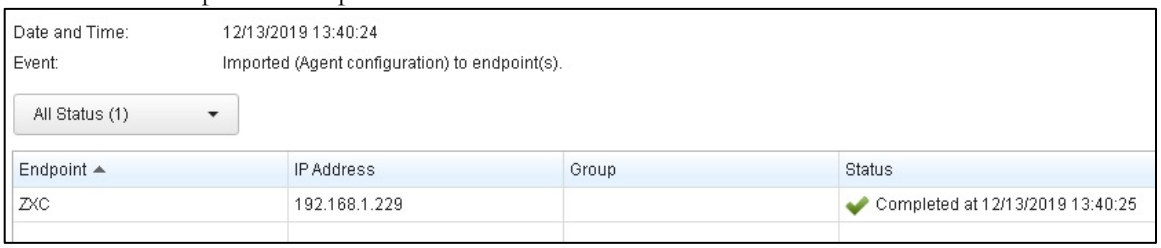
Below are the parameters for config.xml related to Digital Signature Update:

Parameter	Setting	Value	Description
PredefinedTrustedCertification	Type	updater	Updater=An application that has specified digital signature is treated as an installer.

Parameter	Setting	Value	Description
			Lockdown=An application that has specified digital signature is not treated as an installer.
	Hash	<SHA-1_hash_value>	SHA1-hash value of specified digital signature.
	Label	<label>	Description of specified digital signature.
	Subject	<subject>	Subject of specified digital signature.
	Issuer	<issuer>	Issuer of specified digital signature.

Table 11 - Digital Signature Updater in config.xml

5. Return to **IM -> Agents -> Right click your Target Agent -> Send Command -> Import Settings -> Agent Configuration -> Select the modified config.xml -> Click Import** and **Apply**
6. Wait till the Import is Completed



7. Run the file with the Digital Signature you just added

3.2.7.2 Configure Trusted Digital Signature Update via TMSL Agent

1. Open Command Prompt as Administrator
2. Navigate to C:\Program Files\Trend Micro\Safe Lock
3. To enable the Trusted Hash and Predefined Trusted Updater, please enter the command below:

```
slcmd.exe set trustedcertification enable
slcmd.exe set predefinedtrustedupdater enable
```

4. Enter the following command to add the Installer's Hash Value to Trusted Hash

```
slcmd.exe add trustedcertification -c c:\my_company.cer -u
```

Below are the parameters that can be used for Trusted Hash

Parameter	Required?	Description
-c <file_path>	Required	Add digital signature file path.

Parameter	Required?	Description
-l <label_name>	Optional	Specify a label name for the rule.
-u	Optional	Using the optional -u value treats the file of the specified hash value as a Trusted Updater where TMSL Agent adds files, which created / modified from the file of the specified hash value to the Approved List. This parameter requires to enable "Predefined Trusted Updater"

Table 12 - Trusted Hash Parameters

5. Run the file with the Digital Signature you just added.

Chapter 4: Intelligent Manager Management

4.1 > Agent and IM Connection

4.1.1 Agent and IM Communication

To ensure TMSL Agent and IM Communication. Please consider the following:
1. Make sure that Safe Lock agents can resolve the Safe Lock Intelligent Manager server's hostname, FQDN, or IP address.
2. The following ports should be opened or allowed

Purpose	Client Port	Console Port
Command Deploy	TCP Inbound 14336	TCP Outbound 14336
Download Patch	Management console's port (default is 443)	
Log/Status Upload	TCP Outbound 8000/8001	TCP Inbound 8000/8001

Table 13 - TMSL Agent and IM Communication Channels

4.1.2 Verifying IM to TMSL Agent Connection

You can perform Connection Verification to Agents or Group from **IM > Agents > Select Agents/Group > Send Command > Check Connection**

4.1.3 Verifying TMSL Agent to IM Connection

You can perform Connection Verification to IM by using CLI command:

```
SLCmd.exe -p <password> test managedmode
```

```
C:\Program Files\Trend Micro\Safe Lock>SLCmd.exe -p tm_txone test managedmode
Server status (port 8000): OK
Server status (port 8001): OK
```

4.2 > Event Management

Depending on how Safe Lock is configured, there may be many events in IM. This part describes how to properly manage the events in order to be able to monitor them from IM side

1. For Agent Events. This will be seen either through **IM Dashboard or Logs & Reports > Agent Events**. Notice that on Agent Events, there is a Marked Column which values may be Open for events that have yet to be processed or Closed for events that have already finished processing.

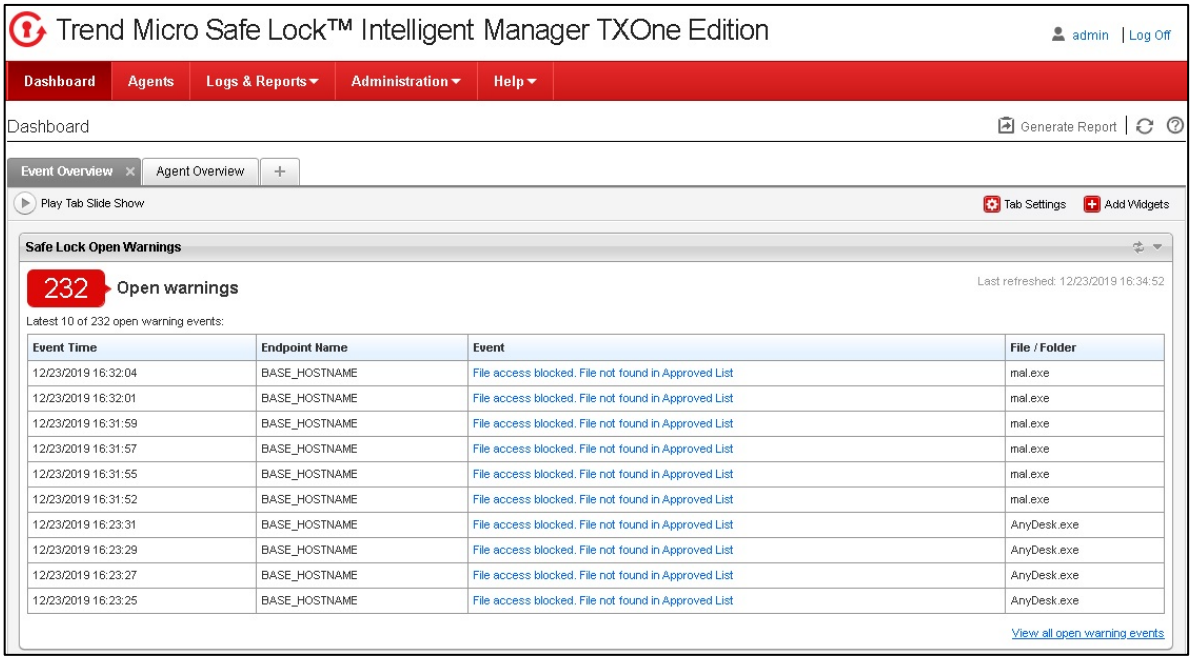


Figure 1 - IM Dashboard

Agent Events

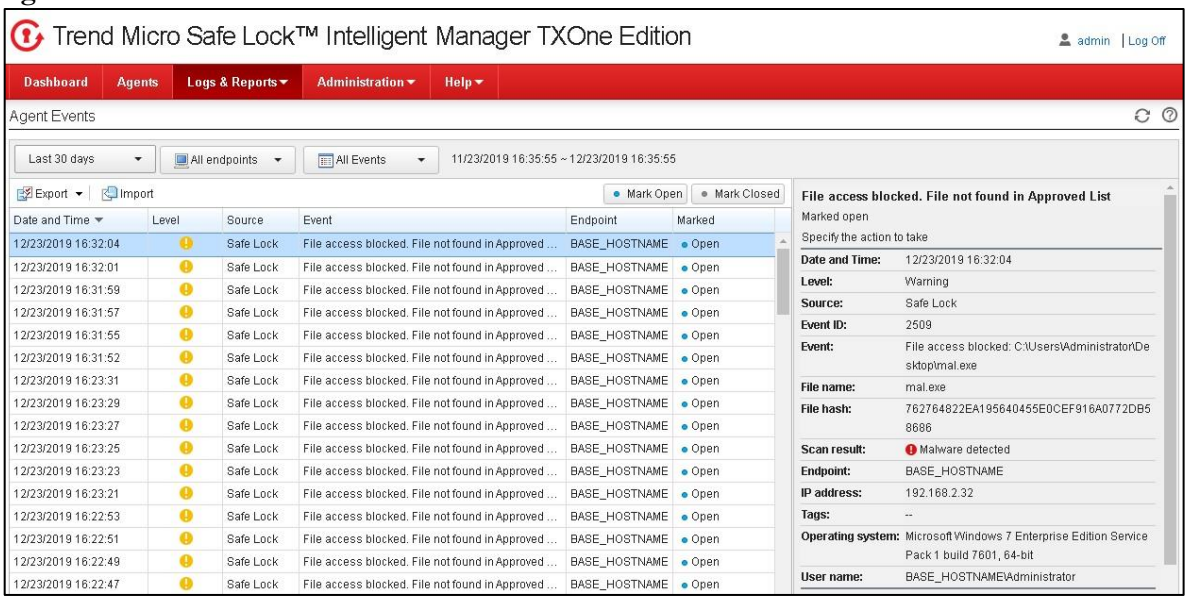
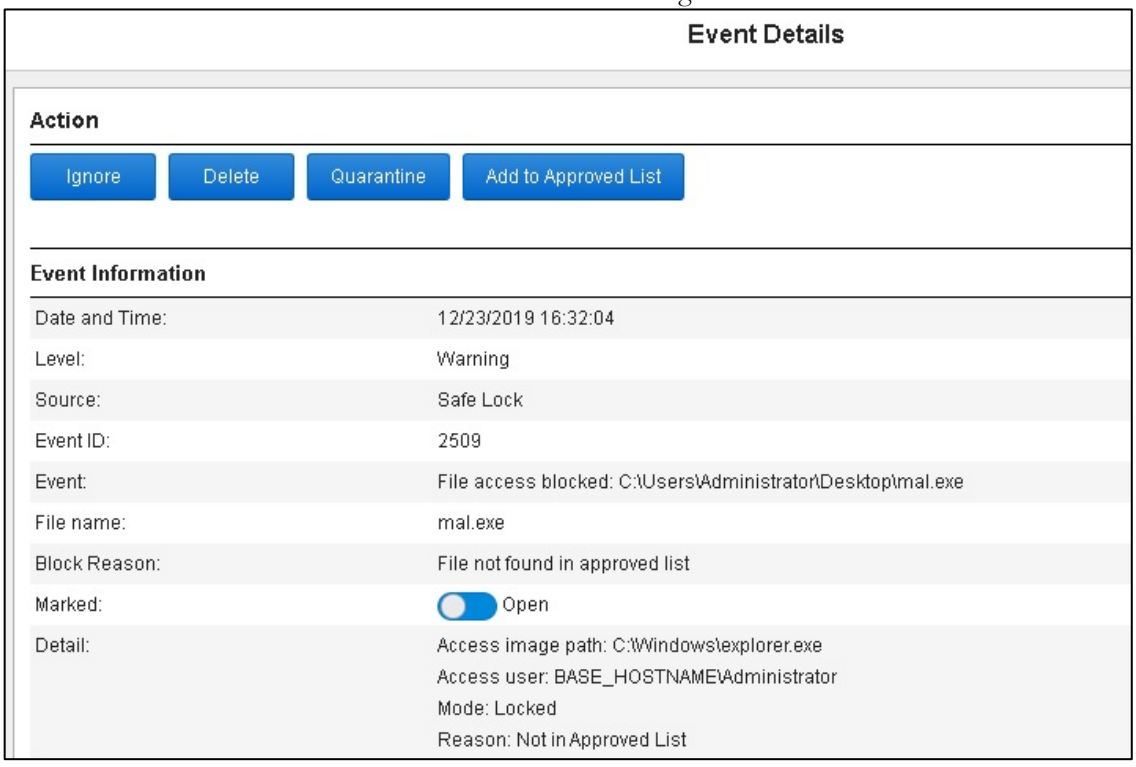


Figure 2 - Agent Events

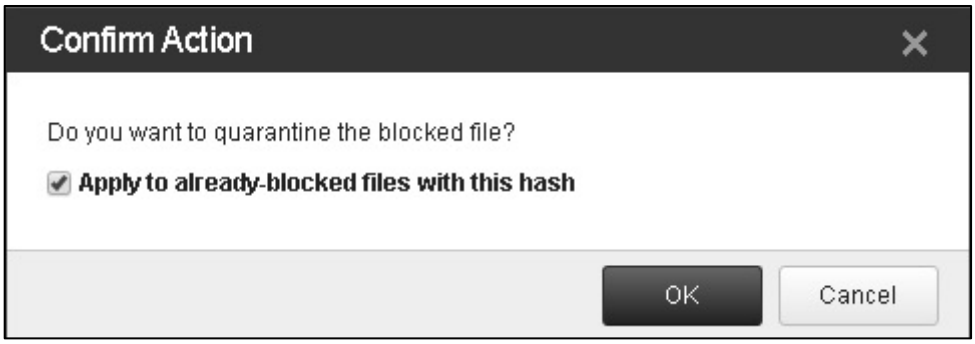
2. You can select an event and view its details. The following actions should be available



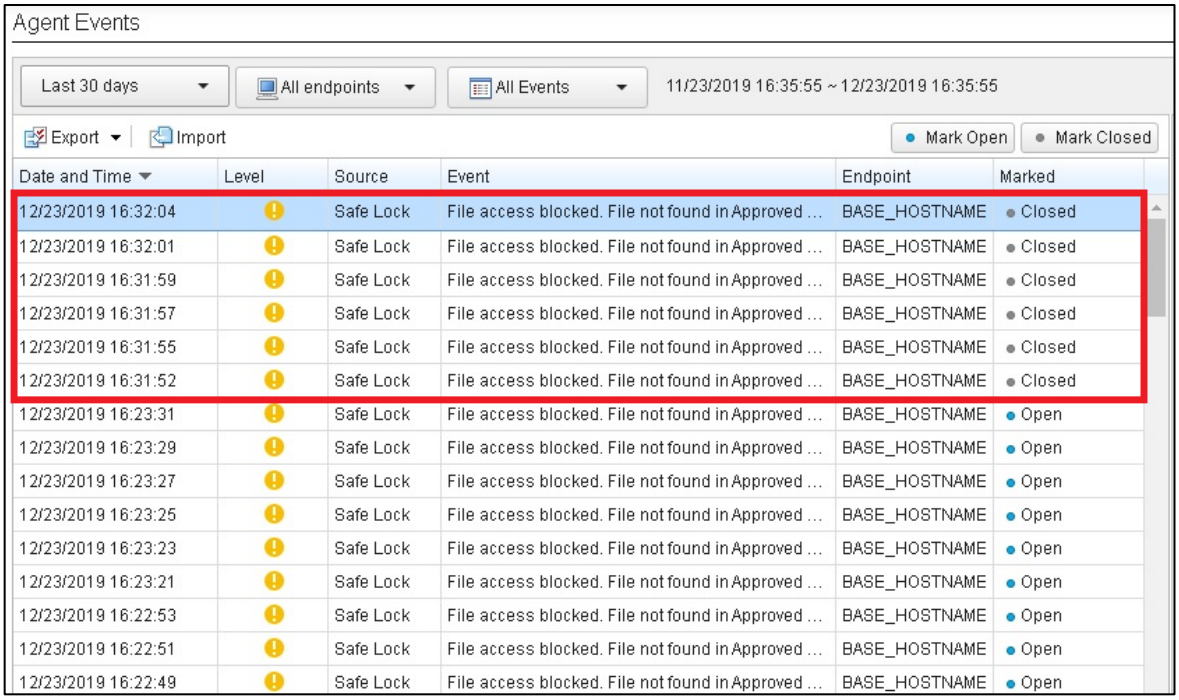
You will also see in the Event Details if the blocked file is detected as a Malware

Scan Result	
Scan result:	Malware detected
Threat ID:	1
Threat name:	TROJ_FR.8FCD9C8E
Virus Scan Engine:	11.000.1006
Virus Pattern:	15.491.00
Spyware Pattern:	2.231.00
IntelliTrap Pattern:	0.251.00
IntelliTrap Exception Pattern:	1.661.00

3. Depending on the Action you want to use. You will get this prompt and an option to Apply the action on all events pertaining to the same file. Put a tick on the option Apply to already-blocked files with this hash then click **Ok.**



4. Since we already put an action to the Event; it means that the events, along with the similar ones pertaining to the same file will now be Marked as **Closed**



5. You may also manage individual events just by simply clicking on **Mark Open** or **Mark Closed**.

4.3 > Log Purge Settings

You can manage Log Purge Settings by clicking on Logs & Reports > Log Settings. You may refer to SLIM Sizing Guide for specific details for disk consumption for IM Logs and Events.