txOne networks | Keep the Operation Running

3.0 TXOne StellarProtect

Installation Guide

Unified agent providing asset lifetime all-terrain protection

Windows

Document Part No.: APEM39736/230619

Release Date: July 2023

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

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, and StellarProtect 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

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

This Installation Guide introduces TXOne StellarProtect ™ and guides administrators through installation and deployment.

Topics in this chapter include:

About the Documentation

TXOne Networks StellarProtect 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.
Administrator's Guide	A PDF document that discusses StellarProtect 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: https://kb.txone.com/ http://success.trendmicro.com

Audience

TXOne StellarProtect ™ documentation is intended for administrators responsible for StellarProtect ™ 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

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

Terminology	Description
server	The StellarOne console server program
agents	The host running the StellarProtect program

Terminology	Description
managed agents managed endpoints	The hosts running the StellarProtect program that are known to the StellarOne server program
target endpoints	The hosts where the StellarProtect ™ managed agents will be installed
Administrator (or StellarProtect administrator)	The person managing the StellarProtect agents
StellarProtect console	The user interface for configuring and managing StellarProtect settings
StellarOne (management) console	The user interface for configuring and managing the StellarProtect agents managed by StellarOne
CLI	Command Line Interface
license activation	Includes the type of StellarProtect 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 agent files. If you accept the default settings during installation, you will find the installation folder at one of the followinglocations:
	
	`C:\Program Files\TXOne\StellarProtect`
	
	`C:\Program Files\TXOne\StellarProtect (Legacy Mode)`

Chapter 1

Introduction

This section introduces TXOne StellarProtect the unified agent, and gives an overview of its functions.

Topics in this chapter include:

About TXOne Stellar

TXOne Stellar provides a context-focused security solution for OT endppoints and cyber-physical systems (CPS), aiming to defend operation stability with continuous detection and response aligned to the specific requirements of the OT domain.

TXOne Stellar platform is composed of the centralized menagement console server and unified agents apt for legacy OT devices and modern cyber-physical systems.

- StellarOne™ , designed to streamline administration of the agents installed on modernized systems and legacy systems, along with its intuitive centralized management, consistent policy enforcement, and action-oriented alerts that empower security teams of all sizes and skill levels to successfully mature their organization's security posture.
- StellarProtect ™ / StellarProtect (Legacy Mode), using the single-agent design that delivers seamless asset-centric protection and ensures coverage for modern CPS and legacy OT devices throughout their entire asset lifecycle. The lightweight unified agent simplifies security by combining CPS Detection and Response (CPSDR), threat prevention, operations lockdown, and device control.
    - CPSDR: Embodied within the advanced Operations Behavior Anomaly Detection feature, which establishes a unique baseline fingerprint of each agent-device during practicable operating states and performs fingerprint deviation analysis by means of an expansive industrial application repository and ransomware detection engine to defend against unexpected changes that may impact stability.

      Moreover, TXOne Stellar brings the contextualization of security into an operation-led view to allow both the operation and security teams to achieve their goals without needing to compromise. To illustrate, if a device suddenly tried to start launching different applications, it would be blocked from doing so.

      From the operation view, this may be an unplanned auto-update that, if run, would take the device offline to reboot. From a security

view, this could be an attempt to access an encryption library that is about to be used to execute ransomware. By applying the operation context, both security and operation-initiated changes can be detected, and appropriate responses are taken.

In both cases, CPSDR stopped the event before it could occur. The security team followed up and resolved the ransomware infection in a different part of the environment. The operation team scheduled the required update for during an upcoming planned maintenance window.

- Multi-Method Threat Prevention: Provides advanced threat scan on the basis of ICS root of trust and operations-focused machine learning to secure the agent-devices against known and unknown malware threats without compromising operational availability.
- Operations Lockdown: For fixed-function and devices with limited patching availability,operations lockdown enforcement prohibits unauthorized changes, including alterations to registry and function parameters.
- Trusted Peripheral Control: Unauthorized access from external sources, such as USB devices, is configurable and controlled to reduce physical access threats.

Leveraging an expansive ICS application and certificate library and exclusive ransomware detection engine, TXOne Stellar maintains CPS operational integrity through behavioral anomaly detection and eliminates configuration drift for legacy and fixed-use assets with device lockdown. Security teams can confidently deliver detection and response outcomes across the OT terrain, with TXOne Stellar effectively secure organization's security posture while maintaining its business operations stability.

Key Features and Benefits

The StellarProtect provides following features and benefits.

TABLE 1-1. Features and Benefits

FEATURE	BENEFIT
Cyber-Physical System Detection and Response (CPSDR)	The CPSDR requires a deep understanding of what the expected behaviors for each device are. Embodied within the advanced Operations Behavior Anomaly Detection feature, which primarily defends against unexpected changes that may impact operational stability by comparing daily operation processes and behaviors with a unique baseline of each agent-device and performing comprehensive behavioral analysis not only via identifying baseline deviation but also using TXOne Networks' exclusive industrial application repository and ransomware detection engine.
One unified agent	TXOne StellarProtect simplifies security by combining multi-method threat prevention, operations lockdown, and OT anomaly detection. The unified agent provides long-term support throughout the asset life cycle from modern to legacy.
Scan functions for modern and legacy systems	For modern systems, the StellarProtect provides **Multi-Method Threat Prevention**; the OT/ICS root of trust and advanced threat scan secure OT/ICS assets with no interruption to operations. This feature is the core protection of StellarProtect. TXOne Networks integrates signature-based and AI-based malware detection engine to provide real-time scanning of any file or process activity. Meanwhile, the StellarProtect (Legacy Mode) offers **Threat Prevention** that persistently scan new and changed files, along with system memory, to provide security assessment for maximum protection against malware in fixed-use and legacy systems.
Application Lockdown	This operations lockdown feature prevents malware attacks and increases protection level by allowing only the files defined in an Approved List to be executed. By preventing programs, DLL files, drivers, and scripts not specified on the Approved List of applications from running (also known as application trust listing), StellarProtect and StellarProtect (Legacy Mode) provide both improved productivity and system integrity by blocking malicious software and preventing unintended use. Furthermore, to ensure operational integrity, Intelligent Runtime Learning allows runtime executable files that are generated by applications in the Approved List to run smoothly.

Feature	Benefit
Approved List Management	When software needs to be installed or updated, you can use one of the following methods to make changes to the endpoint that automatically adds new or modified files to the Approved List, all without having to unlock TXOne StellarProtect or StellarProtect (Legacy Mode): • Maintenance Mode • Trusted Updater (Legacy Mode only) • Predefined Trusted Updater List (Legacy Mode only) • Command Line Interface (CLI) • Trusted hash • Trusted certificate
DLL Injection Prevention	This feature detects and blocks API call behaviors used by malicious software. Blocking these threats helps prevent malicious processes from running.
Device Control	This feature prevents insider threats by only allowing usage of USB ports on a case-by-case administrator reviewed basis. **Note** For StellarProtect (Legacy Mode), Device Control is included as one of the features of *Exploit Prevention* settings.
Maintenance Mode	To perform file updates on endpoints, users can configure Maintenance Mode settings to define a period when StellarProtect or StellarProtect (Legacy Mode) allows all file executions and adds all files that are created, executed, or modified to the Approved List.
Role Based Administration	TXOne StellarProtect and StellarProtect (Legacy Mode) both provide a separate Administrator and User account, providing full control during installation and setup, as well as simplified monitoring and maintenance after deployment.
Self Protection	With self protection features, StellarProtect/StellarProtect (Legacy Mode) are capable of defending its processes and resources, required to function properly, from being disabled by programs or actual users.

Feature	Benefit
Graphical and Command Line Interfaces	Anyone who needs to check the software can use the console, while system administrators can take advantage of the command line interface (CLI) to access all of the features and functions available.
Features designed specifically for modernized assets: • OT Application Safeguard • Operations Behavior Anomaly Detection	For modernized assets, StellarProtect offers features such as **OT Application Safeguard** and **Operations Behavior Anomaly Detection** that detect behavioral anomalies and quickly determine operational credibility using an expansive library of OT/ICS applications and certificates. **OT Application Safeguard** intelligently locates and secures the operational integrity of the critical OT/ICS applications by preventing the un-authorized changes. TXOne Networks continuously builds up the only OT/ICS context-focused database that can identify thousands of applications and certificates to ensure undisturbed operations. Meanwhile, **Operations Behavior Anomaly Detection** detects abnormal operations and exercises least privilege-based control to prevent malware-free attacks by means of its auto-learn runtime behavior to adapt to the dynamic needs of autonomous operations.
Features designed specifically for legacy assets: • Write Protection • Fileless Attack Prevention • Exploit Prevention settings	For fixed-use and legacy systems, StellarProtect (Legacy Mode) provides more options available from Application Lockdown settings. **Write Protection** blocks modification and deletion of files, folders, and registry entries; **Fileless Attack Prevention** detects and blocks unapproved process chains and arguments that may lead to a fileless attack event. For advanced threat prevention, StellarProtect (Legacy Mode) *Exploit Prevention* settings includes Intrusion Prevention, Execution Prevention, and Device Control to stop threats from spreading to the endpoint or executing.

What's New

TXOne StellarProtect 3.0 provides following new features and enhancements.

TABLE 1-2. What's New in TXOne StellarProtect 3.0

FEATURE	BENEFIT
Cyber-Physical System Detection and Response (CPSDR)	Embodied within the advanced Operations Behavior Anomaly Detection feature, which establishes a unique baseline fingerprint of each agent-device during practicable operating states and performs fingerprint deviation analysis by means of an expansive industrial application repository and exclusive ransomware detection engine to defend against unexpected changes that may impact stability. Since every agent continuously analyzes its host device to establish and maintain a unique baseline fingerprint, in real-time, unexpected behaviors and deviations from this fingerprint can be detected at the individual agent level and then secondarily at the centralized control level to inform wider instability issues and prompt preventative actions to be taken.

System Requirements

This section introduces the system requirements for StellarProtect, including hardware and OS requirements.

Software and Hardware Requirements

TXOne StellarProtect/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/StellarProtect (Legacy Mode)

HARDWARE	DESCRIPTION

Available free disk space	400MB
	
	Note
	• Recommended free disk space for StellarProtect Single Installer required during the installation process: 1.5GB
	• Minimum memory usage required when Application Lockdown and Real-Time Scan are both enabled:
	  • StellarProtect: 350MB
	  • StellarProtect (Legacy Mode): 300MB
	• Minimum memory usage required when Application Lockdown is enabled and Real-Time Scan is disabled:
	  • StellarProtect: 120MB
	  • StellarProtect (Legacy Mode): 100MB

Monitor and resolution	VGA (640 x 480), 16 colors

TABLE 1-4. Required Software for StellarProtect

SOFTWARE	DESCRIPTION
.NET framework	Version 3.5 SP1 or 4.0 available

Note

StellarProtect (Legacy Mode) does not have the software requirement for .NET framework.

By default, StellarProtect/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's use.

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

Important

- StellarProtect/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 antivirus products
- Ensure that the following root certification authority (CA) certificates are installed with intermediate CAs, which are found in `StellarSetup.exe`. These root CAs should be installed on the StellarProtect/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 (Legacy Mode only)
  - DigiCert Trusted Root G4 (Legacy Mode only)

  To check root CAs, refer to the Microsoft support site.

Note

Memory Randomization (Legacy Mode only), API Hooking Prevention (Legacy Mode only), and DLL Injection Prevention are not supported on 64-bit platforms.

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), LTSC 2015, Anniversary Update, LTSC 2016, Creators Update, Fall Creators Update, April 2018 Update, October 2018 Update*, LTSC 2019, May 2019 Update, November 2019 Update, May 2020 Update, October 2020 Update, May 2021 Update, November 2021 Update, LTSC 2021, 2022 Update
- Windows 11 (NoSP) [Pro/Enterprise] (64bit) 2022 Update
- Windows Embedded POSReady 2009 (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)

Note

Windows 10 October 2018 Update is also known as version 1809, of which Microsoft resumed the public rollout on November 13, 2018.

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)

Note

- See the latest StellarProtect readme file for the most up-to-date list of supported operating systems for agents.
- See *StellarProtect (Legacy Mode) Limitations by Operating Systems on page A-1* for the limitations of the StellarProtect (Legacy Mode) installed on certain operating systems.

Chapter 2

Installation

This chapter shows how to install the TXOne StellarProtect/StellarProtect (Legacy Mode) agent.

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 **Agents** management screen. See *Deployment Using StellarOne on page 3-3* for more information.
- 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. See *Deployment for Standalone Agents on page 3-2* for more information.

Getting the Agent's Installer Package

For agents managed by the StellarOne server, see *Getting the Agent's Installer Package from StellarOne on page 2-2*.

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

Getting the Agent's Installer Package from StellarOne

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

Procedure

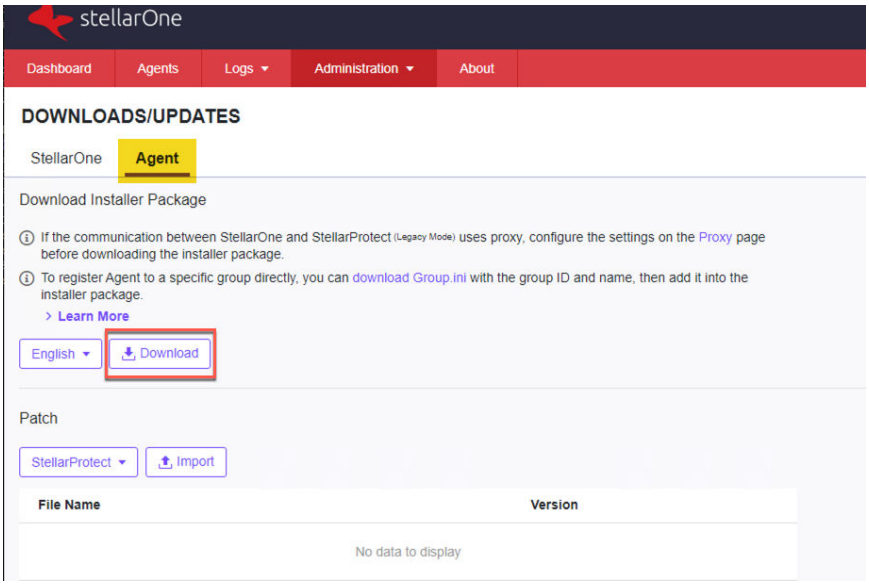
1. Log on the StellarOne web console.

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** and click **Download** to download the agent's Installer Package.

FIGURE 2-1. StellarOne Downloads/Updates Screen - Agent Page



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

Note

The installer package downloaded from StellarOne contains StellarOne data files and license information, and can be used for StellarProtect or StellarProtect (Legacy Mode) installation. After being invoked, the installer package can identfy the version of Windows installed on the endpoint and launch the suitable agent 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 latest 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.
3. Be sure you are on the **Product Download/Update** tab page.
4. Find the file name starting with `txsp-single-installer-` 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 installer package can identify the version of Windows installed on the endpoint and launch the suitable agent installer for the endpoint to install.

Installation Methods

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

Attended Installation of StellarProtect

Procedure

1. Launch the installer `StellarSetup.exe`.

Note

- The installer package downloaded from the StellarOne server differs slightly from that downloaded from the Software Download Center. One contains the StellarOne data files and license information while the other one doesn't.
- For Windows Server 2016 and later versions, the installation of StellarProtect requires turning off Windows Defender first.

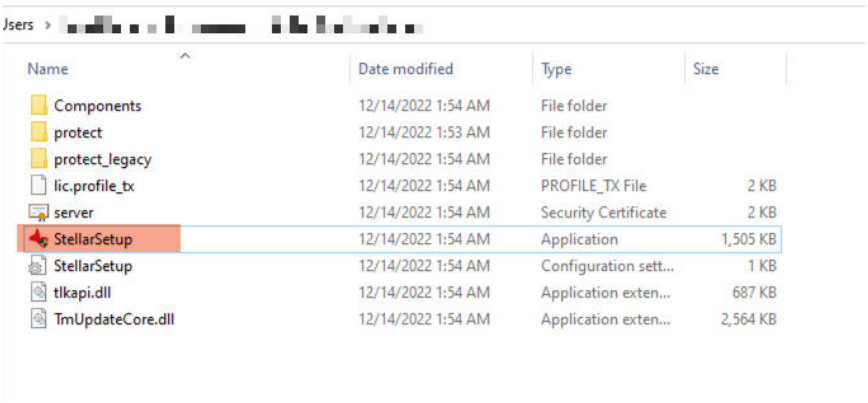


FIGURE 2-2. Installer Package Downloaded from StellarOne

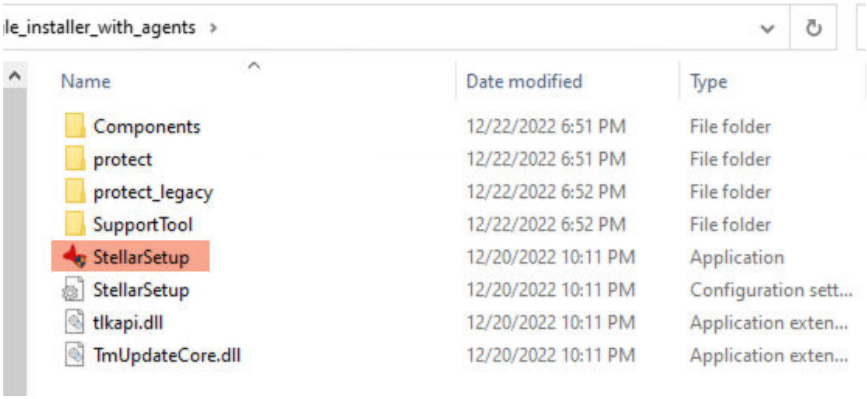


FIGURE 2-3. Standalone Installer Package Downloaded from Software Download Center

Note

To register StellarProtect agent to a specific group managed by StellarOne during the installation, after downloading the `Group.ini` file from the StellarOne server, 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.

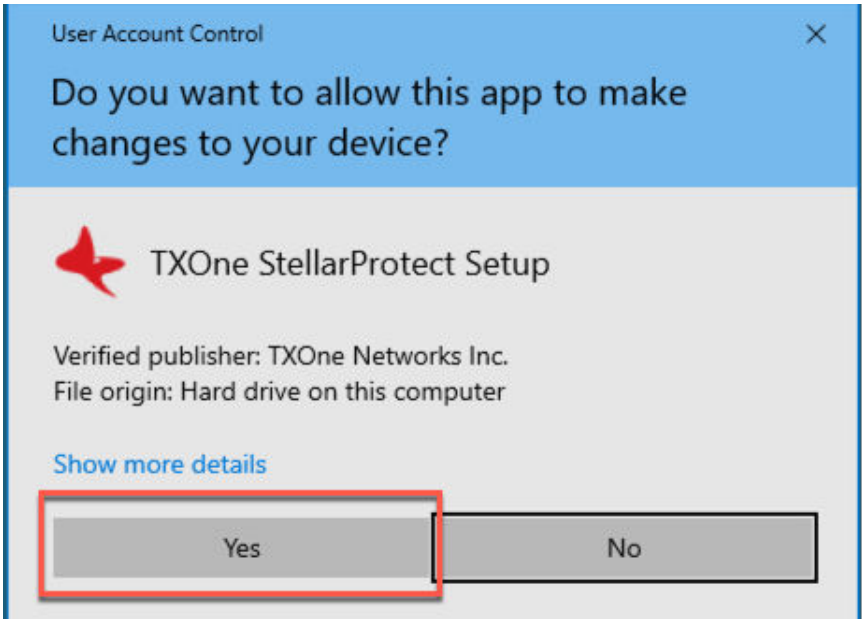


FIGURE 2-4. StellarProtect Setup Screenshot

3. Click **Next** to continue.

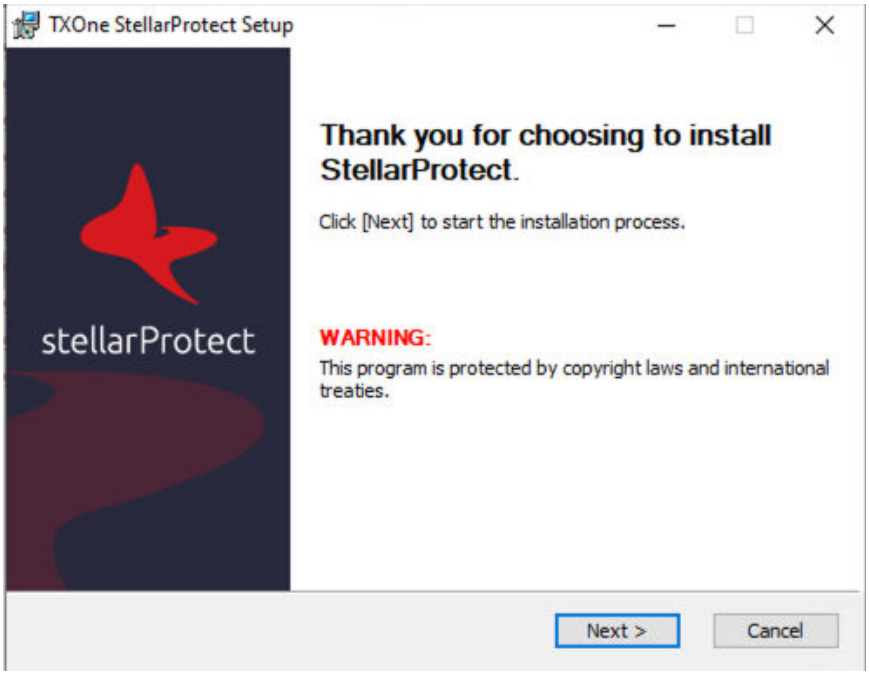


FIGURE 2-5. StellarProtect Installation Wizard

4. A success message indicating valid license appears. Click **Next** to continue.

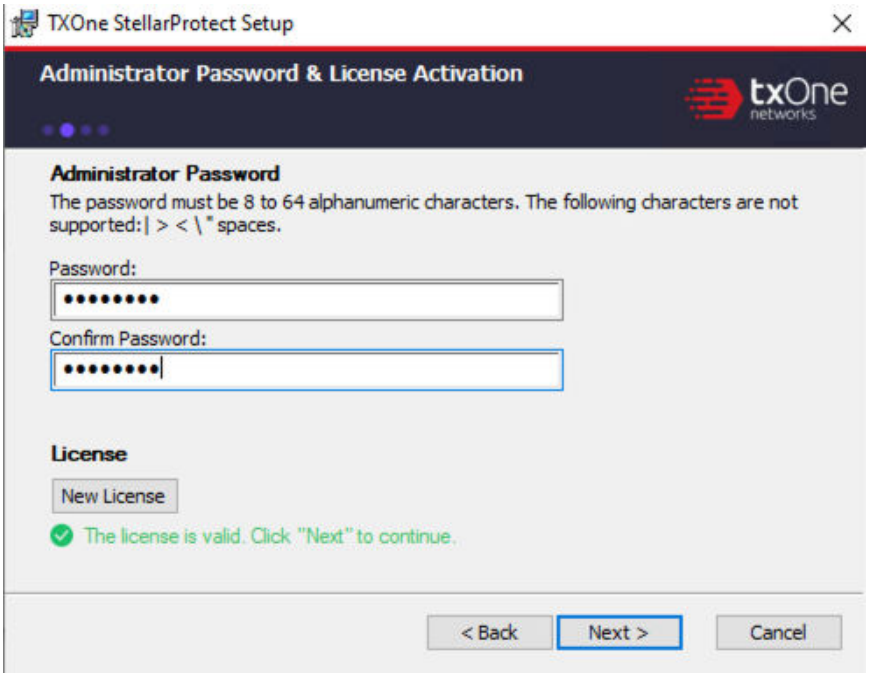


FIGURE 2-6. Admin Password & License Activation

Note

- If the agent's installer package is downloaded from StellarOne, the installer will automatically check and complete the license activation.
- For standalone agents, see *License Activation for Standalone Agent on page 2-90*.

5. 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**.

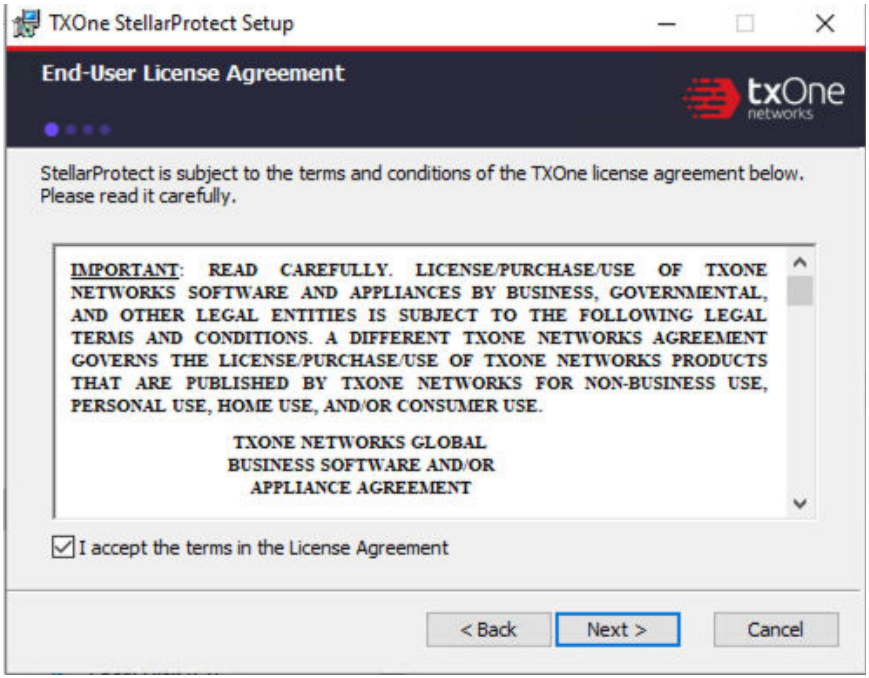


FIGURE 2-7. End-User License Agreement

6. Create an administrator password.

Note

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

Important

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

7. Specify the asset information of the installed device with correct ICS/OT-relative information such as vendor name, model, location and a description, and then click **Next**.

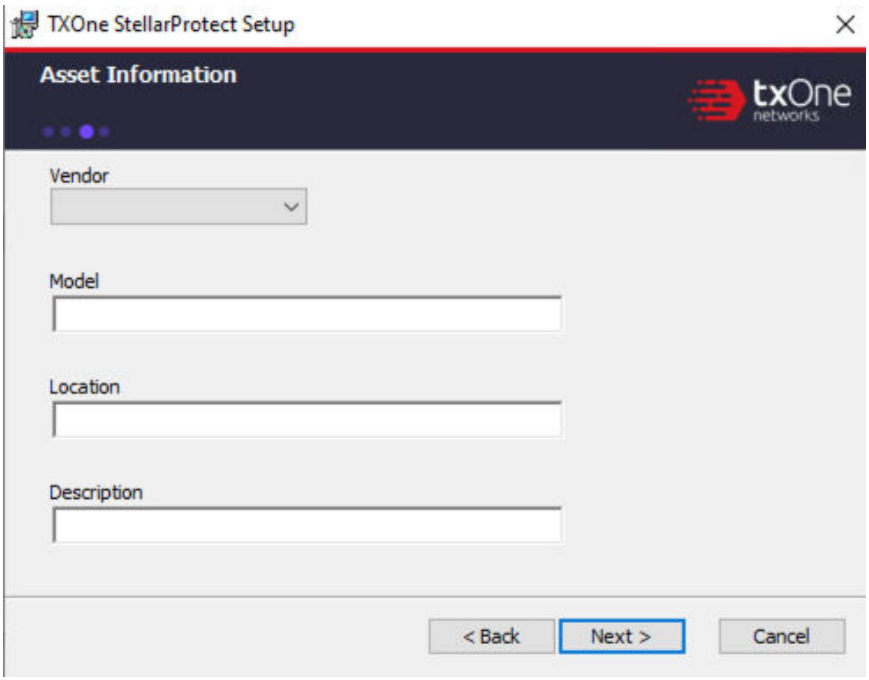


FIGURE 2-8. Asset Information

8. Confirm the installation settings including installation directory and optional component settings.

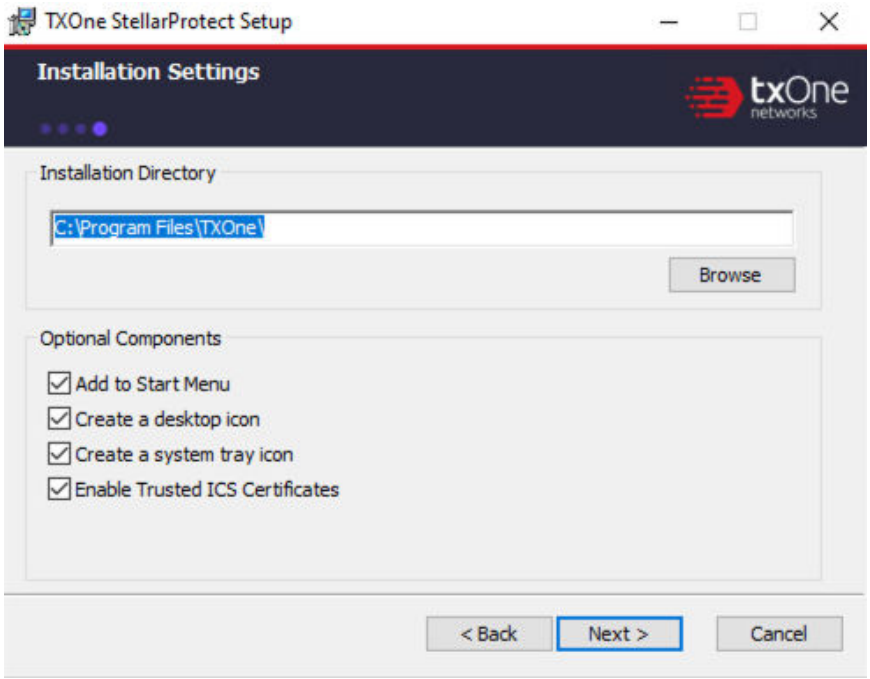


FIGURE 2-9. StellarProtect Installation Settings

Note

You can choose to whether or not add an icon to the start menu, create a desktop icon, or create a system tray icon.

Important

TXOne Networks suggests checking **Enable Trusted ICS Certificates**. This feature ensures that StellarProtect can sync up trusted ICS/OT certificates and enhance ICS/OT applications, thus those installers can always be recognized by StellarProtect.

9. If StellarProtect detects the incompatible software on the endpoint, it will display a message. If not, this message won't appear.

Note

Incompatible software means some TrendMicro product such as OfficeScan series, ApexOne, Worry-Free Business Security, Worry-Free Business Security Service. StellarProtect will try to uninstall them to avoid any possible incompatible issue.

a. During the uninstallation of the incompatible software, a progress bar appears and indicates the status.

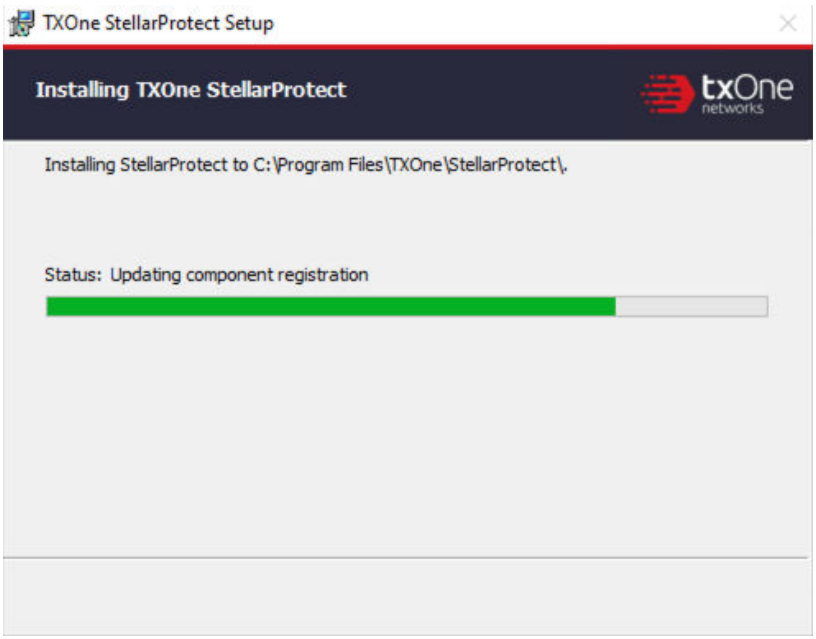
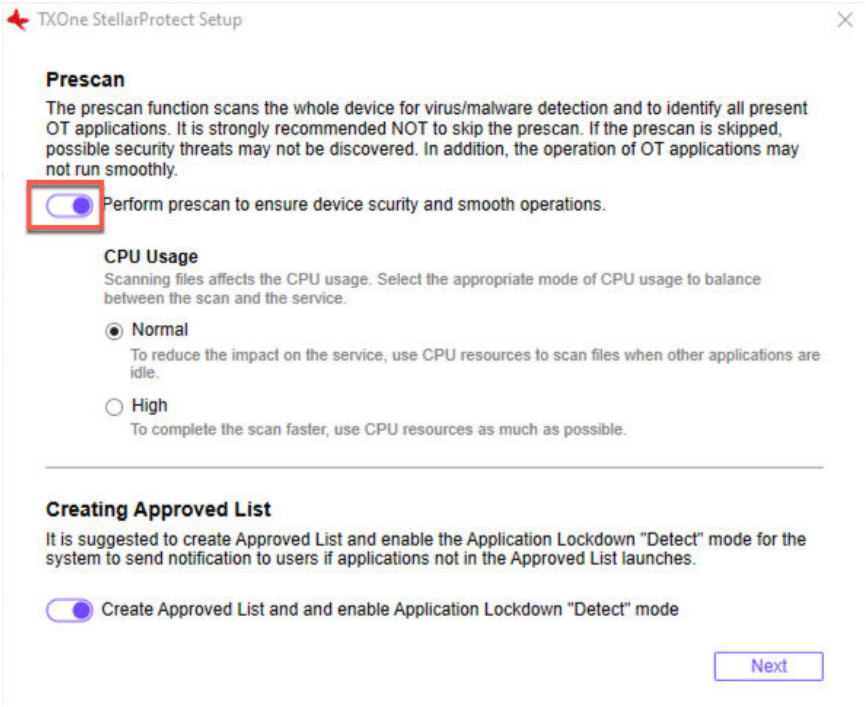


FIGURE 2-10. Status of Installing StellarProtect

10. (Optional but highly recommended) Toggle on the **Perform prescan...** to start the prescan task. If you toggle it off, go to **Step 11** for next procedure.

FIGURE 2-11. Prescan Toggle


TXOne StellarProtect Setup
Prescan
The prescan function scans the whole device for virus/malware detection and to identify all present OT applications. It is strongly recommended NOT to skip the prescan. If the prescan is skipped, possible security threats may not be discovered. In addition, the operation of OT applications may not run smoothly.
Perform prescan to ensure device scurity and smooth operations.
CPU Usage
Scanning files affects the CPU usage. Select the appropriate mode of CPU usage to balance between the scan and the service.
Normal
To reduce the impact on the service, use CPU resources to scan files when other applications are idle.
High
To complete the scan faster, use CPU resources as much as possible.
Creating Approved List
It is suggested to create Approved List and enable the Application Lockdown "Detect" mode for the system to send notification to users if applications not in the Approved List launches.
Create Approved List and and enable Application Lockdown "Detect" mode
Next

Important

- TXOne Networks recommends performing the Prescan to enable the agent to detect potential security threats and also learn the ICS/OT applications installed on the endpoint before completing the installation process.
- If you skip the Prescan, StellarProtect will not be able to recognize the ICS/OT applications before it resumes production, and will need to learn them as they are executed for the first time; this may cause delays in the ICS/OT application runtime.
- StellarProtect provides a more time-efficient option **HIGH** that will require higher CPU usage during the Prescan. If no other vital applications are running on the system, you can select the option **HIGH** to significantly reduce scan time.

Note

Since the StellarOEM license edition does not support the scanning function, this procedure will not appear in its installation process.

a. Before the Prescan starts, the installer will perform a component update based on the chosen configuration. The update process will display a message as shown below.

Note

For the standalone agents to perform the update successfully, it is required to allow them to access the Internet for connecting to the Active Update server. If they can't have the Internet connection, the component update will fail; however, users can still choose to proceed to the next step.

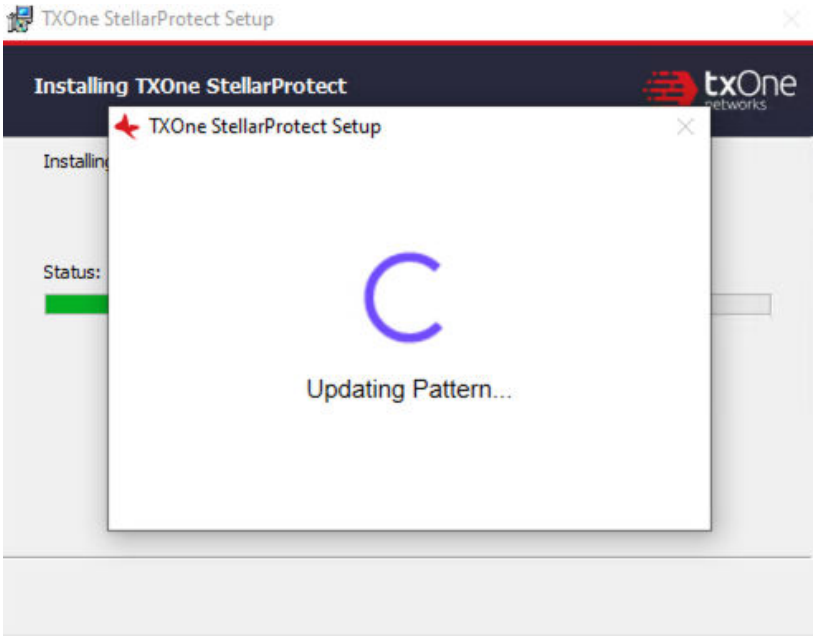


FIGURE 2-12. Update Pattern before Prescan

b. View the scan settings and click the **Start** button to start the prescan.

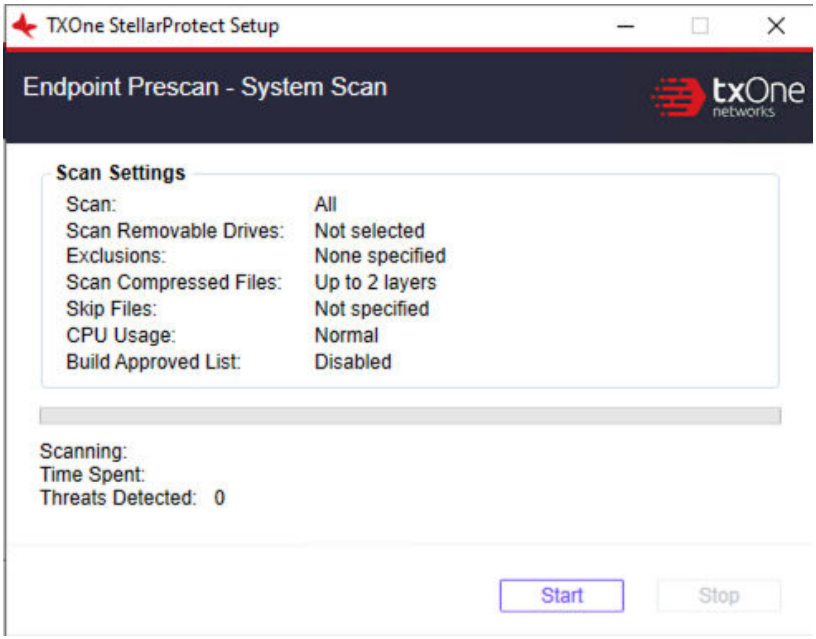


FIGURE 2-13. View Scan Settings before Prescan

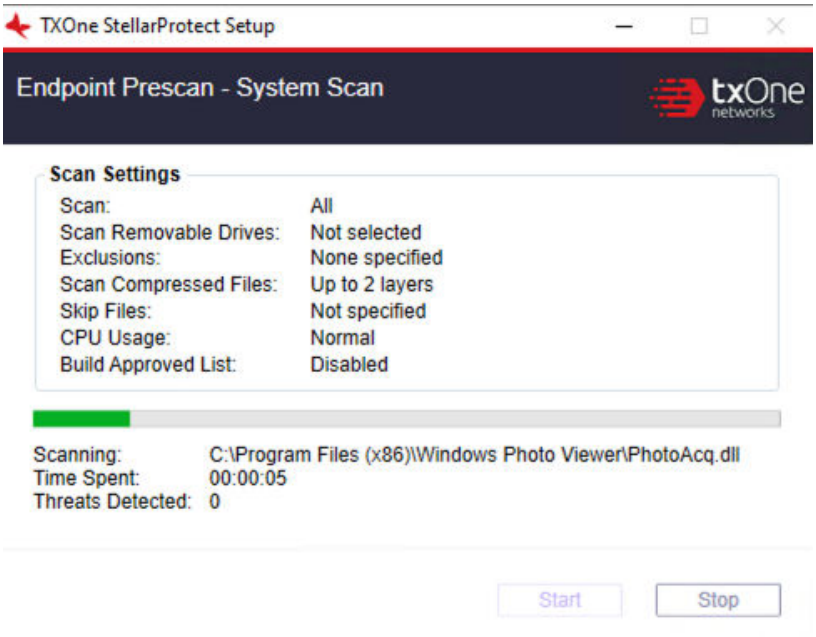
Note

Scan settings are described as follows. Please note that only StellarOne administrator can configure the scan settings after the StellarProtect agent is succesfully installed.

- **Scan**: This is the default anti-virus scan, following our template
- **Scan Removable Drives**: Selected removable drives are scanned
- **Exclusion**: Which files or folders won't be scanned
- **Scan Compressed Files**: By default, the agent scans up to 2 layers of compression during the installation. After installed, the agent can be configured to scan up to 20 layers of compression via StellarOne.
- **Skip Files:** Specific files that will be skipped
- **CPU Usage:** CPU resources that pre-scan occupied.
- **Build Approved List:** Whether the creation of Approved List is enabled or not

c. The progress bar shows the status of the prescan.

FIGURE 2-14. Prescan Status



d. After the prescan, results will be shown for review.

e. If a threat is detected, choose one of the two actions:

- **Quarantine:** Quarantine the threat.
- **Continue:** Take no action at this time.

11. (Optional but highly recommended) At the bottom of the window is the switch toggle for creating the Approved List and enabling Application Lockdown "Detect" mode. Toggle it on to proceed. If you toggle it off, go to **Step 12** for next procedure.

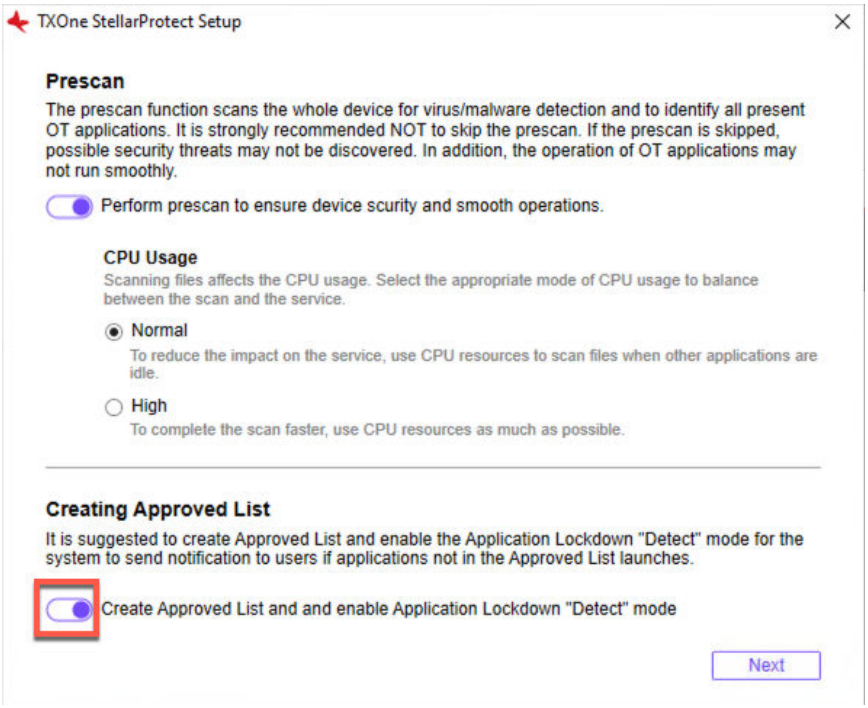


FIGURE 2-15. Create Approved List & Enable Application Lockdown (Detect)

Note

- The Approved List is created for the Application Lockdown "Detect" mode. Once the Application Lockdown "Detect" mode is enabled, the system will send notifications if applications not in the Approved List launch.
- Since the StellarKiosk license edition does not support the Application Lockdown function, this procedure will not appear in its installation process.
- If you choose not to create the Approved List during the installation process, see *Setting Up the Approved List on page 2-38* to perform this task later.

a. The results of adding applications in the Approved List will be shown for review.

b. The creation of Approved List is complete, click **Next**.

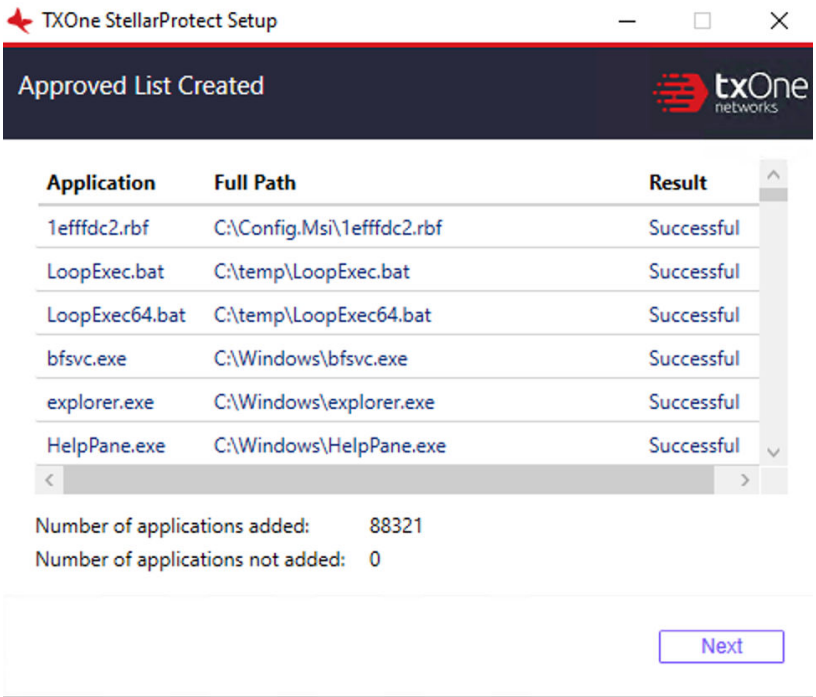
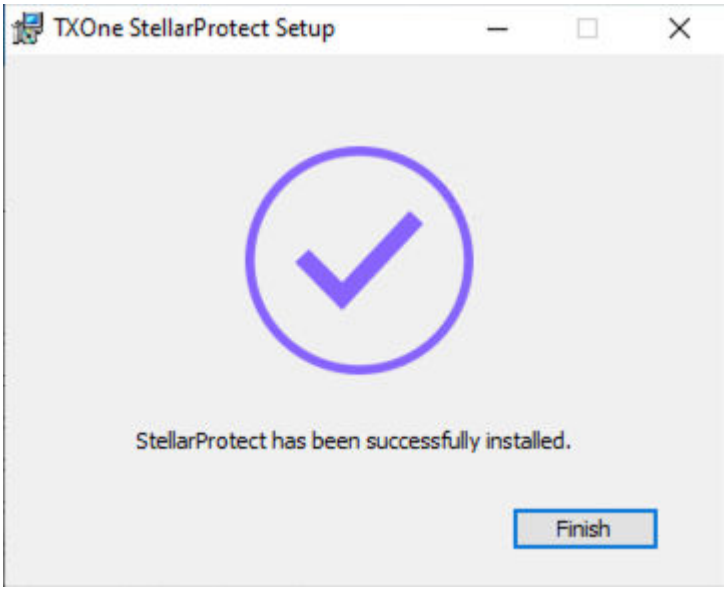


FIGURE 2-16. Approved List Created

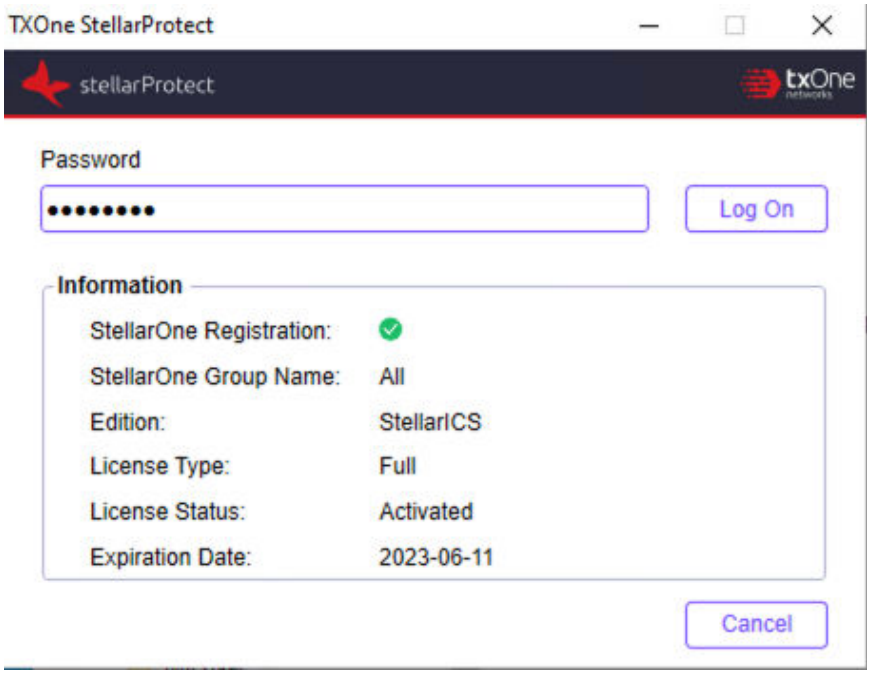
12. The StellarProtect application will be installed.
13. When the installation is complete, the **StellarProtect has been successfully installed** window appears. Click **Finish**.

FIGURE 2-17. StellarProtect Successfully Installed



14. Run StellarProtect and log on with your password.

FIGURE 2-18. Log On StellarProtect



15. Upon logging into StellarProtect successfully, the **Overview** window will display.

    - Before TXOne StellarProtect Application Lockdown feature can protect the endpoint, it must complete the creation of Approved List and enable the Application Lockdown "Enforce" mode. See *Setting Up the Approved List on page 2-38* and refer to *TXOne StellarProtect Administrator's Guide* for more information.
    - To modify more TXOne StellarProtect settings, refer to *TXOne StellarProtect Administrator's Guide* for more information.

Attended Installation of StellarProtect (Legacy Mode)

Procedure

1. Launch the installer `StellarSetup.exe`.

Note

The installer package downloaded from the StellarOne server differs slightly from that downloaded from the Software Download Center. One contains the StellarOne data files and license information while the other one does not.

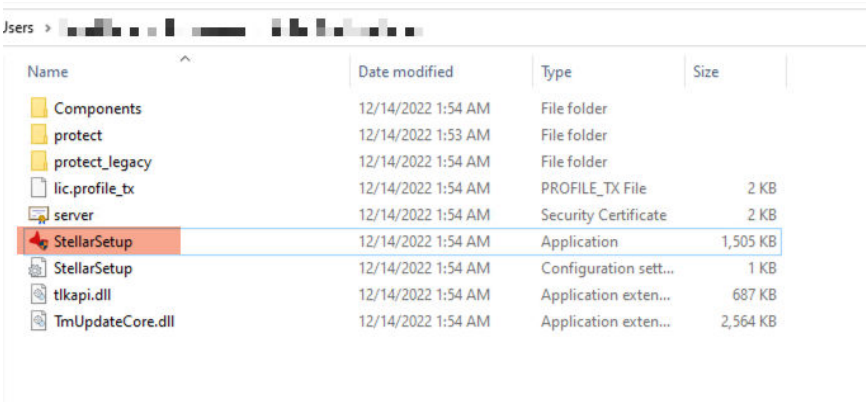


FIGURE 2-19. Installer Package Downloaded from StellarOne

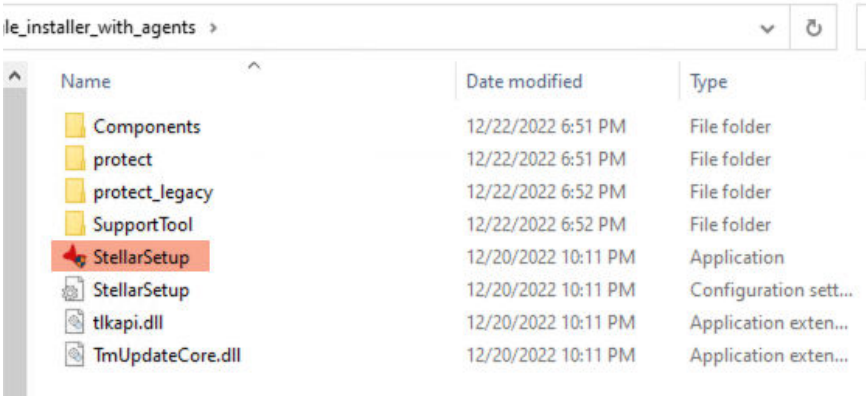


FIGURE 2-20. Standalone Installer Package Downloaded from Software Download Center

Note

To register a StellarProtect (Legacy Mode) agent to a specific group managed by StellarOne during the 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.

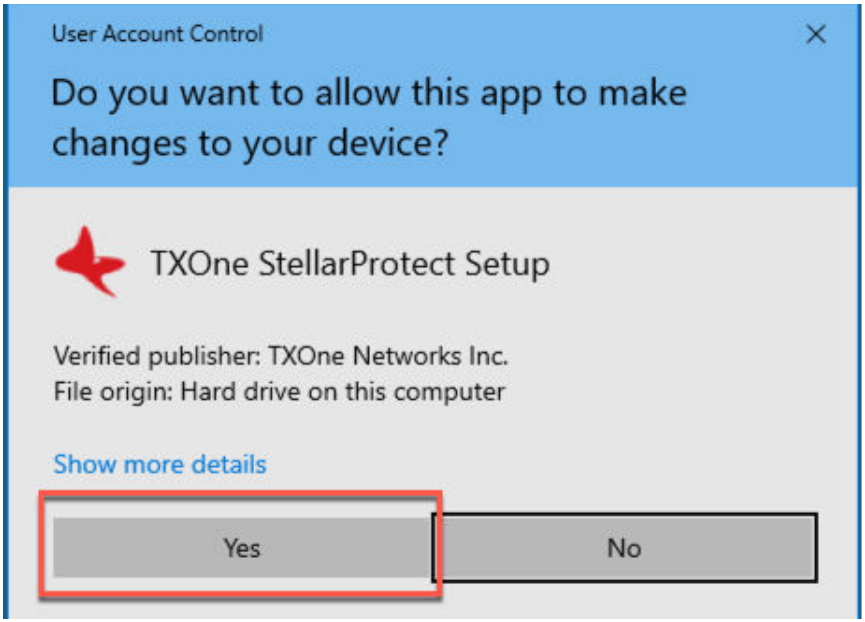


FIGURE 2-21. StellarProtect Setup Screenshot

3. Click **Next** to continue.

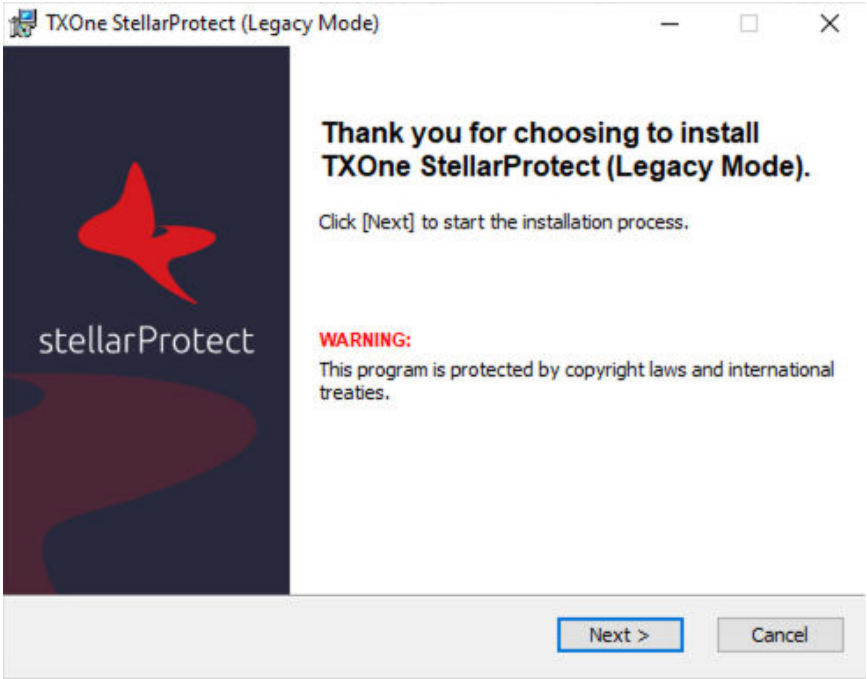


FIGURE 2-22. StellarProtect (Legacy Mode) Installation Wizard

4. A success message indicating valid license appears. Click **Next** to continue.

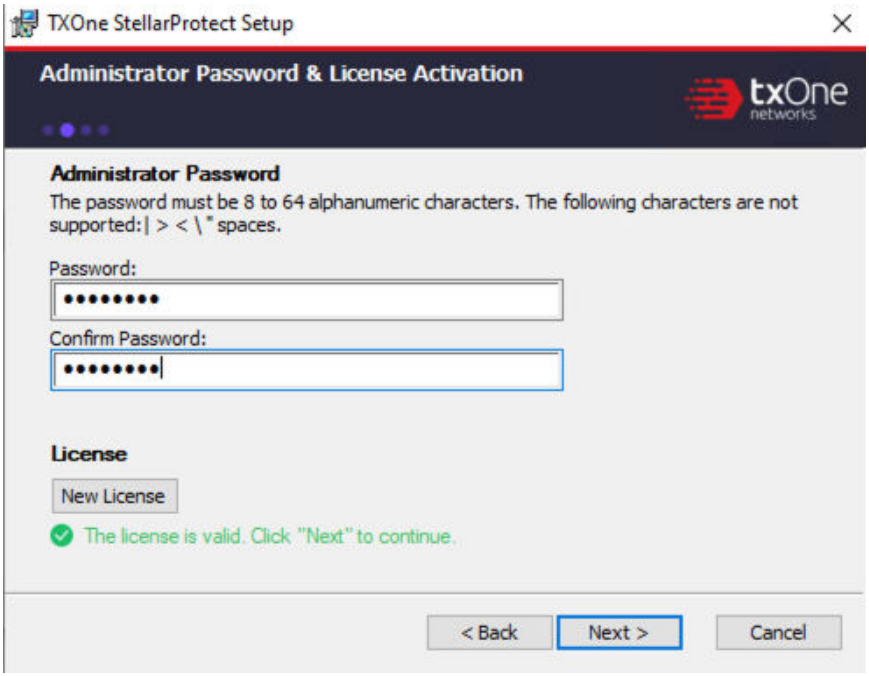


FIGURE 2-23. Admin Password & License Activation

Note

- If the agent's installer package is downloaded from StellarOne, the installer will automatically check and complete the license activation.
- For standalone agents, see *License Activation for Standalone Agent on page 2-90*.

5. 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**.

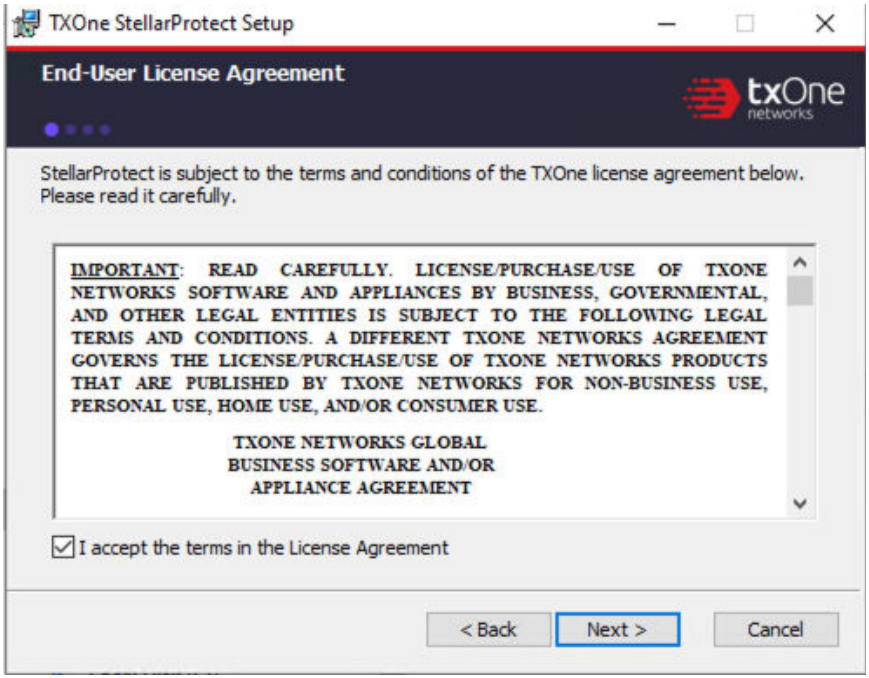


FIGURE 2-24. End-User License Agreement

6. Confirm the installation settings including installation directory and optional component settings.

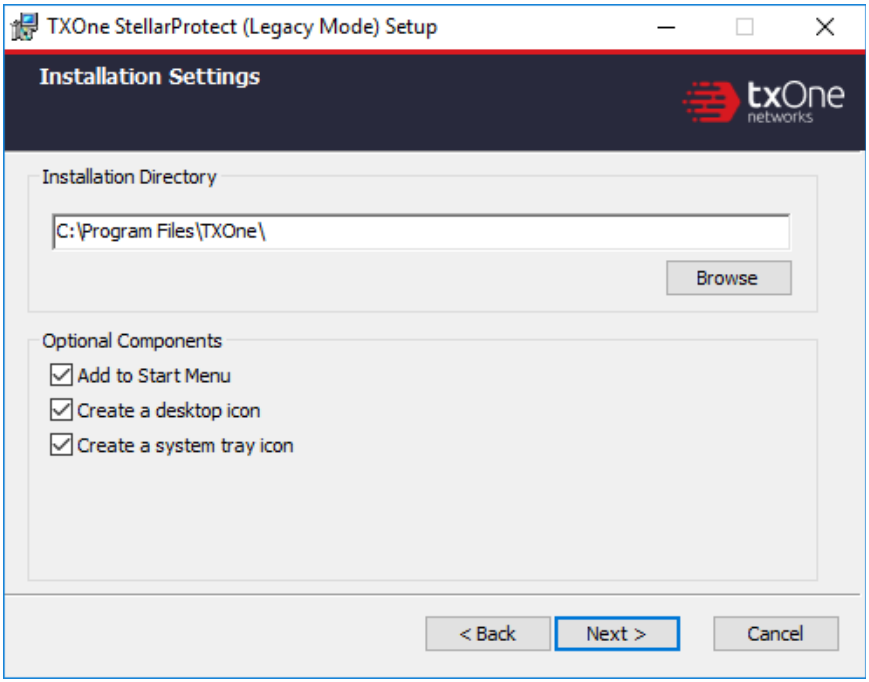


FIGURE 2-25. StellarProtect (Legacy Mode) Installation Settings

Note

You can choose to whether or not add an icon to the start menu, create a desktop icon, or create a system tray icon.

7. 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 (Legacy Mode) administrator password. If you lose the agent administrator password, please contact TXOne Networks for support.

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

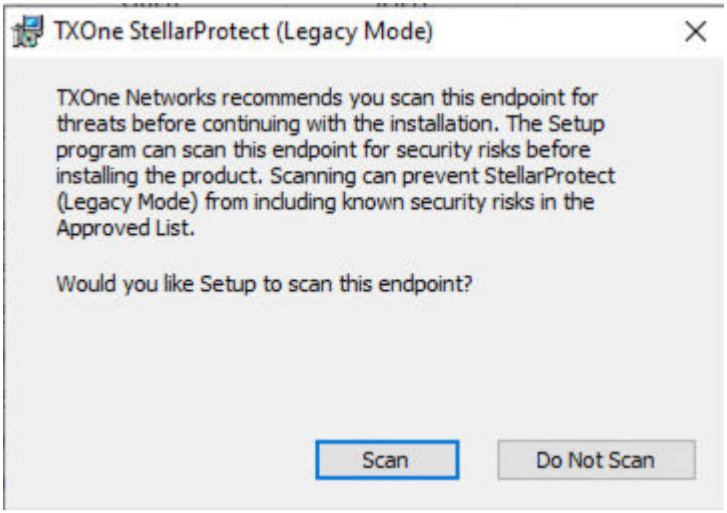


FIGURE 2-26. Scan or Do Not Scan

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` configuration file. See *Properties in the Config File for Silent Installation on page 2-42* for more information.

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

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

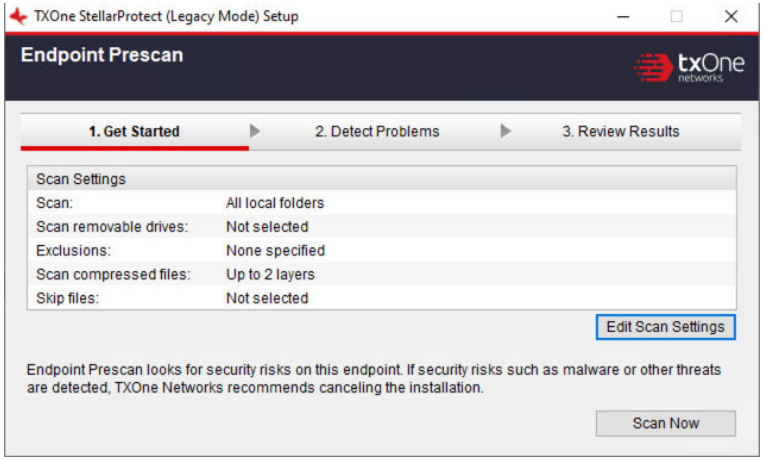


FIGURE 2-27. Endpoint Prescan - Get Started

  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.

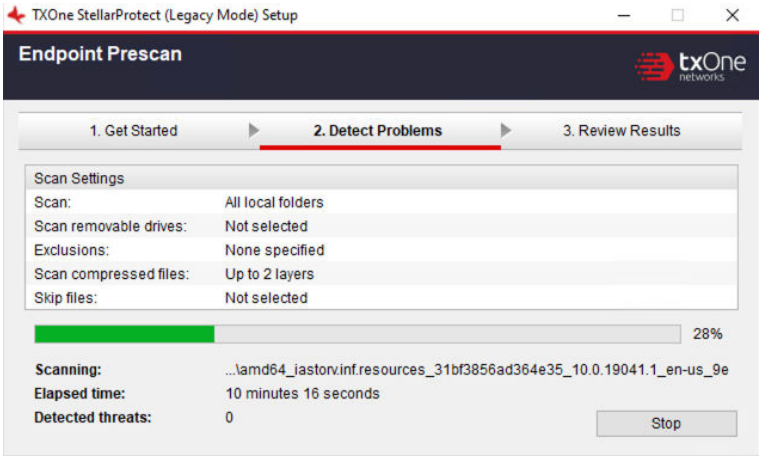


FIGURE 2-28. Endpoint Prescan - Detect Problems

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

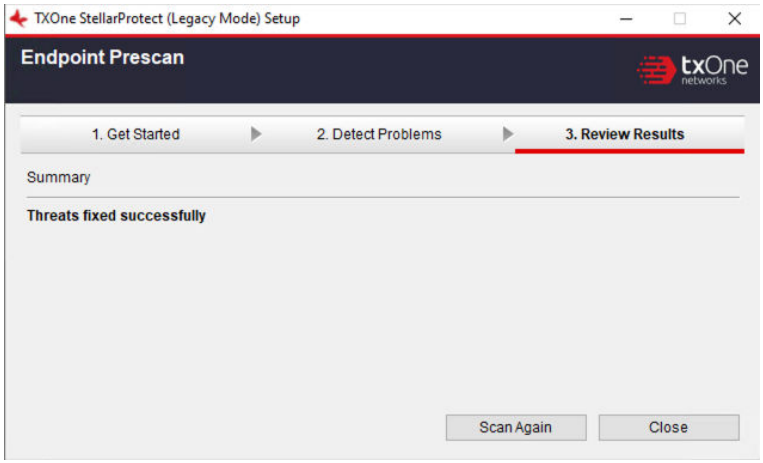


FIGURE 2-29. Endpoint Prescan - Review Results

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` configuration file for silent installation. See *Properties in the Config File for Silent Installation on page 2-42* for more information.

Tip

Perform manual scan to detect and remove threats on endpoints. See *Manual Scan Commands* in the *StellarProtect Administrator's Guide* for more information.

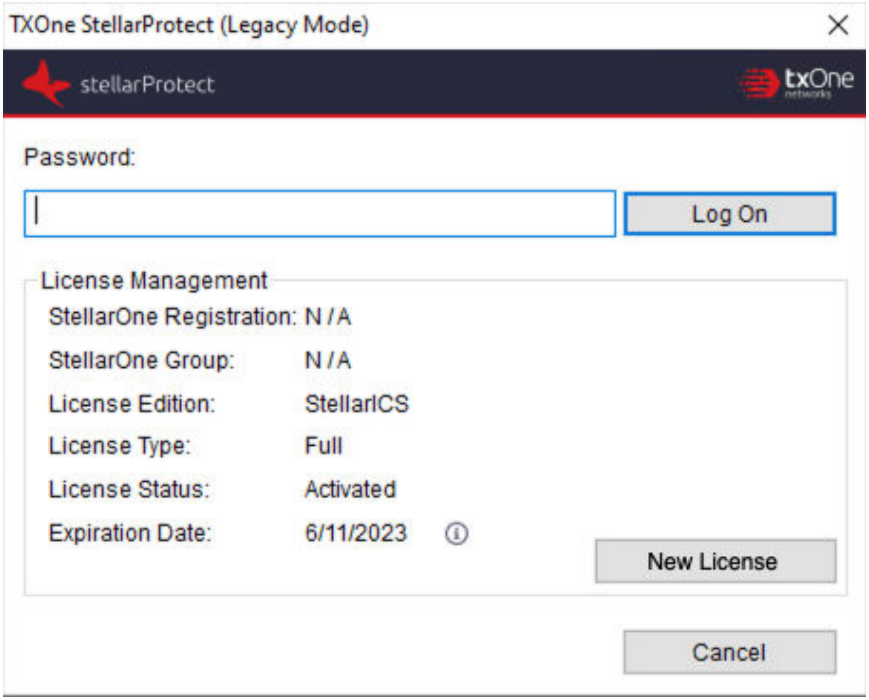
10. When the **Installation Complete** window displays, click **Finish**.

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. See *Exploit Prevention* settings in the *StellarProtect Administrator's Guide* for more information.

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

FIGURE 2-30. 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.

       See *Setting Up the Approved List on page 2-38* for detailed instructions.

    b. Modify the TXOne StellarProtect (Legacy Mode) settings. See *TXOne StellarProtect Administrator's Guide* for more information.

Setting Up the Approved List

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

The following instructions take StellarProtect (Legacy Mode) as an example for how to set up the Approved List for StellarProtect (Legacy Mode) or StellarProtect agent. StellarProtect would require you to follow similar procedures with slight differences in the GUI.

Note

If you choose not to create the Approved List during the StellarProtect installation process, refer to the following procedures to perform the task.

Procedure

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

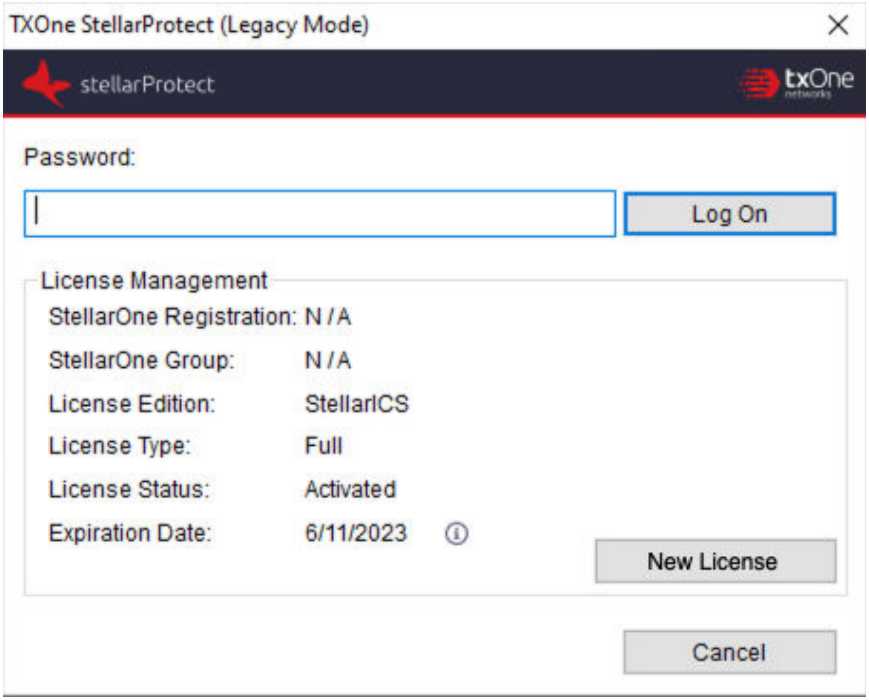


FIGURE 2-31. StellarProtect (Legacy Mode) Log On Screen

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

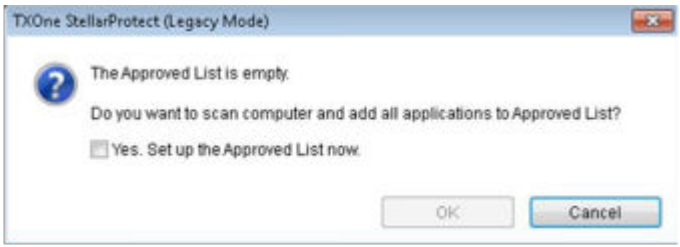


FIGURE 2-32. The Approved List is Empty

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.

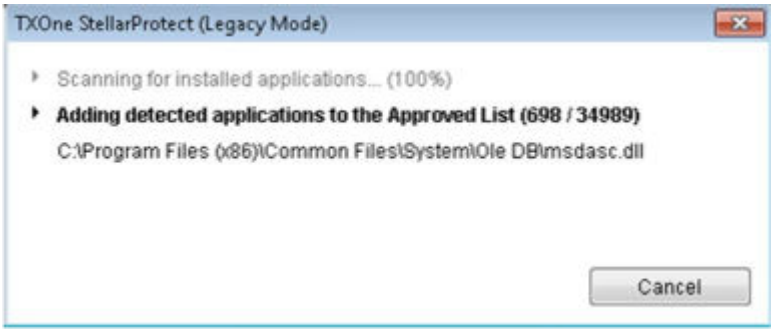


FIGURE 2-33. Scanning for Creating Approved List

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

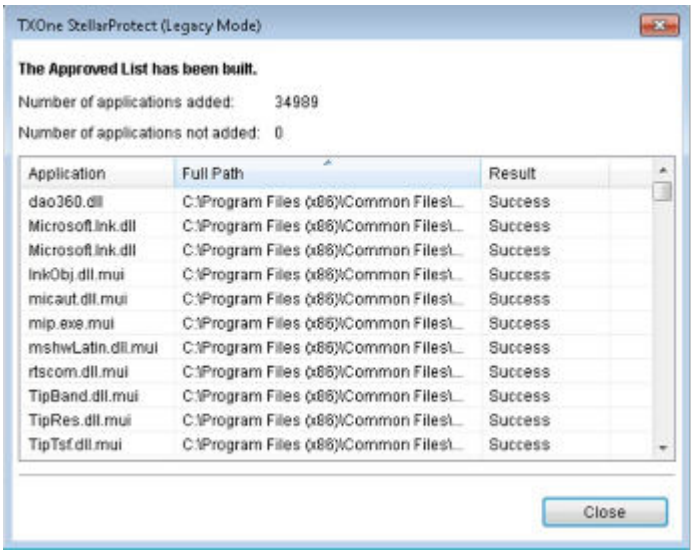


FIGURE 2-34. Approved List Created

Note

- When TXOne StellarProtect/StellarProtect (Legacy Mode) Application Lockdown is enabled, only applications that are in the Approved List will be able to run. See Administrator's Guide for more information.
- When the endpoint is creating or updating its Approved List, no policy settings can be deployed.

6. Click **Close**.

Silent Installation

StellarProtect/StellarProtect (Legacy Mode) provides an optional silent installation based on a pre-defined setup 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 by double-clicking the installer or via the command line interface (CLI).

- See *Configuration File for Silent Installation on page 2-42* for more information about the setup config file and the properties used
- See *Comparison of Configuration Files for Silent Installation on page 2-77* for the differences between the setup config files of StellarOne managed and the standalone agents
- See *Sample Config File for Silent Installation on page 2-79* as a reference of the sample config file for silent installation
- See *Encrypting Config File for Silent Installation on page 2-86* for how to encrypt the setup config file by using the command prompt
- See *Executing Silent Installation on page 2-87* for detailed instructions on executing silent installation on the endpoint

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

- See *Installer Command Line Interface Parameters on page 2-88* for more information about the CLI parameters.

Configuration File for Silent Installation

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

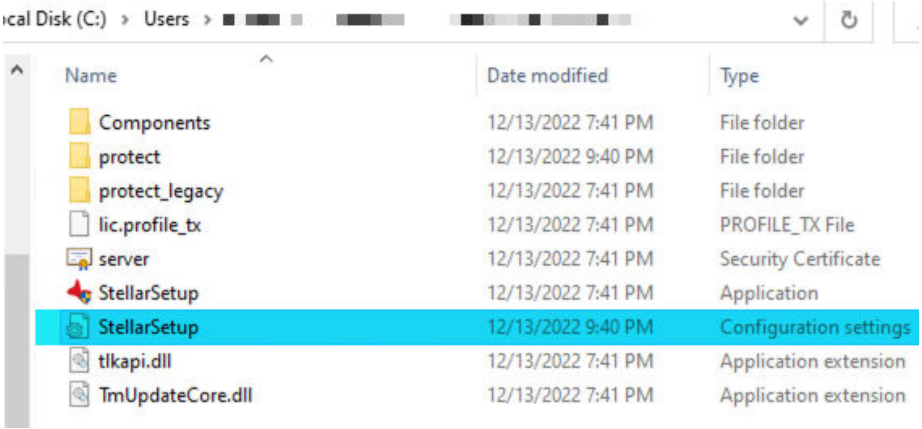


FIGURE 2-35. `StellarSetup.ini` in the Installer Package downloaded from StellarOne

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 values are specified in the setup file, the default values 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 2-1. Properties in the `StellarSetup.ini` File

SECTION	PROPERTY	DEFAULT VALUE	DESCRIPTION
[Shared_license]	product_serial_number txone_license_file	empty string	The product serial number and license file used for license activation **Important** The corresponding [shared_license] property varies depending on your support provider. See *Comparison of Configuration Files for Silent Installation on page 2-77* for more information.

Section	Property	Default Value	Description
[shared_server]	host cert	empy string server.crt	StellarOne hostname or IP address 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 when the proxy server is configured to authenticate by username and password.
	password	empy string	Administrator 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: • 0: Do not use silent mode • 1: Use silent mode
	password	empy string	Specify the Administrator password for logging on the agent console.

Section	Property	Default Value	Description

			 **Important**
			To install in silent mode, you must also specify the Administrator `password` value. For example:
			`password=P@ssW0rd`
			`silent=1`

	`user_password`	empy string	Specify the User password for loggin on the agent console.  **Important** The Administrator and User passwords cannot be the same.

Section	Property	Default Value	Description
			Note Only the Administrator can enable/ disable the User account and grant it access to limited features on the agent console.
[protect_server] [legacy_server]	port	9443 8000	StellarOne's port for connecting to the StellarProtect or StellarProtect (Legacy Mode) client
[protect_listen] [legacy_listen]	port	14336	The client listening port for StellarOne
[protect_update] [legacy_update]	source	empy string	The 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: • Specify the file path to the installation sample config file • Specify the sample file name and put the file as the top-level file in the installer package

Section	Property	Default Value	Description
			Note 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 `C:\Program Files\TXOne` (Default install path is decided in MSI installer	The installation path of the StellarProtect installer.
	`enable_start_menu`	`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.

Section	Property	Default Value	Description
	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
	cpu_usage_mode	0	0: Normal (Single thread scan) 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. Specify the path to the folder containing the config file to be imported, e.g., C:\txsp_config

Section	Property	Default Value	Description
[legacy_Property]	PRESCAN	1	Prescan the endpoint before installing StellarProtect (Legacy Mode). Possible values: • 0: Do not prescan the endpoint • 1: Prescan the endpoint
	WEL_SIZE	10240	Windows Event Log size (KB). Possible values: Positive integer **Note** Default value for new installations. Upgrading StellarProtect (Legacy Mode) does not change any user- defined WEL_SIZE values set in the previous installation.
	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:

Section	Property	Default Value	Description
			• 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 Monitor events is reached in the Windows Event Log. For Windows XP or earlier platforms: • 0: Overwrite events as needed

Section	Property	Default Value	Description
			• 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: • 0: Do not log • 1: Log
	USR_DEBUGLOGLEVEL	256	The number of debug log entries allowed for user sessions
	SRV_DEBUGLOG_ENABLE	1	Enable debug logging for service sessions. Possible values: • 0: Do not log • 1: Log

Section	Property	Default Value	Description
	SRV_DEBUGLOGLEVEL	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: • 0: Disable debug log • 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: • 0: Disable debug log • 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: • 0: Disable debug log • 1: Enable debug log
	BM_SRV_DEBUGLOG_LEVEL	51	Debug level of Behavior Monitoring Core service
	INTEGRITY_MONITOR	0	Enable Integrity Monitor. Possible values: • 0: Disable • 1: Enable

Section	Property	Default Value	Description
	PREDEFINED_TRUSTED_UPDATER	0	Enable Predefined Trusted Updater. Possible values: • 0: Disable • 1: Enable
	WINDOWS_UPDATE_SUPPORT	0	Enable Windows Update Support. Possible values: • 0: Disable • 1: Enable
	STORAGE_DEVICE_BLOCKING	0	Blocks storage devices, including CD/DVD drives, floppy disks,and USB devices, from accessing managed endpoints. Possible values: • 0: Allow access from storage devices • 1: Block access from storage devices
	INIT_LIST	0	Initialize the Approved List during installation. Possible values: • 0: Do not initialize the Approved list During installation • 1: Initialize the Approved List during installation

Section	Property	Default Value	Description
			Note `LIST_PATH` has priority over `INIT_LIST`. For example: If `LIST_PATH = liststore.db` and `INIT_LIST=1` `liststore.db` is imported and `INIT_LIST` is ignored.
	`LOCKDOWN`	0	Turn Application Lockdown on after installation. Possible values: • 0: Turn off Application Lockdown • 1: Turn on Application Lockdown
	`FILELESS_ATTACK_PREVENTION`	0	Enable the Fileless Attack Prevention feature. Possible values: • 0: Disable • 1: Enable
	`SERVICE_CREATION_PREVENTION`	0	Enable the Service Creation Prevention feature. Possible values:

Section	Property	Default Value	Description
			• 0: Disable • 1: Enable

Section	Property	Default Value	Description
			Note StellarProtect (Legacy Mode) temporarily disables the Service Creation Prevention feature under the following conditions: • Updating or installing new applications using installers allowed by Trusted Updater. The feature is automatically re-enabled after the Trusted Updater process is complete • Enabling Windows Update **Support**

Section	Property	Default Value	Description
	INTELLIGENT_RUNTIME_LEARNING	0	The agent will allow runtime execution files 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:

Section	Property	Default Value	Description
			• 0: Ignore • 1: Quarantine • 2: Ask server
	MAX_EVENT_DB_SIZE	1024	Maximum database file size (MB). Possible values: Positive integer
	INIT_LIST_EXCLUDED_EXTENSION1	log	A file extension 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 extensions by creating new entries with names that start with INIT_LIST_EXCLUDED_EXTENSION, while ensuring that each entry name is unique. For example: INIT_LIST_EXCLUDED_EXTENSION=bmp 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

Section	Property	Default Value	Description
			• 2: Continue installation when no 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: • <folder_path> • <empty>: Defaults to `%windir%\temp\prescan\log`

	SCAN_TYPE	Full	The type of scan executed during silent installation. Possible values:
			• Full: Scan all folders on the endpoint
			• Quick: Scans the following folders:
			  • Fixed root drives, e.g.,
			  `c:\`
			  `d:\`
			  • System root folder, e.g.,
			  `c:\Windows`
			  • 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\Drivers`
			• 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_FOLDER` entries

Section	Property	Default Value	Description
			Note 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: • 0: Do not scan compressed files • 1~20: Scan up to the specified number of layers of a compressed file
	MAX_FILE_SIZE	0	The largest file allowed for scan • 0: Scan files of any sizes • 1~9999: Only scan files equal to or smaller than the specified size (MB)
	SCAN_REMOVABLE_DRIVE	0	Scan removable drives. Possible values: • 0: Do not scan removable drives • 1: Scan removable drives

Section	Property	Default Value	Description
	FORCE_PRESCAN	0	Perform a prescan before installation. Possible values: • 0: Disable • 1: Enable
[legacy_BlockNotification] **Important** 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: • 0: Disable • 1: Enable
	ALWAYS_ON_TOP	1	Display the file blocking notification on top of other screens. Possible values: • 0: Disable • 1: Enable
	SHOW_DETAILS	1	Display file name, file path, and event time in the notification. Possible values: • 0: Disable • 1: Enable
	AUTHENTICATE	1	Authenticate the user by requesting the administrator password when closing a notification. Possible values: • 0: Disable

Section	Property	Default Value	Description
			• 1: Enable
	TITLE	empty string	Notification title Possible values: <notification_title>
	MESSAGE	empty string	Notification content Possible values: <notification_content>
[legacy_EventLog]	Enable	1	Log events related to StellarProtect (Legacy Mode). Possible values: • 1: Log • 0: Do not log
	Level_WarningLog	1	Log “Warning” level events related to StellarProtect (Legacy Mode). Possible values: • 1: Log • 0: Do not log
	Level_InformationLog	0	Log “Information” levelevents related to StellarProtect (Legacy Mode). Possible values: • 1: Log • 0: Do not log
	BlockedAccessLog	1	Log files blocked by StellarProtect (Legacy Mode). Possible values: • 1: Log • 0: Do not log

Section	Property	Default Value	Description
	ApprovedAccessLog	1	Log files approved by StellarProtect (Legacy Mode). Possible values: • 1: Log • 0: Do not log
	ApprovedAccessLog_TrustedUpdater	1	Log Trusted Updater approved access. Possible values: • 1: Log • 0: Do not log
	ApprovedAccessLog_DllDriver	0	Log DLL/Driver approved access. Possible values: • 1: Log • 0: Do not log
	ApprovedAccessLog_ExceptionPath	1	Log Application Lockdown exception path approved access. Possible values: • 1: Log • 0: Do not log
	ApprovedAccessLog_TrustedCert	1	Log Trusted Certificates approved access. Possible values: • 1: Log • 0: Do not log
	ApprovedAccessLog_WriteProtection	1	Log Write Protection approved access. Possible values: • 1: Log

Section	Property	Default Value	Description
			• 0: Do not log
	ApprovedAccessLog_TrustedHash	1	Log Trusted Hash approved access. Possible values: • 1: Log • 0: Do not log
	SystemEventLog	1	Log events related to the system. Possible values: • 1: Log • 0: Do not log
	SystemEventLog_ExceptionPath	1	Log exceptions to Application Lockdown. Possible values: • 1: Log • 0: Do not log
	SystemEventLog_WriteProtection	1	Log Write Protection events. Possible values: • 1: Log • 0: Do not log
	ListLog	1	Log events related to the Approved list. Possible values: • 1: Log • 0: Do not log
	UsbMalwareProtectionLog	1	Log events that trigger USB Malware Protection. Possible values: • 1: Log • 0: Do not log

Section	Property	Default Value	Description
	ExecutionPreventionLog	1	Log events that trigger Execution Prevention. Possible values: • 1: Log • 0: Do not log
	IntegrityMonitoringLog_FileCreated	1	Log file and folder created events. Possible values: • 1: Log • 0: Do not log
	IntegrityMonitoringLog_FileModified	1	Log file modified events. Possible values: • 1: Log • 0: Do not log
	IntegrityMonitoringLog_FileDeleted	1	Log file and folder deleted events. Possible values: • 1: Log • 0: Do not log
	IntegrityMonitoringLog_FileRenamed	1	Log file and folder renamed events. Possible values: • 1: Log • 0: Do not log
	IntegrityMonitoringLog_RegValueModified	1	Log registry value modified events. Possible values: • 1: Log • 0: Do not log

Section	Property	Default Value	Description
	IntegrityMonitoringLog_RegValueDeleted	1	Log registry value deleted events. Possible values: • 1: Log • 0: Do not log
	IntegrityMonitoringLog_RegKeyCreated	1	Log registry key created events. Possible values: • 1: Log • 0: Do not log
	IntegrityMonitoringLog_RegKeyDeleted	1	Log registry key deleted events. Possible values: • 1: Log • 0: Do not log
	IntegrityMonitoringLog_RegKeyRenamed	1	Log registry key renamed events. Possible values: • 1: Log • 0: Do not log
	DeviceControlLog	1	Log events related to device access control. Possible values: • 1: Log • 0: Do not log
[legacy_MaintenanceMode]	ENABLE_DURATION	0	Start maintenance mode with this duration immediately after the install process is finished. Possible values: 0- 999 Unit: Hours

Section	Property	Default Value	Description
			Note The setting of this property applies to standalone agents only.
	SCAN	0	Enable malware scanning for quarantining suspicious files or adding new or changed files to the Approved List. Possible values: • 0: No scan (default) • 1: Quarantine StellarProtect (Legacy Mode) scans files that are created, executed, or modified during the maintenance and quarantines suspicious files • 2: AL StellarProtect (Legacy Mode) scans files that are created, executed, or modified during the maintenance and adds these files (including files that are detected as malicious) to the Approved List

Section	Property	Default Value	Description
[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 Possible values: 0~2147483647
	MAX_RETRY_INTERVAL	7680	Maximum interval, in seconds, between attempts to resend events to StellarOne Possible values: 0~2147483647
[legacy_MessageRandomization]	TOTAL_GROUP_NUM	1	Number of groups controlled by the server. Possible values: 0~2147483646
	OWN_GROUP_INDEX	0	Index of group which this agent belongs to. Possible values: 0~2147483646
	TIME_PERIOD	0	Maximum amount of time agents have to upload data (in seconds). Possible values: 0~2147483647

Section	Property	Default Value	Description
Note StellarProtect (Legacy Mode) agents respond as soon as possible to direct requests from StellarOne. For details, see *Applying Message Time Groups* in the *TXOne StellarProtect Administrator's Guide*.			

Hidden Properties in the Config File for Silent Installation

StellarProtect's Hidden Properties in `StellarSetup.ini` File

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

Section	Property	Default Value	Description
`[protect_install]`	`BYPASS_WINDEFEND_CHECK`	0	Bypass checking Windows Defender status

Note

- The `BYPASS_WINDEFEND_CHECK` property is designed for Windows 7 and Windows Server 2016+ platforms, on which the default setup of StellarProtect requires disabling Windows Defender first. To get the StellarProtect installed without disabling Windows Defender, you can set the value of `BYPASS_WINDEFEND_CHECK` to `1`, and then the endpoint will bypass Windows Defender check.
- If you would like to bypass checking Windows Defender status to get the StellarProtect installed without disabling Windows Defender, insert a line under the `[protect_install]` section, and then type `bypass_windefend_check: 1`

StellarProtect (Legacy Mode) Hidden Properties in `StellarSetup.ini` File

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 used for agent feature settings
	`LIST_PATH`	empty string	The file path to the Approved List file
	`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.

Section	Property	Default Value	Description
	INIT_LIST_PATH_OPTIONAL	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_EXCLUDED_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 INIT_LIST_EXCLUDED_FOLDER Ensure each entry name is unique. For example: INIT_LIST_EXCLUDED_FOLDER= c:\folder1 INIT_LIST_EXCLUDED_FOLDER2 =c:\folder2 INIT_LIST_EXCLUDED_FOLDER3 =c:\folder3 Possible values • Folder path supports a maximum length of 260 characters. • Folder paths that do not exist may be specified.

Section	Property	Default Value	Description
			• 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. Possible values: • 0: Disable (Default) • 1: Enable
	USER_PASSWORD	empty string	Specify the User password to enable the User account and set its password
[legacy_AGENT]	FIXED_IP	empty string	Set the agent IP address to communcate with the StellarProtect (Legacy Mode) server Possible values: • A.B.C.D/E • A, B, C, D: 0~255 • E: 1~32

Section	Property	Default Value	Description
			Note 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]`
			Possible values:
			<folder_path>
			Multiple folders can be specified by creating new entries whose name starting with `SPECIFIC_FOLDER`
			Every entry name needs to be unique. For example:
			`SPECIFIC_FOLDER=c:\folder1`
			`SPECIFIC_FOLDER2=c:\folder2`
			`SPECIFIC_FOLDER3=c:\folder3`

	`EXCLUDED_FILE`	empty string	An absolute file path to exclude from scanning Possible values: <file_path>

Section	Property	Default Value	Description

			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:
			
			`EXCLUDED_FOLDER=c:\file1`
			
			`EXCLUDED_FOLDER2=c:\file2`
			
			`EXCLUDED_FOLDER3=c:\file3`

Section	Property	Default Value	Description
	EXCLUDED_EXTENSION	empty string	A file extension to 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

Comparison of Configuration Files for Silent Installation

TXOne Networks pre-defines most of the values of the properties within the `StellarSetup.ini` file, which can be used directly or adapted for different installation requirements.

If the agent installer package, containing the `StellarSetup.ini` file, is downloaded from a StellarOne server, you can just change the `silent` value to `1` and specify the password in the `[shared_install]` section of the setup config file, and then execute the silent installation. See *Executing Silent Installation on page 2-87* for how to execute the silent installation.

However, if the agent installer package is downloaded from the Software Download Center, you would need to specify the values of certain properties as listed below.

- **License data**:

  `[shared_license]`

- `product_serial_number`
- `txone_license_file`

or

- `license_key`

Important

The corresponding `[shared_license]` property varies depending on your support provider:

- If `[shared_license]` consists of `product_serial_number` and `txone_license_file` properties, use the **license file** for product activation.
- If `[shared_license]` consists of `license key` property, use the **license key** for product activation.

See *Getting the License File and PSN on page 2-95* for more information about the license file and product serial number.

- **Server data such as IP address and certificate**:

  `[shared_server]`

  - `host`
  - `cert`

- **Component update server link**:

  `[protect_update]/[legacy_update]`

  - `source`

Note

- For standalone agents, the server data are not required to specify. However, the license data and the component update source should be specified for the installer to launch and perform successful component updates.
- If you would like to use a proxy server for communication with StellarOne, please also configure the `shared_proxy` properties.

See *Sample Config File for Silent Installation on page 2-79* for an example of the defined setup config file.

See *Getting the License File and PSN for Standalone Agents on page 2-95* for how to get the license file and product serial number for standalone agents.

Sample Config File for Silent Installation

See below as an example of the defined setup configuration file (`StellarSetup.ini`) used for agents installed in StellarOne managed and silent modes. You can define your own configuration settings by changing the values.

Note

- For standalone agents, the server information (values of `[shared_server]`) are not required to specify. However, the license data and the component update source (values of `[shared_license]` and `[protect_update]/[legacy_update]`) should be specified for the installer to launch and perform successful component updates.
- If you would like to use a proxy server for communication with StellarOne, configure the `shared_proxy` properties as well.

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

Note

If `[shared_license]` consists of `license key` property, use **license key** for product activation.

```
[shared_license]
product_serial_number = TEXXXXXX-SAMP-LEXX-XXXX-TXONESPXXXXX
txone_license_file = Stellar<License>Edition_XXXXXXXXXXXXX.txt
txone_license_env = prod
[shared_server]
host = 10.1.195.100
cert = server.crt
[shared_proxy]
host =
port =
username =
password =
[shared_install]
silent = 1
password = 11111111
user_password =
[protect_server]
port = 9443
[protect_listen]
port = 14336
[protect_update]
```

```
source = https://10.1.195.100/rest/stellar-au/duplicate/protect
[protect_config]
include =
[legacy_server]
port = 8000
[legacy_listen]
port = 14336
[legacy_update]
source = https://10.1.195.100/rest/stellar-au/duplicate/enforce
[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, see *Getting the License File and PSN on page 2-95*.

Encrypting Config File for Silent Installation

StellarProtect/StellarProtect (Legacy Mode) supports encrypting the setup config file to prevent sensitive data leakage. The encrypted config file name is fixed to `StellarSetup.bin`.

Procedure

1. Prepare your `StellarSetup.ini` as mentioned in *Silent Installation on page 2-41*.
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.

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, almost all the values needed should be automatically generated. If no additional configuration requirements are needed, you can just change the `silent` value to `1` and specify the password in the `[shared_install]` section of the configuration file.

   Note

   If the agent installer package is downloaded from the Software Download Center, see *Comparison of Configuration Files for Silent Installation on page 2-77* for more information.

2. Place the defined `StellarSetup.ini` file in the installation package.
3. Choose one of the methods to launch the `StellarSetup.exe` installer.
   - Double-click the installer `StellarSetup.exe`.
   - Use the command prompt to execute `StellarSetup.exe` with the argument `-s`, e.g., type `C:\package>StellarSetup.exe -s`

   Note

   To view relevant information or progress status of the silent installation, check logs filed under `C:\Windows\Temp`.

4. Run StellarProtect or StellarProtect (Legacy Mode) and log on with the configured password.
5. After successfully logging into StellarProtect or StellarProtect (Legacy Mode), the **Overview** window will be displayed.

Installer Command Line Interface Parameters

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

TABLE 2-2. StellarProtect Installer Command Line Options

PARAMETER	VALUE	DESCRIPTON
`-s`		Run the installer silently **Note** During the installation process, you can view the following log files in the folder `C:\windows\temp` to check the status of the prescan and initial approved process: `StellarProtect \StellarProtectPrescan_YYYYMMDD.log`
`-e`		Encrypt the config file for installation

TABLE 2-3. StellarProtect (Legacy Mode) Installer Command Line Options

PARAMETER	VALUE	DESCRIPTON
`-s`		Run the installer silently **Note** During the installation process, you can view the following log files in the folder `C:\windows\temp` to check the status of the prescan and initial approved process: • Prescan process: `YYYYMMDDHHMMSS_wk_PreScanProgress.log` • Initial approved process: `YYYYMMDDHHMMSS_wk_InitListProgress.log`
`-p`	<administrator_password>	Specify the administrator password
`-d`	<path>	Specify the installation path
`-nd`		Do not create a desktop shortcut
`-ns`		Do not add a shortcut to the **Start** menu
`-ni`		Hide the task tray icon
`-cp`	<path>	Specify the StellarProtect (Legacy Mode) configuration file **Note** The StellarProtect (Legacy Mode)configuration file can be exported after installing StellarProtect (Legacy Mode).

Parameter	Value	Descripton
`-lp`	<path>	Specify the Approved List **Note** After installing StellarProtect (Legacy Mode) and creating the Approved List, the list can be exported.
`-qp`	<path>	Specify the folder path for quarantined files when custom action is set to “quarantine” mode
`-nps`		Do not execute Prescan
`-ips`		Do not cancel installation when Prescan detects threats

An example of using CLI for silent installation without creating a desktop shortcut would look like this:

```
StellarSetup.exe -s -p <administrator_password> -nd
```

License Activation for Standalone Agent

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

Procedure

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

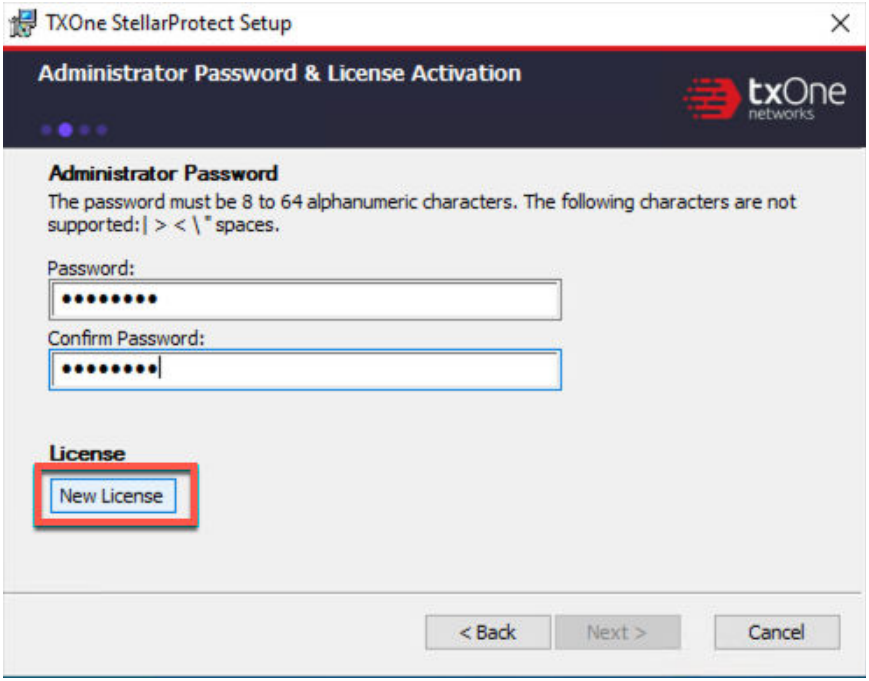


FIGURE 2-36. License Activation - New License Button

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:

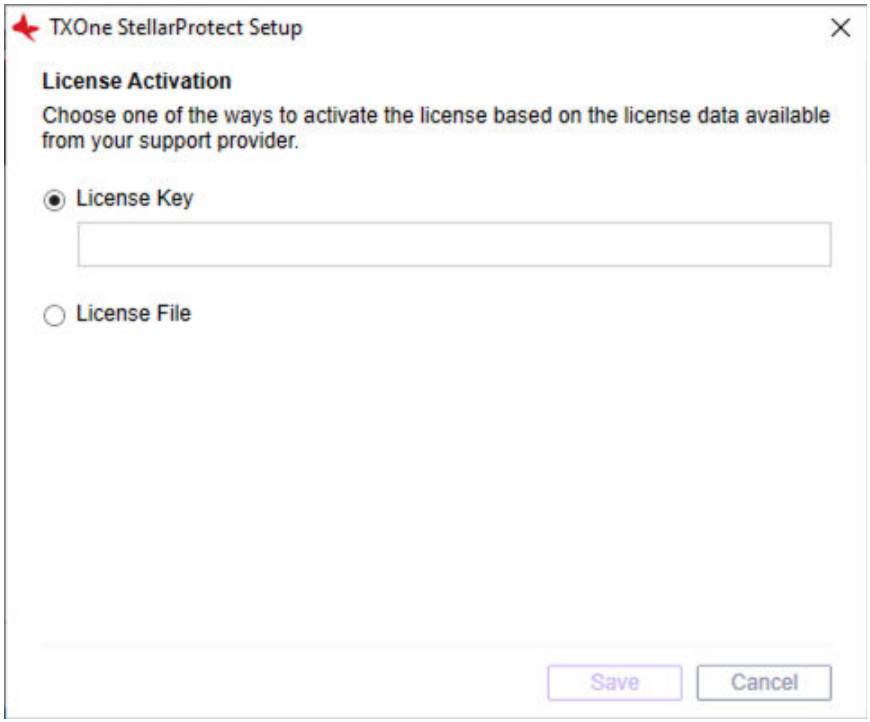


FIGURE 2-37. License Activation - License Key or License File

- 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 should be automatically generated. Check if it matches the license data provided by your support provider.

  - Click **Save**.

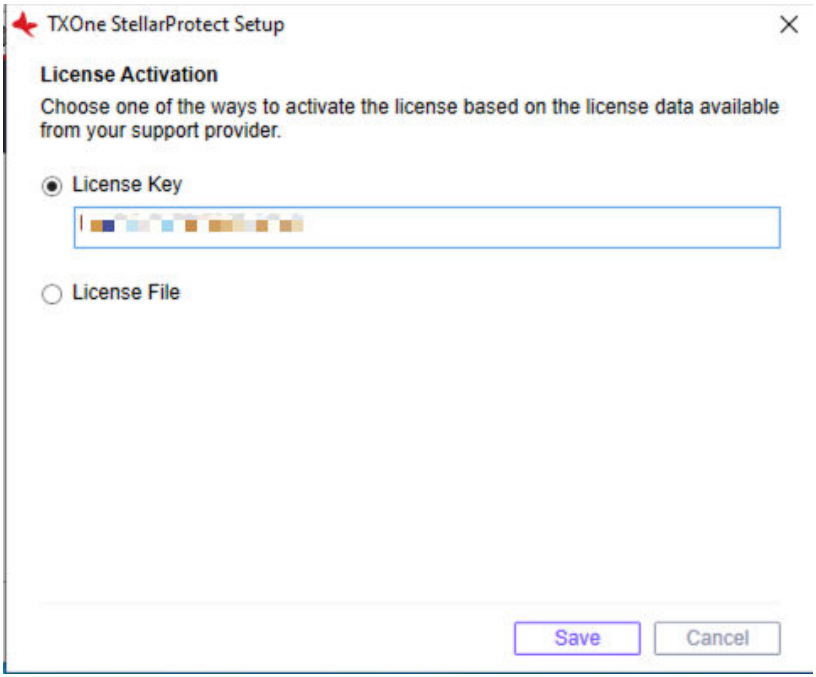


FIGURE 2-38. License Activation - License Key

- Click **License File**
  - Select the License File (a `.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, see *Getting the License File and PSN for Standalone Agents on page 2-95* for detailed instructions.

  - Click **Save**.

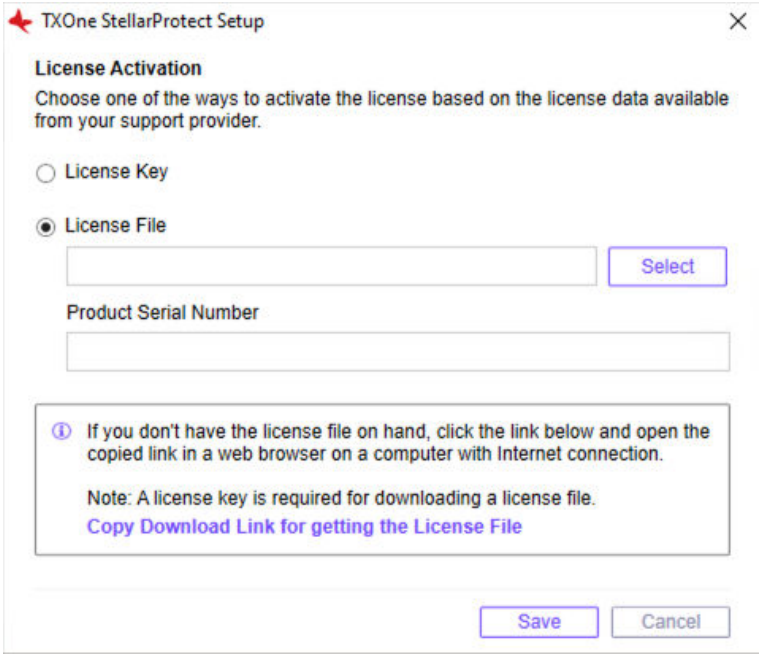


FIGURE 2-39. License Activation - License File

Note

- If a license file expiration error message appears and the agent's installer package was downloaded from StellarOne, please get the latest License File and Product Serial Number from StellarOne. See *Getting the Latest License File from StellarOne on page 2-102* for instructions.
- A full license can not be converted to a trial license.

3. A success message appears. Click **Next** to proceed to the next procedure for the installation.

Note

- For StellarProtect agent, the next procedure should be **Step 7** in *Attended Installation of StellarProtect on page 2-5*.
- For StellarProtect (Legacy Mode) agent, the next procedure should be **Step 8** in *Attended Installation of StellarProtect (Legacy Mode) on page 2-25*.

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 2-95*
- *Getting the Latest License File from StellarOne on page 2-102*

Getting the License File and PSN for Standalone Agents

To activate licenses 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 installation process with GUI. See *About the Download Link for Getting License File on page 2-98* 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.

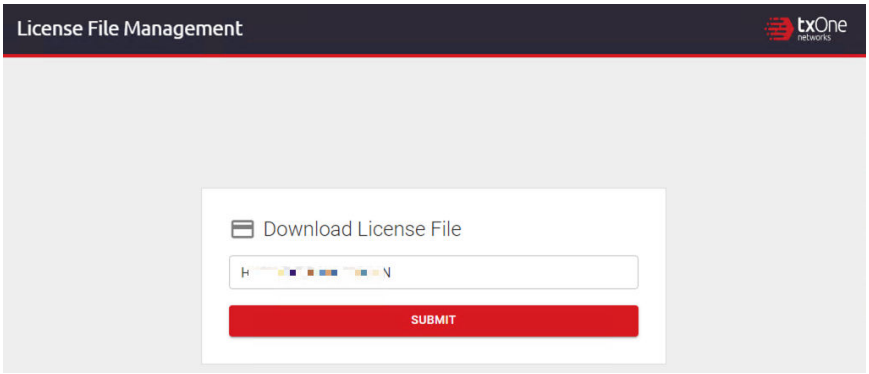


FIGURE 2-40. License File Management

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.

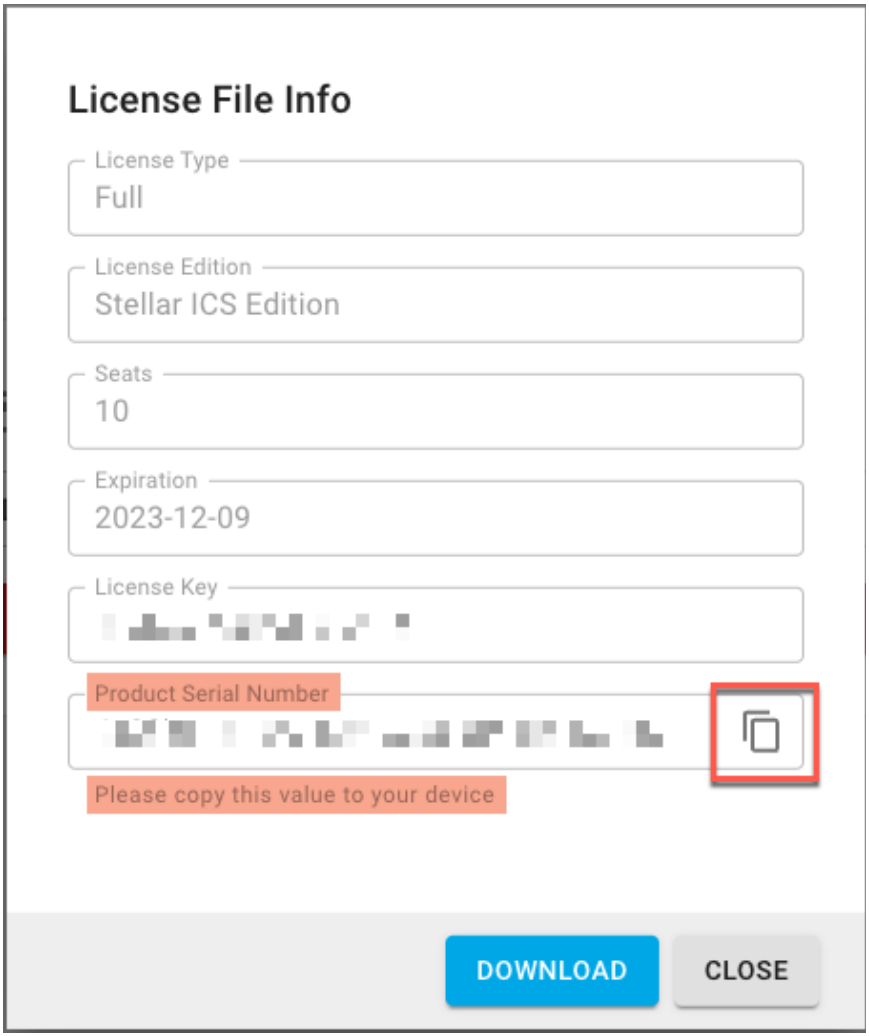


FIGURE 2-41. License Information

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).

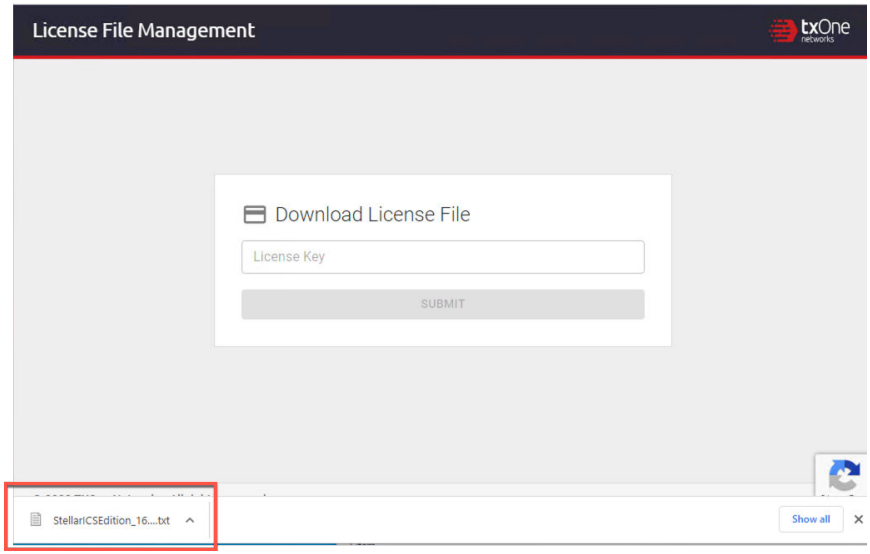


FIGURE 2-42. License File Downloaded

Note

Please find the license file in the downloads folder.

About the Download Link for Getting License File

Users can also copy the URL of TXOne **License File Management** web page during the installation process with GUI.

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.

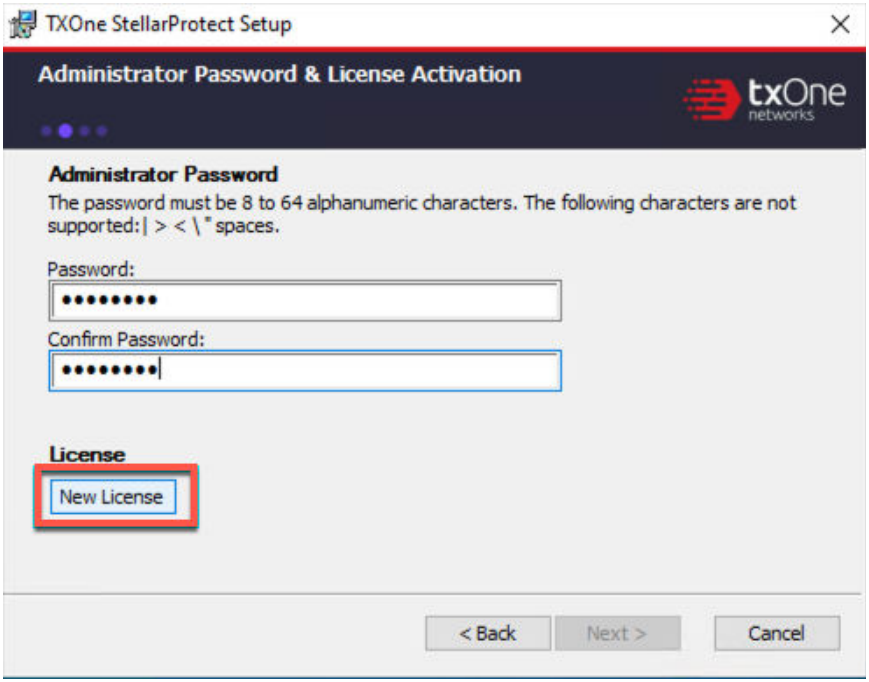


FIGURE 2-43. License Activation - New License Button

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.

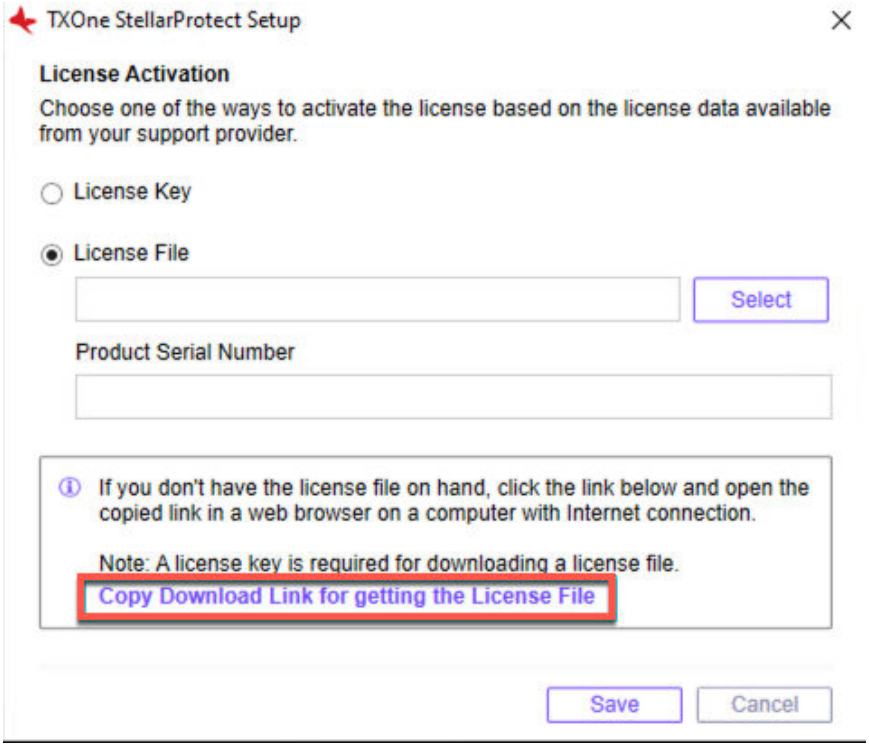


FIGURE 2-44. Copy the Download Link

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

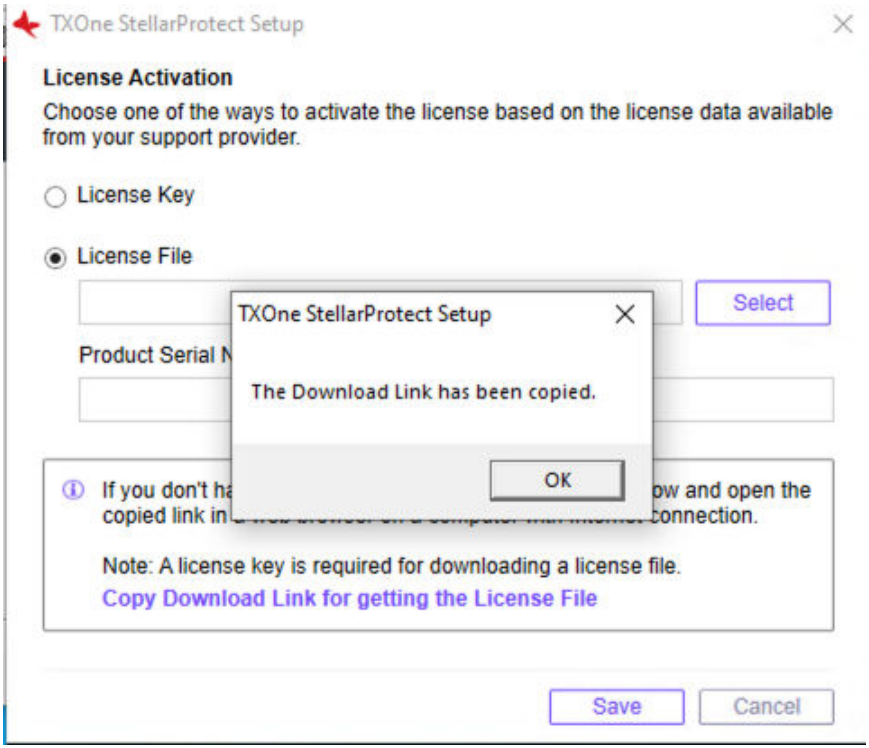


FIGURE 2-45. Download Link Copied

5. Open the copied link in a web browser on a computer with Internet connection. You will be directed to TXOne **License File Management** website.

Note

See *Getting the License File and PSN for Standalone Agents on page 2-95* 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.

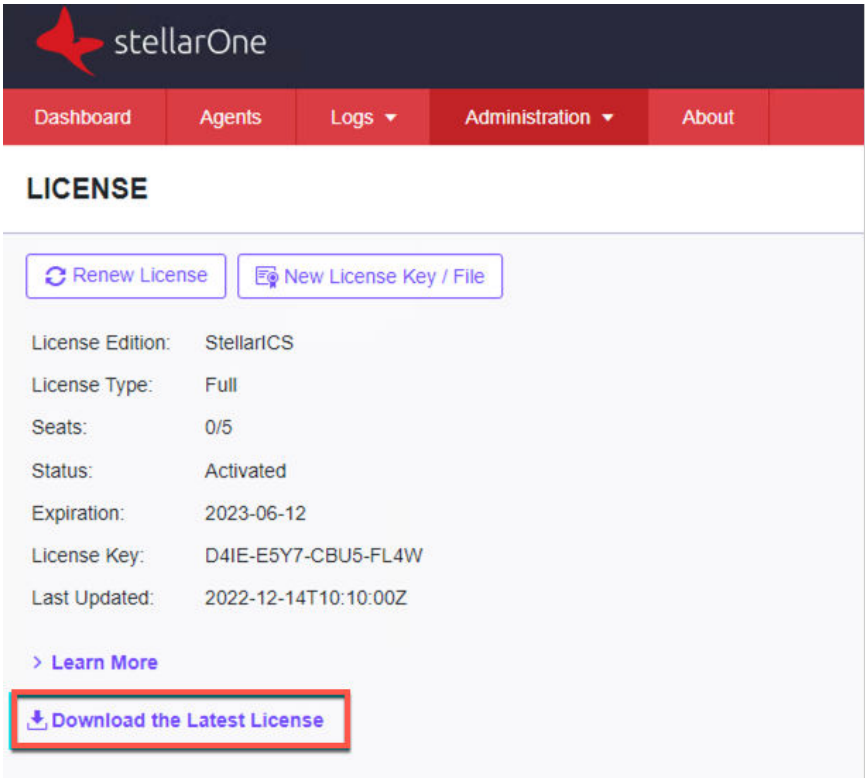


FIGURE 2-46. Download License File from StellarOne

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.

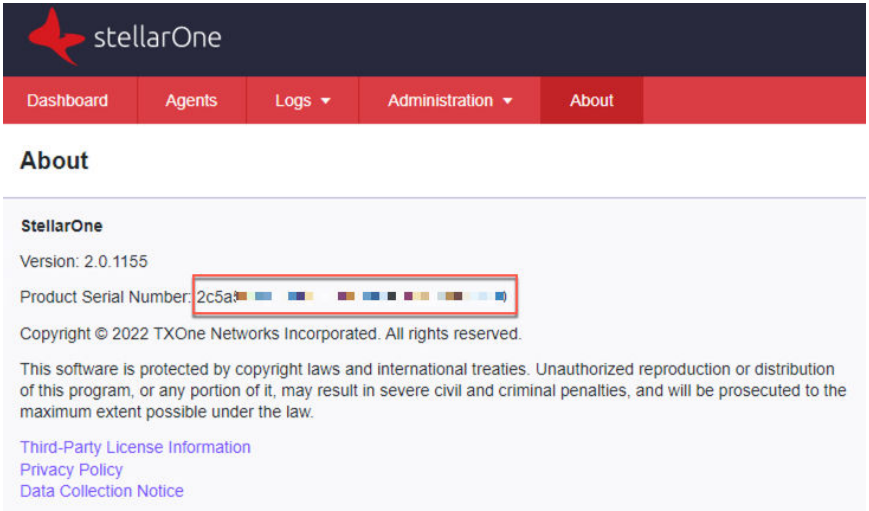


FIGURE 2-47. Get Product Serial Number from StellarOne

Replicating Installation Configuration for Multiple Standalone Agents

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

Procedure

1. See *Getting the License File and PSN for Standalone Agents on page 2-95* 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` config file as mentioned in *Sample Config File for Silent Installation on page 2-79*.

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.

Proxy Settings

If StellarProtect/StellarProtect (Legacy Mode) agents use a proxy server for both communication with StellarOne and scan component updates, it is configurable using `StellarSetup.ini` before installation and the command line interface afterwards.

- For more information about using `StellarSetup.ini` to configure the proxy settings before installation, refer to *Configuration File for Silent Installation on page 2-42*
- For more information about using command line interface to configure the proxy settings after installation, see *TXOne StellarProtect Administrator's Guide* for the list of all commands.

Chapter 3

Agent Configuration File Deployment

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

For mass deployment, TXOne Networks recommends first installing StellarProtect or StellarProtect (Legacy Mode) on a test endpoint to confirm the correct operation of all parameters, since a customized configuration may require a valid agent configuration file and Approved List.

Note

Refer to *TXOne StellarProtect Administrator's Guide* for more information about the Approved List and 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, import the sample config file to the target agents.

Two alternative configuration deployment methods are available:

- Without using the GUI: Use the `StellarSetup.ini` file
  - For StellarProtect, find the `import_source` property in the `[protect_client]` section in the `StellarSetup.ini` file, and then specify the path to the folder containing the sample config file. See *Configuration File for Silent Installation on page 2-42* for more details.
  - For StellarProtect (Legacy Mode), manually add the `CONFIG_PATH` property in the `StellarSetup.ini` file, and then specify the file path to the sample config file. See *Hidden Properties in the Config File for Silent Installation on page 2-71* for more details.
- With the GUI: See below as the instructions on how to use the **Export/Import Settings** buttons on the agent console

Note

Only StellarProtect (Legacy Mode) supports exporting/importing settings with the GUI.

Procedure

1. Open the agent 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 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.

Note

Only StellarProtect (Legacy Mode) supports this function.

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

Note

Only StellarProtect (Legacy Mode) supports this function.

Procedure

1. Prepare a customized agent configuration file or Approved List.
   a. Export and download an agent configuration file or Approved List.
   b. Customize the downloaded file.

Note

To ensure successful import, verify that the file to import meets the following requirements:

- File is in the CSV format and uses UTF-8 encoding
- For Approved List, maximum file size supported is 20 MB
- For agent configuration file, maximum file size supported is 1 MB

2. Click **Agents** from the StellarOne console. The **Agent management** screen appears.
3. To import the customized file to agents, follow the steps below.
   a. From the Endpoint column, select one or more agents.
   b. Click **Import/ Export**
   c. Select **Import Approved List** or **Import Agent Configuration**. The import dialog will appear.
4. To import the customized file to an agent group, follow the steps below.
   a. From the left panel, select an agent group and go to **Import / Export**.
   b. Select **Import Approved List** or **Import Agent Configuration**. The import dialog will appear.
5. By default, StellarOne does the following:
   - **Approved List**: accumulates items from the customized Approved List to the target Approved Lists. To replace the target Approved Lists with the customized Approved List, select **Overwrite the existing Approved List**.
   - **Agent Configuration**: overwrites the target Approved Lists with the customized Approved List.
6. Click **Browse** to select the customized file.
7. Click **OK**.

Chapter 4

Upgrade

This chapter describes how to upgrade the StellarProtect and StellarProtect (Legacy Mode) agents by installing patches.

Topics in this chapter include:

Supported Upgrade Paths

The following tables illustrate the supported upgrade paths for StellarProtect and StellarProtect (Legacy Mode) agents.

TABLE 4-1. Supported Upgrade Paths for StellarProtect

CURRENT VERSION	SUPPORTED TARGET UPGRADE VERSION	LOCAL UPGRADE	REMOTE UPGRADE
2.2	3.0	√	√
2.1	2.2 / 3.0	√	√
2.0	2.1 / 2.2 / 3.0	√	√
1.2 Patch 1	2.0 / 2.1 / 2.2 / 3.0	√	√
1.2	1.2 Patch 1 / 2.0 / 2.1 / 2.2 / 3.0	√	√
1.1	1.2 / 1.2 Patch 1 / 2.0 / 2.1 / 2.2 / 3.0	√	√
1.0	1.1 / 1.2 / 1.2 Patch 1 / 2.0 / 2.1 / 2.2 / 3.0	√	N/A

TABLE 4-2. Supported Upgrade Paths for StellarProtect (Legacy Mode)

CURRENT VERSION	SUPPORTED TARGET UPGRADE VERSION	LOCAL UPGRADE	REMOTE UPGRADE
1.5	3.0	√	√
1.4	1.5 / 3.0	√	√
StellarProtect (Legacy Mode) 1.3	1.4 / 1.5 / 3.0	√	√
1.2 Patch 1	StellarProtect (Legacy Mode) 1.3 / 1.4 / 1.5 / 3.0	√	√
1.2	1.2 Patch 1	√	√

Current Version	Supported Target Upgrade Version	Local Upgrade	Remote Upgrade
1.1	1.2 / 1.2 Patch 1	√	√
StellarEnforce 1.0	1.1 / 1.2 / 1.2 Patch 1	√	N/A

Note

- The StellarEnforce was renamed StellarProtect (Legacy Mode) upon the release of version 1.3.
- To directly upgrade StellarEnforce/StellarProtect (Legacy Mode) from versions below 1.2 Patch 1 to versions older than 1.2 Patch1, add the patch file hash as the trusted hash and enable the PTU function before executing the upgrade.

Preparing the Agent for Upgrade to a Later Version

See the following table for the appropriate actions to take according to your chosen installation method.

Note

- The latest updates can be downloaded from the StellarProtect Software Download Center.
- Before upgrading, close the StellarProtect or StellarProtect (Legacy Mode) agent console and/or wksupporttool UI, and check the *Supported Upgrade Paths on page 4-2* for StellarProtect or StellarProtect (Legacy Mode).

WARNING!

- If the agents are managed by StellarOne, ensure you upgrade the StellarOne server first before upgrading the StellarProtect or StellarProtect (Legacy Mode) agents.
- Do not register StellarProtect (Legacy Mode) 3.0 to StellarOne 2.2 or older versions.

TABLE 4-3. Post-Installation Agent Upgrade

INSTALLATION METHOD	REQUIRED ACTION	SETTINGS RETAINED
Local upgrade	**StellarProtect**: Extract the patch zip file and deploy patching by running `txone_sp_full_patch_win_en.exe`.	Compatible settings retained

	StellarProtect (Legacy Mode):
	Deploy patching by running `PATCH-FILE.exe`, e.g., if you want to upgrade the agent to version 3.0, deploy patching by running `txsplm-3.0-agent-b1051-patch-en.exe`.
	To execute a silent upgrade, open the command prompt as an administrator and enter the following command:
	`PATCH-FILE.exe -s -a -s/g`
	For example, type
	`txsplm-3.0-agent-b1051-patch-en.exe -s -a -s/g`
	to deploy the 3.0 patch file in silent mode.
		Compatible settings retained

Remote upgrade	See the StellarOne Administrator's Guide for how to deploy patches to the agents remotely.	Compatible settings retained

Installation Method	Required Action	Settings Retained
	Note TXOne recommends using StellarOne 2.0 console or above to remotely deploy patches to the managed agents.	

Chapter 5

License Renewal

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

License Renewal for Standalone Agents

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

Note

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

The following instructions take StellarProtect as an example for how to renew license for standalone StellarProtect or StellarProtect (Legacy Mode) agents. StellarProtect (Legacy Mode) would require you to follow similar procedures with slight differences in the GUI.

Procedure

1. Click the **New License** button on the StellarProtect logon screen.

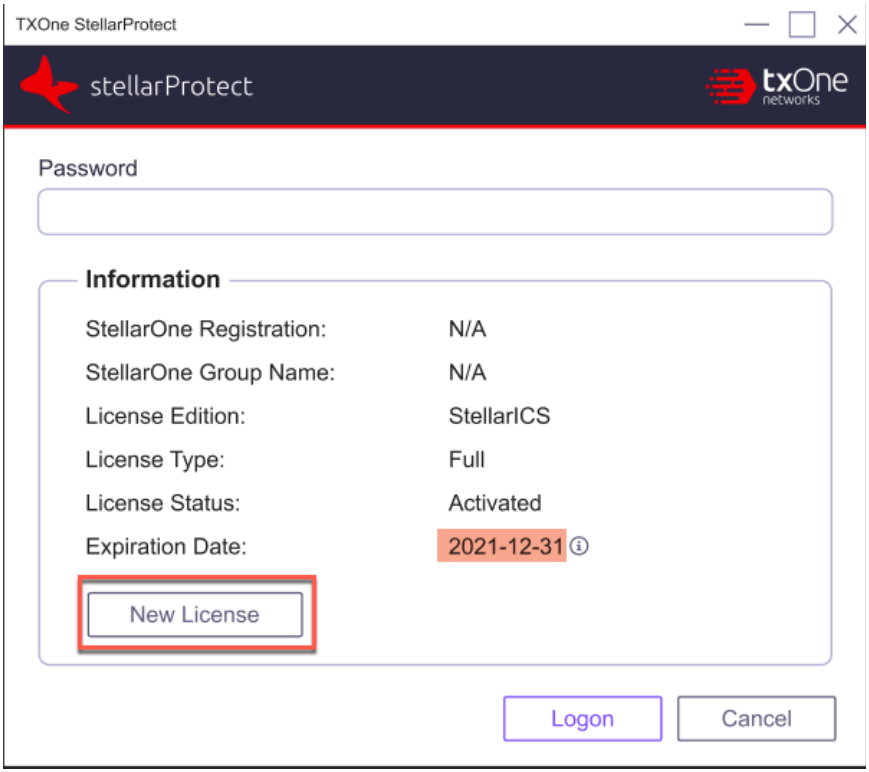


FIGURE 5-1. Renew License for Standalone Agents

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**.

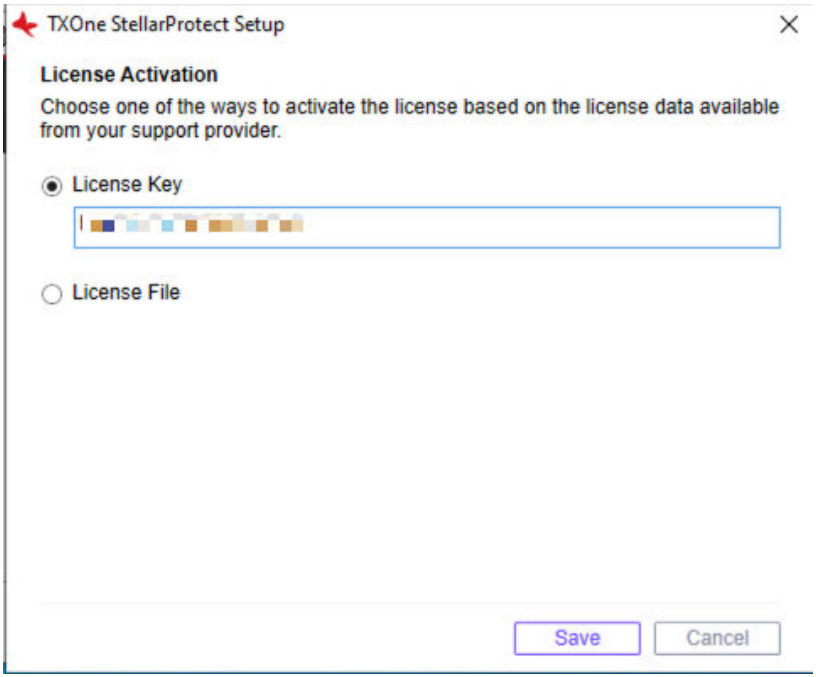


FIGURE 5-2. Use License Key for Activation

- Click **License File**
  - Select the License File (a `.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 2-95* for detailed instructions.

- Click **Save**.

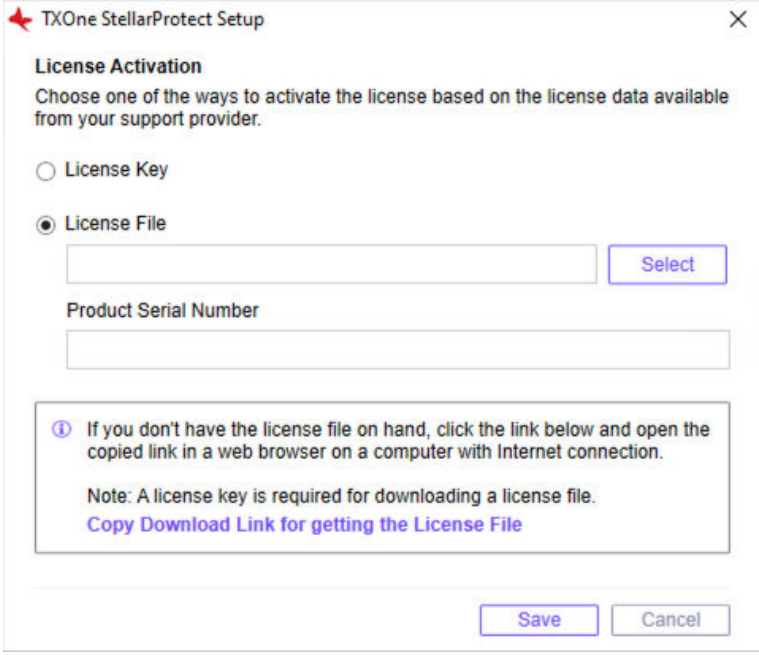
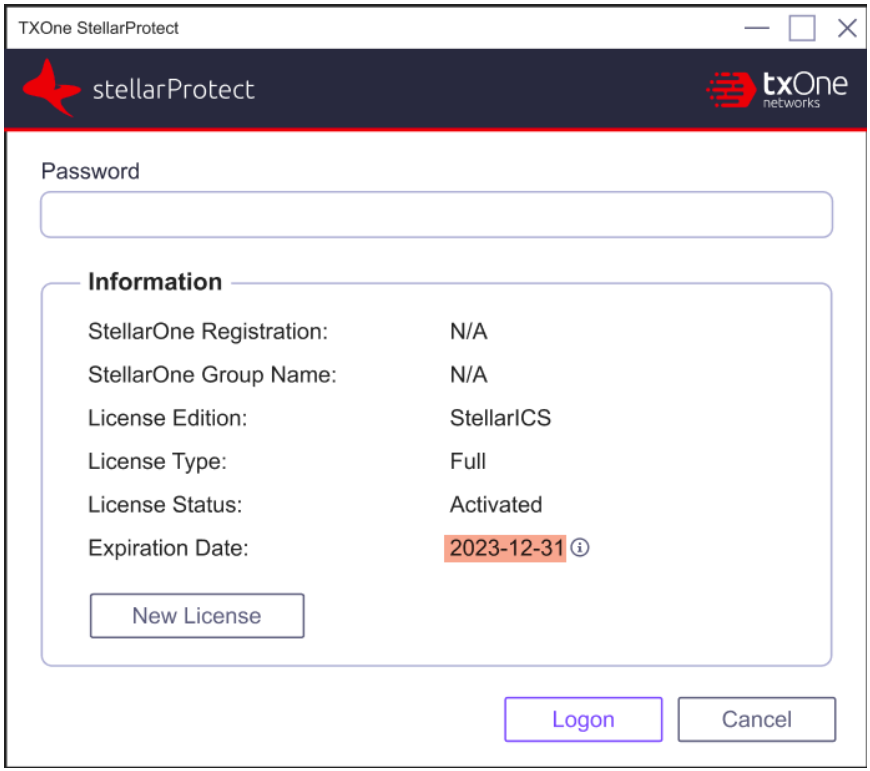


FIGURE 5-3. Use License File for Activation

3. Check the StellarProtect logon screen for the updated license expiration date.

FIGURE 5-4. License Renewed for Standalone Agents


TXOne StellarProtect
stellarProtect
txOne networks
Password
Information
StellarOne Registration:
N/A
StellarOne Group Name:
N/A
License Edition:
StellarICS
License Type:
Full
License Status:
Activated
Expiration Date:
2023-12-31
New License
Logon
Cancel

Chapter 6

Uninstalling StellarProtect/ StellarProtect (Legacy Mode)

Follow the instructions to uninstall StellarProtect or StellarProtect (Legacy Mode).

Note

StellarProtect or StellarProtect (Legacy Mode) administrator password is required to uninstall StellarProtect or StellarProtect (Legacy Mode) from an endpoint.

Important

Please make sure the StellarProtect or StellarProtect (Legacy Mode) UI is not open.

Procedure

1. On an endpoint with the StellarProtect or StellarProtect (Legacy Mode) agent installed, launch StellarProtect or StellarProtect (Legacy Mode) Setup.
2. Follow one of the procedures listed below according to your operating system:

Operating System	Procedure

• Windows 10 Professional
• Windows 10 Enterprise
• Windows 10 IoT Enterprise
• Windows 10 Fall Creators Update (Redstone 3)
• Windows 10 April 2018 Update (Redstone 4)
• Windows 10 November 2018 Update (Redstone 5)
• Windows 11 Professional
	a. Go to **Start** > **Settings**.
	b. Depending on your version of Windows 10, locate the **Apps & Features** section under one of the following categories:
	  • **System**
	  • **Apps**
	c. On the left pane, click **Apps & Features**.
	d. In the list, click **StellarProtect** or **StellarProtect (Legacy Mode)**.
	e. Click **Uninstall**.

• Windows 7 • Windows 8 • Windows Vista • Windows Server 2008 • Windows Server 2012 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022 • Windows Storage Server 2012 • Windows Storage Server 2016	a. Go to **Start** > **Control Panel** > **Program and Features**. b. In the list, double-click **TXOne StellarProtect** or **TXOne StellarProtect (Legacy Mode)**.
• Windows Server 2003 • Windows XP • Windows 2000	a. Go to **Start** > **Control Panel** > **Add or Removew Programs**. b. In the list, select **TXOne StellarProtect (Legacy Mode)**. c. Click **Remove**.

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

4. Enter in the StellarProtect or StellarProtect (Legacy Mode) administrator password and click **Next**.
5. Make sure StellarProtect's or StellarProtect (Legacy Mode)'s UI is completely closed before clicking **OK**.
6. The message box indicating StellarProtect or StellarProtect (Legacy Mode) being successfully removed will appear. Click **Finish**.

Note

For Windows 7 and Windows Server 2016+ platforms, the installation of StellarProtect requires disabling Windows Defender first. Consequently, after uninstalling StellarProtect, TXOne Networks recommends that you manually enabling Windows Defender for security reasons.

Chapter 7

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 7-1. 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 7-2. 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.

Appendix A

StellarProtect (Legacy Mode) Limitations by Operating Systems

StellarProtect (Legacy Mode) installed on the following operating systems has the limitations as described below.

Operating Systems	Limitations

Windows 10	• 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.
	• 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.

Windows 10 Fall Creators Update	OndDrive integration is not supported. Ensure that OneDrive integration is disabled before installing StellarProtect (Legacy Mode).

Operating Systems	Limitations

Windows 10 April 2018 Update (Redstone 4) and later versions	• OndDrive integration is not supported. Ensure that OneDrive integration is disabled before installing StellarProtect (Legacy Mode).
	• See the following limitations when working with folders where the *case sensitive* attribute has been enabled:
	  • Enabling the *case sensitive* attribute for a folder may prevent StellarProtect (Legacy Mode) from performing certain actions (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 from folders where the *case sensitive* attribute is enabled. Additionally, StellarProtect (Legacy Mode) is unable to provide any information for the blocked processes, except for file path.
	  • The StellarProtect (Legacy Mode) agent cannot verify file signatures of files saved in folders where the *case sensitive* attribute is enabled. As a result, DAC exceptions related to signatures cannot work.

Windows XP Embedded SP1	The custom action of “quarantine” for Application Lockdown or Real-Time Scan is not supported
• Windows 2000 SP4 (without update rollup) • Windows XP SP1 • Windows XP Embedded • Windows 2000 Server SP4	The following functions are not supported: • DLL/Driver Lockdown • Script Lockdown • Integrity Monitoring • USB Malware Protection • Storage Device Blocking • Maintenance Mode • Predefined Trusted Updater

Index

TXONE NETWORKS INCORPORATED

222 West Las Colinas Boulevard, Suite 1650
Irving, TX 75039 U.S.A
Email: support@txone.com
www.txone.com

www.txone.com

Item Code: APEM39736/230619