txOne networks

Keep the Operation Running

1.3 **TXOne StellarProtect** (Legacy Mode)
Installation Guide

The trust list-based solution for locking down fixed-function computers

Windows

SC 2022 awards EUROPE

WINNER

Document Part No.: APEM139619/221104

Release Date: November 2022

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

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

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

TXOne Networks always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any TXOne Networks document, please contact us at docs@txone-networks.com.

Evaluate this documentation on the following site:

http://docs.txone-networks.com/en-us/survey.aspx

Privacy and Personal Data Collection Disclosure

Certain features available in TXOne Networks products collect and send feedback regarding product usage and detection information to TXOne Networks. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want TXOne Networks to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that TXOne StellarProtect (Legacy Mode) collects and provides detailed instructions on how to disable the specific features that feedback the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by TXOne Networks is subject to the conditions stated in the TXOne Networks Privacy Notice:

https://www.txone.com/privacy-policy/

Table of Contents

Chapter 4: Local Agent Uninstallation

Chapter 5: Technical Support

Index

Preface

This Installation Guide introduces TXOne StellarProtect (Legacy Mode) and guidesadministrators through installation and deployment.

Topics in this chapter include:

About the Documentation

TXOne StellarProtect (Legacy Mode) documentation includes the following:

Table 1. TXOne StellarProtect (Legacy Mode) Documentation

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

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

http://docs.trendmicro.com

Audience

TXOne StellarProtect (Legacy Mode) documentation is intended for administrators responsible for StellarProtect (Legacy Mode) management, including agent installation.These users are expected to have advanced networking and server management knowledge.

Document Conventions

The following table provides the official terminology used throughout the TXOne StellarProtect (Legacy Mode) documentation:

Table 2. Document Conventions

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

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

Chapter 1

Introduction

TXOne StellarProtect (Legacy Mode) delivers a simple, no-maintenance solution to lockdown and protect fixed-function computers, helping protect businesses against security threats and increase productivity.

Topics in this chapter include:

- *About TXOne StellarProtect (Legacy Mode) on page 1-2*

About TXOne StellarProtect (Legacy Mode)

TXOne StellarProtect (Legacy Mode) 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 andwithout the need for regular software or system updates, StellarProtect (Legacy Mode) can reliably secure computers in industrial and commercial environments with little performance impact or downtime.

What's New

TXOne StellarProtect (Legacy Mode) 1.3 includes the following new features andenhancements.

Table 1-1. What's New in TXOne StellarProtect (Legacy Mode) 1.3

Feature	Description
Enhanced event processing	The enhanced StellarProtect (Legacy Mode) process flow of Approved List and policy deployment increases system operation efficiency.
Enhanced agent-server communication	StellarProtect (Legacy Mode) agent-server communication has been enhanced to support the connection checking and central management configuration using the Command Line Interface.

Agent Features and Benefits

StellarProtect (Legacy Mode) 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 trust

listing), StellarProtect (Legacy Mode) provides both improved productivity and system integrity by blocking malicious software and preventing unintended use.

StellarProtect (Legacy Mode) Write Protection blocks modification and deletion of files,folders, and registry entries.

Exploit Prevention

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

For advanced threat prevention, StellarProtect (Legacy Mode) includes intrusion prevention, execution prevention, application lockdown, and device controlto stop threats from spreading to the endpoint or executing.

Approved List Management

When software needs to be installed or updated, you can use one of the following methods to make changes to the endpoint and automatically add new or modified files to the Approved List, all without having to unlock TXOne StellarProtect (Legacy Mode):

- Maintenance Mode

- Trusted Updater

- Predefined Trusted Updater List

- Command Line Interface (CLI):

    - Trusted hash

    - Trusted certification

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

TXOne StellarProtect (Legacy Mode) provides a separate administrator and Restricted Useraccount, providing full control during installation and setup, as well as simplified monitoring and maintenance after deployment.

Graphical and Command Line Interfaces

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

Self Protection

Self Protection provides ways for TXOne StellarProtect (Legacy Mode) to defend its processes and resources, required to function properly, from being disabledby programs or actual users.

Self Protection blocks all attempts to terminate the following services:

- Trend Micro Unauthorized Change Prevention Service (TMBMSRV.exe)
- Trend Micro Personal Firewall (TmPfw.exe)
- TXOne StellarProtect (Legacy Mode) Service (WkSrv.exe)

System Requirements

This section introduces StellarProtect (Legacy Mode) system requirements.

Hardware Requirements

TXOne StellarProtect (Legacy Mode) does not have specific hardware requirements beyondthose specified by the operating system, with the following exceptions:

Table 1-2. Required Hardware for StellarProtect (Legacy Mode)

Hardware/Software	Description
Available disk space	350MB minimum
Monitor Interface and resolution	VGA (640x480), 16 colors

Important

StellarProtect (Legacy Mode) cannot be installed on a system that already runs one of thefollowing:

- Trend Micro OfficeScan
- Trend Micro Titanium
- Other Trend Micro endpoint solutions
- Other endpoint solutions except Windows Defender Antivirus

Tip

For the x64 platform removing x86 folders in the installation package can reduce the size of the installer and vice versa.

Operating Systems

> **Important**
>
> Ensure that the following root certification authority (CA) certificates are installed with intermediate CAs, which are found in WKSrv.exe. These root CAs should be installed on the StellarProtect (Legacy Mode) agent environment to communicate with StellarOne.
>
> - Intermediate_Symantec Class 3 SHA256 Code Signing CA
>
> - Root_VeriSign Class 3 Public Primary Certification Authority - G5
>
> - DigiCert Assured ID Root CA
>
> - DigiCert Trusted Root G4
>
> To check root CAs, refer to the Microsoft support site:
>
> https://technet.microsoft.com/en-us/library/cc754841.aspx

> **Note**
>
> - Memory Randomization, API Hooking Prevention, and DLL Injection Prevention are not supported on 64-bit platforms.
>
> - See the latest StellarProtect (Legacy Mode) readme file for the most up-to-date list ofsupported operating systems for agents.

Windows Client:

- Windows 2000 (SP4) [Professional] (32bit)

- Windows XP (SP1/SP2/SP3) [Professional/Professional for Embedded Systems] (32bit)

> **Note**
>
> StellarProtect (Legacy Mode) installed on Windows 2000 SP4 (without update rollup) or Windows XP SP1 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, Maintenance Mode, and Predefined Trusted Updater.
>
> To support these features, install Filter Manager:

- For Windows 2000 Service Pack 4, apply the update KB891861 from the Microsoft Update Catalog website.

- For Windows XP SP1, upgrade to Windows XP SP2.

- Windows Vista (NoSP/SP1/SP2) [Business/Enterprise/Ultimate] (32bit)

- Windows 7 (NoSP/SP1) [Professional/Enterprise/Ultimate/Professional for Embedded Systems/Ultimate for Embedded Systems] (32/64bit)

- Windows 8 (NoSP) [Pro/Enterprise] (32/64bit)

- Windows 8.1 (NoSP) [Pro/Enterprise/with Bing] (32/64bit)

- Windows 10 [Pro/Enterprise/IoT Enterprise] (32/64bit)
  Anniversary Update, Creators Update, Fall Creators Update,
  April 2018 Update, November 2018 Update, May 2019 Update,
  November 2019 Update, May 2020 Update, October 2020 Update,
  May 2021 Update, November 2021 Update, 2022 Update

- Windows 11 (NoSP) [Pro/Enterprise] (64bit) 2022 Update

📝 **Note**

- Unlock the endpoint before updating your Windows 10 operating system to the Anniversary Update, Creators Update, Fall Creators Update, April 2018 Update, October 2018 Update, or later versions.

- OneDrive integration in Windows 10 Fall Creators Update, Spring Creators Update, or later versions is not supported. Ensure that OneDrive integration is disabled before installing StellarProtect (Legacy Mode).

- To improve performance, disable the following Windows 10 components:

  - Windows Defender Antivirus. This may be disabled via group policy.
  - Window Update. Automatic updates may require the download of large files which may affect performance.
  - Windows Apps (Microsoft Store) auto-update. Checking for frequent updates may cause performance issues.

- In Windows 10 April 2018 Update (Redstone 4) and later, StellarProtect (Legacy Mode) has the following limitations when working with folders where the case sensitive attribute has been enabled:

  - Enabling the case sensitive attribute for a folder may prevent StellarProtect (Legacy Mode) from performing certain actions (eg. prescan, custom actions) on that folder. Folders that do not have the attribute enabled are not affected.

  - StellarProtect (Legacy Mode) blocks all processes started from folders where the case sensitive attribute is enabled. Additionally, StellarProtect (Legacy Mode) is unable to provide any information for the blocked processes, except for file path.

  - The StellarProtect (Legacy Mode) agent cannot verify file signatures of files saved in folders where the case sensitive attribute is enabled. As a result, DAC exceptions related to signatures cannot work.

- Windows XP Embedded (SP1/SP2) (32bit)

- Windows Embedded Standard 2009 (NoSP) (32bit)

- Windows Embedded POSReady 2009 (32bit)

- Windows Vista for Embedded Systems (NoSP/SP1/SP2) (32bit)

- Windows Embedded Standard 7 (NoSP/SP1) (32/64bit)

- Windows Embedded POSReady 7 (NoSP) (32/64bit)

- Windows Embedded 8 Standard (NoSP) (32/64bit)

- Windows Embedded 8 Industry (NoSP) [Pro/Enterprise] (32/64bit)

- Windows Embedded 8.1 Industry (NoSP) [Pro/Enterprise/Sideloading] (32/64bit)

- Windows Embedded POSReady (32bit)

📝 **Note**

- StellarProtect (Legacy Mode) installed on Windows XP Embedded does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, Maintenance Mode, and Predefined Trusted Updater.

- StellarProtect (Legacy Mode) does not support a custom action of "quarantine" on Windows XP Embedded SP1.

Windows Server:

- • Windows 2000 Server (SP4) (32bit)

📝 **Note**

StellarProtect (Legacy Mode) installed on Windows 2000 Server SP4 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, Maintenance Mode, and Predefined Trusted Updater.

- Windows Server 2003 (SP1/SP2) [Standard/Enterprise/Storage] (32bit)

- Windows Server 2003 R2 (NoSP/SP2) [Standard/Enterprise/Storage] (32bit)

- Windows Server 2008 (SP1/SP2) [Standard/Enterprise/Storage] (32/64bit)

- Windows Server 2008 R2 (NoSP/SP1) [Standard/Enterprise/Storage] (64bit)

- Windows Server 2012 (NoSP) [Essentials/Standard] (64bit)

- Windows Server 2012 R2 (NoSP) [Essentials/Standard] (64bit)

- Windows Server 2016 (NoSP) [Standard] (64bit)

- Windows Server 2019 (NoSP) [Standard] (64bit)

- Windows Server 2022 (NoSP) [Standard] (64bit)

- Windows Storage Server 2012 (NoSP) [Standard] (64-bit)

- Windows Storage Server 2012 R2 (NoSP) [Standard] (64-bit)

- Windows Storage Server 2016 (NoSP) (64bit)

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

- Windows Server 2003 R2 for Embedded Systems (NoSP/SP2) (32bit)

- Windows Server 2008 for Embedded Systems (SP1/SP2) (32/64bit)

- Windows Server 2008 R2 for Embedded Systems (NoSP/SP1) (64bit)

- Windows Server 2012 for Embedded Systems (NoSP) (64bit)

- Windows Server 2012 R2 for Embedded Systems (NoSP) (64bit)

Agent Upgrade Preparation

This version of StellarProtect (Legacy Mode) supports upgrade from the following versions:

•   StellarProtect (Legacy Mode) 1.0

•   StellarProtect (Legacy Mode) 1.1

•   StellarProtect (Legacy Mode) 1.2

•   StellarProtect (Legacy Mode) 1.2 patch 1

📝 Note

Before upgrading, close the wksupporttool UI and/or StellarProtect (Legacy Mode) agent console.

⚠ WARNING!

Before upgrading, take the appropriate actions below as noted for your chosen installation method and the version of your installed StellarProtect (Legacy Mode) agent.

The latest updates can be downloaded from the StellarProtect (Legacy Mode) SoftwareDownload Center at http://downloadcenter.trendmicro.com/.

Table 1-3. Fresh Installation of the StellarProtect (Legacy Mode) Agent

Installation Method	Installed Agent Version	Required Action	Settings Retained

Local installation using Windows installer	StellarProtect (Legacy Mode) 1.0 / 1.1/1.2/1.2 Patch 1	It's necessary to manually add the install file (SL_Install.exe) into the trusted HASH list before use it.	No settings retained

Installation Method	Installed Agent Version	Required Action	Settings Retained
Local installation using command line interface installer	StellarProtect (Legacy Mode) 1.0 / 1.1/1.2/1.2 Patch 1	It's necessary to manually add the install file (SL_Install.exe) into the trusted HASH list before use it.	No settings retained

Table 1-4. Post-Installation Agent Upgrade (Legacy OS – Supports SHA1)

Installation Method	Installed Agent Version	Required Action	Settings Retained
For example, deploy patching by running stellar_patch.exe. To do a silent install instead, open the command prompt as an administrator and enter the following command: > stellar_patch.exe -s -a –s/g	StellarProtect (Legacy Mode) 1.0 / 1.1/1.2/1.2 Patch 1	No preparation needed	Compatible settings retained
Remote installation	StellarProtect (Legacy Mode) 1.1/1.2/1.2 Patch 1 Note: StellarProtect (Legacy Mode) 1.0 supports only local installation.	No preparation needed	Compatible settings retained

Table 1-5. Post-Installation Agent Upgrade (Modern OS – Supports SHA2)

Installation Method	Installed Agent Version	Required Action	Settings Retained
For example, deploy patching by running stellar_patch.exe. To do a silent install instead, open the command prompt as an administrator and enter the following command: > stellar_patch.exe -s -a –s/g	StellarProtect (Legacy Mode) 1.2 Patch 1 Note: For agents with versions below 1.2 Patch 1, local upgrade for standalone StellarProtect (Legacy Mode) agents is not supported. Please implement either workaround listed below: - Remotely upgrade StellarProtect (Legacy Mode) agents from StellarOne web console - Add the patch file hash as trusted hash and then perform local upgrade.	No preparation needed	Compatible settings retained
Remote installation	StellarProtect (Legacy Mode) 1.0/1.1/1.2/1.2 Patch 1	No preparation needed	Compatible settings retained

Agent Use Overview

TXOne StellarProtect (Legacy Mode) is a trust list-based solution that locks down computers, preventing all applications not on the Approved List from running. StellarProtect (Legacy Mode) can be configured and maintained using the graphical user interface (GUI) agent console or the command line interface

(CLI). System updates can be applied without turning off Application Lockdown at the endpoint through Maintenance Mode, trust hash, trust certification, predefined trusted updater list or by using the Trusted Updater.

Consider this typical use case scenario:

1. Set up the Approved List and turn on Application Lockdown on the endpoint so that unapproved applications cannot be run.

2. Use Maintenance Mode, trust hash, trust certification, predefined trusted updater list or by using the Trusted Updater to update or install software.

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

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

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

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

OK

Figure 1-1. TXOne StellarProtect (Legacy Mode) blocking message

Chapter 2

Local Agent Installation

This chapter describes local TXOne StellarProtect (Legacy Mode) agent installation andsetup procedures.

Topics in this chapter include:

Local Installation Overview

Procedure

1. Verify that the endpoint meets the TXOne StellarProtect (Legacy Mode) systemrequirements.

   For details, see *System Requirements on page 1-4*.

2. Install TXOne StellarProtect (Legacy Mode) using your preferred installation method.

   TXOne StellarProtect (Legacy Mode) can be installed using either the WindowsInstaller or the command line interface (CLI) installer.

   Table 2-1. StellarProtect (Legacy Mode) Local Installation Methods

Installation Method	Benefits
Windows Installer	The Windows Installer provides simplified step-by-step installation wizard for first-time or single installation and is also suitable for preparing for mass deployment for cloned endpoint systems.
	For details, see *Installing from Windows on page 2-3*.
Command line interface installer	The command line interface (CLI) installer provides silent installation and can be integrated into a batch file for mass deployment.
	For details, see *Installation Using the Command Line on page 2-13*.

   > **Note**
   >
   > 1. To customize installations using either the Windows Installer or thecommand line interface (CLI) installer, modify the Setup.inifile.
   >
   > 2. To register StellarProtect (Legacy Mode) agent to a specific group via StellarOne console, after downloading the

Group.inifile to StellarOne console, user must also add it in the
Installer Package of StellarProtect (Legacy Mode) agent.

For details, see *Customizing Installation Parameters on page 2-17*.

3.   Configure the new installation.

a. Open the TXOne StellarProtect (Legacy Mode) console and set up the ApprovedList.

Before TXOne StellarProtect (Legacy Mode) can protect the endpoint, it must check the endpoint for existing applications and files necessary forthe system to run correctly.

For details, see *Setting Up the Approved List on page 2-10.*

b. Modify the TXOne StellarProtect (Legacy Mode) settings.

c. (Optional) Deploy the updated settings to multiple agents.

To deploy settings to multiple TXOne StellarProtect (Legacy Mode) agents, use anagent configuration file.

Installing from Windows

To install TXOne StellarProtect (Legacy Mode), you must log on using an account with administrator privileges.

Procedure

1. Double-click SL_Install.exe.

    If a **User Account Control** warning from Windows appears, click **Yes**.
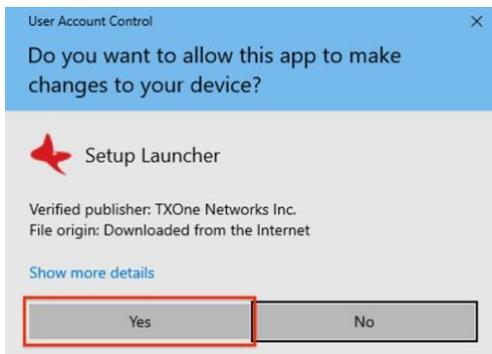
2. When the installation wizard opens, click **Next**.
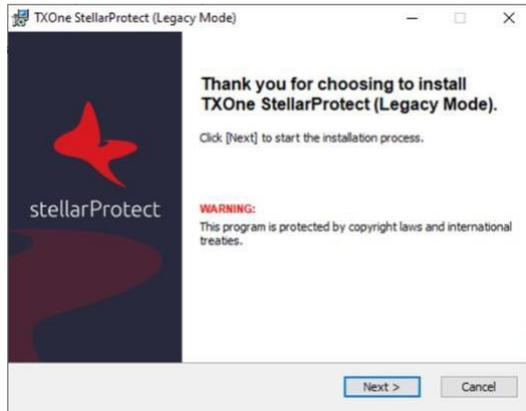
> **Note**
>
> If there is another version of StellarProtect (Legacy Mode) on the
> endpoint, the installer will remove it before installing the latest version.

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

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

Important

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

---
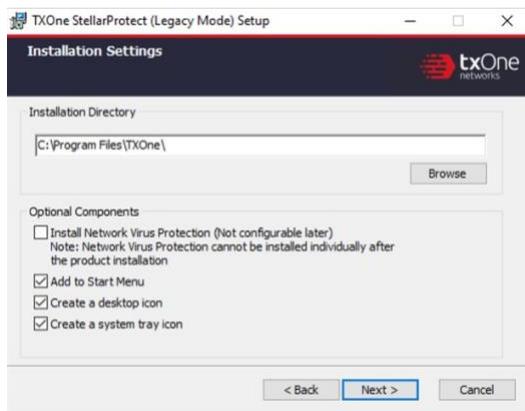
5. Provide the Activation Code and specify an administrator password for TXOne StellarProtect (Legacy Mode).

> **Note**
>
> The password must be 8 to 64 alphanumeric characters. The following characters are not supported: | > < \ " spaces. The StellarProtect (Legacy Mode) administrator password is unrelated to the Windows administrator password.

> ⚠ **WARNING!**
>
> Please store securely and do not lose the StellarProtect (Legacy Mode) administrator password. If you lose the StellarProtect (Legacy Mode) administrator password, pleasecontact TXOne Networks for support.

---

6. Click **Next**.

A message appears asking if you would like to scan the endpoint for threats before continuing with the installation.
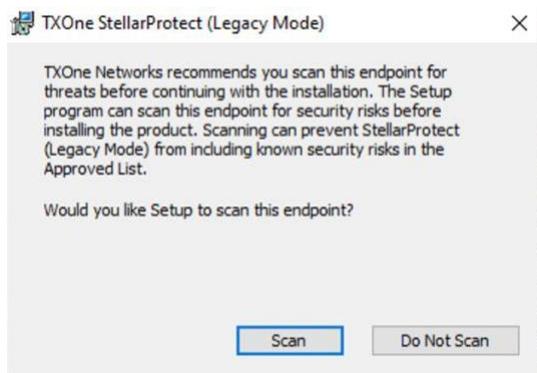
7. (Optional) Scan the endpoint for threats before continuing with the installation. TXOne Networks recommends you perform this scan.

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

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

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

    c. Click **Scan Now**.

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

> **Note**
>
> You cannot stop a scan process when you set the *PRESCANCLEANUP* and *FORCE_PRESCAN* options in the Setup.ini file.
>
> For more information, see *Prescan Section on page 2-37*.

> **Tip**
>
> Perform a manual scan to detect and remove threats on endpoints. For more information, see *Manual Scan Commands* in the Administrator's Guide.

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

> **Note**
>
> The **Do Not Scan** and close buttons are not applicable when you set the *PRESCANCLEANUP* and *FORCE_PRESCAN* options in the Setup.ini file.
>
> For more information, see *Prescan Section on page 2-37*.

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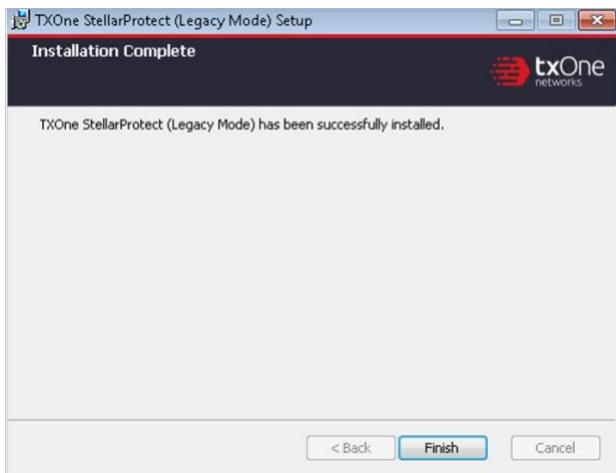
> **Note**
>
> Optionally enable memory randomization on older operating systems such as Windows XP or Windows Server 2003, which may lack or offer limited Address Space Layout Randomization (ASLR) support. See *Exploit Prevention Settings* in the Administrator's Guide for more information.

Setting Up the Approved List

Before TXOne StellarProtect (Legacy Mode) can protect the endpoint, it must check the endpoint for existing applications and files necessary for the system to runcorrectly.

Procedure

1. Open the StellarProtect (Legacy Mode) console.

   The StellarProtect (Legacy Mode) log on screen appears.
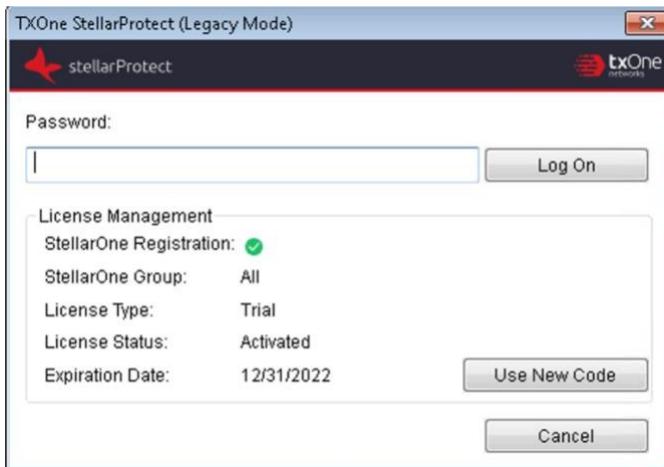
2. Provide the password and click **Log On**.

   StellarProtect (Legacy Mode) asks if you want to set up the Approved List now.
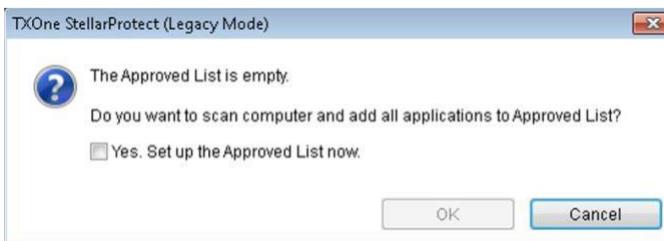
3. At the notification window, select **Yes. Set up the Approved List now** and click **OK**.

    StellarProtect (Legacy Mode) scans the endpoint and adds all applications to theApproved List.
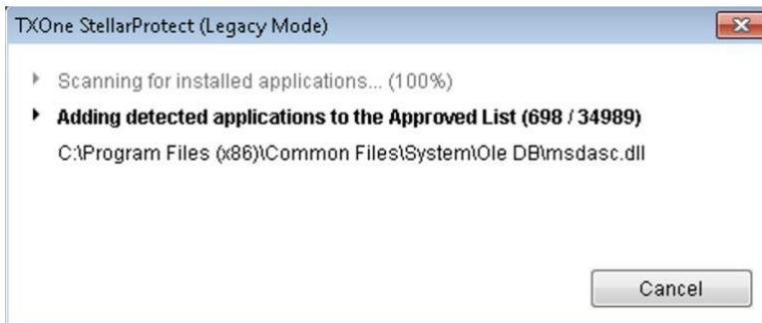
StellarProtect (Legacy Mode) displays the Approved List Configuration
Results.
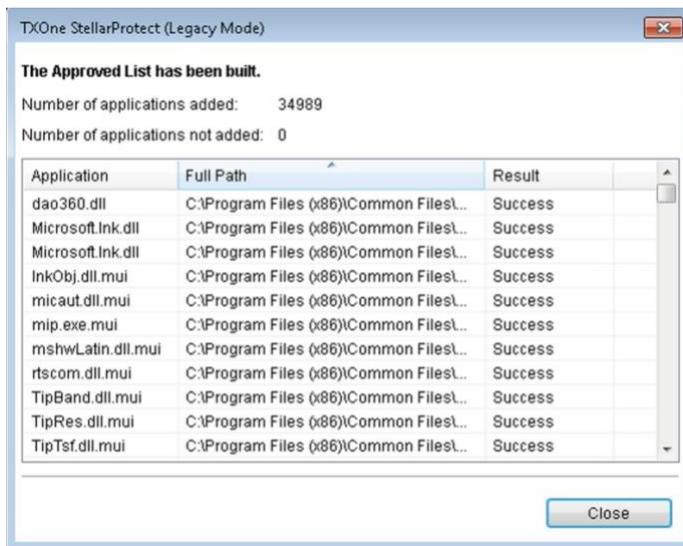
Note

> When TXOne StellarProtect (Legacy Mode) Application
> Lockdown is on, onlyapplications that are in the Approved List
> will be able to run.

---

4. Click **Close**.

Installation Using the Command Line

Administrators can install StellarProtect (Legacy Mode) from the command line interface(CLI) or using a batch file, allowing for silent installation and mass deployment.

For mass deployment, TXOne Networks recommends first installing StellarProtect (Legacy Mode) on a test endpoint since a customized installation may require a valid configuration file and Approved List. See the TXOne StellarProtect (Legacy Mode) Administrator's Guide for more information about the Approved List and configuration file.

⚠️ **WARNING!**

- Please store your StellarProtect (Legacy Mode) administrator password carefully. If youlose your StellarProtect (Legacy Mode) administrator password, please contact TXOne Networks support.

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

🟠 **Important**

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

📝 **Note**

The password must be 8 to 64 alphanumeric characters. The following characters are not supported: | > < \ " spaces. The StellarProtect (Legacy Mode) administratorpassword is unrelated to the Windows administrator password.

Installer Command Line Interface Parameters

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

Table 2-2. StellarProtect (Legacy Mode) Installer Command Line Options

Parameter	Value	Description
-q		Run the installer silently
		Note
		During the installation process, you can view the following log files in the folder C:\windows \temp to check the status of the prescan and initial approved process:
		• Prescan process: YYYYMMDDHHMMSS_wk_PreScanProgress. log
		• Initial approved process: YYYYMMDDHHMMSS_wk_InitListProgress .log
-p	<administrator_ password>	Specify the administrator password
-d	<path>	Specify the installation path
-ac	<activation_cod e>	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 StellarProtect (Legacy Mode) configuration file
		Note
		The StellarProtect (Legacy Mode) configuration file can be exported after installing StellarProtect (Legacy Mode).

Parameter	Value	Description
-lp	\<path>	Specify the Approved List **Note** After installing StellarProtect (Legacy Mode) 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

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

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

Important

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

Customizing Installation Parameters

📝 **Note**

The installer applies the specified arguments in the following order:

- Encrypted setup.bin

- Command line interface (CLI)

- setup.ini

If setup.bin exists, the installer applies the configuration in setup.bin takes precedence and ignores settings from the CLI and setup.ini file.

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 StellarProtect (Legacy Mode) desktop shortcut will not be created.

To change the default installation parameters using a Setup.ini file, follow the steps below.

Procedure

1. Locate the Setup.ini file in the installation folder.

2. Customize the installation parameters as required.

For information on installation parameters and their possible values, see .

3. Optionally encrypt the Setup.ini file to prevent unauthorized access to important settings.

a. From the installation folder, copy the Setup.ini file and the WKSupportTool.exe file to your desktop.

b. Run a command prompt window as administrator.

c. Navigate to the desktop and type *WKSupportTool.exe*

d. *encryptsetupini Setup.ini Setup.bin* to encrypt the Setup.inifile and name the encrypted file as "Setup.bin".

e. Save the Setup.bin file in the installation folder and remove the Setup.ini file.

Setup.ini File Arguments

Note

The installer applies the specified arguments in the following order:

*   Encrypted setup.bin

*   Command line interface (CLI)

*   setup.ini

If setup.binexists, the installer applies the configuration in setup.bintakes precedence and ignores settings from the CLI and setup.ini file.

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 StellarProtect (Legacy Mode)desktop shortcut will not be created.

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

Property Section

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

Table 2-3. Setup.ini File *[PROPERTY]* **Section Arguments**

Key	Description	Possible Values	Default Value	Encrypted
ACTIVATION_CODE	Activation Code	<activation_code>	<empty>	No
NO_DESKTOP	Create a shortcut on desktop	• *0*: Create shortcut *1*: Do not create shortcut	*0*	No
NO_STARTMENU	Create a shortcut in the Start menu	• *0*: Create shortcut • *1*: Do not create shortcut	*0*	No
NO_SYSTRAY	Display the system tray icon and Windows notifications	• *0*: Create system tray icon • *1*: Do not create system tray icon	*0*	No
NO_NSC	Install firewall for network virus protection	• *0*: Create firewall • *1*: Do not create firewall	*1*	No
CONFIG_PATH	Configuration file path	• <path>	<empty>	No
LIST_PATH	Approved List path for import	• <path>	<empty>	No
APPLICATION FOLDER	Installation path for agent program	• <path>	<empty>	No
PASSWORD	Password which is used for **SLCmd.exe** and StellarProtect (Legacy Mode) console	• <password>	<empty>	No
CUSTOM_ACTION	Custom action for blocked events	• *0*: Ignore • *1*: Quarantine • *2*: Ask server	*0*	No

Key	Description	Possible Values	Default Value	Encrypted
QUARANTINE_ FOLDER_PATH	Quarantine path for agent program	<path>	<empty>	No
INTEGRITY_M ONITOR	Enable Integrity Monitor	• *0*: Disable • *1*: Enable	*0*	No
PREDEFINED_ TRUSTED_UP DATER	Enable Predefined Trusted Updater	• *0*: Disable • *1*: Enable	*0*	No
WINDOWS_UPD ATE_SUPPORT	Enable Window Update Support	• *0*: Disable • *1*: Enable	*0*	No
PRESCAN	Prescan the endpoint before installing StellarProtect (Legacy Mode)	• *0*: Do not prescan the endpoint • *1*: Prescan the endpoint	*1*	No
MAX_EVENT_D B_SIZE	Maximum database file size (MB)	Positive integer	*1024*	No
WEL_SIZE	Windows Event Log size (KB)	Positive integer **Note** Default value for new installations. Upgrading StellarProtect (Legacy Mode)does not change any user-defined *WEL_SIZE* values set in the previous	*10240*	No

		installation.		

Key	Description	Possible Values	Default Value	Encrypted
WEL_RETENTION	Windows Event Log option when maximum event log size is reached on Windows Event Log	For Windows XP orearlier platforms: • *0*: Overwrite events as needed • *1* - *365*: Overwrite events older than (1-365) days • *-1*: Do not overwrite events(Clear logs manually) For Windows Vista or later platforms: • *0*: Overwrite events as needed(oldest events first) • *1*: Archive the logwhen full, do not overwrite events • *-1*: Do not overwrite events(Clear logs manually)	*0*	No
WEL_IN_SIZE	Windows Event Log size for Integrity Monitor events (KB)	Positive integer	*10240*	No

WEL_IN_RETE NTION	Windows Event Log option for when maximum event log size for Integrity Monitor events is reached in the Windows EventLog	For Windows XP orearlier platforms: • *0*: Overwrite events as needed • *1* - *365*: Overwrite events older than (1-365) days • *-1*: Do not overwrite events(Clear logs manually) For Windows Vista or later platforms: • *0*: Overwrite events as needed(oldest events first) • *1*: Archive the logwhen full, do not overwrite events • *-1*: Do not overwrite events(Clear logs manually)	*0*	No
USR_DEBUGLO G_ENABLE	Enable debug logging for user sessions	• *0*: Do not log *1*: Log	*0*	No
USR_DEBUGLO GLEVEL	The number of debug log entries allowed for user sessions	• *256*	*256*	No
SRV_DEBUGLO G_ENABLE	Enable debug logging for service sessions	• *0*: Do not log • *1*: Log	*0*	No
SRV_DEBUGLO GLEVEL	The number of debug log entries allowed	• *256*	*256*	No

Key	Description	Possible Values	Default Value	Encrypted
	for service sessions			
SILENT_INST ALL	Execute installation in silent mode	• *0*: Do not use silent mode • *1*: Use silent mode	*0*	No

 Important

To use silent mode, you must also specify the ACTIVATION_CODE and PASSWORD keys and values. For example:

[PROPERTY]

ACTIVATION_CODE=XX-XXXXX-XXXXX-XXXXX-XXXXX

PASSWORD=P@ssW0Rd

SILENT_INSTALL=1

Key	Description	Possible Values	Default Value	Encrypted
STORAGE_DE V ICE_BLOCKIN G	Blocks storage devices, including CD/DVD drives, floppy disks, and USB devices, from accessing managed endpoints	• *0*: Allow accessfrom storage devices • *1*: Block access from storage devices	*0*	No

Key	Description	Possible Values	Default Value	Encrypted
INIT_LIST	Initialize the Approved List during installation	• 0 : Do not initialize the Approved list During installation • 1: Initialize the Approved List during installation	*0*	No
	📝 Note *LIST_PATH* has priority over *INIT_LIST*. For example: *[PROPERTY]* *LIST_PATH=liststore.db INIT_LIST=1* In this case, liststore.db is imported and *INIT_LIST* is ignored.			
INIT_LIST_P ATH	A folder path to be traversed for the Approved List initialization Each local disk's root directory will be traversed if empty	<folder path>	<empty>	No

INIT_LIST_P ATH_OPTION AL	A folder path to be traversed for the Approved List initialization Each local disk's root directory will be traversed if empty	\<folder path>	\<empty>	No
INIT_LIST_E XCLUDED_FO LDER	An absolute folder path to exclude from automatic file	\<folder path>	\<empty>	No

Key	Description	Possible Values	Default Value	Encrypted
	enumeration for Approved List initialization The configuration applies to the Approved List first initialized and all subsequent Approved List updates Specify multiple folders by creating new entries with names that start with *INIT_LIST_EXCLUDED_FOLDER*. Ensure each entry name is unique. For example: *INIT_LIST_EXCLUDED_FOLDER= c:\folder1* *INIT_LIST_EXCLUDED_FOLDER2 =c:\folder2* *INIT_LIST_EXCLUDED_FOLDER3 =c:\folder3*	📝 **Note** • Folder path supports a maximum length of 260 characters. • Folder paths that do not exist may be specified. • The exclusion applies to subfolders.		

INIT_LIST_E XCLUDED_EX TENSION	A file extension to exclude from automatic file enumeration forApproved List initialization The configuration applies to the Approved List first initialized and all subsequent Approved List updates Specify multiple extensions by creating new entries with names that start with *INIT_LIST_EXC LUDED_EXTENSI ON*, while ensuring that each entry name is unique. For example: *INIT_LIST_EXC LUDED_EXTENSI ON=bmp* *INIT_LIST_EXC LUDED_EXTENSI ON2=png*	<file extension> 📝 **Note** Specifying file extensions of executable files (e.g. exe, dll and sys) may cause issues with Application Lockdown.	*INIT_LIST_EXC LUDED_EXTEN SION1=log* *INIT_LIST_EXC LUDED_EXTEN SION2=txt* *INIT_LIST_EXC LUDED_EXTEN SION3=ini*	No
LOCKDOWN	Turn Application Lockdown on after installation	• *0*: Turn off Application Lockdown • *1:* Turn on Application Lockdown	*0*	No

Key	Description	Possible Values	Default Value	Encrypted
FILELESS_AT TACK_ PREVENTION	Enable the Fileless Attack Prevention feature	• *0*: Disable feature • *1*: Enable feature	*0*	No
SERVICE_CRE ATION_PREV ENTION	Enable the Service Creation Prevention feature	• *0*: Disable feature • *1*: Enable feature	*0*	No
	Note StellarProtect (Legacy Mode) temporarily disables the Service Creation Prevention feature under the following conditions: • Updating or installing new applications using installers allowed by Trusted Updater. The feature is automatically re-enabled after the Trusted Updater process is complete • Enabling Windows Update Support Disabling Windows Update Support automatically re-enables the feature			
USR_DEBUGLO G_ENABLE	Enable debug log in user session	• *0*: Disable debug log • *1*: Enable debug log	*0*	No
USR_DEBUGLO GLEVEL	Debug level in user session	*273*	*273*	No

Key	Description	Possible Values	Default Value	Encrypted
SRV_DEBUGLOG_ENABLE	Enable debug log in service session	• *0*: Disable debug log • *1*: Enable debug log	*0*	No
SRV_DEBUGLOGLEVEL	Debug level in service session	• *273*	*273*	No
FW_USR_DEBUGLOG	Enable debug log in user session of firewall	• *0*: Disable debug log • *1*: Enable debug log	*0*	No
FW_USR_DEBUGLOG_LEVEL	Debug level in user session of firewall	number	*273*	No
FW_SRV_DEBUGLOG_ENABLE	Enable debug log in service session of firewall	• *0*: Disable debug log • *1*: Enable debug log	*0*	No
FW_SRV_DEBUGLOG_LEVEL	Debug level in service session of firewall	number	*273*	No
BM_SRV_DEBUGLOG_ENABLE	Enable debug log of Behavior Monitoring Core service	• *0*: Disable debug log • *1*: Enable debug log	*0*	No
BM_SRV_DEBUGLOG_LEVEL	Debug level of Behavior Monitoring Core service	• *51*	*51*	No

Key	Description	Possible Values	Default Value	Encrypted
INTELLIGENT _RUNTIME_LE ARNING	The agent will allow runtime execution files that are generated by applications on the Approved List	• *0: Disable* • *1: Enable*	*O*	No
ACTIVEUPDAT E_SOURCE	Used to specify the ActiveUpdate source	https://txse-p.activeupdate.trend micro.com/ activeupdate (Default)	<empty>	No
ALLOW_NON_ MASS_STORAG E_USB_DEVICE	Allow some drivers (e.g. Touch screen/ Infrared sensor/Android mobile phone) from being loaded when those hardware devices are plugged in and storage device blocking is enable.	• *0: Disable(Default)* • *1: Enable*	<empty>	No

EventLog Section

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

Table 2-4. Setup.ini File *[EVENTLOG]* **Section Arguments**

Key	Description	Possible Values	Default Value	Encrypted
ENABLE	Log events related to StellarProtect (Legacy	• *1*: Log • *0*: Do not log	*1*	No

	Mode)			
LEVEL_WARNI NGLOG	Log "Warning" level events related to StellarProtect (Legacy Mode)	• *1*: Log • *0*: Do not log	*1*	No
LEVEL_INFOR MATIONLOG	Log "Information" level events related to StellarProtect (Legacy Mode)	• *1*: Log • *0*: Do not log	*0*	No
BLOCKEDACCE SSLOG	Log files blocked by StellarProtect (Legacy Mode)	• *1*: Log • *0*: Do not log	*1*	No
APPROVEDACC ESSLOG	Log files approved by StellarProtect (Legacy Mode)	• *1*: Log • *0*: Do not log	*1*	No
APPROVEDAC C ESSLOG_TRUS TEDUPDATER	Log Trusted Updater approved access	• *1*: Log • *0*: Do not log	*1*	No
APPROVEDAC C ESSLOG_TRU STEDHASH	Log Trusted Hash approved access	• *1*: Log • *0*: Do not log	*1*	No
APPROVEDAC C ESSLOG_DLL DRIVER	Log DLL/Driver approved access	• *1*: Log • *0*: Do not log	*0*	No
APPROVEDAC C ESSLOG_EXC	Log Application Lockdown exception path approved access	• *1*: Log • *0*: Do not log	*1*	No

EPTIONPATH				
APPROVEDAC C ESSLOG_TRU STEDCERT	Log Trusted Certifications approved access	• *1*: Log • *0*: Do not log	*1*	No
APPROVEDAC C ESSLOG_WRI T EPROTECTIO N	Log Write Protection approved access	• *1*: Log • *0*: Do not log	*1*	No
SYSTEMEVENT LOG	Log events related to the system	• *1*: Log • *0*: Do not log	*1*	No
SYSTEMEVEN T LOG_EXCEPTI ONPATH	Log exceptions to Application Lockdown	• *1*: Log • *0*: Do not log	*1*	No
SYSTEMEVEN T LOG_WRITEP ROTECTION	Log Write Protection events	• *1*: Log • *0*: Do not log	*1*	No
LISTLOG	Log events related to the Approved list	• *1*: Log • *0*: Do not log	*1*	No
USBMALWAR EP ROTECTIONL OG	Log events that trigger USB Malware Protection	• *1*: Log • *0*: Do not log	*1*	No
EXECUTIONPR EVENTIONLOG	Log events that trigger Execution Prevention	• *1*: Log • *0*: Do not log	*1*	No

NETWORKVIRU SPROTECTIONLOG	Log events that trigger Network Virus Protection	• *1*: Log • *0*: Do not log	*1*	No
INTEGRITYMO NITORINGLOG _FILECREATED	Log file and folder created events	• *1*: Log • *0*: Do not log	*1*	No
INTEGRITYMO NITORINGLOG _FILEMODIFIED	Log file modified events	• *1*: Log • *0*: Do not log	*1*	No
INTEGRITYMO NITORINGLOG _FILEDELETED	Log file and folder deleted events	• *1*: Log • *0*: Do not log	*1*	No
INTEGRITYMO NITORINGLOG _FILERENAME D	Log file and folder renamed events	• *1*: Log • *0*: Do not log	*1*	No
INTEGRITYMO NITORINGLOG _REGVALUEMO DIFIED	Log registry value modified events	• *1*: Log • *0*: Do not log	*1*	No

Key	Description	Possible Values	Default Value	Encrypted
INTEGRITYMO NITORINGLOG _REGVALUEDE LETED	Log registry value deleted events	• *1*: Log • *0*: Do not log	*1*	No
INTEGRITYMO NITORINGLOG _REGKEYCREA TED	Log registry key created events	• *1*: Log • *0*: Do not log	*1*	No
INTEGRITYMO NITORINGLOG _REGKEYDELE TED	Log registry key deleted events	• *1*: Log • *0*: Do not log	*1*	No
INTEGRITYMO NITORINGLOG _REGKEYRENA MED	Log registry key renamed events	• *1*: Log • *0*: Do not log	*1*	No
DEVICECONTR OLLOG	Log events related to device access control	• *1*: Log • *0*: Do not log	*1*	No

Server Section

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

Table 2-5. Setup.ini File *[SERVER]* **Section Arguments**

Key	Description	Possible Values	Default Value	Encrypted
HOSTNAME	Server host name	<host_name>	<empty>	No

PORT_FAST	Server listen port for fast lane	*1- 65535*	<empty>	No
CERT	Certificate filename	<certificate_file_name>	<empty>	No

Agent Section

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

Table 2-6. Setup.ini File *[AGENT]* **Section Arguments**

Key	Description	Possible Values	Default Value	Encrypted
PORT	Agent listening port	*1- 65535*	<empty>	No
FIXED_IP	Set the agent IP address to communcate with the StellarProtect (Legacy Mode) server	• A.B.C.D/E • A,B,C,D: 0~255 • E: 1~32	<empty>	No

Maintenance Mode Section

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

Table 2-7. Setup.ini File *[MAINTENANCEMODE]* **Section Arguments**

Key	Description	Possible Values	Default Value	Encrypted
ENABLE_DURATION	Start maintenance mode with this duration immediately	*0 - 999* Unit: Hours	*0*	No

Key	Description	Possible Values	Default Value	Encrypted
	after the install process is finished			
SCAN	Enable file scanning after the maintenance period	• *0*: No scan (default) • *1*: Quarantine StellarProtect (Legacy Mode) scans files that are created, executed, or modified during the maintenance period and quarantine detected files • *2*: al StellarProtect (Legacy Mode) scans files that are created, executed, or modified during the maintenance period and adds these files (including files that are detected as malicious) to the Approved List	*0*	No

Message Section

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

Table 2-8. Setup.ini File *[MESSAGE]* **Section Arguments**

Key	Description	Possible Values	Default Value	Encrypted
INITIAL_RETRY_INTERVAL	Starting interval, in seconds, between attempts to resend an event to StellarOne This interval doubles in size for each unsuccessful attempt, until it exceeds the *MAX_RETRY_INTERVAL* value	• *0 ~ 2147483647*	*120*	No
MAX_RETRY_INTERVAL	Maximum interval, in seconds, between attempts to resend events to StellarOne	• *0 ~ 2147483647*	*7680*	No

MessageRandomization Section

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

📝 **Note**

StellarProtect (Legacy Mode) agents respond as soon as possible to direct requests fromStellarOne. For details, refer to Applying Message Time Groups in the StellarProtect (Legacy Mode) Administrator's Guide.

Table 2-9. Setup.ini File *[MESSAGERANDOMIZATION]* **Section Arguments**

Key	Description	Possible Values	Default Value	Encrypted
TOTAL_GROUP_ NUM	Number of groups controlled by the server	*0 - 2147483646*	*0*	No
OWN_GROUP_IN DEX	Index of group which this agent belongs to	*0 - 2147483646*	*0*	No
TIME_PERIOD	Maximum amount of time agents have to upload data (in seconds)	*0 - 2147483647*	*0*	No

Proxy Section

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

Table 2-10. Setup.ini File *[PROXY]* **Section Arguments**

Key	Description	Possible Values	Default Value	Encrypted
MODE	Proxy mode	• *0*: No proxy used • *1*: Proxy used with manual settings • *2*: Proxy used with settings retrieved from Internet Explorer automatically	*0*	No
HOSTNAME	Proxy host name	<host_name>	<empty>	No

Key	Description	Possible Values	Default Value	Encrypted
PORT	Proxy port	*1- 65535*	<empty>	No
USERNAME	Proxy user name	<user_name>	<empty>	No
PASSWORD	Proxy password	<password>	<empty>	No

Prescan Section

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

Table 2-11. Setup.ini File *[PRESCAN]* **Section Arguments**

Key	Description	Possible Values	Default Value	Encrypted
IGNORE_THRE AT	Cancel installation after detecting malware threat during prescan	• *0*: Cancel • *1*: Continue installation after detecting malware threat during prescan • *2*: Continue installation when no malware is detected, or after all detected malware is cleaned, deleted, or quarantined successfully without a system reboot	*2*	No
REPORT_FOLD ER	An absolute folder path where prescan	• <folder_path> • <empty>: Defaults to	<empty>	No

Key	Description	Possible Values	Default Value	Encrypted
	result reports are saved	%windir%\temp \prescan\log		
SCAN_TYPE	The type of scan executed during silent installation **Note** The selected value is used as the default value for a UI installation.	• *Full*: Scan all folders on the endpoint • *Quick*: Scans the following folders: • Fixed root drives For example: c:\ d:\ • System root folder For example, c:\Window s • System folder For example, c:\Window s\System • System32 folder For example, c:\Window s \System32 • Driver folder	*Full*	No

Key	Description	Possible Values	Default Value	Encrypted
		For example, c:\Window s \System32 \Drivers		
		• Temp folder		
		For example, c:\Users \Trend \AppData \Local \Temp		
		• Desktop folder including sub folders and files		
		For example, c:\Users \Trend \Desktop		
		• *Specific*: Scan folders specified with *SPECIFIC_FOLD ER* entries		

Key	Description	Possible Values	Default Value	Encrypted
COMPRESS_LA YER	The number of compressed layers to scan when a compressed file is scanned	• *0*: Do not scan compressed files • *1-20*: Scan up to the specified number of layers of a compressed file	*2*	No
MAX_FILE_SIZ E	The largest file allowed for scan	• *0*: Scan files of any sizes • *1 - 9999*: Only scan files equal to or smaller than the specified size (MB)	*0*	No
SCAN_REMOVAB LE_DRIVE	Scan removable drives	• *0*: Do not scan removable drives • *1*: Scan removable drives	*0*	No

Key	Description	Possible Values	Default Value	Encrypted
SPECIFIC_FOLDER	An absolute folder path toscan when thescan type is [Specific]	<folder_path> Multiple folders can be specified by creating new entries whose name starting with *SPECIFIC_FOLDER* Every entry name needs to be unique For example: *SPECIFIC_FOLDER=c: \folder1* *SPECIFIC_FOLDER2= c: \folder2* *SPECIFIC_FOLDER3= c: \folder3*	<empty>	No
EXCLUDED_FILE	An absolute file path to exclude from scanning	<file_path> Multiple files can be specified by creating new entries whose name starting with *EXCLUDED_FILE* Every entry name needs to be unique For example: *EXCLUDED_FILE=c: \ file1.exe* *EXCLUDED_FILE2=c: \file2.exe* *EXCLUDED_FILE3=c: \file3.exe*	<empty>	No

Key	Description	Possible Values	Default Value	Encrypted
EXCLUDED_FOL DER	An absolute folder path toexclude fromscanning	<folder_path> Multiple folders can be specified by creating new entries whose name starting with *EXCLUDED_FOLDER* Every entry name needs to be unique For example: *EXCLUDED_FOLDER=c : \file1* *EXCLUDED_FOLDER2= c: \file2* *EXCLUDED_FOLDER3= c: \file3*	<empty>	No
EXCLUDED_EXT ENSION	A file extensionto exclude from scanning	<file_extension> Multiple extensions can be specified by creating new entries whose name starting with *EXCLUDED_EXTENSIO N* Every entry name needs to be unique For example: *EXCLUDED_EXTENSIO N=bmp* *EXCLUDED_EXTENSIO N2=png*	<empty>	No

Key	Description	Possible Values	Default Value	Encrypted
PRESCANCLEAN UP	Attempt to clean detected files during prescan	• *0*: No action • *1*: Clean, or delete if the clean action is unsuccessful • *2*: Clean, or quarantine if the clean action is unsuccessful • *3*: Clean, or ignore if the clean action isunsuccessful	*2*	No
FORCE_PRESCAN	Perform a prescan beforeinstallation	• *0*: Disable • *1*: Enable	*0*	No

BlockNotification Section

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

See *Property Section on page 2-18* for more information.

🛎 **Important**
To enable the feature, make sure to also enable the display for system tray icons
and notifications. See *NO_SYSTRAY* in this table for details.

Table 2-12. Setup.ini File *[BlockNotification]* **Section Arguments**

Key	Description	Possible Values	Default Value	Encrypted
ENABLE	Display notifications on managed endpoints when StellarProtect (Legacy Mode) blocks an unapproved file	• *0*: Disable • *1*: Enable	*0*	No
ALWAYS_ON_TOP	Display the file blocking notification on top of other screens	• *0*: Disable • *1*: Enable	*1*	No
SHOW_DETAILS	Display file name, file path, and event time in the notification	• *0*: Disable • *1*: Enable	*1*	No
AUTHENTICATE	Authenticate the user by requesting the administrator password when closing a notification	• *0*: Disable • *1*: Enable	*1*	No
TITLE	Notification title	<notification_title>	<empty>	No
MESSAGE	Notification content	<notification_content>	<empty>	No

Chapter 3

Agent Configuration File Deployment

This chapter describes the deployment of settings to multiple TXOne StellarProtect (Legacy Mode) agents using an Agent Configuration File.

Deployment for Standalone Agents

Agents installed in *Standalone* mode are not managed by a TXOne StellarProtect (Legacy Mode) Central Console server. To manually deploy a single configuration to multiple *Standalone* agents, use an agent configuration file.

Exporting or Importing a Configuration File

> 📝 **Note**
>
> TXOne StellarProtect (Legacy Mode) encrypts the configuration file before export. Users mustdecrypt the configuration file before modifying the contents.

Procedure

1. Open the TXOne StellarProtect (Legacy Mode) console using the desktop icon (ifavailable) or the **Start** menu by clicking **All Programs** > **TXOne StellarProtect (Legacy Mode)**.

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

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

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

   a. Click **Export Settings**, 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 Settings**, and locate the database file.

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

   TXOne StellarProtect (Legacy Mode) overwrites the existing

configuration settings withthe settings in the database file.

Deployment using StellarOne

Agents installed in *Managed* mode are managed by a StellarOne server, which can issue remote commands to all managed agents. To deploy agent configuration settings to multiple managed agents, launch the StellarOne web console and use the **Send Command** menu located on the **Agent Management** screen.

Remotely Exporting Agent Settings

You can remotely obtain agent configuration settings and Approved Lists by exporting and downloading them from the StellarOne.

Procedure

1. Click **Agents** > **StellarProtect (Legacy Mode)** from

   the StellarOne.The **Agent Management** screen

   appears.

2. Select a target endpoint.

3. Click **Import / Export** and select one of the following:

   · **Import Approved List**

   · **Import Agent Configuration**

   The StellarOne will issue the command. Progress can be viewed from the pop-up **Details** window.

4. To export settings, repeat the above steps, instead selecting either **Export Approved List** or **Export Agent Configuration**.

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

Command Deployment					×
Date and Time	2021-01-22T19:21:57+08:00				
Event	Exported (Approved List) from DESKTOP-RI4C181.				

All Status (1) ▾

Endpoint	IP Address	Group	Status	Download
DESKTOP-RI4C181	192.168.132.132	Ungrouped	⊘ Completed at 2021-01-22T19:21:59+08:00	Download

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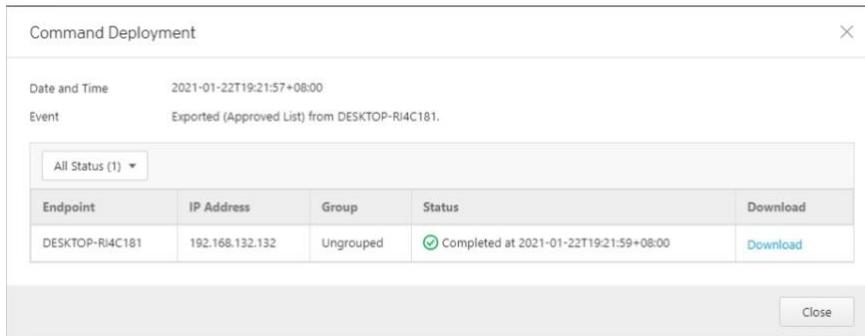
5. Click **View Details** to download the exported settings.

Remotely Importing Agent Settings

You can remotely apply new agent settings to agents from StellarOne. This feature allows you to:

•   Remotely overwrite agent configurations

•   Remotely overwrite Approved Lists

•   Remotely add approved items to Approved Lists

Procedure

1. Prepare a customized agent configuration file or Approved List.

a.   Export and download an agent configuration file or Approved List.

b.   Customize the downloaded file.

> **📝 Note**
>
> To ensure successful import, verify that the file to import meets the following requirements:
>
> - File is in the CSV format and uses UTF-8 encoding
>
> - For Approved List, maximum file size supported is 20 MB
>
> - For agent configuration file, maximum file size supported is 1 MB

2. Click **Agents** from the StellarOne console.

   The **Agent Management** screen appears.

3. To import the customized file to agents, follow the steps below.

   a. From the Endpoint column, select one or more agents.

   b. Click **Import / Export**.

   c. Select **Import Approved List** or **Import Agent Configuration**

   The import dialog will appear.

4. To import the customized file to an agent group, follow the steps below.

   a. From the left panel, select an agent group and go to **Import / Export**.

   b. Select **Import Approved List** or **Import Agent Configuration**.

   The import dialog will appear.

5. By default, StellarOne does the following:

   - **Approved List**: accumulates items from the customized Approved List to the target Approved Lists. To replace the target Approved Lists with the customized Approved List, select **Overwrite the existing Approved List**.

   - **Agent Configuration**: overwrites the target Approved Lists with the customized Approved List.

6. Click **Browse** to select the customized file.

7. Click **OK**.

Chapter 4

Local Agent Uninstallation

This chapter describes TXOne StellarProtect (Legacy Mode) agent uninstallationprocedures.

Topics in this chapter include:

-

Uninstalling Agents from Windows

Procedure

1. On an endpoint with the StellarProtect (Legacy Mode) agent uninstalled, launch TXOneStellarProtect (Legacy Mode) Setup.

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

Option	Description

If you use one of the following operating systems:
 	
• Windows 10 Enterprise
 	
• Windows 10 IoT Enterprise
 	
• Windows 10 Professional
	a. Go to **Start** › **Settings**.
	
	b. Depending on your version of Windows 10, locate the **Apps & features** section under one of the following categories:
	
	   • **System**
	
	   • **Apps**
	
	c. On the left pane, click **Apps & features**.
	
	d. In the list, click TXOne StellarProtect (Legacy Mode).
	
	e. Click **Uninstall**.

If you use one of the following operating systems: • Windows 7 • Windows 8 • Windows Vista • Windows Server 2008 • Windows Server 2012 • Windows Server 2016	a. Go to **Start** › **Control Panel** › **Programs and Features**. b. In the list, double-click TXOne StellarProtect (Legacy Mode).

Option	Description
• Windows Storage Server 2016 • Windows Server 2019	
If you use one of the following operating systems: • Windows Server 2003 • Windows XP • Windows 2000	a. Go to **Start** > **Control Panel** > **Add or Remove Programs**. b. In the list, select TXOne StellarProtect (Legacy Mode). c. Click **Remove**.

StellarProtect (Legacy Mode) Setup opens in uninstaller mode.

2. After StellarProtect (Legacy Mode) Setup opens, click Next.

3. Provide the StellarProtect (Legacy Mode) administrator password, and click Next.

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

Technical Support

Support forTXOne Networks products is provided mutually by TXOne Networks and Trend Micro. All technical support goes through TXOne and Trend Micro engineers.

Learn about the following topics:

- *Troubleshooting Resources on page 5-2*

- *Contacting Trend Micro on page 5-3*

- *Sending Suspicious Content to Trend Micro on page 5-4*

- *Other Resources on page 5-5*

Troubleshooting Resources

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

Using the Support Portal

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

Procedure

1. Go to https://success.trendmicro.com.

2. Select from the available products or click the appropriate button to search for solutions.

3. Use the **Search Support** box to search for available solutions.

4. If no solution is found, click **Contact Support** and select the type of support needed.

> **Tip**
>
> To submit a support case online, visit the following URL:
>
> https://success.trendmicro.com/sign-in
>
> A Trend Micro support engineer investigates the case and responds in 24 hours or less.

Threat Encyclopedia

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

defense strategy.

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

Go to https://www.trendmicro.com/vinfo/us/threat-encyclopedia/#malware and https://www.encyclopedia.txone.com/ to learn more about:

- Malware and malicious mobile code currently active or "in the wild"

- Correlated threat information pages to form a complete web attack story

- Internet threat advisories about targeted attacks and security threats

- Web attack and online trend information

- Weekly malware reports

Contacting Trend Micro and TXOne

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

Table 6-1. Trend Micro Contact Information

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

Table 6-2. TXOne Contact Information

Address	TXOne Networks, Incorporated
	222 West Las Colinas Boulevard, Suite 1650
	Irving, TX 75039 U.S.A
Website	https://www.txone.com
Email address	support@txone.com

- Worldwide support offices:

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

    https://www.txone.com/contact/

- Trend Micro product documentation:

    https://docs.trendmicro.com

Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem

- Appliance or network information

- Computer brand, model, and any additional connected hardware or devices

- Amount of memory and free hard disk space

- Operating system and service pack version

- Version of the installed agent

- Serial number or Activation Code

- Detailed description of install environment

- Exact text of any error message received

Sending Suspicious Content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

https://www.ers.trendmicro.com/

Refer to the following Knowledge Base entry to send message samples to Trend Micro:

https://success.trendmicro.com/solution/1112106

File Reputation Services

Gather system information and submit suspicious file content to TrendMicro:

https://success.trendmicro.com/solution/1059565 Record

the case number for tracking purposes.

Web Reputation Services

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and malware):

https://global.sitesafety.trendmicro.com/

If the assigned rating is incorrect, send a re-classification request to TrendMicro.

Other Resources

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

Download Center

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

https://www.trendmicro.com/download/

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

Index

www.**txone**.com