# txOne networks

Keep the Operation Running

**1.4**

# TXOne StellarProtect (Legacy Mode)
## Installation Guide

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

Windows

# 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 Networks, StellarOne, StellarProtect, and StellarProtect (Legacy Mode) collect 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 3: Agent Configuration File Deployment

# Chapter 4: Uninstalling StellarProtect

# Chapter 5: License Renewal

# Chapter 6: Technical Support

# Index

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.

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.

# Preface

## Preface

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

Topics in this chapter include:

# About the Documentation

TXOne Networks StellarProtect (Legacy Mode) documentation includes the following:

| DOCUMENTATION | DESCRIPTION |
|---|---|
| Readme file | Contains a list of known issues and basic installation steps. It may also contain late-breaking product information not found in the other documents. |
| Installation Guide | A PDF document that discusses requirements and procedures for installing and managing StellarProtect (Legacy Mode). |
| Administrator's Guide | A PDF document that discusses StellarProtect (Legacy Mode) agent installation, getting started information, and server and agent management |
| 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 websites:<br><br>https://kb.txone.com/<br><br>http://success.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 documentation uses the following conventions.

**TABLE 1. 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<br><br>For example, **File** > **Save** means, click **File** and then click **Save** on the interface |
| **Note** | Configuration notes |
| **Tip** | Recommendations or suggestions |
| **Important** | Information regarding required or default configuration settings and product limitations |
| **WARNING!** | Critical actions and configuration options |

# Terminology

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

| TERMINOLOGY | DESCRIPTION |
|---|---|
| server | The StellarOne console server program |
| agents | The host running the StellarProtect (Legacy Mode) program |
| managed agents<br><br>managed endpoints | The hosts running the StellarProtect (Legacy Mode) program that are known to the StellarOne server program |
| target endpoints | The hosts where the StellarProtect (Legacy Mode) managed agents will be installed |
| Administrator (or StellarProtect (Legacy Mode) administrator) | The person managing the StellarProtect (Legacy Mode) agent |
| StellarProtect (Legacy Mode) console | The user interface for configuring and managing StellarProtect (Legacy Mode) settings |
| StellarOne (management) console | The user interface for configuring and managing the StellarProtect (Legacy Mode) agents managed by StellarOne |
| CLI | Command Line Interface |
| license activation | Includes the type of StellarProtect (Legacy Mode) agent installation and the allowed period of usage that you can use the application |
| agent installation folder | The folder on the host that contains the StellarProtect (Legacy Mode) agent files. If you accept the default settings during installation, you will find the installation folder at one of the followinglocations:<br><br>`C:\Program Files\TXOne\StellarProtect (Legacy Mode)` |

# Chapter 1

## Introduction

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

Topics in this chapter include:

# About TXOne Stellar

TXOne Stellar is a first-of-its-kind OT endpoint protection platform, which includes:

- StellarOne™ , the centralized management console designed to streamline administration of both StellarProtect for modernized systems and StellarProtect (Legacy Mode) for legacy systems.

- StellarProtect ™, the unified agent with industrial-grade next-generation antivirus and application lockdown endpoint security deployment for modernized OT/ICS endpoints.

- StellarProtect (Legacy Model) ™, for trust-list based application lockdown of legacy and fixed-use OT/ICS endpoints with anti-malware or on-demand AV scan.

Together, TXOne Stellar allows protection for modernized and legacy systems running side-by-side to be coordinated and maintained from the same management console, helping protect businesses against security threats and increase productivity.

# Key Features and Benefits

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 and without 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.

The StellarProtect (Legacy Mode) provides following features and benefits.

**TABLE 1-1. Features and Benefits**

| FEATURE | BENEFIT |
|---|---|
| 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.<br><br>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.<br><br>For advanced threat prevention, StellarProtect (Legacy Mode) includes intrusion prevention, execution prevention, application lockdown, and devicecontrolto 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 thefollowing 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):<br><br>•    Maintenance Mode<br><br>•    Trusted Updater<br><br>•    Predefined Trusted Updater List<br><br>•    Command Line Interface (CLI)<br><br>•    Trusted hash<br><br>•    Trusted certificate |
| 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. |

| Feature | Benefit |
|---|---|
| Role Based Administration | TXOne StellarProtect (Legacy Mode) provides a separate administrator and Restricted User account, providing full control during installation and setup, as well as simplified monitoring and maintenance after deployment. |
| Graphical and Command Line Interfaces | Anyone who needs to check the software can use the console, while systemadministrators 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: <br><br> • Trend Micro Unauthorized Change Prevention Service (`TMBMSRV.exe`) <br><br> • Trend Micro Personal Firewall (`TmPfw.exe`) <br><br> • TXOne StellarProtect (Legacy Mode) Service (`WkSrv.exe`) |

## What's New

TXOne StellarProtect (Legacy Mode) 1.4 provides following new features and enhancements.

**Table 1-2. What's New in TXOne StellarProtect (Legacy Mode) 1.4**

| Feature | Benefit |
|---|---|
| Anti-Malware Scanning (Real-Time Scan) | With this new feature, the StellarProtect (Legacy Mode) can persistently scan new and changed files, along with system memory, to provide security assessment for maximum protection against malware. |
| Self-management status | The self-management status displayed on the agent's console GUI enables users to know whether the agent is following StellarOne's policy settings. |

| Feature | Benefit |
|---|---|
| Single installer package | A single installer package for the Agent – StellarProtect and StellarProtect (Legacy Mode) is available now. After being invoked, the single installer can identify the version of Windows installed on the endpoint and launch the suitable installer for the endpoint to install. |
| Supporting license key/file | Supports license key and license file for product activation |

# System Requirements

This section introduces the system requirements for StellarProtect (Legacy Mode), including hardware and OS requirements.

## Software and Hardware Requirements

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

**TABLE 1-3. Required Hardware for StellarProtect and StellarProtect (Legacy Mode)**

| HARDWARE | DESCRIPTION |
|---|---|
| Available free disk space | StellarProtect: 400MB<br><br>StellarProtect (Legacy Mode): 400MB<br><br>---<br><br>📝 **Note**<br><br>• Recommended free disk space for StellarProtect Single Installer required during the installation process - 1.5GB<br><br>• Minimum memory usage required when Application Lockdown and Real-Time Scan are both enabled:<br><br>    • StellarProtect: 350MB<br><br>    • StellarProtect (Legacy Mode): 300MB<br><br>• Minimum memory usage required when Application Lockdown is enabled and Real-Time Scan is disabled:<br><br>    • StellarProtect: 120MB<br><br>    • StellarProtect (Legacy Mode): 100MB |
| Monitor and resolution | VGA (640 x 480), 16 colors |

By default, StellarProtect (Legacy Mode) uses port 14336 as the listening port for StellarOne, which is sometimes blocked by firewalls. Please make sure this port is kept open for StellarProtect (Legacy Mode)'s use.

The Active Update server link for StellarProtect (Legacy Mode) has been changed to **https://ttau.cs.txone.com**. Please ensure that you whitelist this URL in your firewall.

> **Important**
>
> - StellarProtect (Legacy Mode) cannot be installed on a system that already runs one of the following:
>
>   - Trend Micro OfficeScan
>
>   - Trend Micro Titanium
>
>   - Other Trend Micro endpoint solutions
>
>   - Other endpointsolutions except Windows Defender Antivirus
>
> - 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](#).

> **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 of supported operating systems for agents.

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

## Operating Systems

**Windows Client:**

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

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

- 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.
>
> - OndDrive 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.
>
>   - Windows 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:
>
>   - Enable the `case sensitive` attribute for a folder may prevent StellarProtect (Legacy Mode) from performing certain actions (e.g., prescan, custom actions) on that folder. Folders that do not have the attribute enabled are not affected.
>
>   - StellarProtect (Legacy Mode) blocks all processes started fromfolders 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)

---

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

---

- 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)

- Widows Embedded POSReady (32bit)

**Windows Server:**

- Windows Server 2000 (SP4) (32bit)

- 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] (64bit)

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

- 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)

---

**Note**

StellarProtect (Legacy Mode) installed on Windows 2000 SP4 (without update rollup), Windows XP SP1, Windows XP Embedded, or 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.

To support these features, install Filter Manager:

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

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

---

## Preparing the Agent for Upgrade to a Later Version

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

- StellarEnforce 1.0

- StellarEnforce 1.1

- StellarEnforce 1.2

- StellarEnforce 1.2 Patch 1

- StellarProtect (Legacy Mode) 1.3

---

> ✎ **Note**
>
> The StellarEnforce was renamed StellarProtect (Legacy Mode) upon the release of version 1.3.

---

The latest updates can be downloaded from the StellarProtect (Legacy Mode) Software Download Center.

---

> ✎ **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.

**TABLE 1-4. Fresh Installation of the StellarProtect (Legacy Mode) Agent**

| INSTALLATION METHOD | INSTALLED AGENT VERSION | REQUIRED ACTION | SETTINGS RETAINED |
|---|---|---|---|
| Local installation using Windows installer | StellarEnforce 1.0 / 1.1 / 1.2 / 1.2 Patch 1 / StellarProtect (Legacy Mode) 1.3 | It's necessary to manually add the install file (SL_Install.exe) into the trusted HASH list and enable PTU function before using it. | No settings retained |

| Installation Method | Installed Agent Version | Required Action | Settings Retained |
|---|---|---|---|
| Local installation using command line interface installer | StellarEnforce 1.0 / 1.1 / 1.2 / 1.2 Patch 1 / StellarProtect (Legacy Mode) 1.3 | It's necessary to manually add the install file (`SL_Install.exe`) into the trusted HASH list before using it. | No settings retained |

**Table 1-5. 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`.<br><br>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` | StellarEnforce 1.0 / 1.1 / 1.2 / 1.2 Patch 1 / StellarProtect (Legacy Mode) 1.3 | No preparation needed | Compatible settings retained |
| Remote Installation | StellarEnforce 1.1 / 1.2 / 1.2 Patch 1 / StellarProtect (Legacy Mode) 1.3<br><br>**Note**<br>StellarEnforce 1.0 supports only local installation. | No preparation needed | Compatible settings retained |

**TABLE 1-6. 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`.<br><br>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` | StellarEnforce 1.2 Patch 1 / StellarProtect (Legacy Mode) 1.3 | No preparation needed | Compatible settings retained |

| Installation Method | Installed Agent Version | Required Action | Settings Retained |
|---|---|---|---|
| | **Note**<br>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:<br><br>• Remotely upgrade StellarProtect (Legacy Mode) agents from StellarOne web console<br><br>• Add the patch file hash as trusted hash, enable PTU function and then perform local upgrade. | | |

| Installation Method | Installed Agent Version | Required Action | Settings Retained |
|---|---|---|---|
| Remote Installation | StellarEnforce 1.0 / 1.1 / 1.2 / 1.2 Patch 1 / StellarProtect (Legacy Mode) 1.3 | 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 ApplicationLockdown 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:
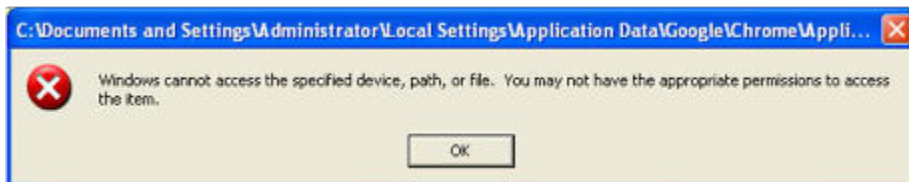


**FIGURE 1-1. StellarProtect (Legacy Mode) Blocking Message**

# Chapter 2

## Installation

This chapter shows how to install the TXOne StellarProtect (Legacy Mode) agent. The StellarProtect (Legacy Mode) agent provides installation methods including **attended installation** and **silent installation**.

Topics in this chapter include:

# Agents Installed in Managed or Standalone Mode

TXOne Stellar offers two modes for agent management:

- 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.

- Agents installed in *Standalone* mode are not managed by a TXOne StellarOne central management console server; instead, they are managed by the local administrator or operator. To manually deploy a single configuration to multiple standalone agents, use an agent configuration file.

# Getting the Agent's Installer Package

For agents managed by the StellarOne web console, refer to *Getting the Agent's Installer Package via StellarOne on page 2-2*.

For standalone agents, refer to *Getting the Standalone Agent's Installer Package on page 2-4*.

## Getting the Agent's Installer Package via StellarOne

For agents managed by the StellarOne web console, follow instructions below to get the agent's installer package.

**Procedure**

1. Log on the StellarOne web console.

> **Note**
>
> If this is the first time the StellarOne console being logged on, refer to [StellarOne Installation Guide](#) for detailed instructions on the initial settings.

2. Go to **Administration** > **Downloads/Updates** > **Agent** to download the agent's Installer Package.

**FIGURE 2-1. StellarOne Downloads/Updates Screen**



A zipped folder is downloaded. Extract the folder and proceed with the installation for the agents.

> **Note**
>
> The Installer Package is packed by StellarOne and can be used for StellarProtect and StellarProtect (Legacy Mode) installations. After being invoked, the single installer can identfy the version of Windows installed on the endpoint and launch the suitable installer for the endpoint to install.

3. (Optional) To register agents to a group during installation, users can also download the Group.ini file.

   a. Click the **download Group.ini** link on the StellarOne **Administration** > **Downloads/Updates** > **Agent** page.

   b. A pop-up windows appears. Select a group for the target agent.

   c. Click **Download**. A file named Group.ini is downloaded.

   d. Place the Group.ini file as the top-level file in the agent's installer package.

## Getting the Standalone Agent's Installer Package

For standalone agents, follow instructions below to get the agent's installer package.

**Procedure**

1. Go to our [Software Download Center](#).

2. Find StellarProtect and click it. You will be directed to the web page with the latest firmware version for StellarProtect (Legacy Mode).

   > **Note**
   >
   > The StellarProtect (Legacy Mode) now shares the same installer package with StellarProtect.

3. Be sure you are on the **Product Download/Update** tab page.

4. Find the file name starting with `txsp-` and click it to download the StellarProtect single installer package.

> **Note**
>
> The StellarProtect single installer package contains the StellarProtect and StellarProtect (Legacy Mode) installers. After being invoked, the single installer package can identify the version of Windows installed on the endpoint and launch the suitable installer for the endpoint to install.

## Installation Methods

This section mainly explains the steps for installing StellarProtect (Legacy Mode) using **Attended Installation** or **Silent Installation**.

## Attended Installation

**Procedure**

1. Launch the installer `StellarSetup.exe`.

> **Note**
>
> The installer package downloaded from StellarOne management console differs slightly from that downloaded from the Software Download Center. One contains the StellarOne data files while the other one does not.

**Figure 2-2. Installer Package Downloaded from StellarOne**



**Figure 2-3. Standalone Installer Package Downloaded from Software Download Center**

---

📝 **Note**

To register StellarProtect (Legacy Mode) agent to a specific group during installation, after downloading the Group.ini file on StellarOne console, the file must be placed as the top-level file in the agent's Installer Package before starting the installation.

---

**2.** Click **Yes** to start the installation.
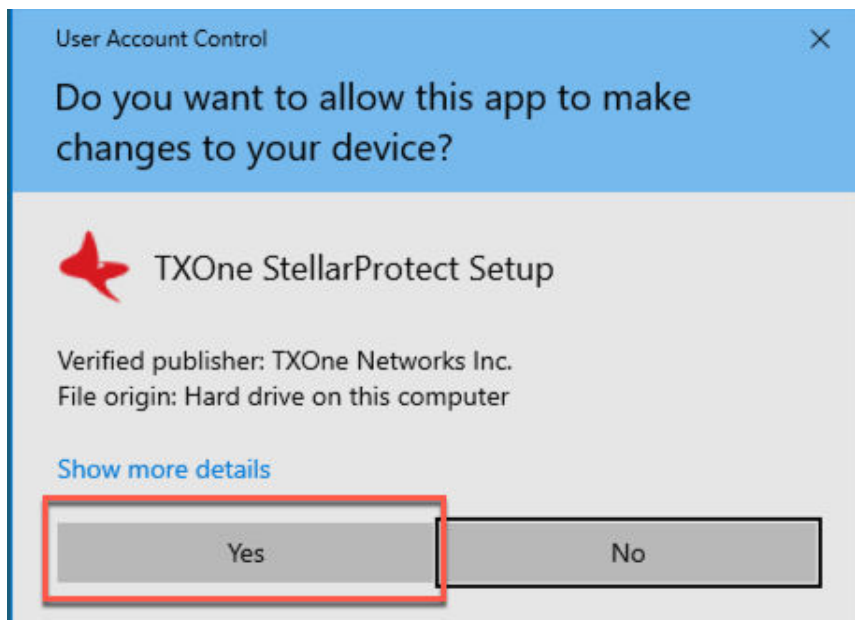


**FIGURE 2-4. StellarProtect (Legacy Mode) Setup Screenshot**

**3.** Click **Next** to continue.
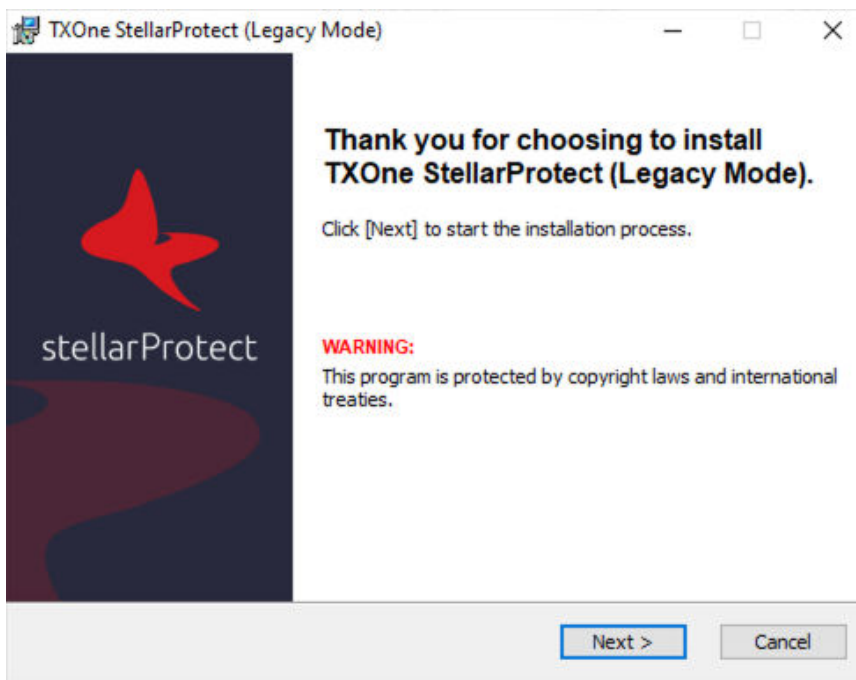
**FIGURE 2-5. StellarProtect (Legacy Mode) Installation Wizard**

4.  The **End-User License Agreement** (EULA) window appears. Please read the content carefully, and then check **I accept the terms in the License Agreement** and click **Next**.
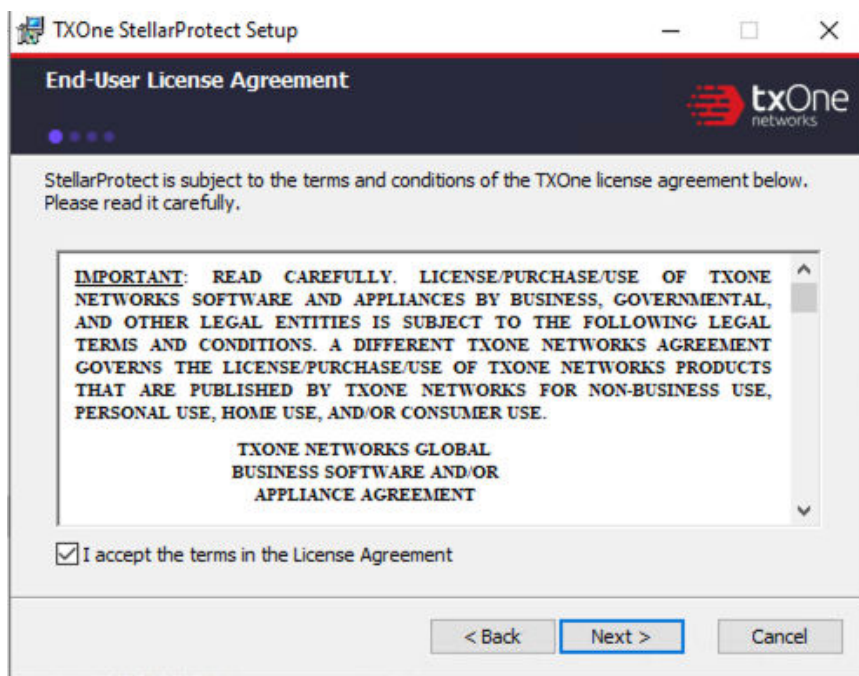
**FIGURE 2-6. End-User License Agreement**

5. Confirm the installation settings including installation directory and optional component settings.
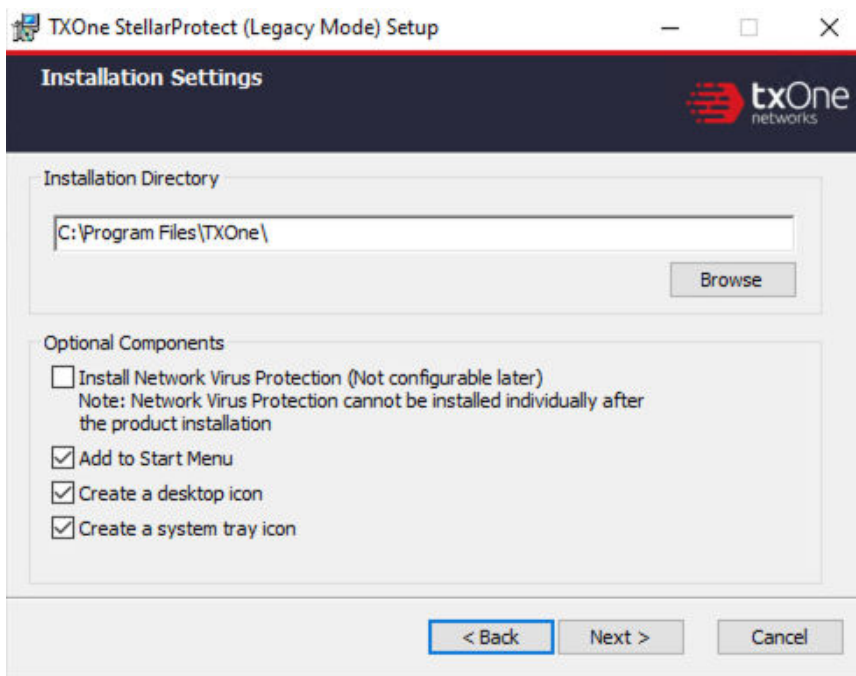
**FIGURE 2-7. StellarProtect (Legacy Mode) Installation Settings**

> **Note**
>
> Users can choose to whether or not add an icon to the start menu, create a desktop icon, or create a system tray icon.

> **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.

**6.** Create an administrator password.

**Note**

Please use a strong administrator password with good quality in 8 to 64 alphanumeric characters. The following characteres are not supported: | > " : < \ spaces.

The StellarProtect (Legacy Mode) administrator password is unrelated to the Windows administrator password.

**Important**

Please store securely and do not lose the StellarProtect administrator password. If you lose the StellarProtect administrator password, please contact TXOne Networks for support.

7. A success message indicating valid license appears. Click **Next** to continue.
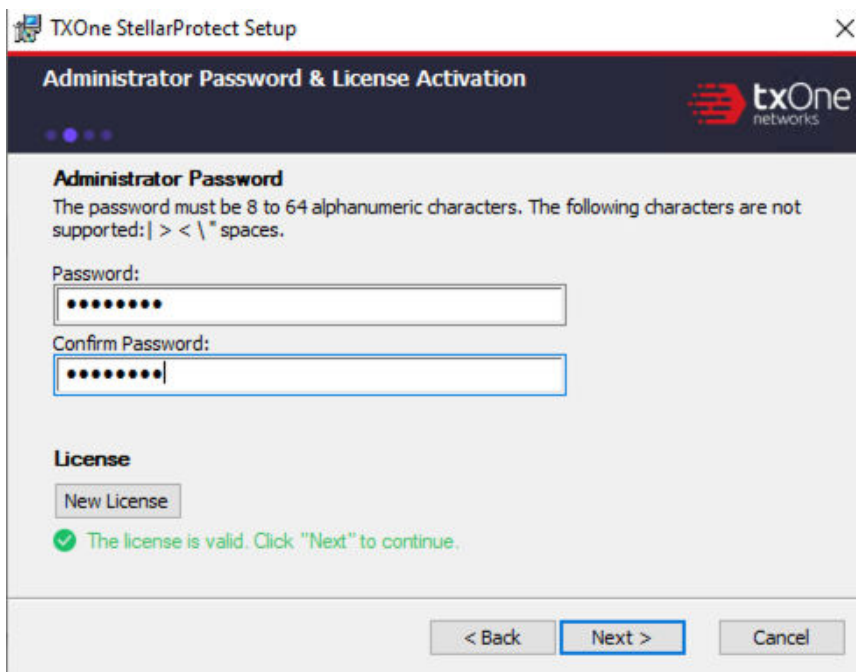
**FIGURE 2-8. Admin Password & License Activation**

> **Note**
>
> - If the agent's installer package is downloaded from StellarOne, the installer will automatically check and complete the license activation.
>
> - For standalone agents, refer to *License Activation for Standalone Agent on page 2-64*.

8. A message appears asking if you would like to scan the endpoint for threats before continuing with the installation.
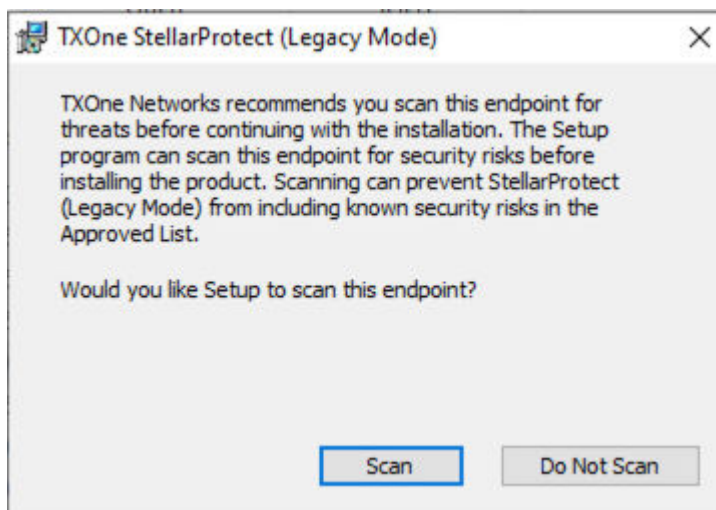
**FIGURE 2-9. Scan or Do Not Scan**

**9.** (Optional) Scan the endpoint for threats before continuing with the installation. TXOne Networks recommends you perform this scan.

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

> 📝 **Note**
>
> The **Do Not Scan** and close buttons are not applicable when you set the FORCE_PRESCAN value to 1 in the StellarSetup.ini file. Rerfer to *Properties in the Config File for Silent Installation on page 2-33*.

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

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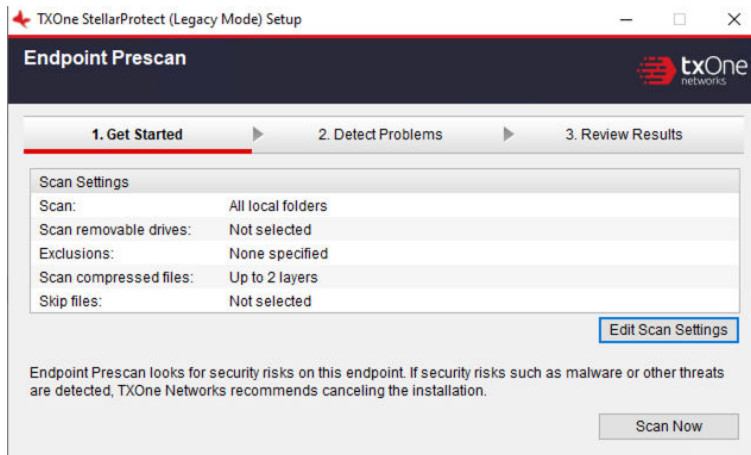


**FIGURE 2-10. Endpoint Prescan - Get Started**

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

c.  Click **Scan Now**. The **Detect Problems** window appears indicating the StellarProtect (Legacy Mode) is performing the prescan.
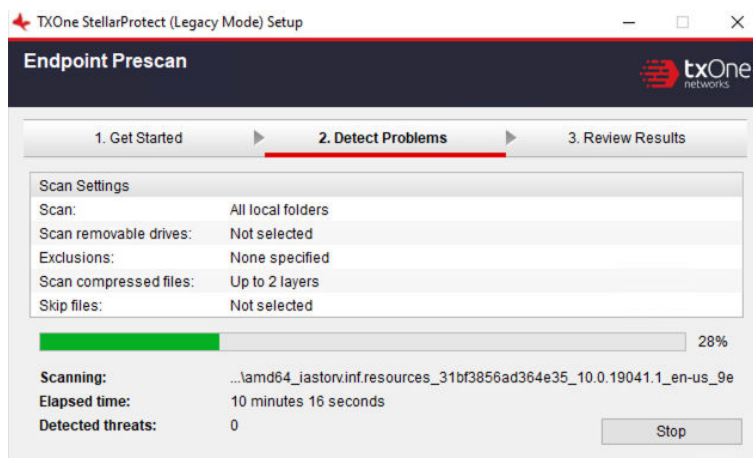


**FIGURE 2-11. Prescan - Detect Problems**

d. After the prescan is completed, the **Review Results** window appears. Click **Close**.
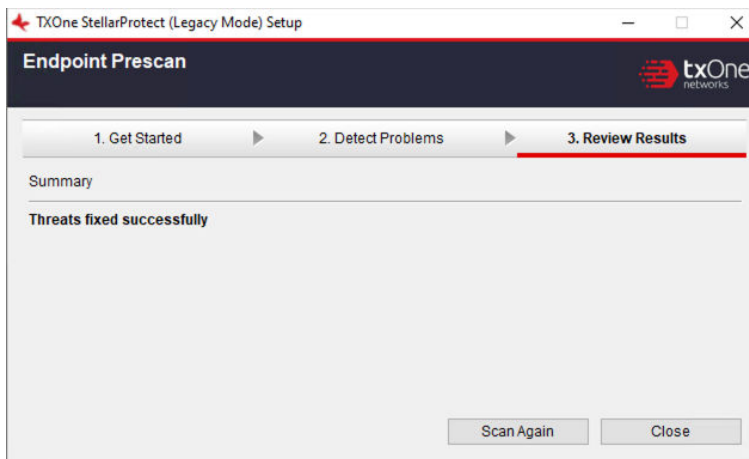


**FIGURE 2-12. Prescan - Review Results**

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 FORCE_PRESCAN value to 1 in the StellarSetup.ini file. Rerfer to *Properties in the Config File for Silent Installation on page 2-33*.

> **Tip**
>
> Performa manual scan to detect and remove threats on endpoints. Refer to *Manual Scan Commands* in the Administrator's Guide for more information.

**10.** 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. Refer to *Exploit Prevention Settings* in the Administrator's Guide for more information.

**11.** Run StellarProtect (Legacy Mode) and log on with your password.

**FIGURE 2-13. Log On StellarProtect (Legacy Mode)**

12. Upon logging on StellarProtect (Legacy Mode) successfully, the **Overview** window will display.

13. Configure the new installation.

   a. Set 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 run correctly.

      Refer to *Setting Up the Approved List on page 2-19*for more details.

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

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

To replicate settings to multiple TXOne StellarProtect (Legacy Mode) agents, use an agent sample configuration file.

## 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 run correctly.

**Procedure**

1.  Open the StellarProtect (Legacy Mode) console. The StellarProtect (Legacy Mode) log on screen appears.

2.  Provide the password and click **Log On**.
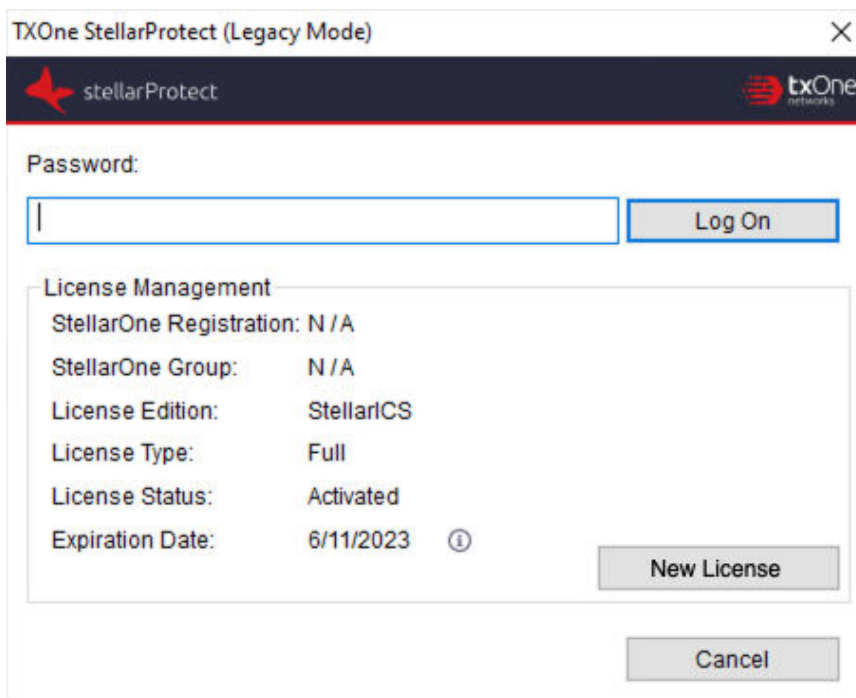
**FIGURE 2-14. StellarProtect (Legacy Mode) Log On Screen**

**3.** StellarProtect (Legacy Mode) asks if you want to set up the Approved List now.
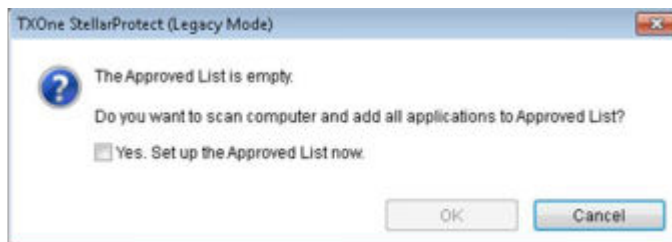


**FIGURE 2-15. The Approved List is Empty**

**4.** 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 the Approved List.
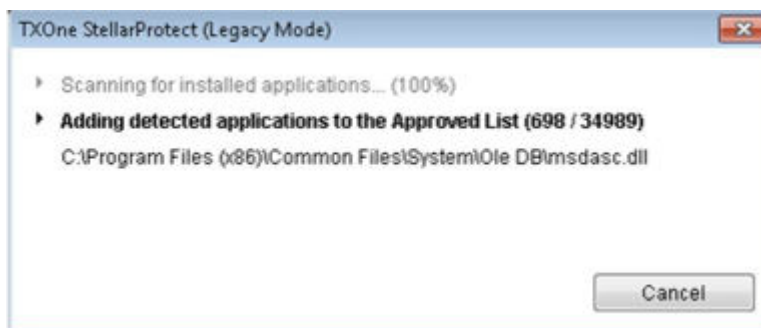


**FIGURE 2-16. Scanning for Creating Approved List**

**5.** StellarProtect (Legacy Mode) displays the Approved List Configuration Results.
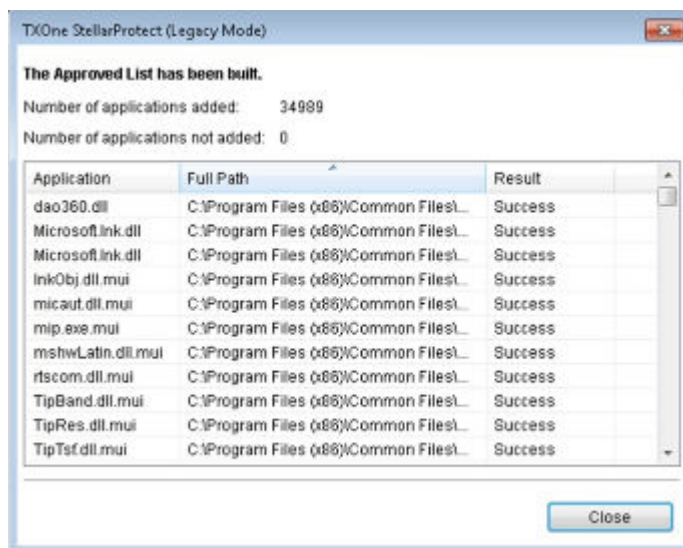


**FIGURE 2-17. Approved List Created**

---

> ✎ **Note**
>
> • When TXOne StellarProtect (Legacy Mode) Application Lockdown is on, only applications that are in the Approved List will be able to run.
>
> • When the endpoint is creating or updating its Approved List, no policy settings can be deployed.

**6.** 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.

### Installer Command Line Interface Parameters

The following table lists the commands available for StellarProtect (Legacy Mode) installation.

**TABLE 2-1. StellarProtect (Legacy Mode) Installer Command Line Options**

| PARAMETER | VALUE | DESCRIPTON |
|-----------|-------|------------|
| -s | | Run the installer silently<br><br>**Note**<br>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:<br><br>• Prescan process: `YYYYMMDDHHMMSS_wk_PreScanProgress.log`<br><br>• Initial approved process: `YYYYMMDDHHMMSS_wk_InitListProgress.log` |
| -p | <administrator_password> | Specify the administrator password |
| -d | <path> | Specify the installation path |
| -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<br><br>**Note**<br>The StellarProtect (Legacy Mode) configuration file can be exported after installing StellarProtect (Legacy Mode). |

| PARAMETER | VALUE | DESCRIPTON |
|---|---|---|
| -lp | <path> | Specify the Approved List<br><br>📝 **Note**<br>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 of using CLI for silent installation without creating a desktop shortcut would look like this:

```
StellarSetup.exe -s -p <administrator_password> -nd
```
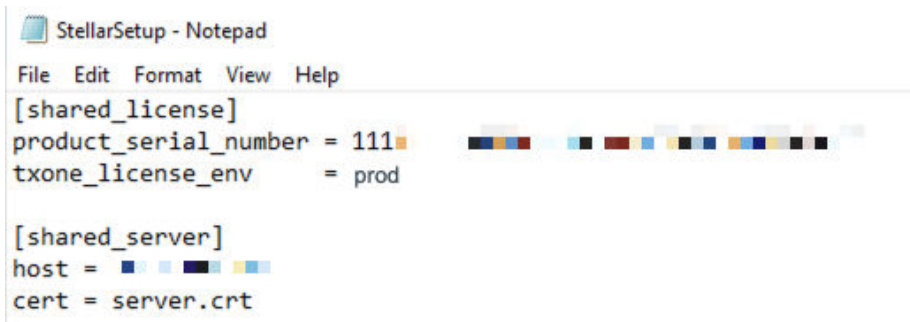
## Silent Installation

StellarProtect (Legacy Mode) provides silent installation based on a pre-defined configuration file. Users can customize the configuration settings in the StellarSetup.ini file to enable silent installation, and then execute StellarSetup.exe in silent mode.

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.

## StellarOne Managed Agent Configuration for Silent Installation



**FIGURE 2-18. Snippet of `StellarSetup.ini` Downloaded from StellarOne**

- If the Agent installer package is downloaded from StellarOne, within the `StellarSetup.ini` config file, the values of the `product_serial_number` and `txone_license_env` properties should be automatically generated. Please specify password and set the `silent` value to `1` in the configuration file. If you would like to manage the agent using StellarOne, please configure the `shared_server` host value with the server IP address.

## Standalone Agent Sample Config File for Silent Installation

See below as an example of the defined configuration file (`StellarSetup.ini`) for standalone agents. You can define your own configuration settings by changing the values.

- The **[shared_...]** entry consists of the properties shared by StellarProtect and StellarProtect (Legacy Mode) Agents.

- The **[protect_...]** entry consists of the properties exclusive to StellarProtect Agent.

- The **[legacy_...]** entry consists of the properties exclusive to StellarProtect (Legacy Mode) Agent.

---

> ⚠️ **Important**
>
> The corresponding `[shared_license]` property varies depending on your support provider:
>
> - Use the **license file** for product activation if `[shared_license]` consists of `product_serial_number` and `txone_license_file` properties.
> - Use the **license key** for product activation if `[shared_license]` consists of `license key` property.

---

The following sample config file uses **license file** for product activation.

```
[shared_license]

product_serial_number = TEXXXXXX-SAMP-LEXX-XXXX-TXONESPXXXXX

txone_license_file = Stellar<License>Edition_XXXXXXXXXXXXX.txt

[shared_server]

host = 10.1.195.100

cert = server.crt

[shared_proxy]

host =

port =

username =

password =

[shared_install]

silent = 1

password =

[protect_server]

port = 9443

[protect_listen]
```

```
port = 14336

[protect_update]

source =

[protect_config]

include =

[legacy_server]

port = 8000

[legacy_listen]

port = 14336

[legacy_update]

source =

[legacy_config]

include =

[protect_install]

asset_vendor = ABB

asset_model = ABB-1X2Y

asset_location = Factory1 North Area

asset_description = This is a machine

install_location = C:\test

enable_start_menu = 1

enable_desktop_icon = 1

enable_systray_icon = 1

enable_trusted_ics_cert = 1

enable_prescan = 1
```

```
enable_lockdown_al_building = 1

enable_lockdown_detection = 1

[protect_prescan]

action = 1

background = 0

cpu_usage_mode = 0

[protect_client]

import_source = C:\txsp_config

[legacy_Property]

PRESCAN = 1

WEL_SIZE = 10240

WEL_RETENTION = 0

WEL_IN_SIZE = 10240

WEL_IN_RETENTION = 0

USR_DEBUGLOG_ENABLE = 1

USR_DEBUGLOGLEVEL = 256

SRV_DEBUGLOG_ENABLE = 1

SRV_DEBUGLOGLEVEL = 256

FW_USR_DEBUGLOG_ENABLE = 0

FW_USR_DEBUGLOG_LEVEL = 273

FW_SRV_DEBUGLOG_ENABLE = 0

FW_SRV_DEBUGLOG_LEVEL = 273

BM_SRV_DEBUGLOG_ENABLE = 0

BM_SRV_DEBUGLOG_LEVEL = 51
```

```
INTEGRITY_MONITOR = 0

PREDEFINED_TRUSTED_UPDATER = 0

WINDOWS_UPDATE_SUPPORT = 0

STORAGE_DEVICE_BLOCKING = 0

INIT_LIST = 0

LOCKDOWN = 0

FILELESS_ATTACK_PREVENTION = 0

SERVICE_CREATION_PREVENTION = 0

INTELLIGENT_RUNTIME_LEARNING = 0

NO_DESKTOP = 0

NO_STARTMENU = 0

NO_SYSTRAY = 0

CUSTOM_ACTION = 0

MAX_EVENT_DB_SIZE = 1024

NO_NSC = 1

INIT_LIST_EXCLUDED_EXTENSION1 = log

INIT_LIST_EXCLUDED_EXTENSION2 = txt

INIT_LIST_EXCLUDED_EXTENSION3 = ini

[legacy_Prescan]

PRESCANCLEANUP = 2

IGNORE_THREAT = 2

REPORT_FOLDER =

SCAN_TYPE = Full

COMPRESS_LAYER = 2
```

```
MAX_FILE_SIZE = 0

SCAN_REMOVABLE_DRIVE = 0

FORCE_PRESCAN = 0

[legacy_BlockNotification]

ENABLE = 0

ALWAYS_ON_TOP = 1

SHOW_DETAILS = 1

AUTHENTICATE = 1

TITLE =

MESSAGE =

[legacy_EventLog]

Enable = 1

Level_WarningLog = 1

Level_InformationLog = 0

BlockedAccessLog = 1

ApprovedAccessLog = 1

ApprovedAccessLog_TrustedUpdater = 1

ApprovedAccessLog_DllDriver = 0

ApprovedAccessLog_ExceptionPath = 1

ApprovedAccessLog_TrustedCert = 1

ApprovedAccessLog_WriteProtection = 1

ApprovedAccessLog_TrustedHash = 1

SystemEventLog = 1

SystemEventLog_ExceptionPath = 1
```

```
SystemEventLog_WriteProtection = 1

ListLog = 1

UsbMalwareProtectionLog = 1

ExecutionPreventionLog = 1

NetworkVirusProtectionLog = 1

IntegrityMonitoringLog_FileCreated = 1

IntegrityMonitoringLog_FileModified = 1

IntegrityMonitoringLog_FileDeleted = 1

IntegrityMonitoringLog_FileRenamed = 1

IntegrityMonitoringLog_RegValueModified = 1

IntegrityMonitoringLog_RegValueDeleted = 1

IntegrityMonitoringLog_RegKeyCreated = 1

IntegrityMonitoringLog_RegKeyDeleted = 1

IntegrityMonitoringLog_RegKeyRenamed = 1

DeviceControlLog = 1

[legacy_MaintenanceMode]

ENABLE_DURATION = 0

SCAN = 0

[legacy_Message]

INITIAL_RETRY_INTERVAL = 120

MAX_RETRY_INTERVAL = 7680

[legacy_MessageRandomization]

TOTAL_GROUP_NUM = 1

OWN_GROUP_INDEX = 0
```

```
TIME_PERIOD = 0
```

---

> 📝 **Note**
>
> - The license file name varies depending on different license editions (ICS/Kiosk/OEM). For example, if you use ICS license edition, the license file name appears like this: `StellarICSEdition_xxxxxxxxxxxx.txt`.
>
> - To get the license file and product serial number, refer to *Getting the License File and PSN for Standalone Agents on page 2-69*.

---

## Configuration for Silent Installation

Users can pre-define the setup configuration for installation. The name is fixed to `StellarSetup.ini`. The launcher will parse `StellarSetup.ini` while executing. You can find `StellarSetup.ini` in the installation folder as shown below:
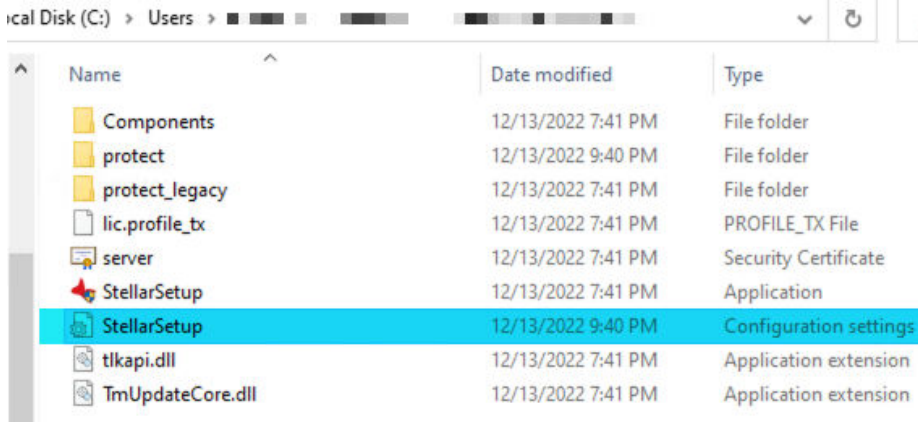


**FIGURE 2-19. `StellarSetup.ini` in the Installer Package**

### Properties in the Config File for Silent Installation

The following table lists the properties in the StellarSetup.ini config file along with the details of their use. If no valueis specified in the setup file, the default value will be used.

---

📝 **Note**

- The **[shared_...]** entry consists of the properties shared by StellarProtect and StellarProtect (Legacy Mode) Agents.

- The **[protect_...]** entry consists of the properties exclusive to StellarProtect Agent.

- The **[legacy_...]** entry consists of the properties exclusive to StellarProtect (Legacy Mode) Agent.

---

**TABLE 2-2. Properties in the StellarSetup.ini File**

| SECTION | PROPERTY | DEFAULT VALUE | DESCRIPTION |
|---|---|---|---|
| [Shared_license | product_serial_ number<br><br>txone_license_f ile | empty string | The product serial number and license file used for license activation |
| [shared_server] | host<br><br>cert | empy string<br><br>server.crt | StellarOne hostname or IP address<br><br>The certificate filename for communicating with StellarOne |
| [shared_proxy] | host | empy string | FQDN, hostname or IP address of Intranet proxy server |
| | port | empy string | Port number of Intranet proxy server |
| | username | empy string | Username of Intranet proxy server, required only |

| Section | Property | Default Value | Description |
|---|---|---|---|
| | | | when the proxy server is configured to authenticate by username and password. |
| | password | empy string | Administrator's password. The password will be required by specific functions, including uninstallation, the command line interface, and support tools. |
| [shared_install] | silent | 0 | Execute installation in silent mode. Possible values: |
| | password | empy string | • 0: Do not use silent mode<br><br>• 1: Use silent mode<br><br>⚠️ **Important**<br>To install in silent mode, you must also specify the password value. For example:<br>`password=P@ssW0rd`<br>`silent=1` |
| [protect_server]<br><br>[legacy_server] | port | 9443<br><br>8000 | StellarOne's port for connecting to the StellarProtect or StellarProtect (Legacy Mode) client |
| [protect_listen] | port | 14336 | The client listening port for StellarOne |

| SECTION | PROPERTY | DEFAULT VALUE | DESCRIPTION |
|---|---|---|---|
| `[legacy_listen]` | | | |
| `[protect_update]` `[legacy_update]` | `source` | empy string | component update server link |
| `[protect_config]` `[legacy_config]` | `include` | empty string | Use an installation sample config file to run the silent installation. Choose one of the ways: <br><br>• Specify the file path to the installation sample config file <br><br>• Specify the sample file name and put the file as the top-level file in the installer package <br><br>**Note** <br>Supports only `.yaml` or `.bin` file format |
| `[protect_install]` | `asset_vendor` | empty string | The vendor's name of the asset. |
| | `asset_model` | empty string | The model name of the asset. |
| | `asset_location` | empty string | The physical location of the asset. |
| | `asset_description` | empty string | The description for the asset. |
| | `install_location` | empty string → default install path | The installation path of the StellarProtect installer. |

| Section | Property | Default Value | Description |
|---|---|---|---|
| | | `C:\Program Files\TXOne` (Default install path is decided in MSI installer | |
| | `enable_start_me nu` | `1` | Enable StellarProtect in the Windows start menu. |
| | `enable_desktop_ icon` | `1` | Enable StellarProtect icon to be placed on the desktop. |
| | `enable_systray_ icon` | `1` | Enable StellarProtect in the Windows system tray. |
| | `enable_trusted_ ics_cert` | `1` | Allow the installer to install ICS code signing certificates during installation. |
| | `enable_prescan` | `1` | Enable malware scan during installation. |
| | `enable_lockdown _al_building` | `1` | Enable the building of Approved List for Application Lockdown. |
| | `enable_lockdown _detection` | `1` | Enable the "detect" mode of Application Lockdown. |
| `[protect_prescan]` | `action` | `1` | 0: None 1: Quarantine |
| | `background` | `0` | 1: only executes when the sytem is in idle status 0: always consumes CPU resource for executing prescan |

| Section | Property | Default Value | Description |
|---------|----------|---------------|-------------|
| | cpu_usage_mode | 0 | 0: Normal (Single thread scan) <br><br> 1: HIGH (Multi-thread scan |
| [protect_client] | import_source | empty string | Use an agent settings sample config file to import the same settings to the target agents. <br><br> Specify the path to the folder containing the config file to be imported, e.g., C:\txsp_config |
| [legacy_Property] | PRESCAN | 1 | Prescan the endpoint before installing StellarProtect (Legacy Mode). Possible values: <br><br> • 0: Do not prescan the endpoint <br><br> • 1: Prescan the endpoint |
| | WEL_SIZE | 10240 | Windows Event Log size (KB). Possible values: Positive integer <br><br> **Note** <br> Default value for new installations. Upgrading StellarProtect (Legacy Mode) does not change any user- defined WEL_SIZE values set in the previous installation. |

| Section | Property | Default Value | Description |
|---|---|---|---|
| | WEL_RETENTION | 0 | Windows Event Log option when maximum event log size is reached on Windows Event Log. Possible values: |
| | | | For Windows XP or earlier platforms: |
| | | | • 0: Overwrite events as needed |
| | | | • 1~365: Overwrite events older than (1~365) days |
| | | | • -1: Do not overwrite events (clear logs manually) |
| | | | For Windows Vista or later platforms: |
| | | | • 0: Overwrite events as needed (oldest events first) |
| | | | • 1: Archive the log when full, do not overwrite events. |
| | | | • -1: Do not overwrite events (clear logs manually) |
| | WEL_IN_SIZE | 10240 | Windows Event Log size for Integrity Monitor events (KB). Possible values: Positive integer |
| | WEL_IN_RETENTION | 0 | Windows Event Log option for when maximum event log size for Integrity |

| Section | Property | Default Value | Description |
|---------|----------|---------------|-------------|
| | | | Monitor events is reached in the Windows Event Log. |
| | | | For Windows XP or earlier platforms: |
| | | | • 0: Overwrite events as needed |
| | | | • 1~365: Overwrite events older than (1~365) days |
| | | | • -1: Do not overwrite events (clear logs manually) |
| | | | For Windows Vista or later platforms: |
| | | | • 0: Overwrite events as needed (oldest events first) |
| | | | • 1: Archive the log when full, do not overwrite events. |
| | | | • -1: Do not overwrite events (clear logs manually) |
| | USR_DEBUGLOG_ENABLE | 1 | Enable debug logging for user sessions. Possible values: <br>• 0: Do not log <br>• 1: Log |
| | USR_DEBUGLOGLEVEL | 256 | The number of debug log entries allowed for user sessions |

| Section | Property | Default Value | Description |
|---|---|---|---|
| | `SRV_DEBUGLOG_EN ABLE` | `1` | Enable debug logging for service sessions. Possible values:<br><br>• 0: Do not log<br><br>• 1: Log |
| | `SRV_DEBUGLOGLEV EL` | `256` | The number of debug log entries allowed for service sessions |
| | `FW_USR_DEBUGLOG _ENABLE` | 0 | Enable debug log in user session of firewall. Possible values:<br><br>• 0: Disable debug log<br><br>• 1: Enable debug log |
| | `FW_USR_DEBUGLOG _LEVEL` | 273 | Debug level in user session of firewall. Possible values: number |
| | `FW_SRV_DEBUGLOG _ENABLE` | 0 | Enable debug log in service session of firewall. Possible values:<br><br>• 0: Disable debug log<br><br>• 1: Enable debug log |
| | `FW_SRV_DEBUGLOG _LEVEL` | 273 | Debug level in service session of firewall. Possible values: number |
| | `BM_SRV_DEBUGLOG _ENABLE` | 0 | Enable debug log of Behavior Monitoring Core service. Possible values:<br><br>• 0: Disable debug log<br><br>• 1: Enable debug log |

| Section | Property | Default Value | Description |
|---------|----------|---------------|-------------|
| | BM_SRV_DEBUGLOG_LEVEL | 51 | Debug level of Behavior Monitoring Core service |
| | INTEGRITY_MONITOR | 0 | Enable Integrity Monitor. Possible values:<br>• 0: Disable<br>• 1: Enable |
| | PREDEFINED_TRUSTED_UPDATER | 0 | Enable Predefined Trusted Updater. Possible values:<br>• 0: Disable<br>• 1: Enable |
| | WINDOWS_UPDATE_SUPPORT | 0 | Enable Windows Update Support. Possible values:<br>• 0: Disable<br>• 1: Enable |
| | STORAGE_DEVICE_BLOCKING | 0 | Blocks storage devices, including CD/DVD drives, floppy disks,and USB devices, from accessing managed endpoints. Possible values:<br>• 0: Allow access from storage devices<br>• 1: Block access from storage devices |
| | INIT_LIST | 0 | Initialize the Approved List during installation. Possible values:<br>• 0: Do not initialize the Approved list During installation |

| Section | Property | Default Value | Description |
|---|---|---|---|
| | | | • 1: Initialize the Approved List during installation <br><br> ---<br> 📝 **Note** <br> `LIST_PATH` has priority over `INIT_LIST`. For example: If <br><br> `LIST_PATH = liststore.db` and <br><br> `INIT_LIST=1` <br><br> `liststore.db` is imported and `INIT_LIST` is ignored. |
| | `LOCKDOWN` | 0 | Turn Application Lockdown on after installation. Possible values: <br><br> • 0: Turn off Application Lockdown <br><br> • 1: Turn on Application Lockdown |
| | `FILELESS_ATTACK _PREVENTION` | 0 | Enable the Fileless Attack Prevention feature. Possible values: <br><br> • 0: Disable <br><br> • 1: Enable |
| | `SERVICE_CREATIO N_PREVENTION` | 0 | Enable the Service Creation Prevention feature. Possible values: |

| Section | Property | Default Value | Description |
|---------|----------|---------------|-------------|
|         |          |               | • 0: Disable<br>• 1: Enable |

| Section | Property | Default Value | Description |
|---------|----------|---------------|-------------|
| | | | **Note**<br>StellarProtect (Legacy Mode) temporarily disables the Service Creation Prevention feature under the following conditions:<br><br>• Updating or installing new applications using installers allowed by Trusted Updater. The feature is automatically re-enabled after the Trusted Updater process is complete<br><br>• Enabling Windows Update Support<br><br>• Disabling Windows Update Support automatically re-enables the feature |
| | `INTELLIGENT_RUN TIME_LEARNING` | 0 | The agent will allow runtime execution files |

| Section | Property | Default Value | Description |
|---|---|---|---|
| | | | that are generated by applications in the Approved |
| | | | List. Possible values: |
| | | | • 0: Disable |
| | | | • 1: Enable |
| | NO_DESKTOP | 0 | Create a shortcut |
| | | | on desktop. Possible values: |
| | | | • 0: Create shortcut |
| | | | • 1: Do not create shortcut |
| | NO_STARTMENU | 0 | Create a shortcut in the Start menu. Possible values: |
| | | | • 0: Create shortcut |
| | | | • 1: Do not create shortcut |
| | NO_SYSTRAY | 0 | Display the system tray icon and Windows notifications. Possible values: |
| | | | • 0: Create system tray icon |
| | | | • 1: Do not create system tray icon |
| | CUSTOM_ACTION | 0 | Custom action for blocked events. Possible values: |
| | | | • 0: Ignore |
| | | | • 1: Quarantine |

| Section | Property | Default Value | Description |
|---|---|---|---|
| | | | • 2: Ask server |
| | `MAX_EVENT_DB_SIZE` | `1024` | Maximum database file size (MB). Possible values: Positive integer |
| | `NO_NSC` | `1` | Install firewall for network virus protection. Possible values:<br><br>• 0: Create firewall<br><br>• 1: Do not create firewall |
| | `INIT_LIST_EXCLUDED_EXTENSION1` | log | Afile extension to exclude from automatic file enumeration for Approved List initialization.<br><br>The configuration applies to the Approved List first initialized and all subsequent Approved List updates.<br><br>Specify multiple extensions by creating new entries with names that start with `INIT_LIST_EXCLUDED_EXTENSION`, while ensuring that each entry name is unique. For example:<br><br>`INIT_LIST_EXCLUDED_EXTENSION=bmp`<br><br>`INIT_LIST_EXCLUDED_EXTENSION2=png` |
| | `INIT_LIST_EXCLUDED_EXTENSION2` | txt | |
| | `INIT_LIST_EXCLUDED_EXTENSION3` | ini | |

| Section | Property | Default Value | Description |
|---|---|---|---|
| | | | **Note** |
| | | | Specifying file extensions of executable files (e.g., exe, dll and sys) may cause issues with Application Lockdown. |
| [legacy_Prescan] | PRESCANCLEANUP | 2 | Attempt to clean detected files during prescan. Possible values: |
| | | | • 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 is unsuccessful |
| | IGNORE_THREAT | 2 | Cancel installation after detecting malware threat during prescan. Possible values: |
| | | | • 0: Cancel |
| | | | • 1: Continue installation after detecting malware threat during prescan |
| | | | • 2: Continue installation when no |

| SECTION | PROPERTY | DEFAULT VALUE | DESCRIPTION |
|---------|----------|---------------|-------------|
| | | | malware is detected, or after all detected malware is cleaned, deleted, or quarantined successfully without a system reboot |
| | `REPORT_FOLDER` | empy string | Anabsolute folder path where prescan result reports are saved. Possible values:<br><br>• <folder_path><br><br>• <empty>: Defaults to `%windir%\temp \prescan\log` |
| | `SCAN_TYPE` | Full | The type of scan executed during silent installation. Possible values:<br><br>• Full: Scan all folders on the endpoint<br><br>• Quick: Scans the following folders:<br><br>  • Fixed root drives, e.g.,<br><br>    `c:\`<br><br>    `d:\`<br><br>  • System root folder, e.g.,<br><br>    `c:\Windows`<br><br>  • System folder, e.g., |

| Section | Property | Default Value | Description |
|---------|----------|---------------|-------------|
|         |          |               | `c:\Windows \System` |
|         |          |               | • System32 folder, e.g., |
|         |          |               | `c:\Windows \System32` |
|         |          |               | • Driver folder, e.g., |
|         |          |               | `c:\Windows \System32\Dri vers` |
|         |          |               | • Temp folder, e.g., |
|         |          |               | `c:\Users \Trend \AppData \Local\Temp` |
|         |          |               | • Desktop folder including sub folders and files, e.g., |
|         |          |               | `c:\Users \Trend \Desktop` |
|         |          |               | • Specific: Scan folders specified with `SPECIFIC_FOLD ER` entries |

| Section | Property | Default Value | Description |
|---|---|---|---|
| | | | **Note**<br>The selected valueis used as the default value for a UI installation |
| | COMPRESS_LAYER | 2 | The number of compressed layers to scan when a compressed file is scanned. Possible values:<br><br>• 0: Do not scan compressed files<br><br>• 1~20: Scan up to the specified number of layers of a compressed file |
| | MAX_FILE_SIZE | 0 | The largest file allowed for scan<br><br>• 0: Scan files of any sizes<br><br>• 1~9999: Only scan files equal to or smaller than the specified size (MB) |
| | SCAN_REMOVABLE_DRIVE | 0 | Scan removable drives. Possible values:<br><br>• 0: Do not scan removable drives<br><br>• 1: Scan removable drives |
| | FORCE_PRESCAN | 0 | Perform a prescan before installation. Possible values: |

| Section | Property | Default Value | Description |
|---|---|---|---|
| | | | • 0: Disable |
| | | | • 1: Enable |
| [legacy_BlockNotification]<br><br>⚠ **Important**<br>To enable this feature, make sure to also enable the display for system tray icons and notifications. See NO_SYSTRAY in this table for details. | ENABLE | 0 | Display notifications on managed endpoints when StellarProtect (Legacy Mode) blocks an unapproved file. Possible values:<br>• 0: Disable<br>• 1: Enable |
| | ALWAYS_ON_TOP | 1 | Display the file blocking notification on top of other screens. Possible values:<br>• 0: Disable<br>• 1: Enable |
| | SHOW_DETAILS | 1 | Display file name, file path, and event time in the notification. Possible values:<br>• 0: Disable<br>• 1: Enable |
| | AUTHENTICATE | 1 | Authenticate the user by requesting the administrator password when closing a notification. Possible values:<br>• 0: Disable<br>• 1: Enable |
| | TITLE | empty string | Notification title |

| SECTION | PROPERTY | DEFAULT VALUE | DESCRIPTION |
|---|---|---|---|
| | | | Possible values: <notification_title> |
| | MESSAGE | empty string | Notification content<br><br>Possible values: <notification_content> |
| [legacy_EventLog] | Enable | 1 | Log events related to StellarProtect (Legacy Mode). Possible values:<br><br>• 1: Log<br><br>• 0: Do not log |
| | Level_WarningLog | 1 | Log "Warning" level events related to StellarProtect (Legacy Mode). Possible values:<br><br>• 1: Log<br><br>• 0: Do not log |
| | Level_InformationLog | 0 | Log "Information" levelevents related to StellarProtect (Legacy Mode). Possible values:<br><br>• 1: Log<br><br>• 0: Do not log |
| | BlockedAccessLog | 1 | Log files blocked by StellarProtect (Legacy Mode). Possible values:<br><br>• 1: Log<br><br>• 0: Do not log |
| | ApprovedAccessLog | 1 | Logfiles approved by StellarProtect (Legacy Mode). Possible values: |

| Section | Property | Default Value | Description |
|---|---|---|---|
| | | | • 1: Log<br>• 0: Do not log |
| | ApprovedAccessLog_TrustedUpdater | 1 | Log Trusted Updater approved access. Possible values:<br>• 1: Log<br>• 0: Do not log |
| | ApprovedAccessLog_DllDriver | 0 | Log DLL/Driver approved access. Possible values:<br>• 1: Log<br>• 0: Do not log |
| | ApprovedAccessLog_ExceptionPath | 1 | Log Application Lockdown exception path approved access. Possible values:<br>• 1: Log<br>• 0: Do not log |
| | ApprovedAccessLog_TrustedCert | 1 | Log Trusted Certificates approved access. Possible values:<br>• 1: Log<br>• 0: Do not log |
| | ApprovedAccessLog_WriteProtection | 1 | LogWrite Protection approved access. Possible values:<br>• 1: Log<br>• 0: Do not log |
| | ApprovedAccessLog_TrustedHash | 1 | Log Trusted Hash approved access. Possible values: |

| Section | Property | Default Value | Description |
|---------|----------|---------------|-------------|
| | | | • 1: Log<br><br>• 0: Do not log |
| | SystemEventLog | 1 | Log events related to the system. Possible values:<br><br>• 1: Log<br><br>• 0: Do not log |
| | SystemEventLog_ExceptionPath | 1 | Log exceptions to Application Lockdown. Possible values:<br><br>• 1: Log<br><br>• 0: Do not log |
| | SystemEventLog_WriteProtection | 1 | Log Write Protection events. Possible values:<br><br>• 1: Log<br><br>• 0: Do not log |
| | ListLog | 1 | Log events related to the Approved list. Possible values:<br><br>• 1: Log<br><br>• 0: Do not log |
| | UsbMalwareProtectionLog | 1 | Log events that trigger USB Malware Protection. Possible values:<br><br>• 1: Log<br><br>• 0: Do not log |
| | ExecutionPreventionLog | 1 | Log events that trigger Execution Prevention. Possible values: |

| Section | Property | Default Value | Description |
|---|---|---|---|
| | | | • 1: Log<br>• 0: Do not log |
| | `NetworkVirusProtectionLog` | 1 | Log events that trigger Network Virus Protection. Possible values:<br>• 1: Log<br>• 0: Do not log |
| | `IntegrityMonitoringLog_FileCreated` | 1 | Log file and folder created events. Possible values:<br>• 1: Log<br>• 0: Do not log |
| | `IntegrityMonitoringLog_FileModified` | 1 | Log file modified events. Possible values:<br>• 1: Log<br>• 0: Do not log |
| | `IntegrityMonitoringLog_FileDeleted` | 1 | Log file and folder deleted events. Possible values:<br>• 1: Log<br>• 0: Do not log |
| | `IntegrityMonitoringLog_FileRenamed` | 1 | Log file and folder renamed events. Possible values:<br>• 1: Log<br>• 0: Do not log |
| | `IntegrityMonitoringLog_RegValueModified` | 1 | Log registry value modified events. Possible values:<br>• 1: Log |

| Section | Property | Default Value | Description |
|---|---|---|---|
| | | | • 0: Do not log |
| | `IntegrityMonito ringLog_RegValu eDeleted` | 1 | Log registry value deleted events. Possible values:<br><br>• 1: Log<br><br>• 0: Do not log |
| | `IntegrityMonito ringLog_RegKeyC reated` | 1 | Log registry key created events. Possible values:<br><br>• 1: Log<br><br>• 0: Do not log |
| | `IntegrityMonito ringLog_RegKeyD eleted` | 1 | Log registry key deleted events. Possible values:<br><br>• 1: Log<br><br>• 0: Do not log |
| | `IntegrityMonito ringLog_RegKeyR enamed` | 1 | Log registry key renamed events. Possible values:<br><br>• 1: Log<br><br>• 0: Do not log |
| | `DeviceControlLo g` | 1 | Log events related to device access control. Possible values:<br><br>• 1: Log<br><br>• 0: Do not log |
| `[legacy_Maintenanc eMode]` | `ENABLE_DURATION` | 0 | Start maintenance mode with this duration immediately after the install process is finished. Possible values:<br>0- 999 |

| Section | Property | Default Value | Description |
|---------|----------|---------------|-------------|
| | | | Unit: Hours |
| | SCAN | 0 | Enable file scanning after the maintenance period. Possible values: |
| | | | •     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 |
| [legacy_Message] | INITIAL_RETRY_INTERVAL | 120 | 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_ITERVAL value |

| Section | Property | Default Value | Description |
|---|---|---|---|
| | | | Possible values: 0~2147483647 |
| | MAX_RETRY_INTERVAL | 7680 | Maximum interval, in seconds, between attempts to resend events to StellarOne<br><br>Possible values: 0~2147483647 |
| [legacy_MessageRandomization]<br><br>───────<br>📝 **Note**<br>StellarProtect (Legacy Mode) agents respond as soon as possible to direct requests from StellarOne. For details, refer to Applying Message Time Groups in the StellarProtect (Legacy Mode) Administrator's Guide<br>─────── | TOTAL_GROUP_NUM | 1 | Number of groups controlled by the server. Possible values:<br><br>0~2147483646 |
| | OWN_GROUP_INDEX | 0 | Index of group which this agent belongs to. Possible values:<br><br>0~2147483646 |
| | TIME_PERIOD | 0 | Maximum amount of time agents have to upload data (in seconds). Possible values:<br><br>0~2147483647 |

**StellarProtect (Legacy Mode) Hidden Properties**

For StellarProtect (Legacy Mode), hidden properties that require users to manually add in the corresponding section are listed in the table below:

| Section | Property | Default Value | Description |
|---|---|---|---|
| [legacy_Property ] | CONFIG_PATH | empty string | The file path to the sample config file for agent feature settings |
| | LIST_PATH | empty string | The file path to the Approved List used to import agent feature settings |
| | APPLICATION FOLDER | empty string | The installation path for agent program |
| | QUARANTINE_ FOLDER_PATH | empty string | The quarantine path for agent program |
| | INIT_LIST_PATH | empty string | A folder path to be traversed for the Approved List initialization. Each local disk's root directory will be traversed if empty. |
| | INIT_LIST_PATH_O PTIONAL | empty string | A folder path to be traversed for the Approved List initialization. Each local disk's root directory will be traversed if empty. |
| | INIT_LIST_E XCLUDED_FOLDER | empty string | An absolute folder path to exclude from automatic file 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 |

| Section | Property | Default Value | Description |
|---|---|---|---|
| | | | `INIT_LIST_EXCLUDED_FOLDER`<br><br>Ensure each entry name is unique. For example:<br><br>`INIT_LIST_EXCLUDED_FOLDER= c:\folder1`<br><br>`INIT_LIST_EXCLUDED_FOLDER2 =c:\folder2`<br><br>`INIT_LIST_EXCLUDED_FOLDER3 =c:\folder3`<br><br>Possible values<br><br>• Folder path supports a maximum length of 260 characters.<br><br>• Folder paths that do not exist may be specified.<br><br>• The exclusion applies to subfolders. |
| | `ALLOW_NON_MASS_STORAGE_USB_DEVICE` | 0 | 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 enabled.<br><br>Possible values:<br><br>• 0: Disable (Default)<br><br>• 1: Enable |
| `[legacy_AGENT]` | `FIXED_IP` | empty string | Set the agent IP address to communcate with the |

| Section | Property | Default Value | Description |
|---|---|---|---|
| | | | StellarProtect (Legacy Mode) server<br><br>Possible values:<br><br>• A.B.C.D/E<br><br>• A, B, C, D: 0~255<br><br>• E: 1~32<br><br>---<br><br>📝 **Note**<br>Ensure that you also input and insert the section title `[legacy_AGENT]` above the `FIXED_IP` line. |
| `[legacy_Prescan]` | `SPECIFIC_FOLDER` | empty string | An absolute folder path to scan when the scan type is set `[Specific]`<br><br>Possible values:<br><br><folder_path><br><br>Multiple folders can be specified by creating new entries whose name starting with `SPECIFIC_FOLDER`<br><br>Every entry name needs to be unique. For example:<br><br>SPECIFIC_FOLDER=c:\folder1<br><br>SPECIFIC_FOLDER2=c:\folder2 |

| Section | Property | Default Value | Description |
|---------|----------|---------------|-------------|
| | | | `SPECIFIC_FOLDER3=c:\folder3` |
| | `EXCLUDED_FILE` | empty string | An absolute file path to exclude from scanning Possible values: <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` |
| | `EXCLUDED_FOLDER` | empty string | An absolute folder path to exclude from scanning <folder_path> Multiple folders can be specified by creating new entries whose name starting with `EXCLUDED_FOLDER` Every entry name needs to be unique For example: |

| Section | Property | Default Value | Description |
|---------|----------|---------------|-------------|
| | | | `EXCLUDED_FOLDER=c:\file1` |
| | | | `EXCLUDED_FOLDER2=c:\file2` |
| | | | `EXCLUDED_FOLDER3=c:\file3` |
| | `EXCLUDED_EXTENSION` | empty string | A file extensiont o exclude from scanning |
| | | | <file_extension> |
| | | | Multiple extensions can be specified by creating new entries whose name starting with `EXCLUDED_EXTENSION` |
| | | | Every entry name needs to be unique |
| | | | For example: |
| | | | `EXCLUDED_EXTENSION=bmp` |
| | | | `EXCLUDED_EXTENSION2=png` |

## Executing Silent Installation

After defining the setup configuration file, execute the silent installation on the endpoint.

**Procedure**

1. If the Agent installer package is downloaded from StellarOne, within the `StellarSetup.ini` config file, the values of the `product_serial_number` and `txon_license_env` should be automatically generated. Please specify password and set the `silent`

value to `1` in the configuration file. If you would like to manage the agent using StellarOne, please configure the server session host value with the server IP address.

> **Note**
>
> For standalone agents, refer to *Standalone Agent Sample Config File for Silent Installation on page 2-25* for more details.

2. Place the defined `StellarSetup.ini` file in the installation package.

3. Choose one of the methods to launch the `StellarSetup.exe` installer.

   - For a silent installation with a GUI, double-click the installer `StellarSetup.exe`.

   - For a silent installation without any GUI, use the command prompt to execute `StellarSetup.exe` with the argument `-s`, e.g., type `C:\package>StellarSetup.exe -s`

     Please note that with this method, the message box mentioned in the following steps will not be shown. To view information related to the installation, check logs filed under `C:\Windows\Temp \StellarProtect`.

4. After the installation is complete, the **StellarProtect (Legacy Mode) has been successfully installed** message box will appear. Click **Finish**.

5. Run StellarProtect (Legacy Mode) and log on with the configured password.

6. After successfully logging on StellarProtect (Legacy Mode), the **Overview** window will be displayed.

## License Activation for Standalone Agent

This section describes the license activation procedures during the installation process for standalone StellarProtect (Legacy Mode) agents.

**Procedure**

1.  Launch the agent's Installer and go through the procedures until the **Administrator Password & License Activaiton** window appears. After inputing and confirming the administrator password, click the **New License** button.
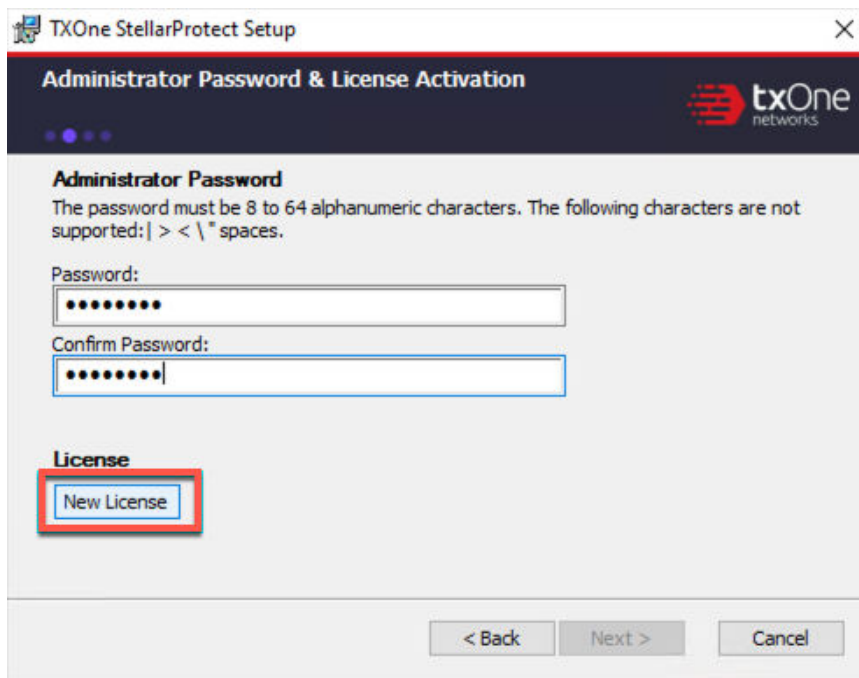


**FIGURE 2-20. License Activation - New License Button**

2.  A pop-up **License Activation** window appears. Choose one of the ways to activate the license based on the license data available from your support provider:
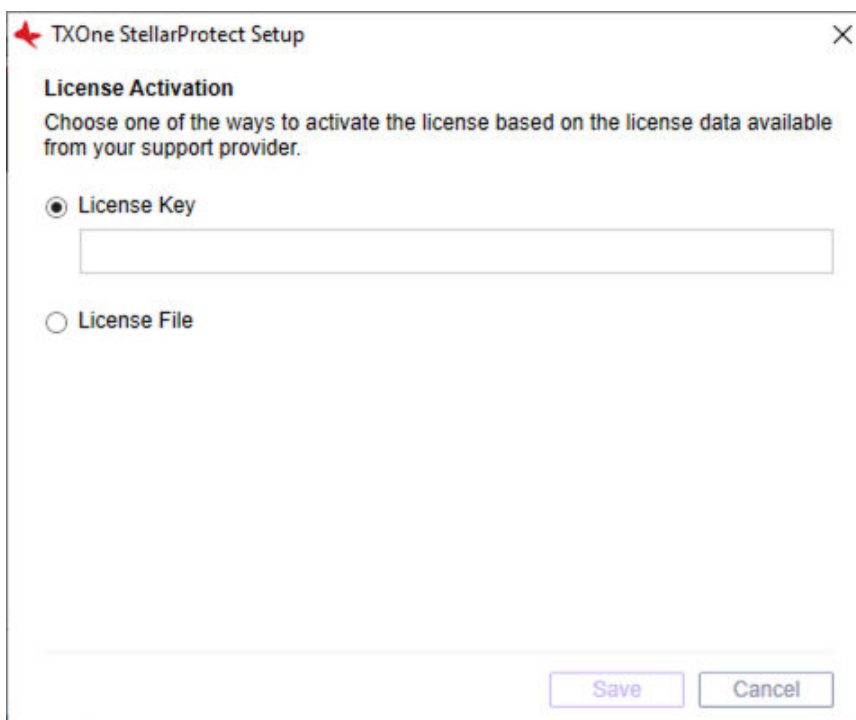
**FIGURE 2-21. License Activation - License Key or License File**

- Click **License Key**

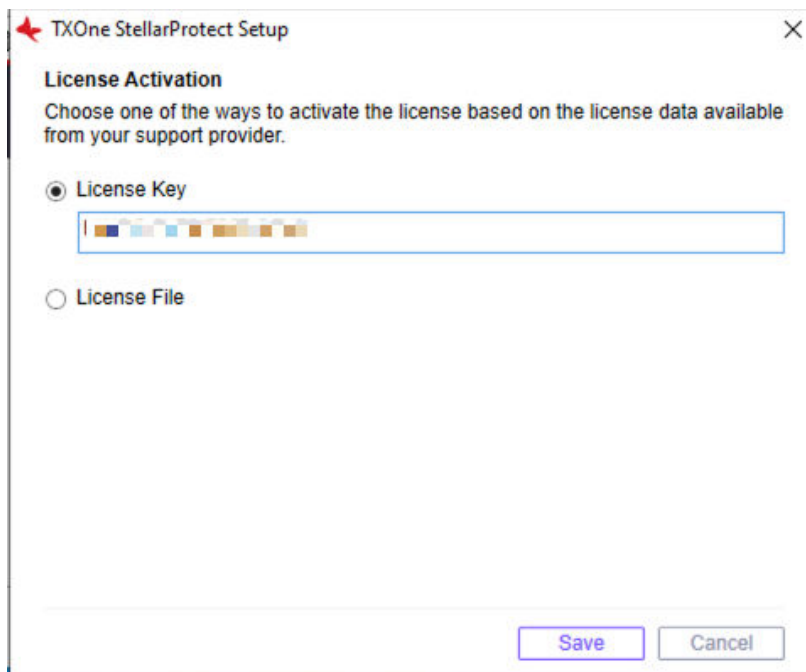    - Specify the License Key in the text field.

        > 📝 **Note**
        >
        > If the agent's installer package is downloaded from StellarOne, the License Key will be automatically generated. Check if it matches the license data provided by your support provider.

- Click **Save**.
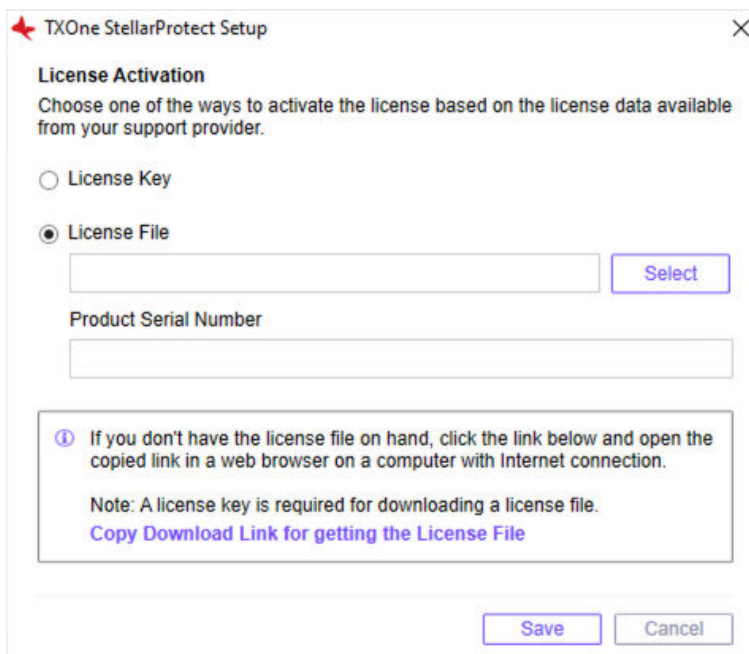
**FIGURE 2-22. License Activation - License Key**

- Click **License File**

  - Select the License File (an .txt file) to import.

  - Specify the Product Serial Number in the text field.

    > **Note**
    >
    > If you don't have the License File and Product Serial Number on hand, refer to *Getting the License File and PSN for Standalone Agents on page 2-69* for detailed instructions.

  - Click **Save**.

**FIGURE 2-23. License Activation - License File**

---

> 📝 **Note**
>
> If a license file expiration error message appears and the agent's installer package was downloaded from StellarOne, you should get the latest License File and Product Serial Number from StellarOne. Refer to *Getting the Latest License File from StellarOne on page 2-76*

---

3. A success message indicating valid license appears. Click **Next** to proceed to next procedure (**Step 8** in *Attended Installation on page 2-5*) for the installation.

## Getting the License File and PSN

This section describes two methods to get the license file and PSN (product serial number):

- *Getting the License File and PSN for Standalone Agents on page 2-69*

- *Getting the Latest License File from StellarOne on page 2-76*

### Getting the License File and PSN for Standalone Agents

To activate license for certain standalone agents, follow the instructions below.

**Procedure**

1. Open the URL: https://mytxone.cs.txone.com/license/activate/txone/stellar in a web browser on a computer with Internet connection.

   > **Note**
   >
   > This URL can also be obtained during the GUI installation process. Refer to *About the Download Link for Getting License File in GUI Installation on page 2-72* for more details.

   > **Important**
   >
   > A license key is required for downloading a license file.

2. You will be directed to the **License File Management** web page. Specify your license key in the **License Key** field.

**FIGURE 2-24. License File Management**

3. Click **SUBMIT**.

4. The **License File Info** pop-up window appears showing the license information. Check if the information listed matches the license data provided by your support provider.

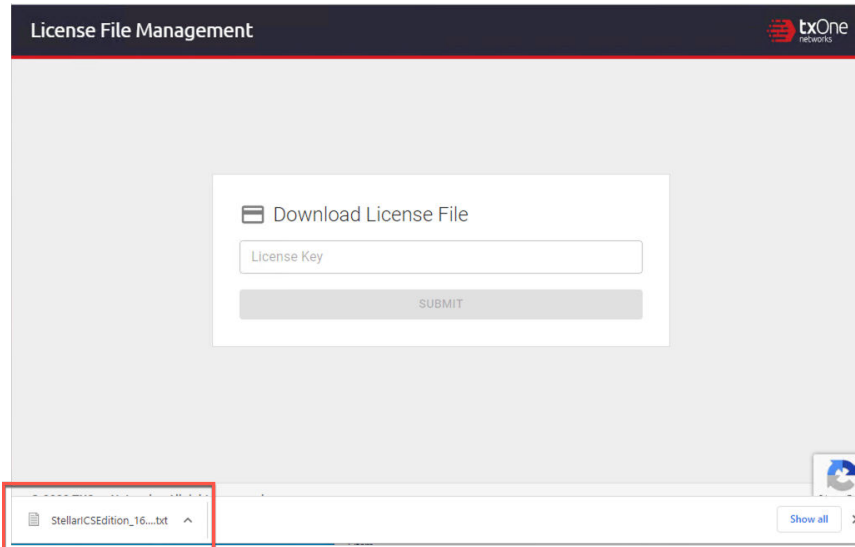5. Click the copy icon to copy and save the **Product Serial Number** for later use.

**FIGURE 2-25. License Information**

> **Important**
>
> The **Product Serial Number** is required for license activation by importing a license file. Ensure that you save it for later use.

**6.** Click **Download** for downloading the license file (a .txt file).
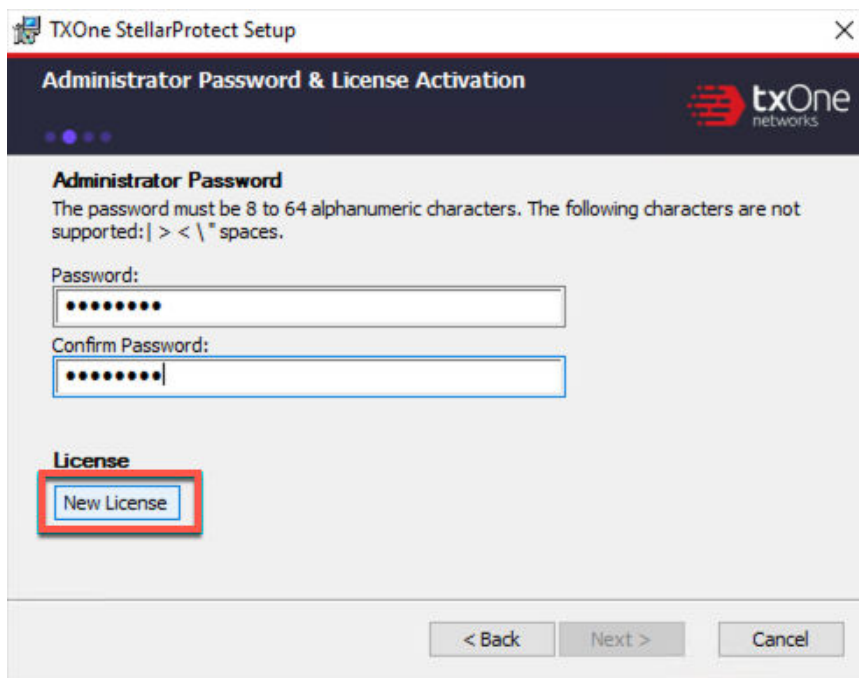


**FIGURE 2-26. License File Downloaded**

> **Note**
>
> Please find the license file in the downloads folder.

### About the Download Link for Getting License File in GUI Installation

If needed, users can also copy the URL of TXOne **License File Management** web page during the GUI installation process.

**Procedure**

1.  Launch the agent's GUI Installer and go through the procedures until the **Administrator Password & License Activation** window appears. After specifying the administrator password, click the **New License** button.



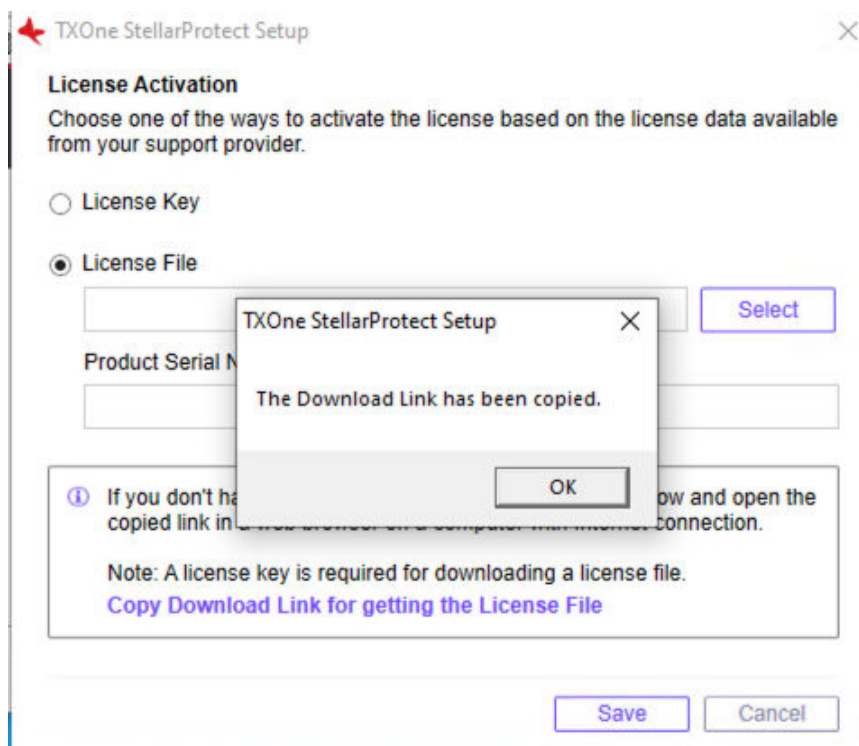**FIGURE 2-27. License Activation - New License Button**

2.  A pop-up **License Activation** window appears. Select **License File**.

3.  Click **Copy Download Link for getting the License File** at the bottom of the **License Activation** window.
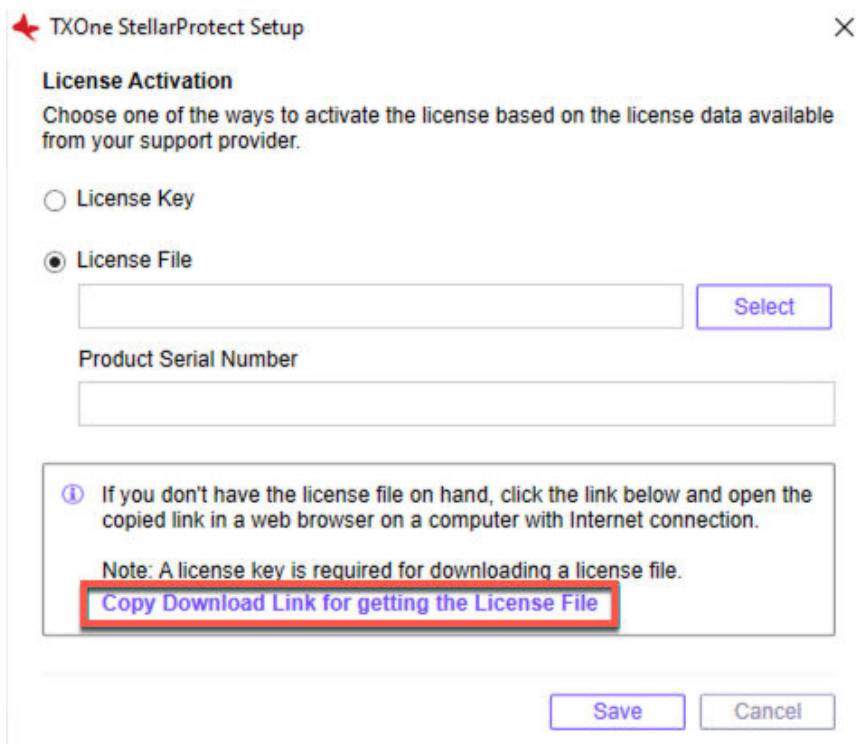
**FIGURE 2-28. Copy the Download Link**

4.  **The Download Link has been copied** message appears.

**FIGURE 2-29. Download Link Copied**

**5.** Open the copied link in a web browser on a computer with Internet connection. You will be directed to TXOne **License File Management** web page.
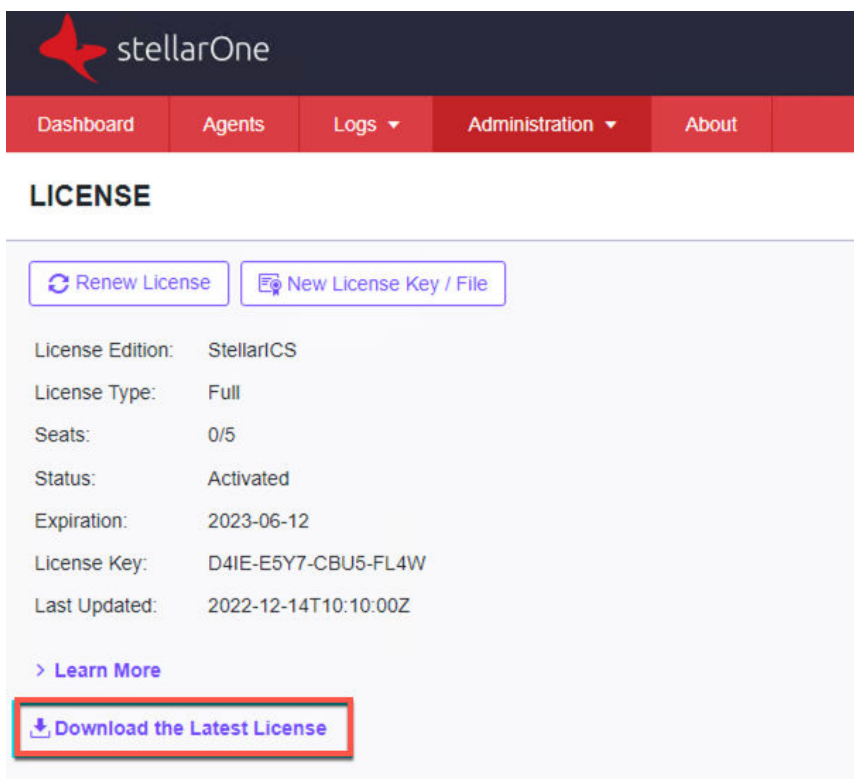
> **Note**
>
> Refer to *Getting the License File and PSN for Standalone Agents on page 2-69* for instructions on how to get the license file from TXOne **License File Management** website.

## Getting the Latest License File from StellarOne

When you use a license file for activating certain agents with the installer package downloaded from StellarOne, if a license expiration error message appears, follow the instructions below to get the latest license file and PSN (Product Serial Number) from StellarOne.

**Procedure**

1. To get the latest license file, go to StellarOne **Administration** > **License**.

2. Click **Download the latest license file** at the bottom of the **License** page.



**FIGURE 2-30. Download lLcense File from StellarOne**

3. The license file (a `.txt` file) has been downloaded to your Downloads folder.

4. To get the PSN, go to StellarOne **About** page.

5. Find and copy the product serial number.
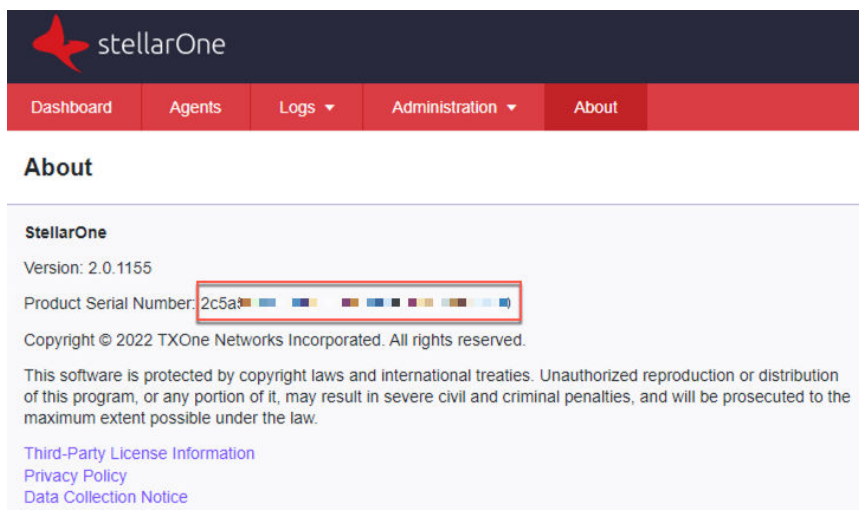


**FIGURE 2-31. Get Product Serial Number from StellarOne**

# Replicating Installation for Multiple Standalone Agents

This section introduces a more efficient method to replicate installation for multiple standalone agents with the same license file and product serial number.

**Procedure**

1. Refer to *Getting the License File and PSN for Standalone Agents on page 2-69* for getting the license file and product serial number.

2. Place the license file as the top-level file in the agent's Installer Package.

3. Prepare your `StellarSetup.ini` as mentioned in *Standalone Agent Sample Config File for Silent Installation on page 2-25*

> 📝 **Note**
>
> Ensure that you specify the product serial number and license file name in the config file.

4. Save the Installer Package in the target endpoints for installation.

5. Launch the Installer in silent mode.

# Encrypting Config File for Installation

StellarProtect (Legacy Mode) supports encrypting the configuration file for installation to prevent sensitive data leakage. The encrypted configuration file name is fixed to `StellarSetup.bin`.

**Procedure**

1. Prepare your `StellarSetup.ini` as mentioned in *Silent Installation on page 2-24*.

2. Encrypt `StellarSetup.ini` by using the command prompt: `StellarSetup.exe -e <CONFIG_FILE>`. The parameter `-e` is used for encrypting the configuration file and generating `StellarSetup.bin` file in the working directory.

3. After the `StellarSetup.bin` file is generated, place it as the top-level file in the installer package.

> 📝 **Note**
>
> For security reasons, the original `StellarSetup.ini` file can be removed from the installer package since the encrypted setup file (`StellarSetup.bin`) can replace it now.

**4.** The installation with encrypted configuration can now be executed.

# 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 StellarOne central management console server. To manually deploy a single configuration to multiple **Standalone** agents, use an agent configuration file.

---

> **Note**
>
> To import a sample config file to multiple agents without using the GUI, add the CONFIG_PATH property with its value specified (the file path to the sample config file) in the StellarSetup.ini file. Refer to *Properties in the Config File for Silent Installation on page 2-33* for more details.

---

**Procedure**

1. Open the TXOne StellarProtect (Legacy Mode) console using the desktop icon (if available) 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**.

     ---

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

     ---

   - 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**.

4.    StellarProtect (Legacy Mode) overwrites the existing configuration settings with the 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.

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 web console. The **Agent** management screen appears.

2.    Select the target endpoint(s).

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**.

5.    A **Command Deployment** window appears showing the exports status.

6.    Click **Download** 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. Fromt he 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

# Uninstalling StellarProtect

Follow the instructions to uninstall StellarProtect (Legacy Mode).

> **Note**
>
> StellarProtect (Legacy Mode)'s administrator password is required to uninstall StellarProtect (Legacy Mode) from an endpoint.

> **Important**
>
> Please make sure the StellarProtect (Legacy Mode) UI is not open.

**Procedure**

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

2. Follow one of the procedures listed below according to your operating system:

| OPERATING SYSTEM | PROCEDURE |
|---|---|
| • Windows 10 Professional<br><br>• Windows 10 Enterprise<br><br>• Windows 10 IoT Enterprise | a. Go to **Start** > **Settings**.<br><br>b. Depending on your version of Windows 10, locate the **Apps & Features** section under one of the following categories:<br><br>    • **System**<br><br>    • **Apps**<br><br>c. On the left pane, click **Apps & Features**<br><br>d. In the list, click **StellarProtect (Legacy Mode)**.<br><br>e. Click **Uninstall**. |
| • Windows 7<br><br>• Windows 8<br><br>• Windows Vista<br><br>• Windows Server 2008<br><br>• Windows Server 2012<br><br>• Windows Server 2016<br><br>• Windows Server 2019<br><br>• Windows Storage Server 2012<br><br>• Windows Storage Server 2016 | a. Go to **Start** > **Control Panel** > **Program and Features**<br><br>b. In the list, double-click **TXOne StellarProtect (Legacy Mode)**. |
| • Windows Server 2003<br><br>• Windows XP<br><br>• Windows 2000 | a. Go to **Start** > **Control Panel** > **Add or Removew Programs**<br><br>b. In the list, select **TXOne StellarProtect (Legacy Mode)**.<br><br>c. Click **Remove**. |

**3.** After the StellarProtect (Legacy Mode) Setup opens, click **Next**.

4.   Enter in the StellarProtect (Legacy Mode) administrator password and click **Next**.

5.   Make sure StellarProtect (Legacy Mode)'s UI is completely closed before clicking **OK**.

6.   The message box indicating StellarProtect (Legacy Mode) being successfully removed will appear. Click **Finish**.

# Chapter 5

## License Renewal

This chapter describes how to renew license for standalone StellarProtect (Legacy Mode) agent.

# License Renewal for Standalone Agents

For standalone agents, users can renew license directly on the agent console.

---

📝 **Note**

For StellarProtect (Legacy Mode) agents managed by StellarOne server, please renew license via the StellarOne web console. Refer to <u>StellarOne Administrator's Guide</u> for instructions.

---

**Procedure**

1. Click the **New License** button on the StellarProtect (Legacy Mode) logon screen.
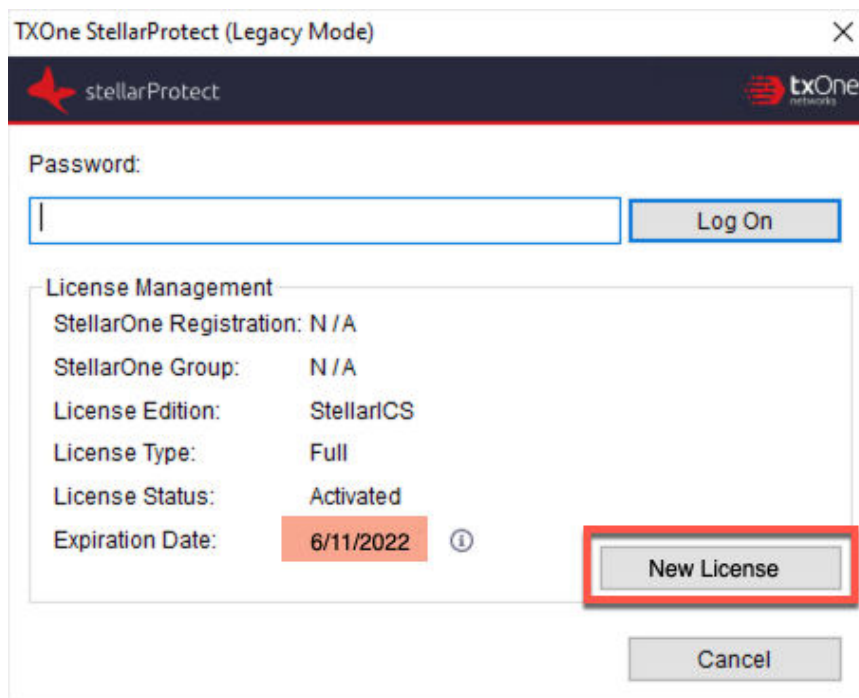
**FIGURE 5-1. Renew License for Standalone Agents**

2. A pop-up **License Activation** window appears. Choose one of the ways to activate the license based on the license data available from your support provider:

- Click **License Key**

  - Specify the License Key in the text field.

  - Click **Save**.
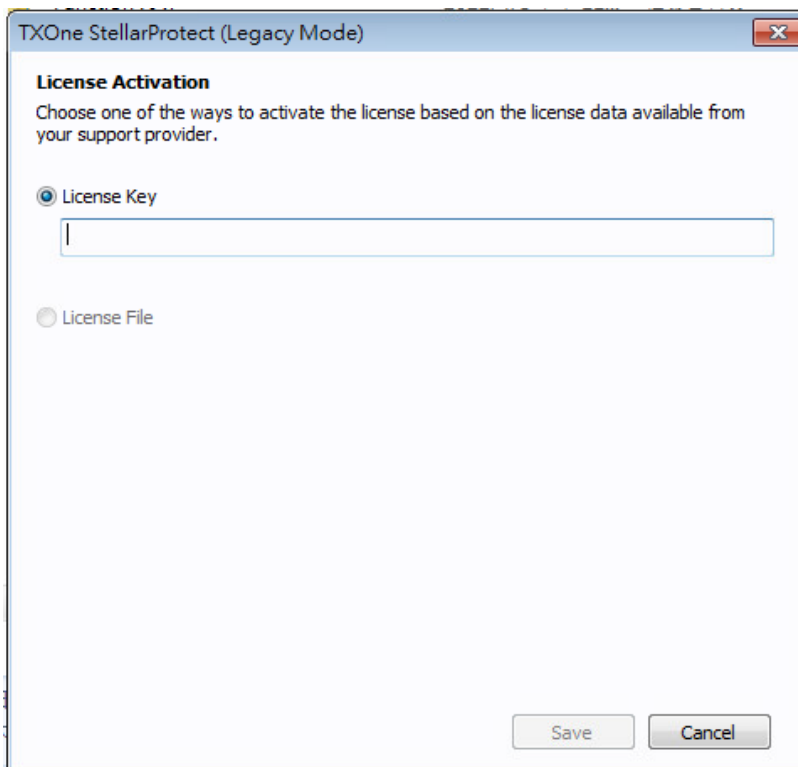
**FIGURE 5-2. Use License Key for Activation**

- Click **License File**

  - Select the License File (an `.txt` file) to import.
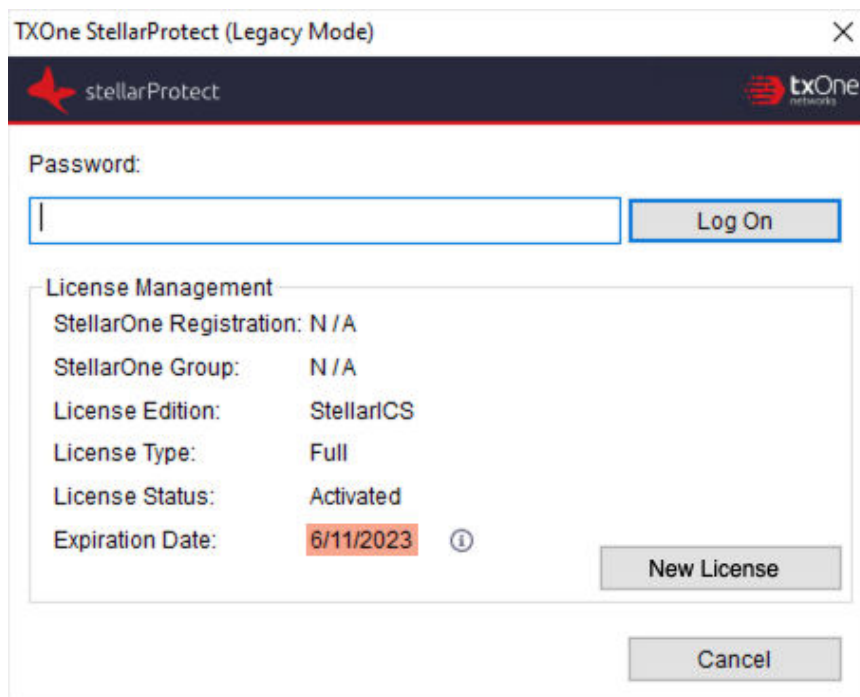
  - Specify the Product Serial Number in the text field.

    ---

    ![Note icon] **Note**

    If you don't have the License File and Product Serial Number on hand, refer to *Getting the License File and PSN for Standalone Agents on page 2-69* for detailed instructions.

    ---

  - Click **Save**.

**3.** Check the StellarProtect (Legacy Mode) logon screen for the updated license expiration date.

**FIGURE 5-3. License Renewed for Standalone Agents**

# Chapter 6

## Technical Support

Support for TXOne 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

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/smb-new-request

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 and TXOne representatives are available by below contact information:

**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://ers.trendmicro.com/

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

http://esupport.trendmicro.com/solution/en-US/1112106.aspx

## File Reputation Services

Gather system information and submit suspicious file content to Trend Micro:

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 Trend Micro.

# 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

txOne
networks

www.**txone**.com