txOne networks | Keep the Operation Running

# 2.1 TXOne StellarProtect

## Installation and Administrator's Guide

All-terrain protection for mission critical assets

Windows

SC 2022 awards EUROPE WINNER

Document Part No.: APEM219658/221221

Release Date: January 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, StellarProtect, and StellarProtect (Legacy Mode) collect and provides detailed instructions on how to disable the specific features that feedback the information.

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

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

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

# Table of Contents

## Preface

## Chapter 1: Introduction

## Chapter 2: Installation

## Index

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

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

# Preface

## Preface

This Installation and Administrator's Guide introduces TXOne Networks StellarProtect ™ and convers all aspects of product installation and management.

Topics in this chapter include:

- *About the Documentation on page viii*
- *Audience on page viii*
- *Document Conventions on page viii*
- *Terminology on page ix*

# 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 and Administrator's Guide | A PDF document that discusses requirements and procedures for installing and managing StellarProtect. |
| Knowledge Base | An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following websites:<br>https://kb.txone.com/<br>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 |
| **Bold** | Menus and menu commands, command buttons, tabs, and options |
| *Italics* | References to other documents |
| `Monospace` | Sample command lines, program code, web URLs, file names, and program output |
| **Navigation** > **Path** | The navigation path to reach a particular screen<br>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 |
| managed agents<br>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 ™ agent |
| 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:<br>`C:\Program Files\TXOne\StellarProtect` |

# Chapter 1

## Introduction

This section introduces TXOne StellarProtect ™, which provides industrial-grade next-generation antivirus and lockdown protection for your assets, and gives an overview of its functions.

Topics in this chapter include:

- *About TXOne Stellar on page 1-2*
- *Key Features and Benefits on page 1-2*
- *What's New on page 1-3*
- *System Requirements on page 1-4*
- *Preparing the Agent for Upgrade to a Later Version on page 1-7*

# About TXOne Stellar

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

- StellarOne™ , the centralized management console designed to streamline administration of both StellarProtect for modernized systems and StellarProtect (Legacy Mode) for legacy systems.
- StellarProtect ™, the unified agent with industrial-grade next-generation antivirus and application lockdown endpoint security deployment for modernized OT/ICS endpoints.
- StellarProtect (Legacy Model) ™, for trust-list based application lockdown of legacy and fixed-use OT/ICS endpoints with anti-malware or on-demand AV scan.

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

# Key Features and Benefits

The StellarProtect provides following features and benefits.

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

| FEATURE | BENEFIT |
|---|---|
| Application Lockdown | Prevents malware attacks and increases protection level by allowing only the files defined in an Approved List to be executed |
| Industrial-Grade Next-Generation Antivirus | OT/ICS root of trust and advanced threat scan secure OT/ICS assets with no interruption to operations |
| Operations Behavior Anomaly Detection | Detects abnormal operations and exercises least privilege-based control to prevent malware-free attacks |

| Feature | Benefit |
|---|---|
| OT Application Safeguard | Intelligently locates and secures the integrity of the OT/ICS process from OT/ICS targeted attacks by device |
| Device Control | Prevents insider threats by only allowing usage of USB ports on a case-by-case administrator reviewed basis |
| Maintenance Mode | To perform file updates on endpoints, users can configure Maintenance Mode settings to define a period when StellarProtect allows all file executions and adds all files that are created, executed, or modified to the Approved List. |
| Compatibility with Trend Micro Portable Security 2 and 3 | StellarProtect is compatible with Trend Micro Portable Security products. |

## What's New

TXOne StellarProtect 2.1 provides following new features and enhancements.

**Table 1-2. What's New in TXOne StellarProtect 2.1**

| Feature | Benefit |
|---|---|
| Self-management status | The self-management status displayed on the agent's console GUI enables users to know whether the agent is following StellarOne's policy settings. |
| Silent manual scan | The silent manual scan CLI would trigger agents to perform silent manual scan and send the scan result to StellarOne. |
| Single installer package | A single installer package for the Agent – StellarProtect and StellarProtect (Legacy Mode) is available now. After being invoked, the single installer package can identify the version of Windows installed on the endpoint and launch the suitable installer for the endpoint to install. |
| Supporting license key/file | Supports license key and license file for product activation |

# System Requirements

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

## Software and Hardware Requirements

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

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

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

By default, StellarProtect 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 has been changed to **https://ttau.cs.txone.com**. Please ensure that you whitelist this URL in your firewall.

**Important**

- StellarProtect 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 agent environment to communicate with StellarOne.
  - Intermediate Symantec Class 3 SHA256 Code Signing CA
  - Root VeriSign Class 3 Public Primary Certification Authority - G5

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

**Tip**

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

## Operating Systems

### Windows Client:

- Windows 7 (NoSP/SP1) [Professional/Enterprise/Ultimate] (32/64bit)
- Windows 8 (NoSP) [Pro/Enterprise] (32/64bit)
- Windows 8.1 (NoSP) [Pro/Enterprise/with Bing] (32/64bit)
- Windows 10 [Pro/Enterprise/IoT Enterprise] (32/64bit) Anniversary Update, Creators Update, Fall Creators Update, April 2018 Update, November 2018 Update, May 2019 Update, November 2019 Update, May 2020 Update, October 2020 Update, May 2021 Update, November 2021 Update, 2022 Update
- Windows 11 (NoSP) [Pro/Enterprise] (64bit) 2022 Update
- Windows Embedded POSReady 7 (NoSP) (32/64bit)
- Windows Embedded 8 Industry (NoSP) [Pro/Enterprise] (32/64bit)
- Windows Embedded 8.1 Industry (NoSP) [Pro/Enterprise/Sideloading] (32/64bit)

### Windows Server:

- 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 2016 (NoSP) (64bit)

## Preparing the Agent for Upgrade to a Later Version

This version of StellarProtect supports upgrade from the following version:

- StellarProtect 1.0
- StellarProtect 1.1
- StellarProtect 1.2
- StellarProtect 1.2 Patch 1
- StellarProtect 2.0

The latest updates can be downloaded from the StellarProtect Software Download Center.

**Note**

Before upgrading, close the StellarProtect agent console.

**WARNING!**

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

**TABLE 1-5. Fresh Installation of the StellarProtect Agent**

| INSTALLATION METHOD | INSTALLED AGENT VERSION | REQUIRED ACTION | SETTINGS RETAINED |
|---|---|---|---|
| Local installation using Windows installer | StellarProtect 1.0 / 1.1 / 1.2 / 1.2 Patch 1 / 2.0 | Manually uninstall | No settings retained |
| Local installation using command line interface installer | StellarProtect 1.0 / 1.1 / 1.2 / 1.2 Patch 1 / 2.0 | Manually uninstall | No settings retained |

**TABLE 1-6. Post-Installation Agent Upgrade**

| INSTALLATION METHOD | INSTALLED AGENT VERSION | REQUIRED ACTION | SETTINGS RETAINED |
|---|---|---|---|
| Extract patch zip file and patching by running `txone_sp_full_patch_win_en.exe` | StellarProtect 1.0 / 1.1 / 1.2 / 1.2 Patch 1 / 2.0 | No preparation needed | Compatible settings retained |
| Remote Installation | StellarProtect 1.1 / 1.2 / 1.2 Patch 1 / 2.0<br>**Note**<br>StellarProtect 1.0 supports only local installation. | StellarOne 2.0 console or above | Compatible settings retained |

# Chapter 2

# Installation

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

Topics in this chapter include:

# Agents Installed in Managed or Standalone Mode

TXOne Stellar offers two modes for agent management:

- Agents installed in ***Managed*** mode are managed by a StellarOne server, which can issue remote commands to all managed agents. To deploy agent configuration settings to multiple managed agents, launch the StellarOne web console and use the **Send Command** menu located on the **Agent** management screen.
- Agents installed in ***Standalone*** mode are not managed by a TXOne StellarOne central management console server; instead, they are managed by the local administrator or operator. To manually deploy a single configuration to multiple standalone agents, use an agent configuration file.

# StellarProtect Installation Flow

The installation of StellarProtect requires performing following tasks:

**Procedure**

1. Get the agent's installer package from the StellarOne web console. Refer to *Getting the Agent's Installer Package via StellarOne on page 2-4* for instructions.

   **Note**

   For standalone agents, get the installer package from the Software Download Center. Refer to *Getting the Standalone Agent's Installer Package on page 2-5* for more details.

2. (Optional) Download the `group.ini` file for registering the agent to StellarOne during the installation process.
3. Determine the installation method:

- *Attended Installation on page 2-6*
- *Silent Installation on page 2-21*

**4.** Launch the agent's installer on the endpoint.

a. Check to accept the EULA (End-User License Agreement)

b. Specify the Administrator password and activate the license

c. Determine the asset information and installation settings

d. Check to remove the detected incompatible software and residual files

e. (Optional but recommended) Prescan for malware scanning and OT application identification

f. (Optional but recommended) Create Approved List and enable Application Lockdown "Detect" mode

**Note**

- Since the StellarOEM license edition does not support Real-Time Malware Scan, **Step 4.e** should not appear during the installation process.
- Since the StellarKiosk license edition does not support Application Lockdown, **Step 4.f** should not appear during the installation process.

## Getting the Agent's Installer Package

For agents managed by the StellarOne web console, refer to *Getting the Agent's Installer Package via StellarOne on page 2-4*.

For standalone agents, refer to *Getting the Standalone Agent's Installer Package on page 2-5*.

## Getting the Agent's Installer Package via StellarOne

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

### Procedure

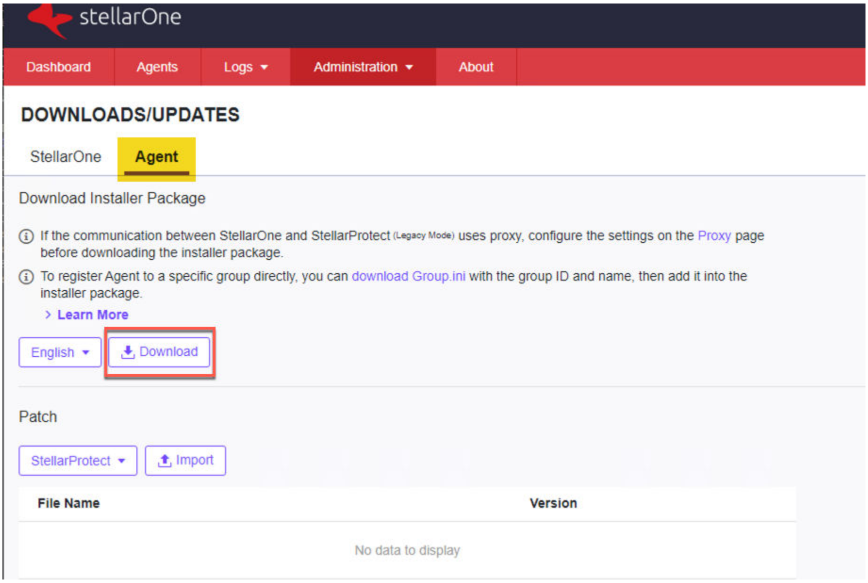
1. Log on the StellarOne web console.

   **Note**

   If this is the first time the StellarOne console being logged on, refer to StellarOne Installation Guide for detailed instructions on the initial settings.

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

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



ⓘ If the communication between StellarOne and StellarProtect (Legacy Mode) uses proxy, configure the settings on the Proxy page before downloading the installer package.

ⓘ To register Agent to a specific group directly, you can download Group.ini with the group ID and name, then add it into the installer package.

| File Name | Version |
|---|---|
| No data to display | |

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

**Note**

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

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

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

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

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

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

## Getting the Standalone Agent's Installer Package

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

**Procedure**

1. Go to our Software Download Center.

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

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

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

**Note**

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

# Installation Methods

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

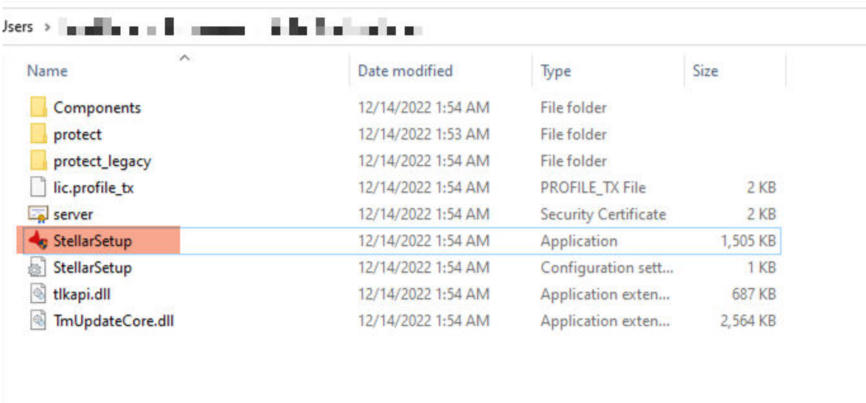
## Attended Installation

**Procedure**

1. Launch the installer `StellarSetup.exe`.

**Note**

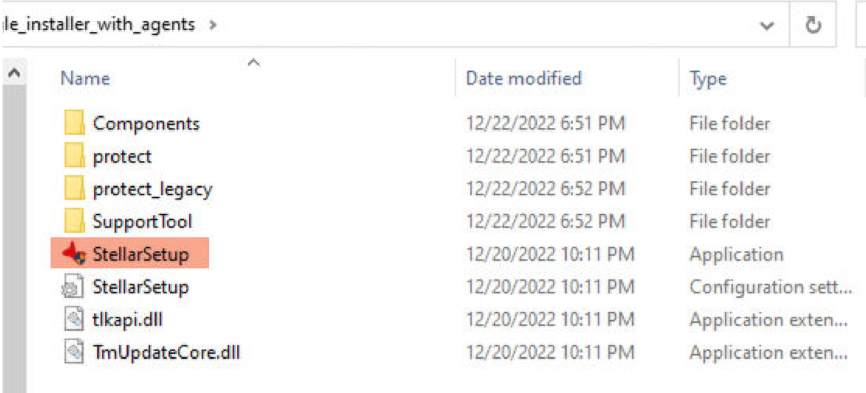
The installer package downloaded from StellarOne management console differs slightly from that downloaded from the Software Download Center. One contains the StellarOne data files while the other one does not.



Jsers > [redacted]

| Name | Date modified | Type | Size |
|---|---|---|---|
| Components | 12/14/2022 1:54 AM | File folder | |
| protect | 12/14/2022 1:53 AM | File folder | |
| protect_legacy | 12/14/2022 1:54 AM | File folder | |
| lic.profile_tx | 12/14/2022 1:54 AM | PROFILE_TX File | 2 KB |
| server | 12/14/2022 1:54 AM | Security Certificate | 2 KB |
| StellarSetup | 12/14/2022 1:54 AM | Application | 1,505 KB |
| StellarSetup | 12/14/2022 1:54 AM | Configuration sett... | 1 KB |
| tlkapi.dll | 12/14/2022 1:54 AM | Application exten... | 687 KB |
| TmUpdateCore.dll | 12/14/2022 1:54 AM | Application exten... | 2,564 KB |

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



le_installer_with_agents >

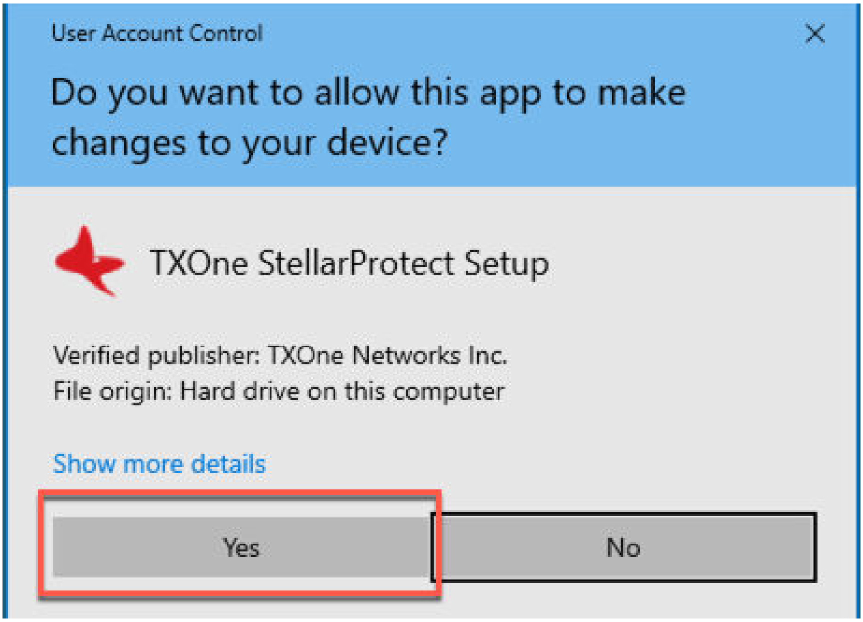
| Name | Date modified | Type |
|---|---|---|
| Components | 12/22/2022 6:51 PM | File folder |
| protect | 12/22/2022 6:51 PM | File folder |
| protect_legacy | 12/22/2022 6:52 PM | File folder |
| SupportTool | 12/22/2022 6:52 PM | File folder |
| StellarSetup | 12/20/2022 10:11 PM | Application |
| StellarSetup | 12/20/2022 10:11 PM | Configuration sett... |
| tlkapi.dll | 12/20/2022 10:11 PM | Application exten... |
| TmUpdateCore.dll | 12/20/2022 10:11 PM | Application exten... |

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

**Note**

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

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



User Account Control

Do you want to allow this app to make changes to your device?

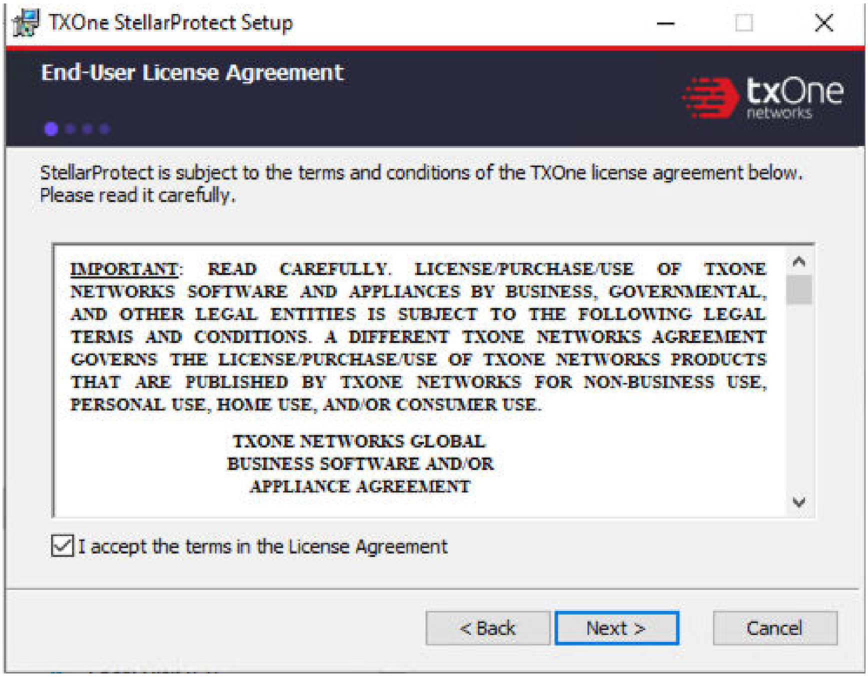
TXOne StellarProtect Setup

Verified publisher: TXOne Networks Inc.
File origin: Hard drive on this computer

**FIGURE 2-4. StellarProtect Setup Screenshot**

3. Click **Next** to continue.

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



StellarProtect is subject to the terms and conditions of the TXOne license agreement below. Please read it carefully.

IMPORTANT: READ CAREFULLY. LICENSE/PURCHASE/USE OF TXONE NETWORKS SOFTWARE AND APPLIANCES BY BUSINESS, GOVERNMENTAL, AND OTHER LEGAL ENTITIES IS SUBJECT TO THE FOLLOWING LEGAL TERMS AND CONDITIONS. A DIFFERENT TXONE NETWORKS AGREEMENT GOVERNS THE LICENSE/PURCHASE/USE OF TXONE NETWORKS PRODUCTS THAT ARE PUBLISHED BY TXONE NETWORKS FOR NON-BUSINESS USE, PERSONAL USE, HOME USE, AND/OR CONSUMER USE.

TXONE NETWORKS GLOBAL
BUSINESS SOFTWARE AND/OR
APPLIANCE AGREEMENT

☑ I accept the terms in the License Agreement

**FIGURE 2-5. End-User License Agreement**

5. Create an administrator password.

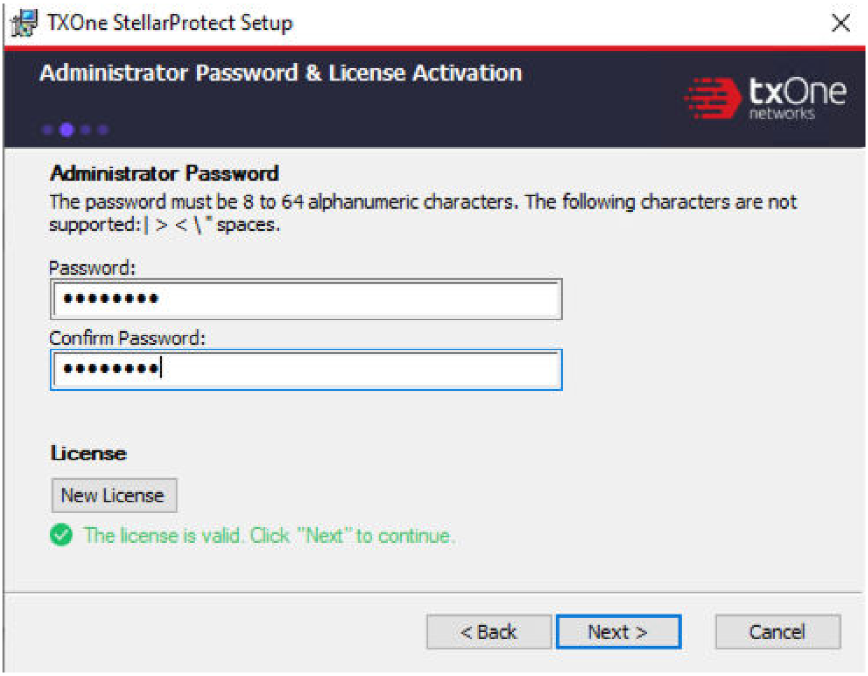
**Note**

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

**Important**

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

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



TXOne StellarProtect Setup

Administrator Password & License Activation

Administrator Password

The password must be 8 to 64 alphanumeric characters. The following characters are not supported: | > < \ " spaces.

Password: ••••••••

Confirm Password: ••••••••

License

The license is valid. 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, refer to *License Activation for Standalone Agent on page 2-57*.

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

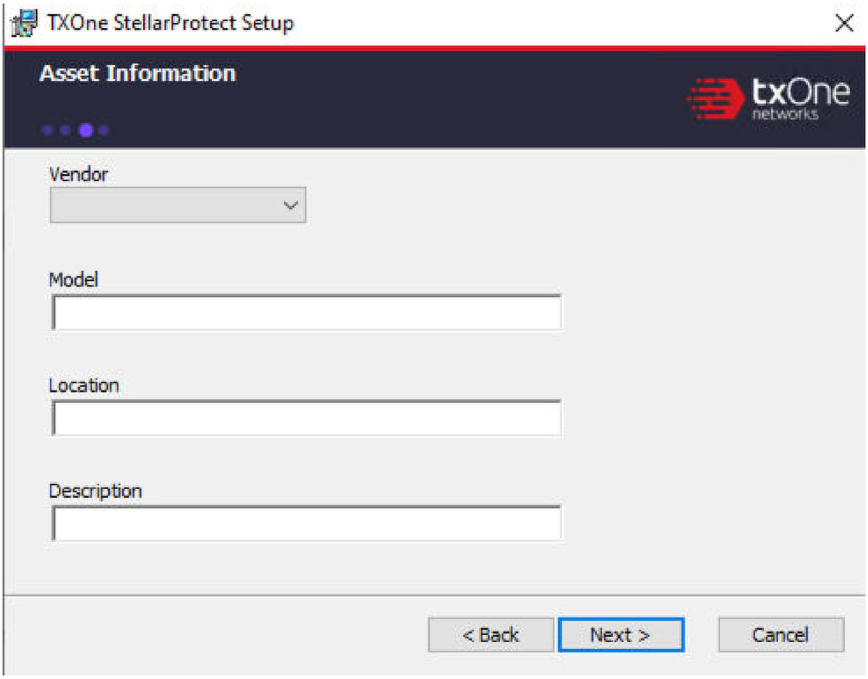
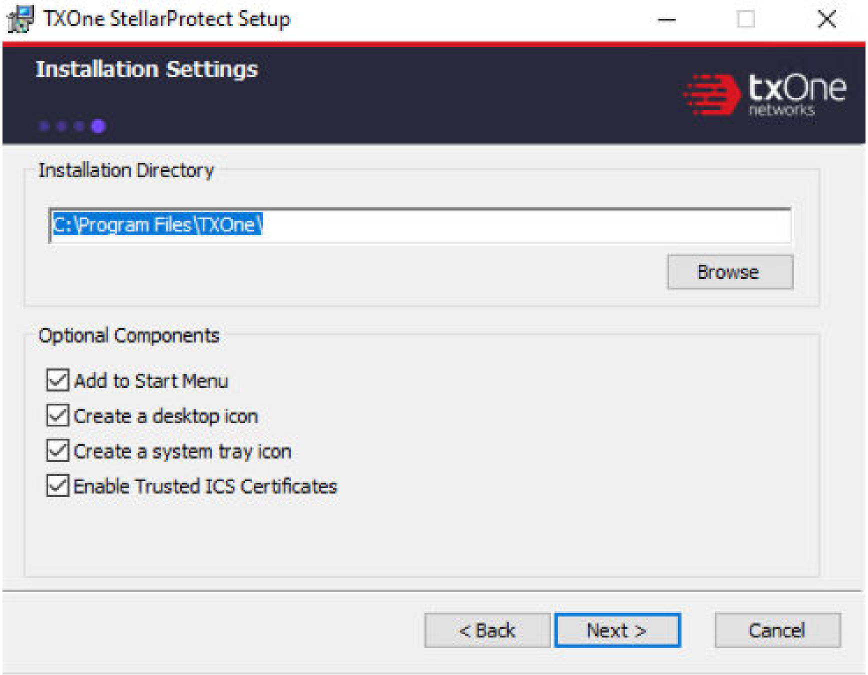


**Figure 2-7. Asset Information**

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


TXOne StellarProtect Setup

Installation Settings

Installation Directory

C:\Program Files\TXOne\

Optional Components

☑ Add to Start Menu

☑ Create a desktop icon

☑ Create a system tray icon

☑ Enable Trusted ICS Certificates

**FIGURE 2-8. StellarProtect Installation Settings**

**Note**

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

**Important**

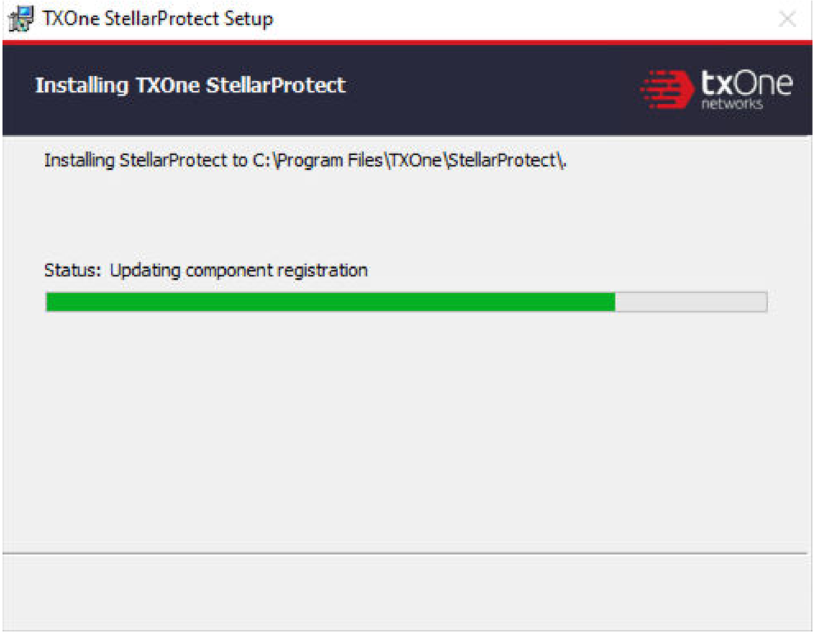
We suggest that users should check **Enable Trusted OT Certificates**. This feature ensures that StellarProtect can sync up trusted ICS/OT certificates and enhance ICS/OT applications, thus those installers can always be recognized by StellarProtect.

**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.



TXOne StellarProtect Setup

Installing TXOne StellarProtect

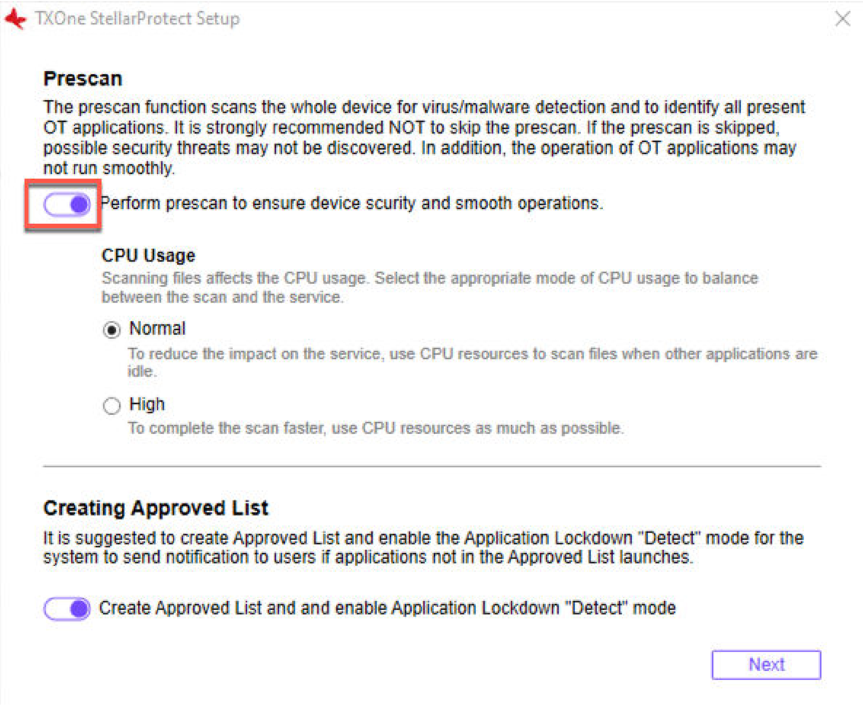
Installing StellarProtect to C:\Program Files\TXOne\StellarProtect\.

Status: Updating component registration

**FIGURE 2-9. Installing Status**

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 2-10. Prescan Toggle**



**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

**Important**

- It is advisory to perform the Prescan for the agent to detect potential security threat and 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.

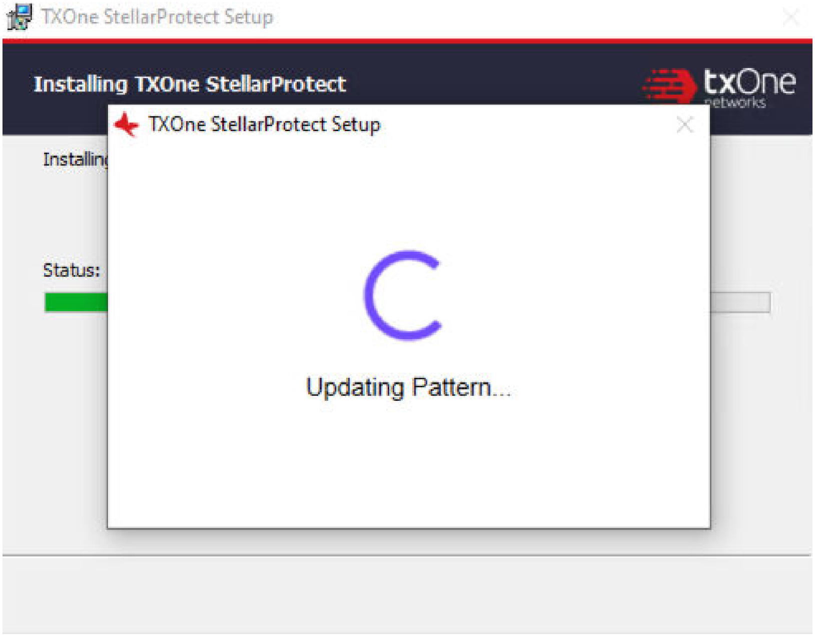
**Note**

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**

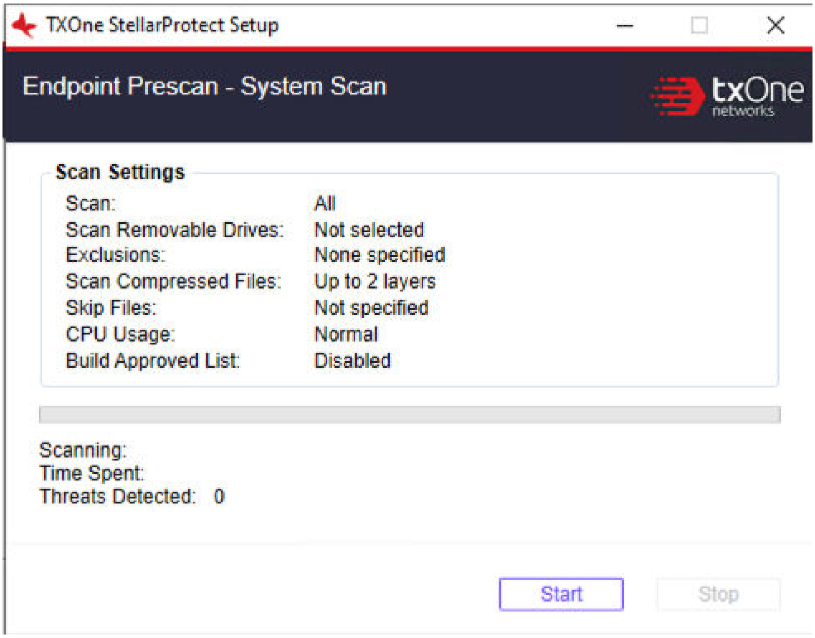
For the standalone agents to perform the update successfully, it is required to allow them to access the Internet for connecting to the Active Update server. If they can't have the Internet connection, the component update will fail; however, users can still choose to proceed to the next step.


TXOne StellarProtect Setup
Installing TXOne StellarProtect
txOne networks
TXOne StellarProtect Setup
Installin
Status:

Updating Pattern...

**Figure 2-11. Updating Pattern before Prescan**

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



Scan Settings

| | |
|---|---|
| Scan: | All |
| Scan Removable Drives: | Not selected |
| Exclusions: | None specified |
| Scan Compressed Files: | Up to 2 layers |
| Skip Files: | Not specified |
| CPU Usage: | Normal |
| Build Approved List: | Disabled |

Scanning:
Time Spent:
Threats Detected: 0

**FIGURE 2-12. Scan Settings before Prescan**

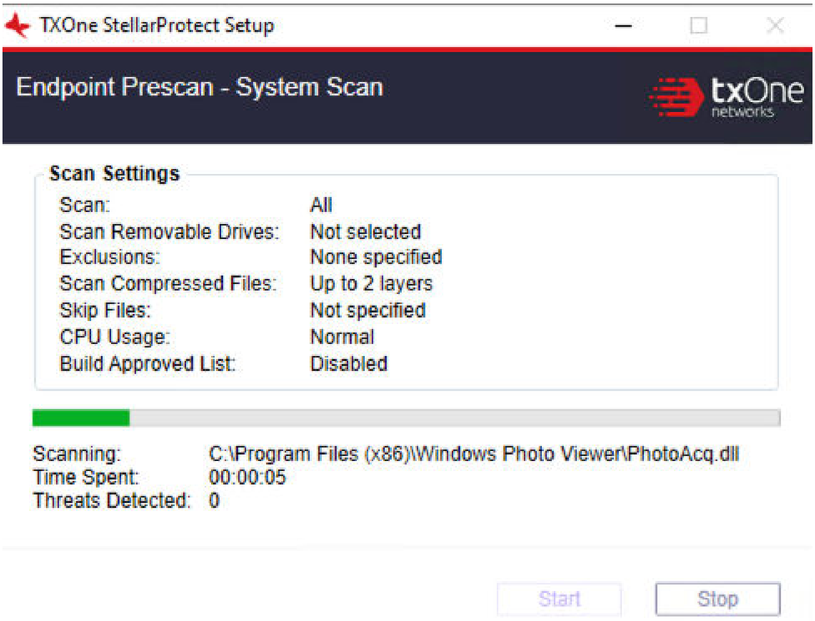
**Note**

Scan settings are described as follows:

- **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:** Scan up to 20 layers of compression
- **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 2-13. Prescan Status**



Endpoint Prescan - System Scan

Scan Settings

```
Scan:                      All
Scan Removable Drives:     Not selected
Exclusions:                None specified
Scan Compressed Files:     Up to 2 layers
Skip Files:                Not specified
CPU Usage:                 Normal
Build Approved List:       Disabled
```

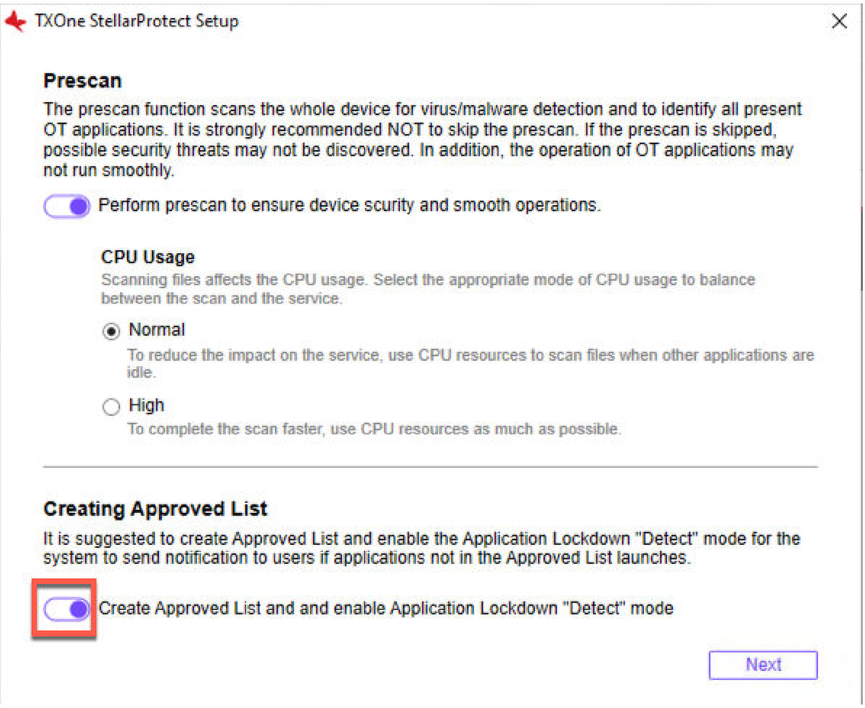
```
Scanning:          C:\Program Files (x86)\Windows Photo Viewer\PhotoAcq.dll
Time Spent:        00:00:05
Threats Detected:  0
```

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.



**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

**FIGURE 2-14. Create Approved List & Enable Application Lockdown (Detect)**

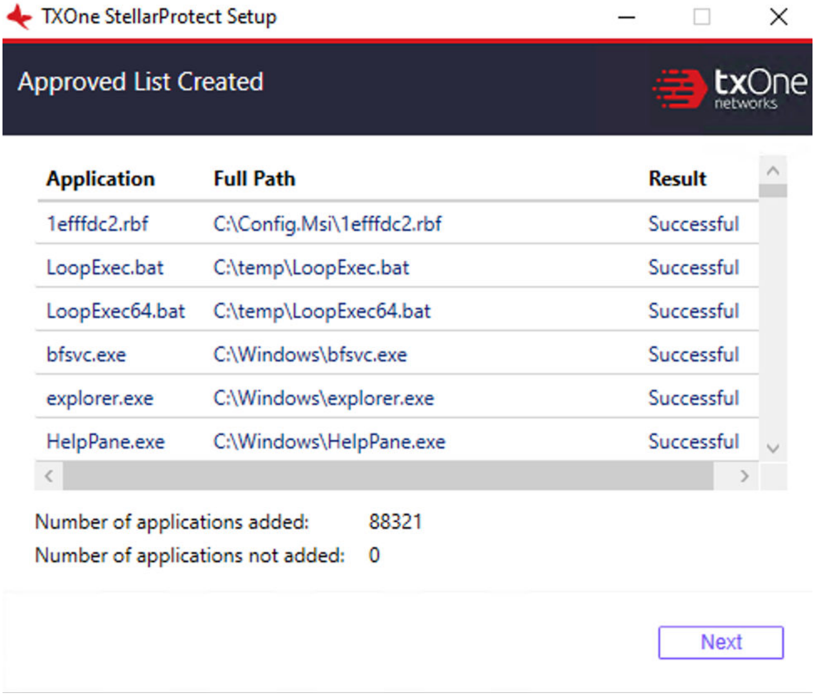
**Note**

- 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.

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**.



| Application | Full Path | Result |
|---|---|---|
| 1efffdc2.rbf | C:\Config.Msi\1efffdc2.rbf | Successful |
| LoopExec.bat | C:\temp\LoopExec.bat | Successful |
| LoopExec64.bat | C:\temp\LoopExec64.bat | Successful |
| bfsvc.exe | C:\Windows\bfsvc.exe | Successful |
| explorer.exe | C:\Windows\explorer.exe | Successful |
| HelpPane.exe | C:\Windows\HelpPane.exe | Successful |

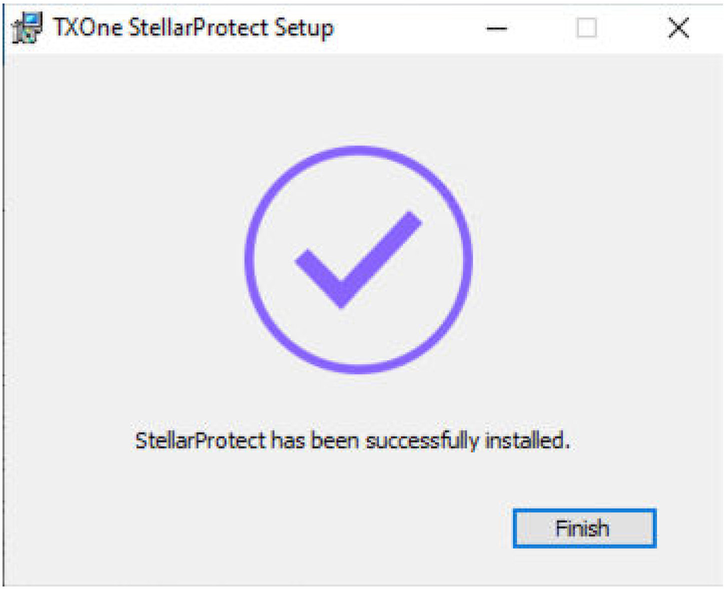
Number of applications added: 88321
Number of applications not added: 0

**FIGURE 2-15. 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**.

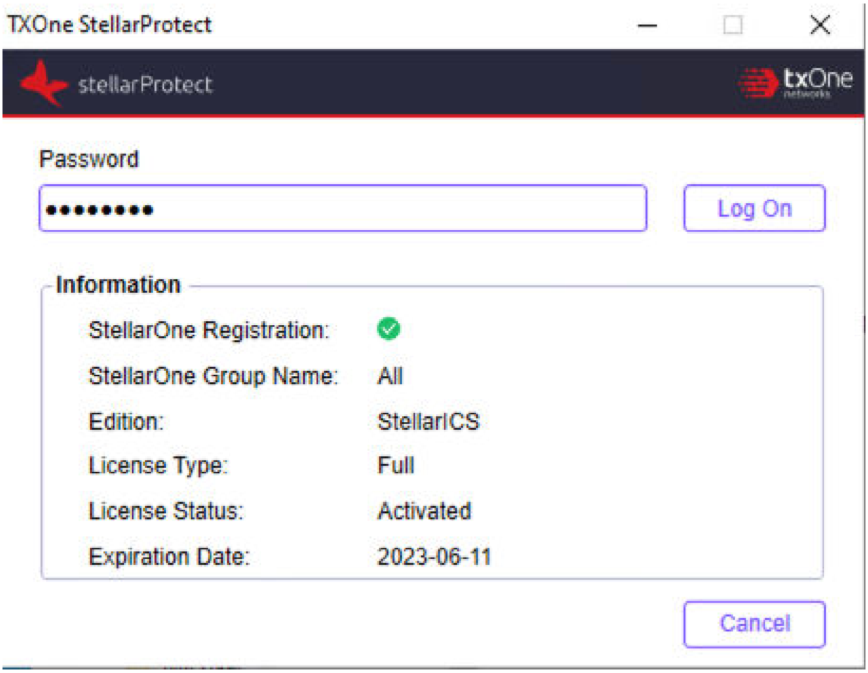
**FIGURE 2-16. StellarProtect Successfully Installed**



StellarProtect has been successfully installed.

14. Run StellarProtect and log on with your password.

**FIGURE 2-17. Log On StellarProtect**



Password

•••••••••

Information

StellarOne Registration: ✓

StellarOne Group Name: All

Edition: StellarICS

License Type: Full

License Status: Activated

Expiration Date: 2023-06-11

15. Upon logging on StellarProtect successfully, the **Overview** window will display. Refer to *Using the StellarProtect Agent Console on page 5-1* for more details.

## Silent Installation

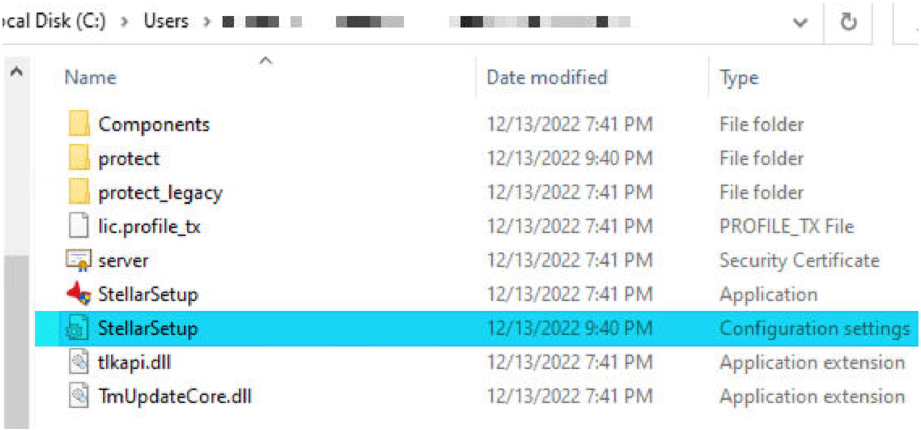
StellarProtect provides silent installation based on a pre-defined configuration file. Users can customize the configuration settings in the `StellarSetup.ini` file to enable silent installation, and then execute `StellarSetup.exe` in silent mode.

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

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

## Configuration for Silent Installation

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

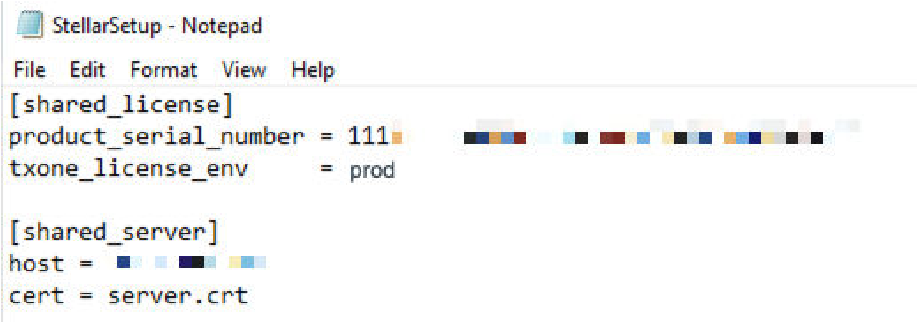


ıcal Disk (C:) › Users › [redacted]

| Name | Date modified | Type |
|---|---|---|
| Components | 12/13/2022 7:41 PM | File folder |
| protect | 12/13/2022 9:40 PM | File folder |
| protect_legacy | 12/13/2022 7:41 PM | File folder |
| lic.profile_tx | 12/13/2022 7:41 PM | PROFILE_TX File |
| server | 12/13/2022 7:41 PM | Security Certificate |
| StellarSetup | 12/13/2022 7:41 PM | Application |
| StellarSetup | 12/13/2022 9:40 PM | Configuration settings |
| tlkapi.dll | 12/13/2022 7:41 PM | Application extension |
| TmUpdateCore.dll | 12/13/2022 7:41 PM | Application extension |

**FIGURE 2-18. `StellarSetup.ini` in the Installer Package**

### StellarOne Managed Agent Configuration for Silent Installation



```
[shared_license]
product_serial_number = 111[redacted]
txone_license_env      = prod

[shared_server]
host = [redacted]
cert = server.crt
```

**FIGURE 2-19. Snippet of `StellarSetup.ini` Downloaded from StellarOne**

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

### Standalone Agent Sample Config File for Silent Installation

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

- The **`[shared_...]`** entry consists of the properties shared by StellarProtect and StellarProtect (Legacy Mode) Agents.
- The **`[protect_...]`** entry consists of the properties exclusive to StellarProtect Agent.
- The **`[legacy_...]`** entry consists of the properties exclusive to StellarProtect (Legacy Mode) Agent.

**Important**

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

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

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

```
[shared_license]

product_serial_number = TEXXXXXX-SAMP-LEXX-XXXX-TXONESPXXXXX

txone_license_file = Stellar<License>Edition_XXXXXXXXXXXX.txt

[shared_server]

host = 10.1.195.100

cert = server.crt

[shared_proxy]

host =

port =

username =

password =

[shared_install]

silent = 1

password =

[protect_server]

port = 9443

[protect_listen]
```

```
port = 14336

[protect_update]

source =

[protect_config]

include =

[legacy_server]

port = 8000

[legacy_listen]

port = 14336

[legacy_update]

source =

[legacy_config]

include =

[protect_install]

asset_vendor = ABB

asset_model = ABB-1X2Y

asset_location = Factory1 North Area

asset_description = This is a machine

install_location = C:\test

enable_start_menu = 1

enable_desktop_icon = 1

enable_systray_icon = 1

enable_trusted_ics_cert = 1

enable_prescan = 1
```

```
enable_lockdown_al_building = 1
enable_lockdown_detection = 1
[protect_prescan]
action = 1
background = 0
cpu_usage_mode = 0
[protect_client]
import_source = C:\txsp_config
[legacy_Property]
PRESCAN = 1
WEL_SIZE = 10240
WEL_RETENTION = 0
WEL_IN_SIZE = 10240
WEL_IN_RETENTION = 0
USR_DEBUGLOG_ENABLE = 1
USR_DEBUGLOGLEVEL = 256
SRV_DEBUGLOG_ENABLE = 1
SRV_DEBUGLOGLEVEL = 256
FW_USR_DEBUGLOG_ENABLE = 0
FW_USR_DEBUGLOG_LEVEL = 273
FW_SRV_DEBUGLOG_ENABLE = 0
FW_SRV_DEBUGLOG_LEVEL = 273
BM_SRV_DEBUGLOG_ENABLE = 0
BM_SRV_DEBUGLOG_LEVEL = 51
```

```
INTEGRITY_MONITOR = 0

PREDEFINED_TRUSTED_UPDATER = 0

WINDOWS_UPDATE_SUPPORT = 0

STORAGE_DEVICE_BLOCKING = 0

INIT_LIST = 0

LOCKDOWN = 0

FILELESS_ATTACK_PREVENTION = 0

SERVICE_CREATION_PREVENTION = 0

INTELLIGENT_RUNTIME_LEARNING = 0

NO_DESKTOP = 0

NO_STARTMENU = 0

NO_SYSTRAY = 0

CUSTOM_ACTION = 0

MAX_EVENT_DB_SIZE = 1024

NO_NSC = 1

INIT_LIST_EXCLUDED_EXTENSION1 = log

INIT_LIST_EXCLUDED_EXTENSION2 = txt

INIT_LIST_EXCLUDED_EXTENSION3 = ini

[legacy_Prescan]

PRESCANCLEANUP = 2

IGNORE_THREAT = 2

REPORT_FOLDER =

SCAN_TYPE = Full

COMPRESS_LAYER = 2
```

```
MAX_FILE_SIZE = 0

SCAN_REMOVABLE_DRIVE = 0

FORCE_PRESCAN = 0

[legacy_BlockNotification]

ENABLE = 0

ALWAYS_ON_TOP = 1

SHOW_DETAILS = 1

AUTHENTICATE = 1

TITLE =

MESSAGE =

[legacy_EventLog]

Enable = 1

Level_WarningLog = 1

Level_InformationLog = 0

BlockedAccessLog = 1

ApprovedAccessLog = 1

ApprovedAccessLog_TrustedUpdater = 1

ApprovedAccessLog_DllDriver = 0

ApprovedAccessLog_ExceptionPath = 1

ApprovedAccessLog_TrustedCert = 1

ApprovedAccessLog_WriteProtection = 1

ApprovedAccessLog_TrustedHash = 1

SystemEventLog = 1

SystemEventLog_ExceptionPath = 1
```

```
SystemEventLog_WriteProtection = 1

ListLog = 1

UsbMalwareProtectionLog = 1

ExecutionPreventionLog = 1

NetworkVirusProtectionLog = 1

IntegrityMonitoringLog_FileCreated = 1

IntegrityMonitoringLog_FileModified = 1

IntegrityMonitoringLog_FileDeleted = 1

IntegrityMonitoringLog_FileRenamed = 1

IntegrityMonitoringLog_RegValueModified = 1

IntegrityMonitoringLog_RegValueDeleted = 1

IntegrityMonitoringLog_RegKeyCreated = 1

IntegrityMonitoringLog_RegKeyDeleted = 1

IntegrityMonitoringLog_RegKeyRenamed = 1

DeviceControlLog = 1

[legacy_MaintenanceMode]

ENABLE_DURATION = 0

SCAN = 0

[legacy_Message]

INITIAL_RETRY_INTERVAL = 120

MAX_RETRY_INTERVAL = 7680

[legacy_MessageRandomization]

TOTAL_GROUP_NUM = 1

OWN_GROUP_INDEX = 0
```

```
TIME_PERIOD = 0
```

**Note**

- The license file name varies depending on different license editions (ICS/Kiosk/OEM). For example, if you use ICS license edition, the license file name appears like this: `StellarICSEdition_xxxxxxxxxxxx.txt`.
- To get the license file and product serial number, refer to *Getting the License File and PSN for Standalone Agents on page 2-59*.

## Properties in the Config File for Silent Installation

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

**Note**

- The **`[shared_...]`** entry consists of the properties shared by StellarProtect and StellarProtect (Legacy Mode) Agents.
- The **`[protect_...]`** entry consists of the properties exclusive to StellarProtect Agent.
- The **`[legacy_...]`** entry consists of the properties exclusive to StellarProtect (Legacy Mode) Agent.

**Table 2-1. Properties in the `StellarSetup.ini` File**

| Section | Property | Default Value | Description |
|---|---|---|---|
| `[Shared_license` | `product_serial_number`<br>`txone_license_file` | empty string | The product serial number and license file used for license activation |
| `[shared_server]` | `host`<br>`cert` | empy string<br>server.crt | StellarOne hostname or IP address |

| Section | Property | Default Value | Description |
|---|---|---|---|
| | | | 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's password. The password will be required by specific functions, including uninstallation, the command line interface, and support tools. |
| `[shared_install]` | `silent` | 0 | Execute installation in silent mode. Possible values:<br>• 0: Do not use silent mode<br>• 1: Use silent mode |
| | `password` | empy string | |

| Section | Property | Default Value | Description |
|---|---|---|---|
| | | | **Important**<br>To install in silent mode, you must also specify the `password` value. For example:<br>`password=P@ssW0rd`<br>`silent=1` |
| `[protect_server]`<br>`[legacy_server]` | `port` | 9443<br>8000 | StellarOne's port for connecting to the StellarProtect or client |
| `[protect_listen]`<br>`[legacy_listen]` | `port` | 14336 | The client listening port for StellarOne |
| `[protect_update]`<br>`[legacy_update]` | `source` | empy string | component update server link |
| `[protect_config]`<br>`[legacy_config]` | `include` | empty string | Use an installation sample config file to run the silent installation. Choose one of the ways:<br>• Specify the file path to the installation sample config file<br>• Specify the sample file name and put the file as the top-level file in the installer package |

| Section | Property | Default Value | Description |
|---|---|---|---|
| | | | **Note**<br>Supports only `.yaml` or `.bin` file format |
| `[protect_install]` | `asset_vendor` | empty string | The vendor's name of the asset. |
| | `asset_model` | empty string | The model name of the asset. |
| | `asset_location` | empty string | The physical location of the asset. |
| | `asset_description` | empty string | The description for the asset. |
| | `install_location` | empty string → default install path<br>`C:\Program Files\TXOne`<br>(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. |
| | `enable_trusted_ics_cert` | `1` | Allow the installer to install ICS code signing certificates during installation. |

| Section | Property | Default Value | Description |
|---|---|---|---|
| | 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<br>1: Quarantine |
| | background | 0 | 1: only executes when the sytem is in idle status<br>0: always consumes CPU resource for executing prescan |
| | cpu_usage_mode | 0 | 0: Normal (Single thread scan)<br>1: HIGH (Multi-thread scan |
| [protect_client] | import_source | empty string | Use an agent settings sample config file to import the same settings to the target agents.<br>Specify the path to the folder containing the config file to be imported, e.g., C:\txsp_config |
| BYPASS_WINDEFEND_CHECK | boolean | false | Bypass checking Windows Defender status. |

| Section | Property | Default Value | Description |
|---|---|---|---|
| | | | **Note**<br>This is a hidden parameter. |
| [legacy_Property] | PRESCAN | 1 | Prescan the endpoint before installing . Possible values:<br>• 0: Do not prescan the endpoint<br>• 1: Prescan the endpoint |
| | WEL_SIZE | 10240 | Windows Event Log size (KB). Possible values: Positive integer<br>**Note**<br>Default value for new installations. Upgrading 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:<br>For Windows XP or earlier platforms:<br>• 0: Overwrite events as needed |

| Section | Property | Default Value | Description |
|---|---|---|---|
| | | | - 1~365: Overwrite events older than (1~365) days<br>- -1: Do not overwrite events (clear logs manually)<br>For Windows Vista or later platforms:<br>- 0: Overwrite events as needed (oldest events first)<br>- 1: Archive the log when full, do not overwrite events.<br>- -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.<br>For Windows XP or earlier platforms:<br>- 0: Overwrite events as needed<br>- 1~365: Overwrite events older than (1~365) days |

| SECTION | PROPERTY | DEFAULT VALUE | DESCRIPTION |
|---|---|---|---|
| | | | • -1: Do not overwrite events (clear logs manually)<br>For Windows Vista or later platforms:<br>• 0: Overwrite events as needed (oldest events first)<br>• 1: Archive the log when full, do not overwrite events.<br>• -1: Do not overwrite events (clear logs manually) |
| | `USR_DEBUGLOG_ENABLE` | 1 | Enable debug logging for user sessions. Possible values:<br>• 0: Do not log<br>• 1: Log |
| | `USR_DEBUGLOGLEVEL` | 256 | The number of debug log entries allowed for user sessions |
| | `SRV_DEBUGLOG_ENABLE` | 1 | Enable debug logging for service sessions. Possible values:<br>• 0: Do not log<br>• 1: Log |
| | `SRV_DEBUGLOGLEVEL` | 256 | The number of debug log entries allowed for service sessions |

| Section | Property | Default Value | Description |
|---|---|---|---|
| | FW_USR_DEBUGLOG_ENABLE | 0 | Enable debug log in user session of firewall. Possible values:<br>• 0: Disable debug log<br>• 1: Enable debug log |
| | FW_USR_DEBUGLOG_LEVEL | 273 | Debug level in user session of firewall. Possible values: number |
| | FW_SRV_DEBUGLOG_ENABLE | 0 | Enable debug log in service session of firewall. Possible values:<br>• 0: Disable debug log<br>• 1: Enable debug log |
| | FW_SRV_DEBUGLOG_LEVEL | 273 | Debug level in service session of firewall. Possible values: number |
| | BM_SRV_DEBUGLOG_ENABLE | 0 | Enable debug log of Behavior Monitoring Core service. Possible values:<br>• 0: Disable debug log<br>• 1: Enable debug log |
| | BM_SRV_DEBUGLOG_LEVEL | 51 | Debug level of Behavior Monitoring Core service |
| | INTEGRITY_MONITOR | 0 | Enable Integrity Monitor. Possible values:<br>• 0: Disable<br>• 1: Enable |
| | PREDEFINED_TRUSTED_UPDATER | 0 | Enable Predefined Trusted Updater. Possible values: |

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

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

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

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

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

| Section | Property | Default Value | Description |
|---|---|---|---|
| | | | **Note**<br>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:<br>• 0: No action<br>• 1: Clean, or delete if the clean action is unsuccessful<br>• 2: Clean, or quarantine if the clean action is unsuccessful<br>• 3: Clean, or ignore if the clean action is unsuccessful |
| | `IGNORE_THREAT` | 2 | Cancel installation after detecting malware threat during prescan. Possible values:<br>• 0: Cancel<br>• 1: Continue installation after detecting malware threat during prescan<br>• 2: Continue installation when no |

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

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

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

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

| Section | Property | Default Value | Description |
|---|---|---|---|
| | | | Possible values: <notification_title> |
| | MESSAGE | empty string | Notification content<br>Possible values: <notification_content> |
| [legacy_EventLog] | Enable | 1 | Log events related to . Possible values:<br>• 1: Log<br>• 0: Do not log |
| | Level_WarningLog | 1 | Log “Warning” level events related to . Possible values:<br>• 1: Log<br>• 0: Do not log |
| | Level_InformationLog | 0 | Log “Information” levelevents related to . Possible values:<br>• 1: Log<br>• 0: Do not log |
| | BlockedAccessLog | 1 | Log files blocked by . Possible values:<br>• 1: Log<br>• 0: Do not log |
| | ApprovedAccessLog | 1 | Logfiles approved by . Possible values:<br>• 1: Log<br>• 0: Do not log |

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

| SECTION | PROPERTY | DEFAULT VALUE | DESCRIPTION |
|---|---|---|---|
| | `SystemEventLog` | 1 | Log events related to the system. Possible values:<br>• 1: Log<br>• 0: Do not log |
| | `SystemEventLog_ExceptionPath` | 1 | Log exceptions to Application Lockdown. Possible values:<br>• 1: Log<br>• 0: Do not log |
| | `SystemEventLog_WriteProtection` | 1 | Log Write Protection events. Possible values:<br>• 1: Log<br>• 0: Do not log |
| | `ListLog` | 1 | Log events related to the Approved list. Possible values:<br>• 1: Log<br>• 0: Do not log |
| | `UsbMalwareProtectionLog` | 1 | Log events that trigger USB Malware Protection. Possible values:<br>• 1: Log<br>• 0: Do not log |
| | `ExecutionPreventionLog` | 1 | Log events that trigger Execution Prevention. Possible values:<br>• 1: Log<br>• 0: Do not log |

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

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

| Section | Property | Default Value | Description |
|---|---|---|---|
|  | `SCAN` | 0 | Enable file scanning after the maintenance period. Possible values:<br>• 0: No scan (default)<br>• 1: Quarantine<br>scans files that are created, executed, or modified during the maintenance period and quarantine detected files<br>• 2: al<br>scans files that are created, executed, or modified during the maintenance period and adds these files (including files that are detected as malicious) to the Approved List |
| `[legacy_Message]` | `INITIAL_RETRY_INTERVAL` | 120 | Starting interval, in seconds, between attempts to resend an event to StellarOne<br>This interval doubles in size for each unsuccessful attempt, until it exceeds the `MAX_RETRY_ITERVAL` value<br>Possible values: 0~2147483647 |
|  | `MAX_RETRY_INTERVAL` | 7680 | Maximum interval, in seconds, between |

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

**Note**

- When ENABLE_PRESCAN is set to 0, ENABLE_LOCKDOWN_AL_BUILDING and ENABLE_LOCKDOWN_DETECTION will be automatically set to 0.
- For StellarProtect, BYPASS_WINDEFEND_CHECK is a hidden property in StellarSetup.ini, designed for Windows 7 and Windows Server 2016+ platforms, on which the installation of StellarProtect requires disabling Windows Defender. When its value is specified as 1, the endpoint will bypass Windows Defender check to get the StellarProtect installed without disabling Windows Defender.
- 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. Type bypass_windefend_check: 1

## Executing Silent Installation

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

### Procedure

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

   **Note**

   For standalone agents, refer to *Standalone Agent Sample Config File for Silent Installation on page 2-23* for more details.

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

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

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

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

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

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

5. Run StellarProtect and log on with the configured password.

6. After successfully logging on StellarProtect, the **Overview** window will be displayed.

## License Activation for Standalone Agent

This section describes the license activation procedures during the installation process for standalone StellarProtect agents.

**Procedure**

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

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.

    **Note**

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

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

    **Note**

    If you don't have the License File and Product Serial Number on hand, refer to *Getting the License File and PSN for Standalone Agents on page 2-59* for detailed instructions.

  - Click **Save**.

    **Note**

    If a license file expiration error message appears and the agent's installer package was downloaded from StellarOne, you should get the latest License File and Product Serial Number from StellarOne. Refer to *Getting the Latest License File from StellarOne on page 2-66*

3. A success message indicating valid license appears. Click **Next** to proceed to next procedure (**Step 7** in *Attended Installation on page 2-6*) for the installation.

## Getting the License File and PSN

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

- *Getting the License File and PSN for Standalone Agents on page 2-59*
- *Getting the Latest License File from StellarOne on page 2-66*

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

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

**Procedure**

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

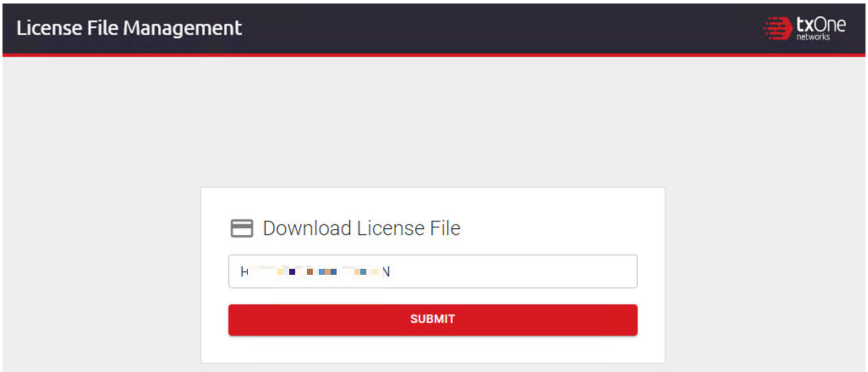
   **Note**

   This URL can also be obtained during the GUI installation process. Refer to *About the Download Link for Getting License File in GUI Installation on page 2-62* 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.



License File Management

Download License File

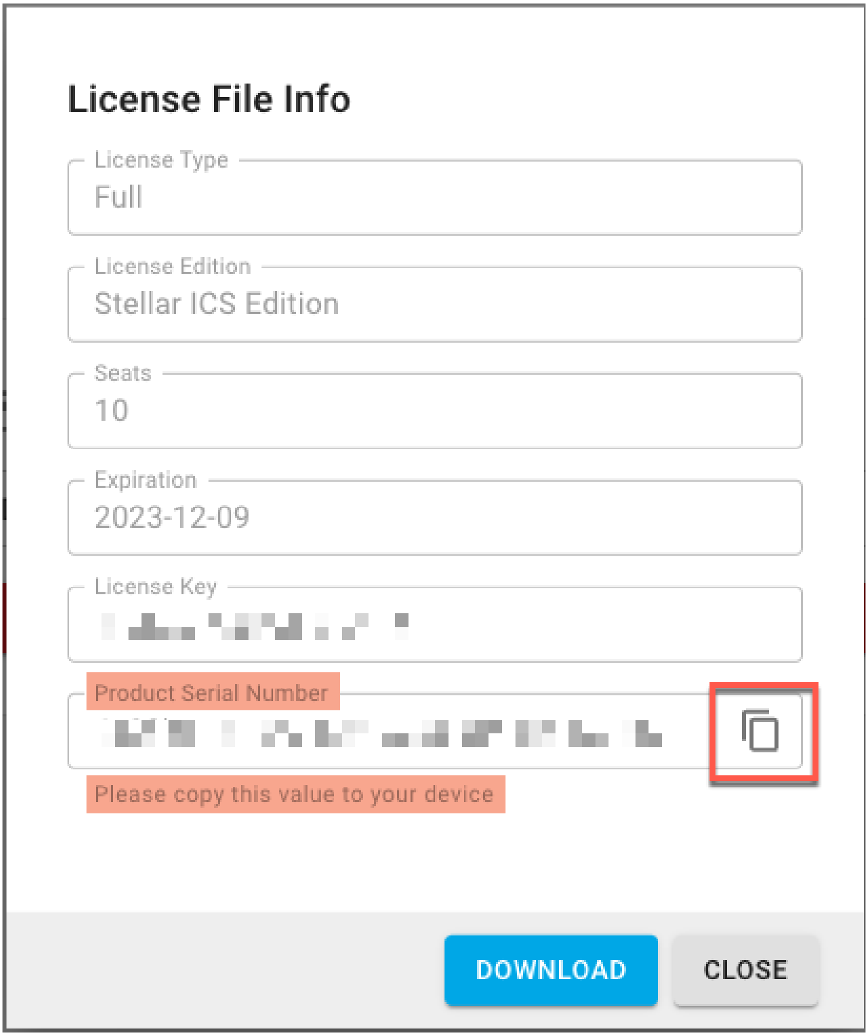
H[redacted]N

**FIGURE 2-20. 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.



License File Info

License Type
Full

License Edition
Stellar ICS Edition

Seats
10

Expiration
2023-12-09

License Key
[redacted]

Product Serial Number
[redacted]

Please copy this value to your device

**FIGURE 2-21. 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).

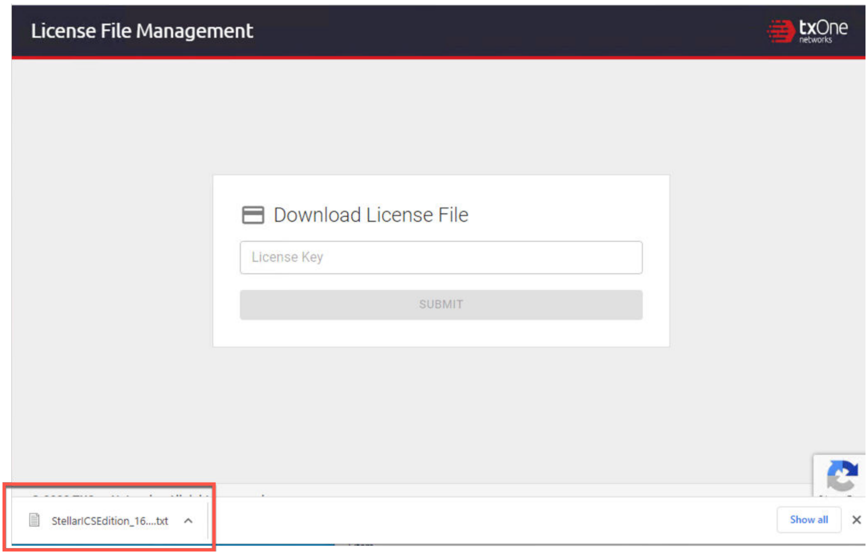


**FIGURE 2-22. License File Downloaded**

**Note**

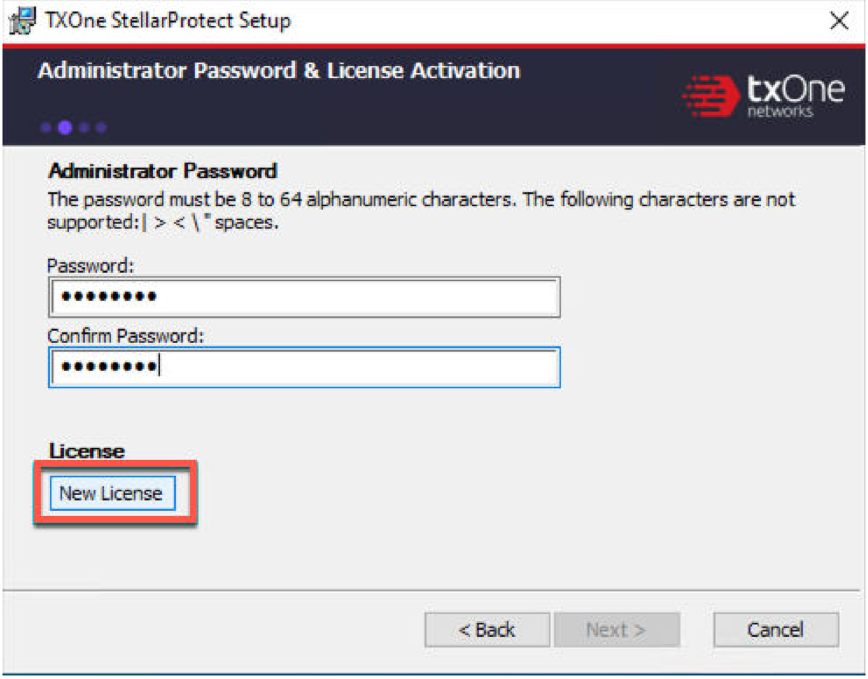
Please find the license file in the downloads folder.

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

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

## Procedure

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



TXOne StellarProtect Setup

Administrator Password & License Activation

Administrator Password

The password must be 8 to 64 alphanumeric characters. The following characters are not supported:| > < \ " spaces.

Password: •••••••••

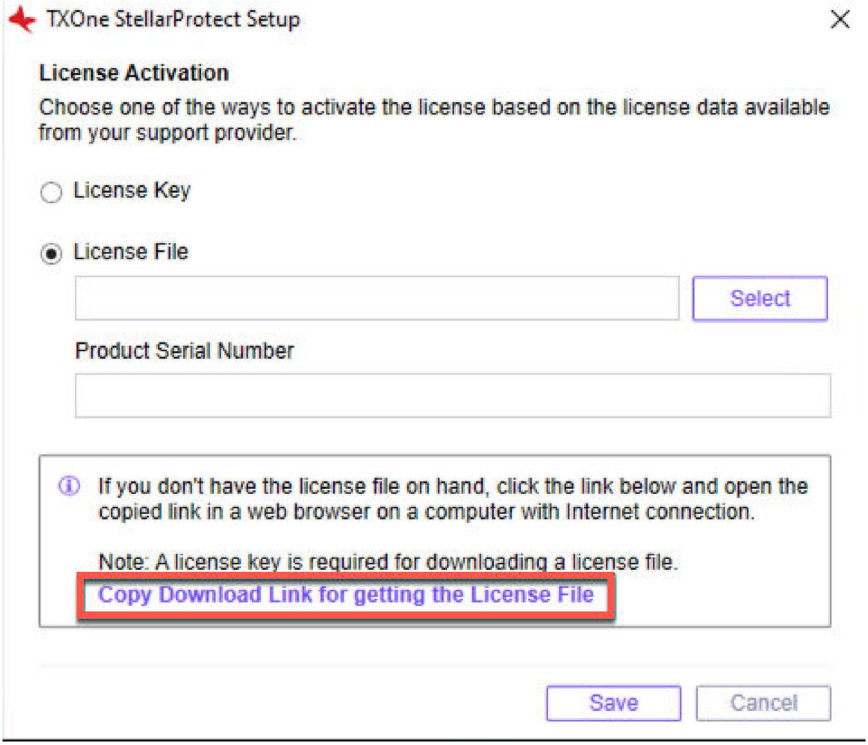
Confirm Password: •••••••••

License

**FIGURE 2-23. 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.



TXOne StellarProtect Setup

License Activation

Choose one of the ways to activate the license based on the license data available from your support provider.

○ License Key

● License File

Product Serial Number

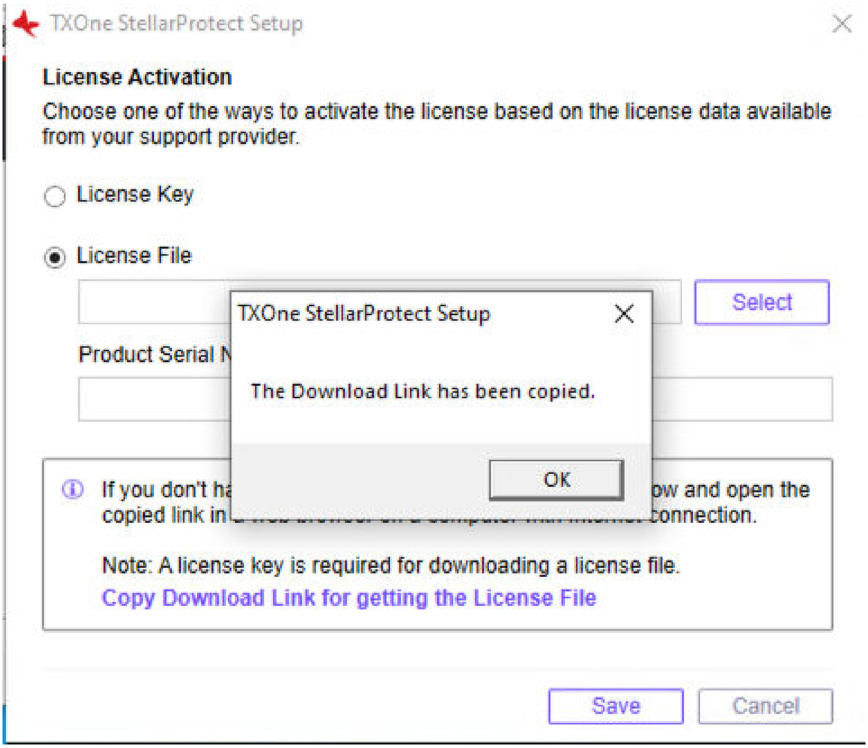
If you don't have the license file on hand, click the link below and open the copied link in a web browser on a computer with Internet connection.

Note: A license key is required for downloading a license file.

Copy Download Link for getting the License File

**FIGURE 2-24. Copy the Download Link**

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



TXOne StellarProtect Setup

License Activation

Choose one of the ways to activate the license based on the license data available from your support provider.

○ License Key

● License File

Product Serial N

If you don't ha ... ow and open the copied link in ... connection.

Note: A license key is required for downloading a license file.

Copy Download Link for getting the License File

TXOne StellarProtect Setup

The Download Link has been copied.

**FIGURE 2-25. Download Link Copied**

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

**Note**

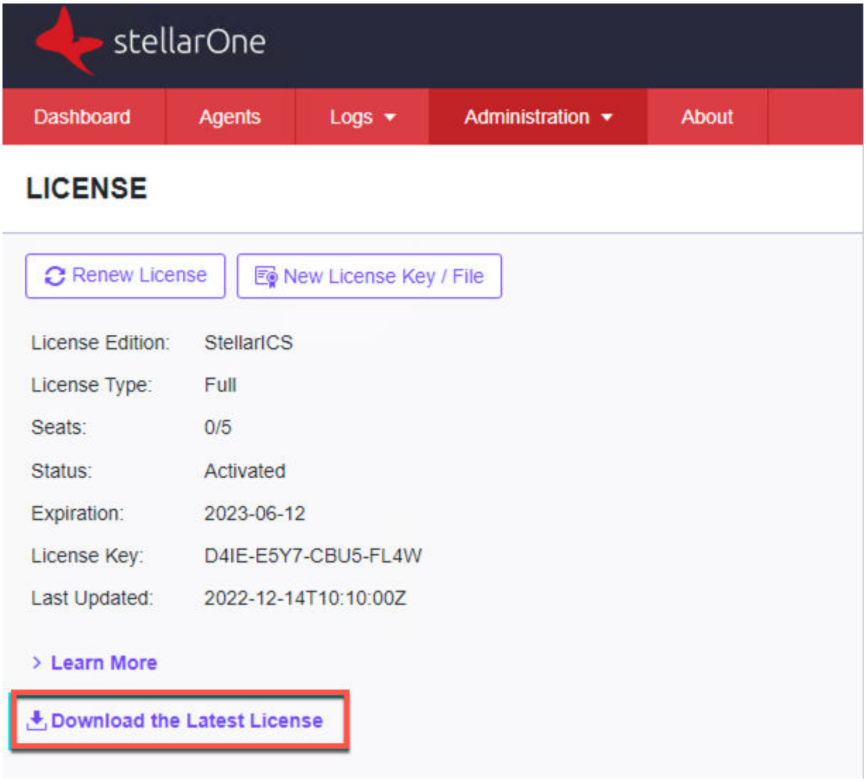
Refer to *Getting the License File and PSN for Standalone Agents on page 2-59* for instructions on how to get the license file from TXOne **License File Management** website.

## 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.



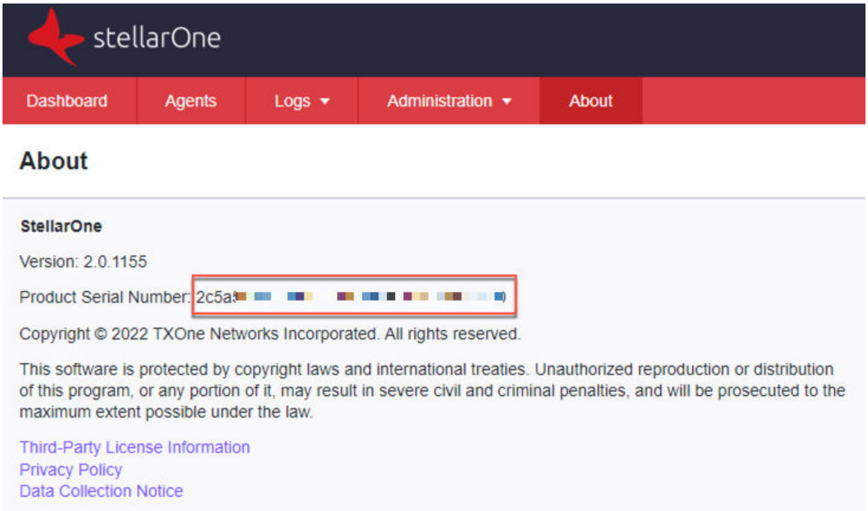
License Edition: StellarICS
License Type: Full
Seats: 0/5
Status: Activated
Expiration: 2023-06-12
License Key: D4IE-E5Y7-CBU5-FL4W
Last Updated: 2022-12-14T10:10:00Z

**FIGURE 2-26. Download lLcense File from StellarOne**

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

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

5. Find and copy the product serial number.



About

**StellarOne**

Version: 2.0.1155

Product Serial Number: 2c5a[redacted]

Copyright © 2022 TXOne Networks Incorporated. All rights reserved.

This software is protected by copyright laws and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Third-Party License Information
Privacy Policy
Data Collection Notice

**FIGURE 2-27. Get Product Serial Number from StellarOne**

## Replicating Installation for Multiple Standalone Agents

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

### Procedure

1. Refer to *Getting the License File and PSN for Standalone Agents on page 2-59* for getting the license file and product serial number.

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

3. Prepare your `StellarSetup.ini` as mentioned in *Standalone Agent Sample Config File for Silent Installation on page 2-23*

   **Note**

   Ensure that you specify the product serial number and license file name in the config file.

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

5. Launch the Installer in silent mode.

## Encrypting Config File for Installation

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

**Procedure**

1. Prepare your `StellarSetup.ini` as mentioned in *Silent Installation on page 2-21*.

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.

## Proxy Settings

StellarProtect use a proxy 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 for Silent Installation on page 2-22*.
- For more information about using command line interface to configure the proxy settings after installation, refer to *List of All Commands on page 6-4*

# Chapter 3

## Uninstalling StellarProtect

Follow the instructions to uninstall StellarProtect.

**Note**

StellarProtect's administrator password is required to uninstall StellarProtect from an endpoint.

**Important**

Please make sure the StellarProtect UI is not open.

**Procedure**

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

| Operating System | Procedure |
|---|---|
| • Windows 10 Professional<br>• Windows 10 Enterprise<br>• Windows 10 IoT Enterprise<br>• Windows 10 Fall Creators Update (Redstone 3)<br>• Windows 10 April 2018 Update (Redstone 4)<br>• Windows 10 November 2018 Update (Redstone 5)<br>• Windows 11 Professional | a. Go to **Start** > **Settings**.<br>b. Depending on your version of Windows 10, locate the **Apps & Features** section under one of the following categories:<br>• **System**<br>• **Apps**<br>c. On the left pane, click **Apps & Features**<br>d. In the list, click **StellarProtect**.<br>e. Click **Uninstall**. |
| • Windows 7<br>• Windows 8<br>• Windows Server 2012<br>• Windows Server 2016<br>• Windows Server 2022<br>• Windows Storage Server 2012<br>• Windows Storage Server 2016 | a. Go to **Start** > **Control Panel** > **Program and Features**<br>b. In the list, double-click **TXOne StellarProtect**. |

3. After the StellarProtect Setup opens, click **Next**.
4. Enter in the StellarProtect administrator password and click **Next**.
5. Make sure StellarProtect's UI is completely closed before clicking **OK**.
6. The message box indicating StellarProtect 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. After uninstalling StellarProtect, it is advisory to manually enable Windows Defender for security reasons.

# Chapter 4

# License Renewal

This chapter describes how to renew license for standalone StellarProtect agent.

# License Renewal for Standalone Agents

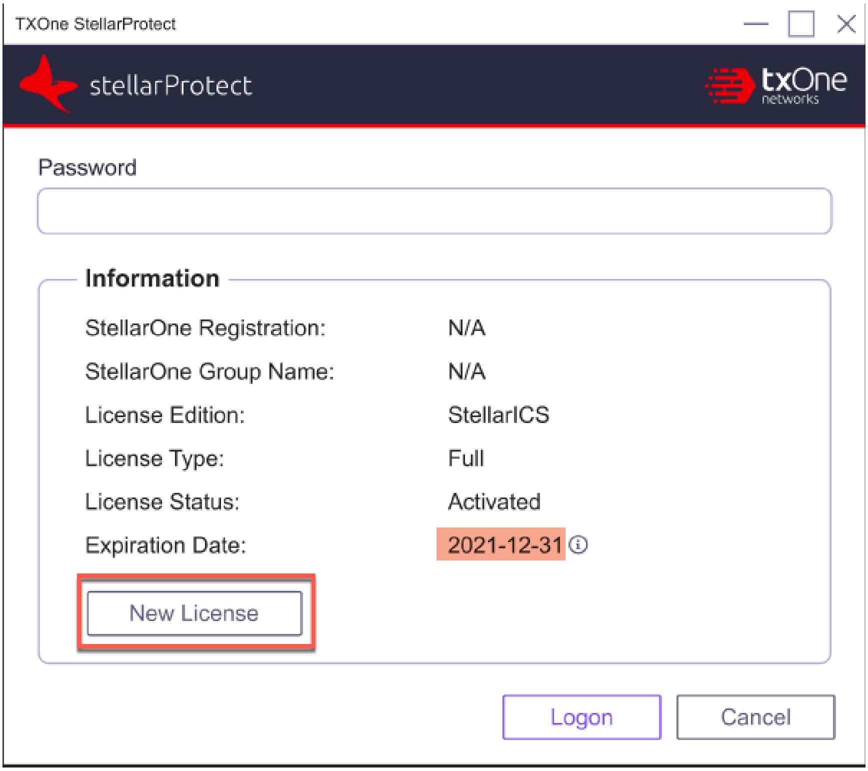
For standalone agents, users can renew license directly on the agent console.

**Note**

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

**Procedure**

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



Password

Information

| | |
|---|---|
| StellarOne Registration: | N/A |
| StellarOne Group Name: | N/A |
| License Edition: | StellarICS |
| License Type: | Full |
| License Status: | Activated |
| Expiration Date: | 2021-12-31 ⓘ |

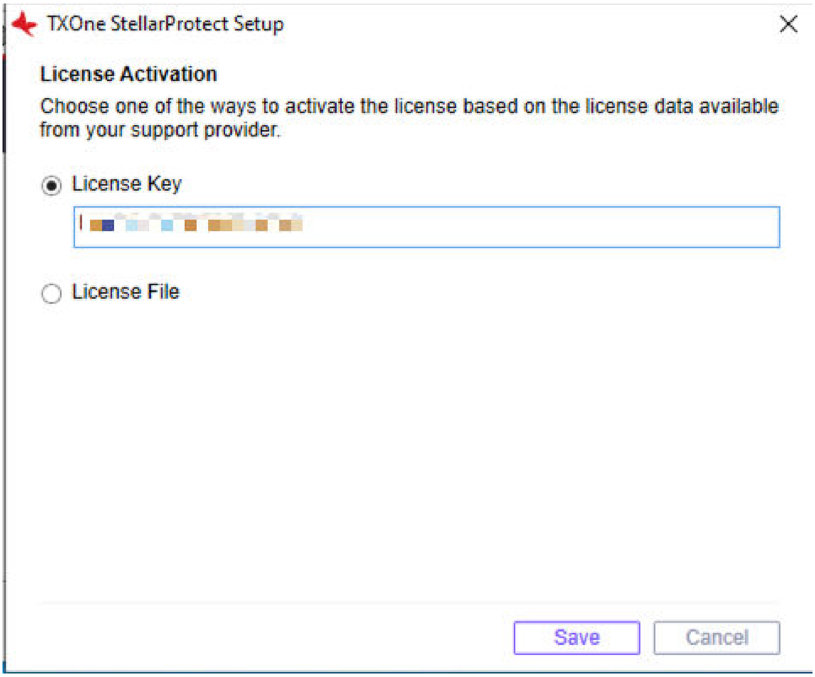
**Figure 4-1. Renew License for Standalone Agents**

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**.



TXOne StellarProtect Setup

License Activation

Choose one of the ways to activate the license based on the license data available from your support provider.

● License Key

[redacted]

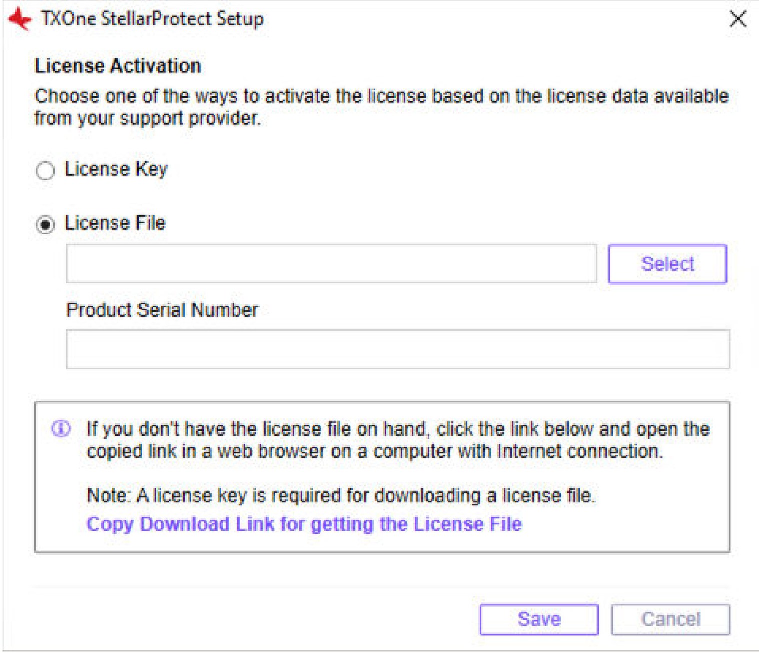
○ License File

**FIGURE 4-2. Use License Key for Activation**

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

> **Note**
>
> 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 2-59* for detailed instructions.

- Click **Save**.



TXOne StellarProtect Setup

License Activation

Choose one of the ways to activate the license based on the license data available from your support provider.

○ License Key

● License File

Product Serial Number

If you don't have the license file on hand, click the link below and open the copied link in a web browser on a computer with Internet connection.

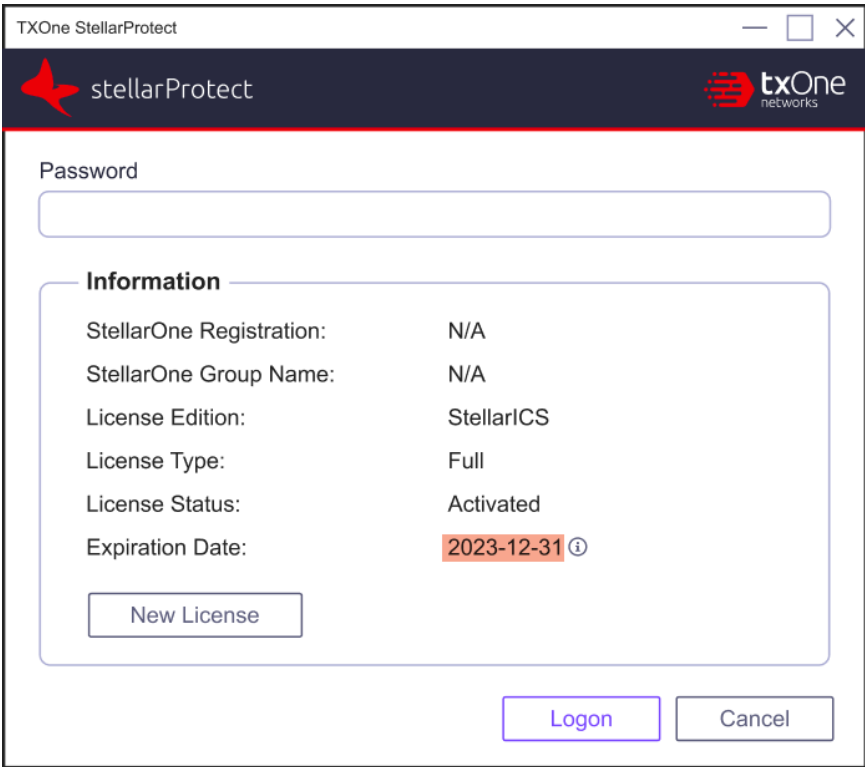
Note: A license key is required for downloading a license file.

Copy Download Link for getting the License File

**FIGURE 4-3. Use License File for Activation**

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

**FIGURE 4-4. License Renewed for Standalone Agents**



**Information**

StellarOne Registration: N/A

StellarOne Group Name: N/A

License Edition: StellarICS

License Type: Full

License Status: Activated

Expiration Date: 2023-12-31

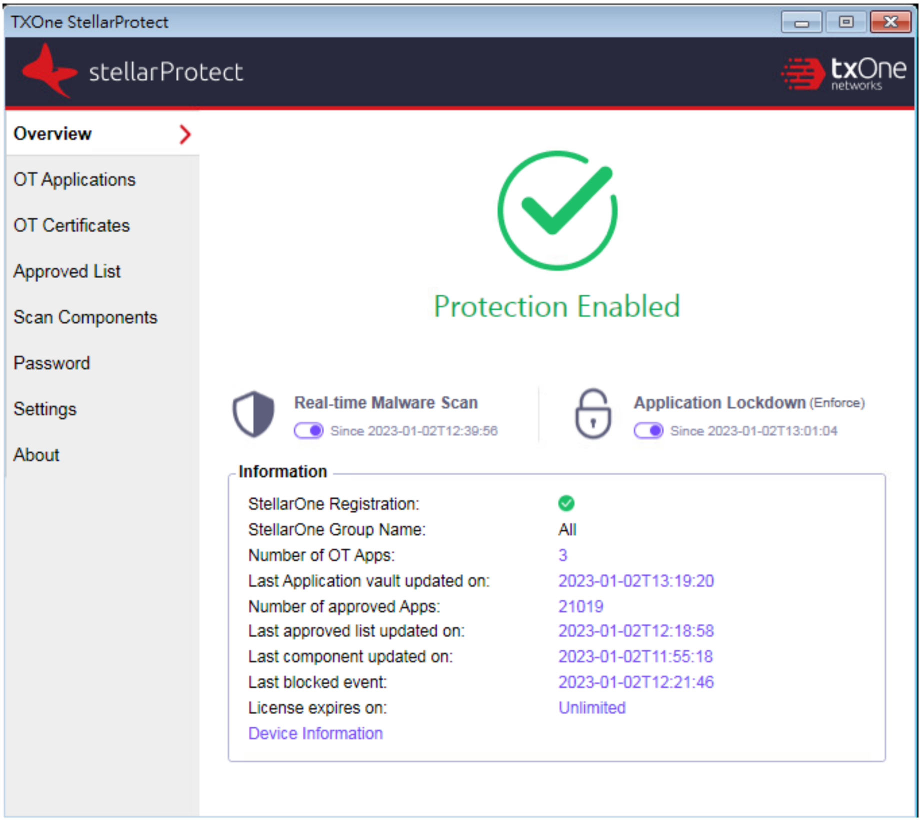
# Chapter 5

# Using the StellarProtect Agent Console

This chapter describes how to operate TXOne StellarProtect's various functions using the agent console on the endpoint.

Topics in this chapter include:

# Side Navigation Menu of StellarProtect Console



Protection Enabled

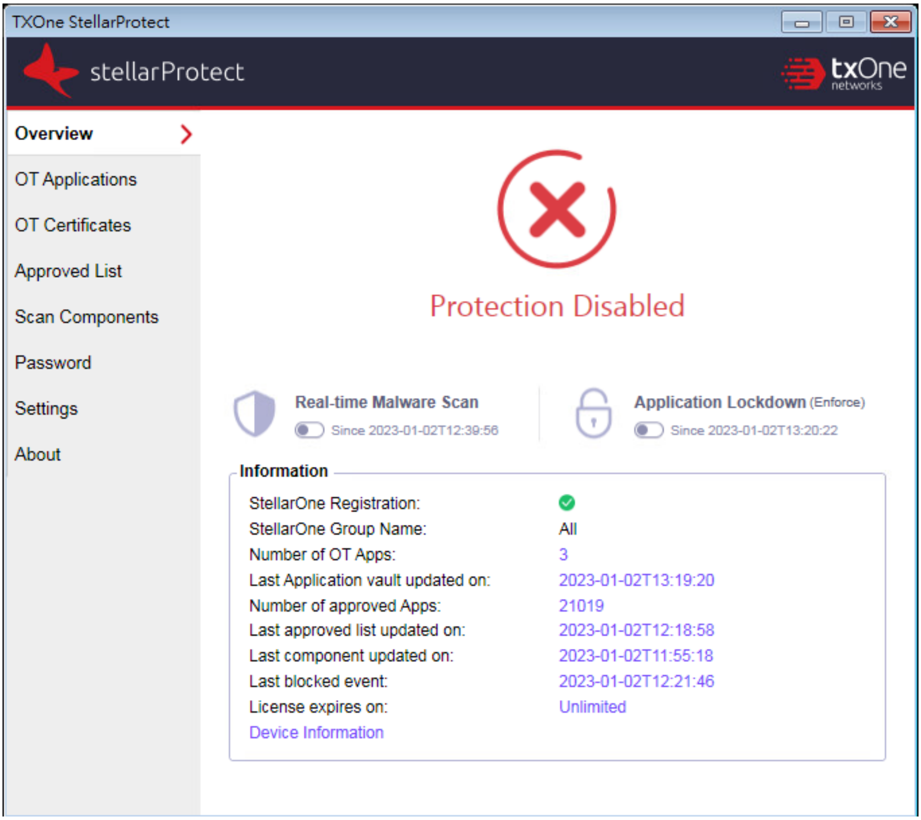
Real-time Malware Scan
Since 2023-01-02T12:39:56

Application Lockdown (Enforce)
Since 2023-01-02T13:01:04

Information

StellarOne Registration: ✓
StellarOne Group Name: All
Number of OT Apps: 3
Last Application vault updated on: 2023-01-02T13:19:20
Number of approved Apps: 21019
Last approved list updated on: 2023-01-02T12:18:58
Last component updated on: 2023-01-02T11:55:18
Last blocked event: 2023-01-02T12:21:46
License expires on: Unlimited
Device Information

**FIGURE 5-1. Overview of StellarProtect Console - Protection Enabled**



Protection Disabled

Real-time Malware Scan
Since 2023-01-02T12:39:56

Application Lockdown (Enforce)
Since 2023-01-02T13:20:22

Information

| | |
|---|---|
| StellarOne Registration: | ✓ |
| StellarOne Group Name: | All |
| Number of OT Apps: | 3 |
| Last Application vault updated on: | 2023-01-02T13:19:20 |
| Number of approved Apps: | 21019 |
| Last approved list updated on: | 2023-01-02T12:18:58 |
| Last component updated on: | 2023-01-02T11:55:18 |
| Last blocked event: | 2023-01-02T12:21:46 |
| License expires on: | Unlimited |

Device Information

**FIGURE 5-2. Overview of StellarProtect Console - Protection Disabled**

The **Overview** serves as the portal as well as one of the side navigation options on StellarProtect console. It displays the current status of the StellarProtect system. The green check indicates the Real-time Malware Scan and/or Application Lockdown are/is enabled, while the red cross indicates the endpoint is vulnerable to security threats.

For StellarProtect agent with **StellarICS** license edition, below the green check or red cross icon, a shield-shape icon with a toggle on the left indicates whether the endpoint is currently protected by StellarProtect's Real-time

Malware Scan; and a lock-shape icon with a toggle on the right indicates whether the Application Lockdown "Enforce" mode is enabled

For StellarProtect agent with **StellarKiosk** license edition, below the green check or red cross icon, a shield-shape icon with the toggle indicates whether the endpoint is currently protected by StellarProtect's Real-time Malware Scan.

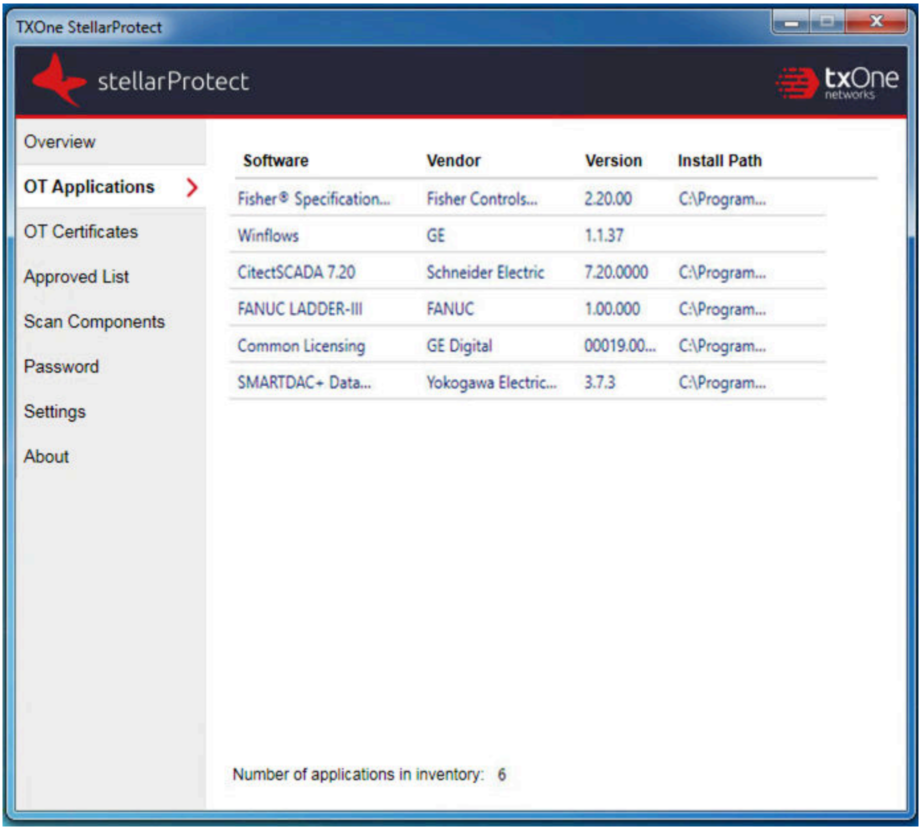
For StellarProtect agent with **StellarOEM** license edition, below the green check or red cross icon, a lock-shape icon with a toggle on the right indicates whether the Application Lockdown "Enforce" mode is enabled.

The following current information about endpoint protection will be shown:

- **StellarOne registration**: Green check indicates the StellarProtect agent is successfully registered to a designated group via StellarOne web console; red cross indicates registration to certain group is failed.
- **StellarOne group name**: This item shows the group name the agent belongs to. When users mouse over the name of the group, information about group name, group ID, and policy version will appear.
- **Number of OT Apps**: This item shows how many OT applications are in the endpoint.
- **Last OT inventory updated on**: This item shows the date and time the OT Inventory was last updated on this endpoint.
- **Number of approved Apps**: This item shows the number of the applications that have been added in the Approved List on this endpoint.
- **Last approved list updated on**: The last time the Approve List was updated.
- **Last component updated on**: The last time component was updated.
- **Last blocked event**: Clicking the link shows the recent 1000 blocked events.
- **License expires on**: This item shows when StellarProtect’s current license will expire.

- **Device Information**: Clicking the link shows the endpoint's device information including Vendor, Model, Location, and Remark.

### OT Applications



| Software | Vendor | Version | Install Path |
|---|---|---|---|
| Fisher® Specification... | Fisher Controls... | 2.20.00 | C:\Program... |
| Winflows | GE | 1.1.37 | |
| CitectSCADA 7.20 | Schneider Electric | 7.20.0000 | C:\Program... |
| FANUC LADDER-III | FANUC | 1.00.000 | C:\Program... |
| Common Licensing | GE Digital | 00019.00... | C:\Program... |
| SMARTDAC+ Data... | Yokogawa Electric... | 3.7.3 | C:\Program... |

Number of applications in inventory: 6

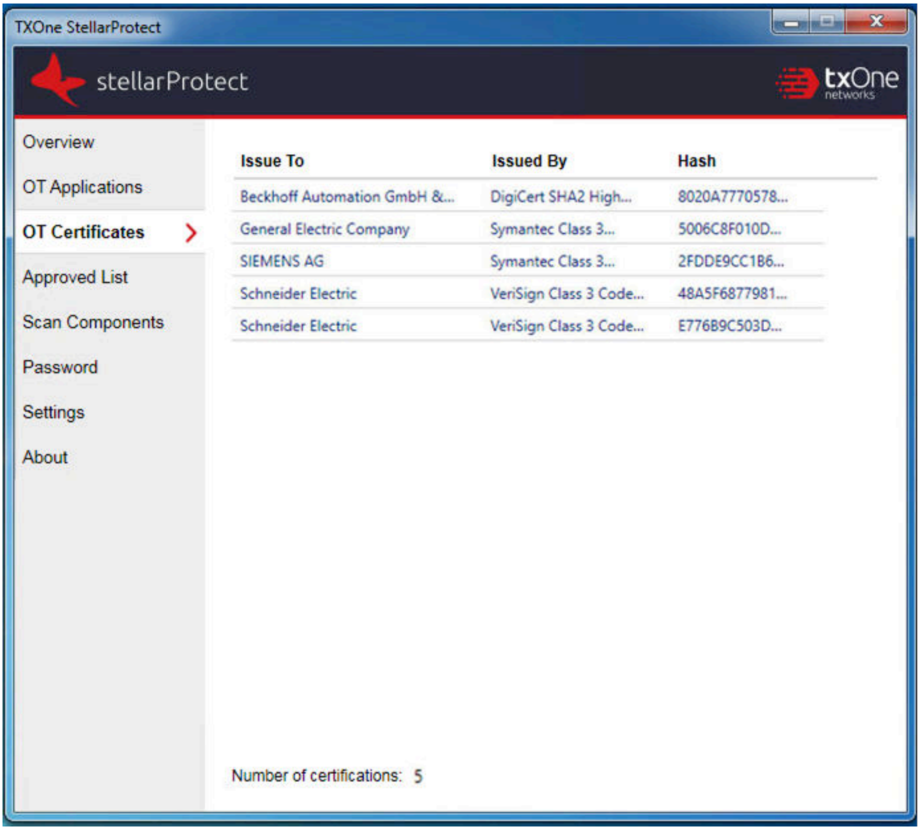
**FIGURE 5-3. OT Applications**

This function lists all OT/ICS application systems recognized by StellarProtect on this endpoint, and lists the software name, vendor name, product version and installation path of each application system.

The number of OT/ICS application systems that StellarProtect can recognize will continue to increase with updates to the OT/ICS Application Inventory, which is maintained by the TXOne research laboratory based on OT/ICS product analysis.

This information will be synchronized to the StellarOne backend for device management.

### OT Certificates



| Issue To | Issued By | Hash |
|---|---|---|
| Beckhoff Automation GmbH &... | DigiCert SHA2 High... | 8020A7770578... |
| General Electric Company | Symantec Class 3... | 5006C8F010D... |
| SIEMENS AG | Symantec Class 3... | 2FDDE9CC1B6... |
| Schneider Electric | VeriSign Class 3 Code... | 48A5F6877981... |
| Schneider Electric | VeriSign Class 3 Code... | E776B9C503D... |

Number of certifications: 5

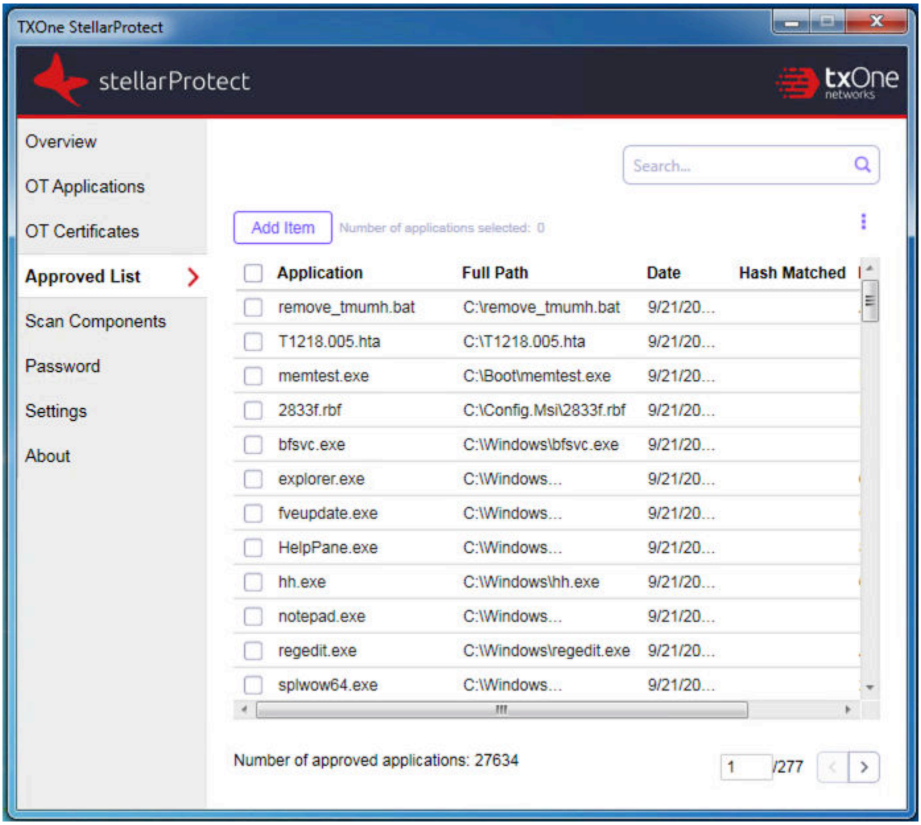
**FIGURE 5-4. OT Certificates**

Digital signature is currently the most secure software product identification technology, which can ensure that the signed software component is not illegally modified, and can identify that the software was released by the original manufacturer.

The number of OT/ICS certificates that StellarProtect can recognize will increasewith updates from the OT/ICS Application Inventory. This inventory is producedby the TXOne research laboratory and based on OT/ICS product analysis.

This information will be synchronized to the StellarOne backend for management.

## Approved List



Number of applications selected: 0

| □ | Application | Full Path | Date | Hash Matched |
|---|---|---|---|---|
| □ | remove_tmumh.bat | C:\remove_tmumh.bat | 9/21/20... | |
| □ | T1218.005.hta | C:\T1218.005.hta | 9/21/20... | |
| □ | memtest.exe | C:\Boot\memtest.exe | 9/21/20... | |
| □ | 2833f.rbf | C:\Config.Msi\2833f.rbf | 9/21/20... | |
| □ | bfsvc.exe | C:\Windows\bfsvc.exe | 9/21/20... | |
| □ | explorer.exe | C:\Windows... | 9/21/20... | |
| □ | fveupdate.exe | C:\Windows... | 9/21/20... | |
| □ | HelpPane.exe | C:\Windows... | 9/21/20... | |
| □ | hh.exe | C:\Windows\hh.exe | 9/21/20... | |
| □ | notepad.exe | C:\Windows... | 9/21/20... | |
| □ | regedit.exe | C:\Windows\regedit.exe | 9/21/20... | |
| □ | splwow64.exe | C:\Windows... | 9/21/20... | |

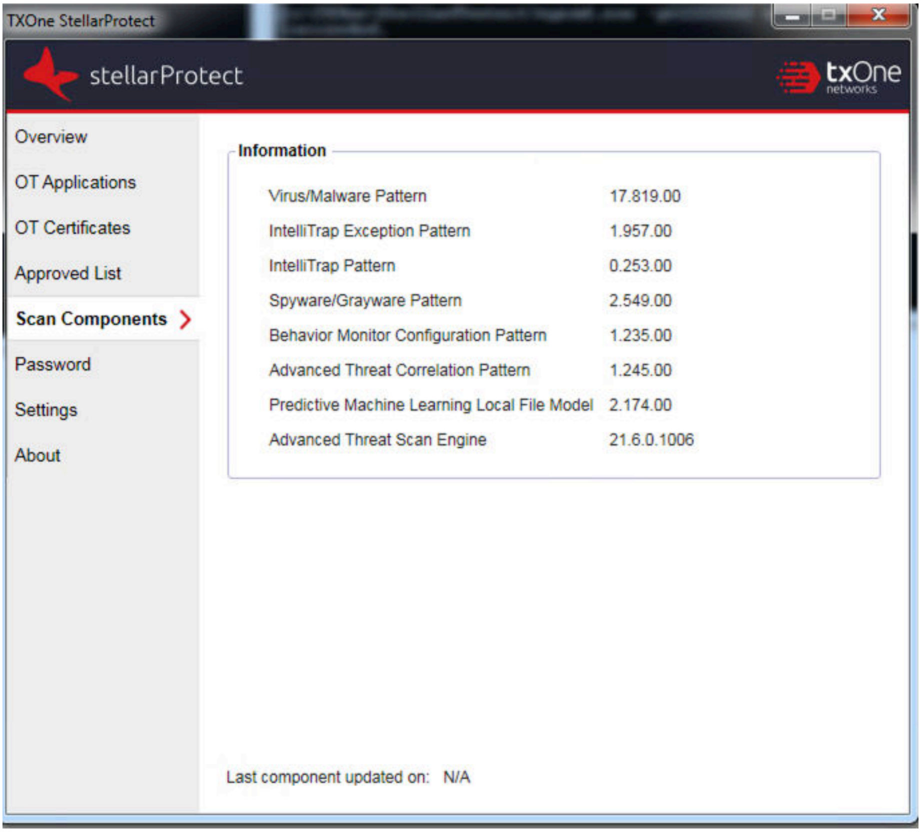
Number of approved applications: 27634

1 /277

**FIGURE 5-5. Approved List**

Applications found during prescan are added in the Approved List. Users can add and search for applications in this window. Users can also import or export trusted hashes by clicking the three-dot dropdown menu.

### Scan Components



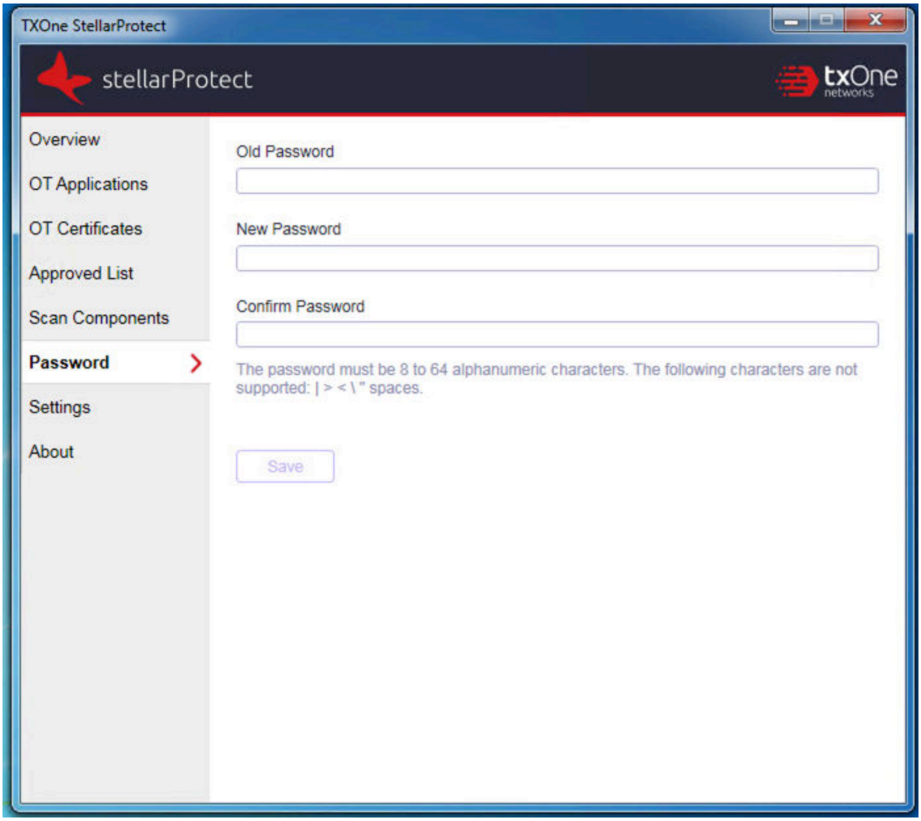
| | |
|---|---|
| Virus/Malware Pattern | 17.819.00 |
| IntelliTrap Exception Pattern | 1.957.00 |
| IntelliTrap Pattern | 0.253.00 |
| Spyware/Grayware Pattern | 2.549.00 |
| Behavior Monitor Configuration Pattern | 1.235.00 |
| Advanced Threat Correlation Pattern | 1.245.00 |
| Predictive Machine Learning Local File Model | 2.174.00 |
| Advanced Threat Scan Engine | 21.6.0.1006 |

Last component updated on: N/A

**FIGURE 5-6. Scan Components**

This navigation option list all critical scan engines and patterns with versions used by StellarProtect.

### Password

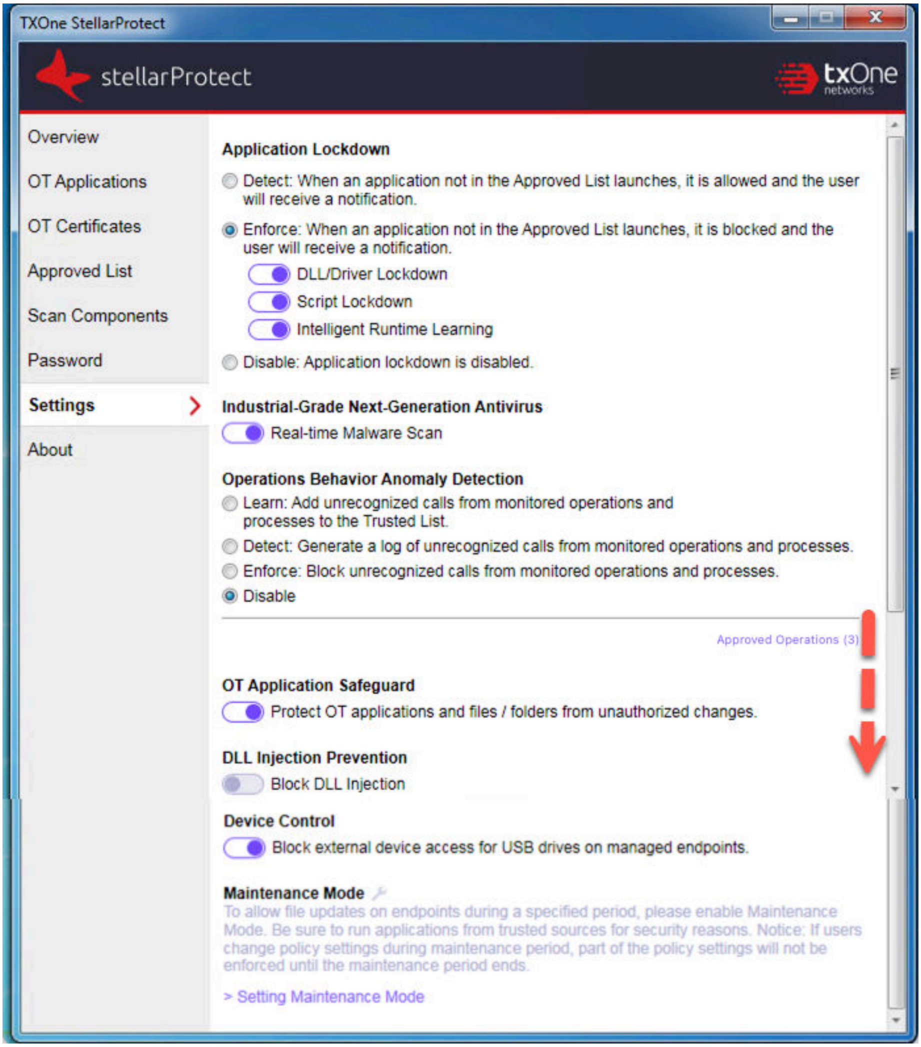


The password must be 8 to 64 alphanumeric characters. The following characters are not supported: | > < \ " spaces.

**FIGURE 5-7. Password Setting**

This navigation option functions as the StellarProtect administrator password change. The user must enter the correct old password, enter the same new password twice, confirm that the length of the new password meets the requirements, and press **Save** to complete the change.

## Settings



**Application Lockdown**

○ Detect: When an application not in the Approved List launches, it is allowed and the user will receive a notification.

● Enforce: When an application not in the Approved List launches, it is blocked and the user will receive a notification.

- ● DLL/Driver Lockdown
- ● Script Lockdown
- ● Intelligent Runtime Learning

○ Disable: Application lockdown is disabled.

**Industrial-Grade Next-Generation Antivirus**

● Real-time Malware Scan

**Operations Behavior Anomaly Detection**

○ Learn: Add unrecognized calls from monitored operations and processes to the Trusted List.

○ Detect: Generate a log of unrecognized calls from monitored operations and processes.

○ Enforce: Block unrecognized calls from monitored operations and processes.

● Disable

Approved Operations (3)

**OT Application Safeguard**

● Protect OT applications and files / folders from unauthorized changes.

**DLL Injection Prevention**

○ Block DLL Injection

**Device Control**

● Block external device access for USB drives on managed endpoints.

**Maintenance Mode**

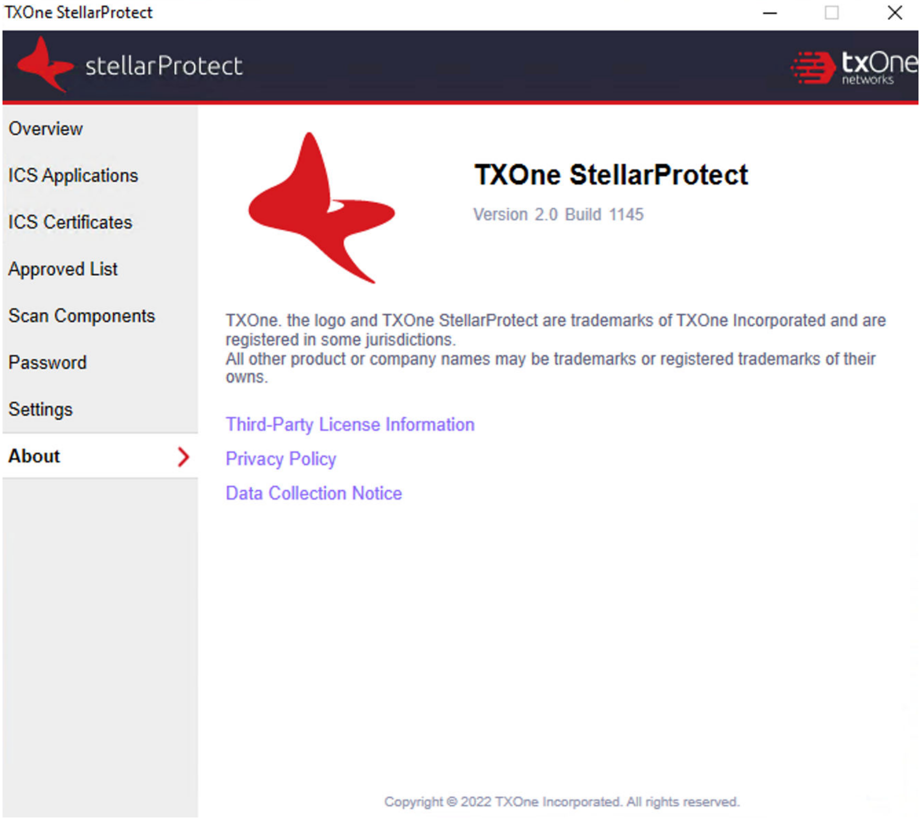
To allow file updates on endpoints during a specified period, please enable Maintenance Mode. Be sure to run applications from trusted sources for security reasons. Notice: If users change policy settings during maintenance period, part of the policy settings will not be enforced until the maintenance period ends.

> Setting Maintenance Mode

**FIGURE 5-8. Settings**

This section mainly describes the StellarProtect configuration options. Refer to *Settings of StellarProtect Console on page 5-13* for the introduction of the seven main protection functions. Each function has a switch that can be turned on or off.

### About



TXOne StellarProtect

Version 2.0 Build 1145

TXOne. the logo and TXOne StellarProtect are trademarks of TXOne Incorporated and are registered in some jurisdictions.
All other product or company names may be trademarks or registered trademarks of their owns.

Third-Party License Information

Privacy Policy

Data Collection Notice

Copyright © 2022 TXOne Incorporated. All rights reserved.

**FIGURE 5-9. About**

This includes StellarProtect product information, version and build number, as well as third-party license information.

# Settings of StellarProtect Console

### Application Lockdown

This feature prevents malware attacks and increases protection level by allowing only the files defined in the Application List to execute. Three modes are available for selection: **Detect**, **Enforce** and **Disable**.

**Detect**: The applications that are not in the Approved List will be allowed to run, and users will receive a notification.

**Enforce**: The applications that are not in the Approved List will be blocked from running, and users will receive a notification.

When users select the **Detect** or **Enforce** mode, three more protection options are available:

- **DLL/Driver Lockdown**: DLL/Driver Lockdown prevents unapproved DLLs or drivers from being loaded into the memory of protected endpoints.
- **Script Lockdown**: Script Lockdown prevents unapproved script files from being run on protected endpoints.
- **Intelligent Runtime Learning**: To ensure undisturbed operations, Intelligent Runtime Learning allows runtime executable files that are generated by applications in the Approved List to run smoothly.

**Disable**: The Application Lockdown can also be disabled if needed, but it is advisory to have this function enabled.

### Industrial-Grade Next-Generation Antivirus

Industrial-grade next-generation antivirus (real-time malware scan) is the core protection of StellarProtect. TXOne integrates signature-based and AI-based antivirus software to provide real-time scanning of any file or process activity.

StellarProtect integrates OT/ICS application system recognition technology, which can greatly reduce the occurrence of false alarms.

Users can click the switch to turn the function on or off

### Operations Behavior Anomaly Detection

Operationally abnormal behavior may be caused by advanced attacks (such as fileless attacks). StellarProtect can detect the behavior of these threats and keep logs for later analysis.

This function mainly allows StellarProtect to monitor specific high-risk applications, including `wscript.exe`, `cscript.exe`, `mshta.exe`, `powershell.exe` and `psexec.exe`, to stop legitimate programs from being misused. Users can add other monitoring processes via the StellarOne web console.

This function has four modes, including:

- **Learn**: After activating this function, StellarProtect will monitor unrecognized program calls and add them to the approved operations for learning more about OT/ICS-related program call behaviors.
- **Detect**: After activating this function, StellarProtect will monitor unrecognized program calls and log them for future analysis.
- **Enforce**: After activating this function, StellarProtect will monitor unrecognized program calls and block them to secure the endpoint.
- **Disable**: When **Operations Behavior Anomaly Detection** is set to **Disable**, the protection is turned off.

In either **Detect** or **Enforce** mode, users have one more option, **Aggressive Mode**, for higher antivirus security. This feature activates protection through process parameter recognition. By adding parameter identification in the monitoring task, users can check the operation process and its accompanied changes in parameters under monitoring.

### OT Application Safeguard

OT/ICS application patches or hotfixes may cause anti-virus false alarms, including potential blocking. StellarProtect can use OT/ICS inventory technology to verify legal updates for the OT/ICS applications, and can keep recognized OT/ICS applications updated without blocking or alerts.

This function supports StellarProtect by identifying OT/ICS application technology and providing protection that is consistent with OT/ICS application system updates.

After enabling "Protect OT application and files/folders from unauthorized changes", ICS application executable files will be protected automatically without user definition. On the other hand, StellarProtect will monitor and protect the files and folders defined by the administrator on StellarOne web console.

#### DLL Injection Prevention

DLL injection is a high-risk attack in the OT/ICS field, and StellarProtect can prevent this type of attack when this feature is enabled.

**Note**

DLL injection can only be enabled in 32-bit Windows OSes.

#### Device Control

Device Control is the function of StellarProtect to control external USB storage devices to ensure that only authorized USB devices can be used on endpoints protected by StellarProtect.

This function mainly provides identification and protection from external USB storage devices. Use the USB device's Vendor ID (VID), Product ID (PID) and Serial Number (SN) to determine whether the device is a trusted USB storage device.

Device Control grants a one-time permission to approved USB storage access after administrator authentication. When an unauthorized USB storage device is inserted into the endpoint the first time, the user will be prompted to enter the administrator password. This is set up as a single authorization to increase user convenience.

Meanwhile, StellarProtect will send a blocked event notification to StellarOne, and the administrator can view the blocked event on the StellarOne console and decide to continue blocking or approving the access.

The Device Control use case is as follows:

1. Plug in the USB.
2. The USB will be blocked if Device Control is enabled and the device is untrusted.
3. A pop-up window appears to require users to enter the administrator password.
4. After granted access permission, the USB device can be allowed access until unplugged.

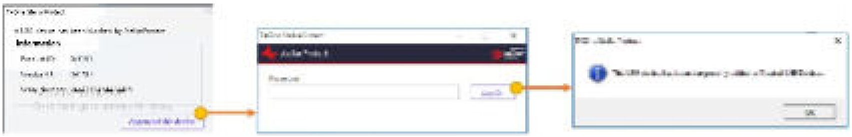


**FIGURE 5-10. Use Case of Device Control**

Users can click the switch to turn on or off the function.

### Maintenance Mode

To perform file updates on endpoints, users can configure Maintenance Mode settings to define a period when StellarProtect allows all file executions and adds all files that are created, executed, or modified to the Approved List.

During the maintenance period, all newly-added files can be updated accompanied with real-time virus scan for consistent security. StellarProtect can learn the newly-added applications and ensure the execution of these applications are under protection.

**Note**

If users change the policy settings of Application Lockdown, OT Application Safeguard, and Real-Time Malware Scan (Industrial-Grade Next-Generation Antivirus) during maintenance period, the policy settings will not be enforced until the maintenance period ends.

# Chapter 6

# Using the Agent Command Line Interface (CLI)

TThis chapter describes how to configure and use TXOne StellarProtect using the command line interface (CLI).

Topics in this chapter include:

# Using OPCmd at the Command Line Interface (CLI)

Administrators can work with TXOne StellarProtect directly from the command line interface (CLI) using the `OPCmd.exe` program.

**Procedure**

1. Open a command prompt window with Windows administrator privileges.
2. Navigate to the TXOne StellarProtect installation folder using the `cd` command.

   For example, type the following command to reach the default location:

   ```
   cd /d "c:\Program Files\TXOne\StellarProtect\"
   ```

3. Type `OPCmd.exe -h` to get usage information for an individual command.

# Overview of StellarProtect CLI

The CLI provides a POSIX-style command line interface. The general usage is as follows:

```
C:> opcmd.exe [global-options] [command [options]]
```

The global-options are options that affect all commands, and must come before the command. A command consists of one or more words, followed by any options that are specific to that command. If an option requires an argument, you may specify the argument in one of the following syntaxes:

### Options

Separate long option and argument with an equal sign:

```
--option=<argument>
```

Argument follows the option character immediately:

`-o<argument>`

If the argument is not optional, you may also separate the option and argument with a space:

`-o <argument>`

**Important**

All options are optional, including global options and command-specific options. In the commands below, if it says an argument is required, it means the argument is required when that option is used.

For the short forms of options, multiple option characters can be combined in one word as long as the option with argument comes last. For example, the following commands are equivalent:

- `opcmd.exe foo -a -b 15 -c`
- `opcmd.exe foo -ac -b15`
- `opcmd.exe foo -cab 15`
- `opcmd.exe foo -acb15`

### Global Options

- Global Option: `-h`, `--help`

  Description: When used alone, shows a brief summary of how to use the CLI. When used with a command, shows help text for that command.

  Argument: No

- Global Option: `-p`, `--password [<password>]`

  Description: Specifies the administrator password for executing protected commands. The `-p` option is mandatory for protected commands. If you don't provide an administrator password with this option on protected commands, the CLI asks for a password before executing the command and may not execute command if the password is incorrect. If you need to run protected commands from a batch file, provide your password with -p and make the batch file readable only to authorized users.

**Note**

To prevent your administrator password from leaking accidently, use `-p` without argument to avoid the shell (`cmd.exe`) from recording your password in the command history.

Argument: Optional. Password in plain text.

- Global Option: `-v`, `--version`

  Description: Show CLI program version.

  Argument: No

## List of All Commands

**Table 6-1. List of All Commands**

| Command | Description | Options |
|---|---|---|
| `opcmd.exe about components` | You can browse versions of components from the GUI program, or you can get the list in YAML format with this command. | None |
| `opcmd.exe -p appinv make` | The StellarProtect service will re-detect installed OT/ICS applications when your scheduled maintenance mode ends. You can also use this command to perform the detection manually at any time. | None |

| COMMAND | DESCRIPTION | OPTIONS |
|---|---|---|
| `opcmd.exe appinv list` | You can browse the list of detected OT/ICS applications from the GUI program oy use this command to get the list in YAML format. | None |
| `opcmd.exe -p config decrypt [-i INPUT-FILE] [-o OUTPUT-FILE]` | Decrypts an encrypted configuration file and outputs decrypted plaintext.<br>**Note**<br>The data security of this command is designed for the protection of configuration files. Do not rely on this command to protect personal privacy data. | `-i, --input INPUT - FILE`: The required argument to specify the filename of an input file. If it's omitted, the program will read from standard input.<br>`-o, --output OUTPUT - FILE`: The required argument to specify the filename of an output file. If it's omitted, the program will write to standard output. |
| `opcmd.exe -p config encrypt [-i INPUT-FILE] [-o OUTPUT-FILE]` | Encrypts a plaintext configuration file and outputs encrypted ciphertext.<br>**Note**<br>The data security of this command is designed for protection of configuration files. Do not rely on this command to protect any personal privacy data. | `-i, --input INPUT-FILE`: The required argument to specify the filename of an input file. If it's omitted, the program will read from standard input.<br>`-o, --output OUTPUT-FILE`: The required argument to specify the filename of an output file. If it's omitted, the program will write to standard output. |
| `opcmd.exe -p config export OUTPUT-FOLDER` | Exports product configuration settings to the specified folder. | None |

| Command | Description | Options |
|---|---|---|
| `opcmd.exe -p config import INPUT-FOLDER` | Imports product configuration settings from the specified folder. | `-n`, `--no_ptn`<br>**Note**<br>Do not import pattern files. |
| `opcmd.exe -p dip disable` | Disables the DLL Injection Prevention function. | None |
| `opcmd.exe -p dip enable` | Enables the DLL Injection Prevention function. | None |
| `opcmd.exe -p lock appinv disable` | Disables OT Application Safeguard | None |
| `opcmd.exe -p lock appinv enable` | Enables OT Application Safeguard | None |
| `opcmd.exe -p lock disable` | Disables the Change Control module to allow file changes on protected files. | None |
| `opcmd.exe -p lockdown approvedlist info` | Shows Application Lockdown Approved List information. | None |
| `opcmd.exe -p lockdown approvedlist init [--overwrite]` | Initializes Appplication Lockdown Approved List. | `-o`, `--overwrite`: This command is used to overwrite existing Application Lockdown Approved List.<br>If `-o` is not specified, detected applications will be added to existing Appplication Lockdown Approved List. |

| Command | Description | Options |
|---|---|---|
| `opcmd.exe -p lockdown approvedlist add -p PATH [--recursive]` | Adds the specified file to the Application Lockdown Approved List | `-p`, `--path PATH`: Adds the specified file to the Application Lockdown Approved List<br>`-r`, `--recursive`: Includes the specified folder and related subfolders |
| `opcmd.exe -p lockdown enable -m MODE` | Enables Application Lockdown | `-m`, `--mode MODE`: Specifies the mode (Detect or Enforce) for Application Lockdown |
| `opcmd.exe -p lockdown disable` | Disables Application Lockdown | None |
| `opcmd.exe -p lockdown exceptionpath -t TYPE -p PATH (--add\|--remove)` | Adds or removes an Application Lockdown exception path | `-t`, `--type TYPE`: Specifies type of exception path (file, folder, folder and subfolder, ecmascript_regexp).<br>`-p`, `--path PATH`: Specifies exception path or regexp. |
| `opcmd.exe -p lockdown info` | Shows Application Lockdown information | None |
| `opcmd.exe -p lockdown script info` | Display all Application Lockdown script rules | None |
| `opcmd.exe -p lockdown script add -e EXTENSION -p INTERPRETER [-p INTERPRETER2] ...` | Adds the specified script extension and the interpreter required to execute the script | `-e`, `--ext EXTENSION`: Specifies script extension<br>`-p`, `--proc INTERPRETER`: Specifies name of script interpreter |
| `opcmd.exe -p lockdown script remove -e EXTENSION [-p INTERPRETER] ...` | Removes the specified script extension and the interpreter required to execute the script | `-e`, `--ext EXTENSION`: Specifies script extension<br>`-p`, `--proc INTERPRETER`: Specifies name of script interpreter |

| Command | Description | Options |
|---|---|---|
| `opcmd.exe -p lockdown subfeature -f SUBFEATURE (--enable\|--disable)` | Toggles sub-feature of Application Lockdown | `-f`, `--feature SUBFEATURE`: Specifies sub-feature (dll_driver, script, intelligent_runtime_learning) |
| `opcmd.exe -p lockdown trustedhash -h HASH (--add\|--remove)` | Adds or removes an Application Lockdown trusted hash | `-h`, `--hash HASH`: Specifies trusted hash<br>**Note**<br>Only `SHA-256` is supported. |
| `opcmd.exe -p lock enable` | Enables Change Control module to prevent file changes on protected files. If Change Control module is disabled by a scheduled maintenance mode, this command will end the maintenance mode immediately. | None |

| Command | Description | Options |
|---|---|---|
| `opcmd.exe -p maintenance start` | Starts or schedules maintenance mode. You can specify a duration and start time to schedule maintenance mode that allows file changes and restores protection automatically | `-d`, `--duration` `DURATION`: Specifies a duration of maintenance mode. A duration can be specified in minutes, hours, or both (for example, -d30, -d2h, -d2h30m). The letter 'm' can be omitted if you want to specify a duration only in minutes.<br>`-s`, `--start` `START-TIME`: Specifies the start time of maintenance mode. The `START-TIME` is in ISO8601 format without time zone, e.g., `-s 2021-04-14T18:00:00`).<br>`-r`, `--activate-rts` `ACTIVATE-REALTIME-SCAN`: Enables real-time scan during maintenance mode. |
| `opcmd.exe -p maintenance stop` | Stops running maintenance mode or cancels scheduled maintenance mode | None |
| `opcmd.exe -p maintenance info` | Shows maintenance mode information | None |
| `opcmd.exe -p oad disable` | Disables Operations Behavior Anomaly Detection | None |

| COMMAND | DESCRIPTION | OPTIONS |
|---|---|---|
| `opcmd.exe -p oad enable -m MODE [-l LEVEL]` | Enables Operations Behavior Anomaly Detection | `-m`, `--mode` `MODE`: The required argument to enable Operations Behavior Anomaly Detection as a specific mode (`learn`, `detect`, `enforce`).<br>`-l`, `--level` `LEVEL`: The required argument to set the scan to be `normal` or `aggressive`. |
| `opcmd.exe -p oad info` | Shows information about Operations Behavior Anomaly Detection | None |
| `opcmd.exe -p oad remove -i ID` | Removes approved operations from Operations Behavior Anomaly Detection | `-i`, `--id` `ID`: The required argument to remove approved operations<br>**Note**<br>The approved operations IDs are represented as integers. |
| `opcmd.exe password` | Allows administrator to change the administrator password via CLI. You are required to enter the old password before setting a new password. | None |
| `opcmd.exe -p proxy get` | Shows proxy server settings | None |

| Command | Description | Options |
|---|---|---|
| `opcmd.exe -p proxy set [-h HOST -p PORT [-u USERNAME] [-P PASSWORD]]` | Sets proxy server settings<br>**Note**<br>To disable proxy use only, use this command without inputing any options. | `-h`, `--host` `HOST`: The required argument to specify the FQDN, hostname, or IP address of the proxy server.<br>`-p`, `--port` `PORT`: The required argument to specify the port number of the proxy server.<br>`-u`, `--username` `USERNAME`: The required argument to specify the username for proxy server authentication.<br>`-P`, `--password` `PASSWORD`: The required argument to specify the password for proxy server authentication. |
| `opcmd.exe -p regexp test -s STRING -p PATTERN` | Checks if the regular expression matches the string. | None |
| `opcmd.exe -p scan task -s START-TIME --daily --weekly --monthly` | Schedules a recurring scan task at specified start time. | `-s`, `--start` `START-TIME`: The required argument to specify the start time of a scheduled scan. The `START-TIME` is in ISO8601 format without time zone, e.g., `-s 2021-04-14T18:00:00`<br>`--daily`: Sets the scheduled scan to run daily<br>`--weekly`: Sets the scheduled scan to run weekly<br>`--monthly`: Sets the scheduled scan to run monthly<br>`--remove`: Removes the scheduled scan |

| Command | Description | Options |
|---|---|---|
| `opcmd.exe -p service start` | After installation, the StellarProtect service will automatically start when your system is powered on. If yourStellarProtect service was stopped for some reason, you can use this command to start the StellarProtect service manually. | None |
| `opcmd.exe -p service stop` | This stops StellarProtect service until the system is powered off. If you need to stop StellarProtect service, you can use this command to stop StellarProtect service manually. | None |
| `opcmd.exe -p scan task --now` | Implements silent manual scan and send the scan result to the StellarOne management console. | None |
| `opcmd.exe update [-s SOURCE]` | Updates product components. | `-s`, `--source SOURCE`: The required argumen to specify the URL of the update source, e.g., `-s http:// tmut.contoso.com / iau_server` |
| `opcmd.exe -p update stop` | Stops the currently running update | None |

| Command | Description | Options |
|---|---|---|
| `opcmd.exe -p usb add [-v VID -p PID -s SN] [-o]` | Adds a trusted USB device | `-v`, `--vid` VID: The required argument to specify Vendor ID by hexadecimal string<br>`-p`, `--pid` `PID`: The required argument to specify Product ID by hexadecimal string<br>`-s` `--sn` `SN`: The required argument to specify Serial Number<br>`-o`, `--onetime`: Grants onetime access to a USB device |
| `opcmd.exe -p usb enable` | Enables USB Device Control | None |
| `opcmd.exe -p usb disable` | Disables USB Device Control | None |
| `opcmd.exe -p usb info -d DRIVE` | Show USB information of the specified drive | `-d`, `--drive` `DRIVE`: The required argument to specify the path to a drive, e.g., `E:` |
| `opcmd.exe -p usb list` | Lists trusted USB devices | None |
| `opcmd.exe -p usb remove [-v VID -p PID -s SN]` | Removes a trusted USB device | `-v`, `--vid` `VID`: The required argument to specify Vendor ID by hexadecimal string<br>`-p`, `--pid` `PID`: The required argument to specify Product ID by hexadecimal string<br>`-s` `--sn` `SN`: The required argument to specify Serial Number |
| `opcmd.exe -p usb status` | Shows USB Device Control status | None |
| `opcmd.exe -p quarantine show` | Shows the list of quarantined files | None |

| Command | Description | Options |
|---|---|---|
| `opcmd.exe -p quarantine restore [QUARANTINENAME]` | Restores the specified quarantined file | None |
| `opcmd.exe -p udso list` | Lists user-defined suspicious objects | `-a`, `--all`: Lists all types of suspicious objects.<br>`-p`, `--file-path`: Lists file path to the suspicious objects<br>`-h`, `--file-sha1`: Lists file SHA1 of the suspicious objects.<br>`-H`, `--file-sha2`: Lists file SHA2 of the suspicious objects |
| `opcmd.exe -p udso scan` | Scans existing processes for user-defined suspicious objects | You'll be asked for confirmation before terminating these suspicious processes. |

| Command | Description | Options |
|---|---|---|
| `opcmd.exe -p update-task` | Schedules a recurring update task at specified start time and interval | `--time START-TIME`: Specifies the start time (HH:MM) of scheduled update.<br>`--daily`: Specifies the scheduled update to run daily.<br>`--weekly DAY-OF-WEEK`: Specifies the scheduled update to run weekly on a given day of a week. Only Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday are valid.<br>`--monthly DAY-OF-MONTH`: Specifies the scheduled update to run monthly on a given day of a month (1-31). Specifies `-1` to run the update on the last day of a month.<br>`--remove`: Removes the scheduled update |

# Chapter 7

## Events

This chapter describes events as they will be recorded within the TXOne StellarProtect Agent. Topics in this chapter include:

## Overview of StellarProtect Event Logs

The StellarProtect agent logs events within three classifications.

- **Level 0: Information** logs important tasks
- **Level 1: Warning** logs incidents
- **Level 2: Critical** logs when critical functions are turned on or off

## Access StellarProtect Event Logs

TXOne StellarProtect leverages the Windows™ Event Viewer to display the **ALL** StellarProtect event log. Access the Event Viewer at **Start** > **Control Panel** > **Administrative Tools**.

**FIGURE 7-1. Windows Event Viewer**

TXOne StellarProtect Agent Console is another entry that allows users to check the StellarProtect **BLOCKED** event log. Access the agent blocked event at **op_ui.exe** > **Overview** > **Information** > **Last blocked event**.

**FIGURE 7-2. Check BLOCKED Events onStellarProtect Console**

## Agent Event Log Descriptions for StellarProtect

This table details the Windows event log descriptions for StellarProtect.

| EVENT ID | LEVEL | CATEGORY | EVENT DESCRIPTION | EVENT DETAILS |
|---|---|---|---|---|
| 256 | Information | System | Service Started | The service has started. |

| Event ID | Level | Category | Event Description | Event Details |
|---|---|---|---|---|
| 257 | Information | System | Policy Applied Successfully (Version: %version%) | Policy has been applied successfully. |
| 258 | Information | System | Patch Applied. File Name: %file_name% | Patch has been applied successfully. |
| 259 | Information | System | Patching in Progress | Patching is in progress. After the earlier-applied patch has been completely updated, the system will automatically try to apply this patch: %deferred_file_name%. |
| 513 | Information | intelli_av | ICS Inventory List Update Succeeded | The ICS Inventory List has been updated successfully. |
| 514 | Information | intelli_av | Real Time Scan Enabled | The real-time scan is enabled. |
| 515 | Information | intelli_av | Scheduled Scan Started | The scheduled scan has started. |

| EVENT ID | LEVEL | CATEGORY | EVENT DESCRIPTION | EVENT DETAILS |
|---|---|---|---|---|
| 516 | Information | intelli_av | Scheduled Scan Ended | A scheduled scan has ended.<br>[Details]<br>Folders scanned: %1<br>Symbolic links: %2<br>Regular files: %3<br>Files scanned: %4<br>Files passed: %5<br>Threats detected: %6 |
| 517 | Information | intelli_av | On-Demand Scan Started | The manually launched scan has started. |
| 518 | Information | intelli_av | On-Demand Scan Ended | A manually launched scan has ended.<br>[Details]<br>Folders scanned: %1<br>Symbolic links: %2<br>Regular files: %3<br>Files scanned: %4<br>Files passed: %5<br>Threats detected: %6 |

| Event ID | Level | Category | Event Description | Event Details |
|---|---|---|---|---|
| 519 | Information | intelli_av | Scheduled Scan Enabled | A scheduled scan has been enabled. Next scan will be on %NextScan%. |
| 520 | Information | intelli_av | Scheduled Scan Disabled | A scheduled scan has been disabled. |
| 521 | Information | intelli_av | Manual Scan Started | A scan manually launched by local user has started. |
| 522 | Information | intelli_av | Manual Scan Ended | A scan manually launched by local user has ended.<br>[Details]<br>Folders scanned: %1<br>Symbolic links: %2<br>Regular files: %3<br>Files scanned: %4<br>Files passed: %5<br>Threats detected: %6 |
| 768 | Information | anomaly_detect | Operations Behavior Anomaly Detection Enabled | Mode: %Mode%<br>Level: %Level% |

| Event ID | Level | Category | Event Description | Event Details |
|---|---|---|---|---|
| 769 | Information | anomaly_detect | Approved Operation Added to Operations Behavior Anomaly Detection | Access User: %USERNAME%<br>ID: %ID%<br>Target Process: %PATH% %ARGUMENT%<br>Parent Process 1: %PATH% %ARGUMENT%<br>Parent Process 2: %PATH% %ARGUMENT%<br>Parent Process 3: %PATH% %ARGUMENT%<br>Parent Process 4: %PATH% %ARGUMENT% |

| Event ID | Level | Category | Event Description | Event Details |
|---|---|---|---|---|
| 770 | Information | anomaly_detect | Operations Behavior Anomaly Detection Removed from Approved Operation | ID: %ID%<br>Target Process: %PATH% %ARGUMENT%<br>Parent Process 1: %PATH% %ARGUMENT%<br>Parent Process 2: %PATH% %ARGUMENT%<br>Parent Process 3: %PATH% %ARGUMENT%<br>Parent Process 4: %PATH% %ARGUMENT% |
| 784 | Information | anomaly_detect | DLL Injection Prevention Enabled | The DLL Injection Prevention has been enabled. |
| 1280 | Information | device_control | Device Control Enabled | The Device Control has been enabled. |
| 1281 | Information | device_control | Trusted USB Device Added | Vendor ID: %HEX %<br>Product ID: %HEX%<br>Serial Number: %STRING%<br>Type: permanent or one time |

| Event ID | Level | Category | Event Description | Event Details |
|---|---|---|---|---|
| 1282 | Information | device_control | Trusted USB Device Removed | Vendor ID: %HEX %<br>Product ID: %HEX%<br>Serial Number: %STRING% |
| 1792 | Information | lockdown | File Access Allowed: %PATH % | Access Image Path: %PATH%<br>Access User: %USERNAME%<br>Mode: %MODE%<br>List: %LIST% |
| 1793 | Information | lockdown | Added to Approved List in Maintenance Mode | Path: %PATH%<br>Hash: %SHA256_HEXSTR% |
| 1794 | Information | lockdown | Approved List Updated in Maintenance Mode | Path: %PATH%<br>Hash: %SHA256_HEXSTR% |
| 1795 | Information | lockdown | Approved List Initialization Started | Approved List initialization started |
| 1796 | Information | lockdown | Approved List Initialization Completed | Approved List initialization completed<br>Count: %COUNT % |

| Event ID | Level | Category | Event Description | Event Details |
|---|---|---|---|---|
| 1797 | Information | lockdown | Application Lockdown Enabled | Application Lockdown enabled<br>Mode: %MODE% |
| 1798 | Information | lockdown | DLL/Driver Lockdown Enabled | DLL/Driver Lockdown enabled |
| 1799 | Information | lockdown | Script Lockdown Enabled | Script Lockdown enabled |
| 1800 | Information | lockdown | Intelligent Runtime Learning Enabled | Intelligent Runtime Learning enabled |
| 2048 | Information | update | Component Update Started | Component update has started |
| 2049 | Information | update | Component Update Ended | Component update has ended. |
| 2050 | Information | update | Scheduled Component Update Enabled, Next Update Will Be On %NEXT_UPDATE_LOCAL_TIME_STR% (agent's local system time). | Scheduled component update has been enabled. Next update will be on %NEXT_UPDATE_LOCAL_TIME_STR% (agent's local system time). |
| 2051 | Information | update | Scheduled Component Update Disabled. | Scheduled component update has been disabled. |

| Event ID | Level | Category | Event Description | Event Details |
|---|---|---|---|---|
| 4352 | Warning | system | Service Stopped | The service has stopped. |
| 4353 | Warning | system | Unable to Apply Policy (Version: %version%) | The policy can not be applied. |
| 4354 | Warning | system | Unable to Update File: %dst_path% | Unable to update file.<br>Source Path: %src_path%<br>Destination Path: %dst_path %<br>Error Code: %err_code% |
| 4355 | Warning | system | Unable to Apply Patch. File Name: %file_name% | Unable to apply patch.<br>File Name: %file_name%<br>Error Code: %err_code% |

| Event ID | Level | Category | Event Description | Event Details |
|---|---|---|---|---|
| 4609 | Warning | intelli_av | Incoming Files Scanned, Action Taken by Antivirus: %PATH% | Incoming files were scanned by antivirus. Actions were taken according to settings.<br>File Path: %PATH %<br>File Hash: %STRING%<br>Threat Type: %STRING%<br>Threat Name: %STRING%<br>Action Result: %INTEGER%<br>Quarantine Path: %PATH% |

| EVENT ID | LEVEL | CATEGORY | EVENT DESCRIPTION | EVENT DETAILS |
|---|---|---|---|---|
| 4610 | Warning | intelli_av | Incoming Files Scanned, Action Taken by Next-Generation Antivirus: %PATH% | Incoming files were scanned by next-generation antivirus. Actions were taken according to settings.<br>File Path: %PATH%<br>File Hash: %STRING%<br>Threat Type: %STRING%<br>Threat Name: %STRING%<br>Action Result: %INTEGER%<br>Quarantine Path: %PATH% |

| Event ID | Level | Category | Event Description | Event Details |
|---|---|---|---|---|
| 4611 | Warning | intelli_av | Local Files Scanned, Action Taken by Antivirus: %PATH% | Local files were scanned by antivirus. Actions were taken according to settings.<br>File Path: %PATH %<br>File Hash: %STRING%<br>Threat Type: %STRING%<br>Threat Name: %STRING%<br>Action Result: %INTEGER%<br>Quarantine Path: %PATH% |

| Event ID | Level | Category | Event Description | Event Details |
|---|---|---|---|---|
| 4612 | Warning | intelli_av | Local Files Scanned, Action Taken by Next-Generation Antivirus: %PATH% | Local files were scanned by next-generation antivirus. Actions were taken according to settings.<br>File Path: %PATH %<br>File Hash: %STRING%<br>Threat Type: %STRING%<br>Threat Name: %STRING%<br>Action Result: %INTEGER%<br>Quarantine Path: %PATH% |
| 4613 | Warning | intelli_av | Suspicious Program Execution Blocked: %PATH % | Suspicious program execution was blocked.<br>File Path: %PATH %<br>File Hash: %STRING% |

| Event ID | Level | Category | Event Description | Event Details |
|---|---|---|---|---|
| 4614 | Warning | intelli_av | Suspicious Program Currently Running: %PATH % | Suspicious program is currently running.<br>Process ID: %PID %<br>File Path: %PATH %<br>File Hash: %STRING%<br>File Credibility: %STRING% |
| 4615 | Warning | intelli_av | Application Execution Blocked By Antivirus: %PATH% | Application execution was blocked by antivirus.<br>Target Process: %PATH%<br>File Hash: %STRING%<br>Threat Type: %STRING%<br>Threat Name: %STRING% |

| Event ID | Level | Category | Event Description | Event Details |
|---|---|---|---|---|
| 4617 | Warning | intelli_av | Application Execution Blocked By Next-Generation Antivirus: %PATH% | Application execution was blocked by next-generation antivirus.<br>Target Process: %PATH%<br>File Hash: %STRING%<br>Threat Type: %STRING%<br>Threat Name: %STRING% |
| 4864 | Warning | anomaly_detect | Operations Behavior Anomaly Detection Disabled | Operations Behavior Anomaly Detection has been disabled. |
| 4865 | Warning | anomaly_detect | Process Allowed by Operations Behavior Anomaly Detection: %PATH% %ARGUMENT% | Access User: %USERNAME%<br>Parent Process 1: %PATH% %ARGUMENT%<br>Parent Process 2: %PATH% %ARGUMENT%<br>Parent Process 3: %PATH% %ARGUMENT%<br>Parent Process 4: %PATH% %ARGUMENT%<br>Mode: %Mode% |

| Event ID | Level | Category | Event Description | Event Details |
|---|---|---|---|---|
| 4866 | Warning | anomaly_detect | Process Blocked by Operations Behavior Anomaly Detection: %PATH% %ARGUMENT% | Access User: %USERNAME%<br>Parent Process 1: %PATH% %ARGUMENT%<br>Parent Process 2: %PATH% %ARGUMENT%<br>Parent Process 3: %PATH% %ARGUMENT%<br>Parent Process 4: %PATH% %ARGUMENT%<br>Mode: %Mode% |
| 4880 | Warning | anomaly_detect | DLL Injection Prevention Disabled | DLL Injection Prevention has been disabled. |
| 5120 | Warning | change_control | ICS File Change Blocked by SafeGuard: %PATH% | ICS files changed to executable files were blocked by SafeGuard.<br>Blocked Process: %PATH%<br>Target File: %PATH% |

| Event ID | Level | Category | Event Description | Event Details |
|---|---|---|---|---|
| 5121 | Warning | change_control | ICS Process Manipulation Blocked by SafeGuard: %PATH% | ICS Process Manipulation was blocked by SafeGuard.<br>Blocked Process: %PATH%<br>Target Process: %PATH% |
| 5376 | Warning | device_control | Device Control Disabled | Device Control has been disabled. |
| 5377 | Warning | device_control | USB Access Blocked: %PATH % | Access Image Path: %PATH%<br>Access User: %USERNAME%<br>Vendor ID: %HEX %<br>Product ID: %HEX%<br>Serial Number: %STRING% |

| Event ID | Level | Category | Event Description | Event Details |
|---|---|---|---|---|
| 5888 | Warning | lockdown | File Access Allowed: %PATH% | Access Image Path: %PATH%<br>Access User: %USERNAME%<br>Mode: %MODE%<br>Reason: %ALLOWED_REASON%<br>File hash allowed: %SHA256_HEXSTR% %THROTTLING_INFO_MSG% |
| 5889 | Warning | lockdown | File Access Blocked: %PATH% | Access Image Path: %PATH%<br>Access User: %USERNAME%<br>Mode: %MODE%<br>Reason: %BLOCKED_REASON%<br>File hash blocked: %SHA256_HEXSTR% %THROTTLING_INFO_MSG% |
| 5890 | Warning | lockdown | Unable to Add to or Update Approved List: %PATH% | Unable to add to or update Approved List: %PATH% |

| Event ID | Level | Category | Event Description | Event Details |
|---|---|---|---|---|
| 5891 | Warning | lockdown | Application Lockdown Disabled | Application Lockdown disabled |
| 5892 | Warning | lockdown | DLL/Driver Lockdown Disabled | DLL/Driver Lockdown disabled |
| 5893 | Warning | lockdown | Script Lockdown Disabled | Script Lockdown disabled |
| 5894 | Warning | lockdown | Intelligent Runtime Learning Disabled | Intelligent Runtime Learning disabled |
| 5895 | Warning | lockdown | Approved List Initialization Canceled | Approved List initialization canceled |
| 8706 | Critical | intelli_av | Real Time Scan Disabled | The Real-Time Scan has been disabled. |
| 9216 | Critical | change_control | Maintenance Mode Started | The Maintenance Mode has started. |
| 9217 | Critical | change_control | Maintenance Mode Ended | The Maintenance Mode has ended. |

# Chapter 8

## 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 on page 8-2*
- *Contacting Trend Micro and TXOne on page 8-3*
- *Sending Suspicious Content to Trend Micro on page 8-5*
- *Other Resources on page 8-6*

# 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 8-1. Trend Micro Contact Information**

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

**TABLE 8-2. TXOne Contact Information**

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

- Worldwide support offices:

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

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

- Trend Micro product documentation:

  https://docs.trendmicro.com

## Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional connected hardware or devices
- Amount of memory and free hard disk space
- Operating system and service pack version
- Version of the installed agent
- Serial number or Activation Code
- Detailed description of install environment
- Exact text of any error message received

# Sending Suspicious Content to Trend Micro

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

## Email Reputation Services

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

https://ers.trendmicro.com/

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

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

## File Reputation Services

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

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

Record the case number for tracking purposes.

## Web Reputation Services

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

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

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

# Other Resources

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

## Download Center

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

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

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

# Index

txOne networks

**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: APEM219658/221221