

2.0 TXOne StellarProtect

Installation and Administrator's Guide

All-terrain protection for mission critical assets

Windows



TXOne Networks reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the TXOne Networks website at:

<https://docs.trendmicro.com/en-us/enterprise/txone-stellarprotect.aspx>

© 2022 TXOne Networks. All rights reserved. TXOne Networks, StellarProtect, and StellarOne are trademarks or registered trademarks of TXOne Networks. All other product or company names may be trademarks or registered trademarks of their owners.

Document Part No.:APEM29618/221104

Release Date: November 2022

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

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

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

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

Evaluate this documentation on the following site:

<http://docs.trendmicro.com/en-us/survey.aspx>

Privacy and Personal Data Collection Disclosure

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

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

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

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

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

Table of Contents

Preface

| | |
|-------------------------------|----|
| Preface..... | v |
| About the Documentation | v |
| Audience | vi |
| Document Conventions | vi |

Chapter 1: Introduction

| | |
|--|-----|
| About the TXOne™ Stellar™ Series and StellarProtect™ | 1-2 |
| What's New | 1-2 |
| Agent Features and Benefits | 1-3 |

Chapter 2: Installation

| | |
|--|------|
| System Requirements | 2-2 |
| System Requirements | 2-2 |
| Operating Systems | 2-3 |
| Local Installation | 2-5 |
| Getting the StellarProtect Agent Package | 2-5 |
| Installing the StellarProtect Agent | 2-8 |
| Silent Installation | 2-21 |
| Configuring Silent Installation..... | 2-21 |
| Silent Installation of the StellarProtect Agent | 2-26 |
| Preparing the Agent for Upgrade to a Later Version | 2-30 |

Chapter 3: Uninstalling StellarProtect

Chapter 4: Using the Agent Console

| | |
|------------------------|-----|
| Overview | 4-2 |
| ICS Applications | 4-3 |

| | |
|--|------|
| ICS Certificates | 4-4 |
| Scan Components | 4-6 |
| Password | 4-6 |
| Industrial-Grade Next-Generation Antivirus | 4-7 |
| Device Control | 4-8 |
| OT Application Safeguard | 4-8 |
| Operations Behavior Anomaly Detection | 4-9 |
| DLL Injection Prevention | 4-9 |
| Settings..... | 4-10 |

Chapter 5: Using the Agent Command Line Interface (CLI)

| | |
|--|-----|
| Using OPCmd at the Command Line Interface (CLI)..... | 5-2 |
| Overview..... | 5-2 |
| List of All Commands | 5-4 |

Chapter 6: Events

| | |
|--|-----|
| Overview of StellarProtect Events..... | 6-2 |
| Agent Event List..... | 6-4 |

Chapter 7: Technical Support

| | |
|---|-----|
| Troubleshooting Resources | 7-2 |
| Using the Support Portal | 7-2 |
| Threat Encyclopedia | 7-2 |
| Contacting Trend Micro | 7-3 |
| Speeding Up the Support Call | 7-4 |
| Sending Suspicious Content to Trend Micro | 7-4 |
| Email Reputation Services | 7-4 |
| File Reputation Services | 7-5 |
| Web Reputation Services | 7-5 |
| Other Resources | 7-5 |
| Download Center | 7-5 |

Documentation Feedback 7-6

Index

Index IN-1

Preface

This Administrator's Guide introduces TXOne Networks StellarProtect and covers all aspects of product management.

Topics in this chapter include:

- *About the Documentation on page v*
- *Audience on page vi*
- *Document Conventions on page vi*

About the Documentation

TXOne Networks StellarProtect documentation includes the following:

Table 1. TXOne Networks StellarProtect Documentation

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

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

<http://docs.trendmicro.com>




Audience


TXOne Networks StellarProtect documentation is intended for administrators responsible for StellarProtect management, including agent installation.

Document Conventions

The following table provides the official terminology used throughout the TXOne Networks StellarProtect documentation:

Table 2. Document Conventions

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

| Convention | Description |
|---|--|
|  WARNING! | Critical actions and configuration options |

Chapter 1

Introduction

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

- *About TXOne Stellar and StellarProtect on page 1-2*
- *What's New on page 1-2*
- *Agent Features and Benefits on page 1-3*

About TXOne Stellar and StellarProtect

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

- 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 on-demand AV scan.
- StellarOne, the centralized management console designed to streamline administration of both StellarProtect for modernized systems and StellarProtect (Legacy Model) for legacy systems.

TXOne StellarProtect is an OT/ICS-compatible, high performance and zero touch endpoint protection solution.

What's New

TXOne StellarProtect 2.0 includes the following new features and enhancements.

Table 1-1. What's New in TXOne StellarProtect 2.0

| Feature | Description |
|--|---|
| Application Lockdown | This feature prevents malware attacks and increases protection level by locking down files defined in an Application List. |
| Real-Time Malware Scan in Maintenance Mode | Provides the graphical user interface for setting Maintenance Mode. In addition, A Real-Time Malware Scan toggle is added under the Maintenance Mode option, reminding users to enable scan function during maintenance period. |

Agent Features and Benefits

StellarProtect includes the following features and benefits.

| Feature | Benefit |
|--|--|
| Application Lockdown | Prevent malware attacks and increase protection level by locking down files added in an Application List and protecting the endpoint against unrecognized files. |
| Industrial-Grade Next-Generation Antivirus | OT/ICS root of trust and advanced threat scansecure OT assets with no interruption to operations |
| Operations Behavior Anomaly Detection | Detect abnormal operations and exercise least privilege-based control to prevent malware-free attacks |
| OT Application Safeguard | Intelligently locate and secure the integrity of the ICS process from ICS targeted attacks by device |
| Device Control | Prevent 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. |

Chapter 2

Installation

This chapter shows how to install the TXOne StellarProtect agent. The StellarProtect agent provides several installation types including **local installation** and **silent installation**.

Topics in this chapter include:

- *System Requirements on page 2-2*
- *Local Installation on page 2-5*
- *Silent Installation on page 2-21*
- *Encrypt installation configure on page 2-30*
- *Preparing the Agent for Upgrade to a Later Version on page 2-30*

System Requirements

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

System Requirements

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

Table 2-1. Required Software for StellarProtect

| Software | Description |
|----------------|------------------------------|
| .NET framework | Ver 3.5 SP1 or 4.0 available |

Table 2-2. Required Hardware for StellarProtect

| Hardware | Description |
|----------------------|------------------------------------|
| Available disk space | 350MB minimum 400MB recommended |
| Monitor resolution | 640 x 480 |

By default, StellarProtect uses port 14336, which is sometimes blocked by firewalls. Please make sure this port is kept open for StellarProtect's use.



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

**Important**

Ensure that the following root certification authority (CA) certificates are installed with intermediate CAs, which are found in StellarProtectSetup.exe and StellarProtect.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:

<https://technet.microsoft.com/en-us/library/cc754841.aspx>

Operating Systems

Windows Client:

- Windows 7 (NoSP/SP1) [Professional/Enterprise/Ultimate] (32/64bit)
- Windows 8 (NoSP) [Pro/Enterprise] (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/Sideloadable] (32/64bit)

Windows Server:

- Windows Server 2008 (SP1/SP2) [Standard/Enterprise/ Storage] (32/64bit)
- Windows Server 2008 R2 (SP1) (Standard/Enterprise/Storage] (64bit)
- Windows Server 2012 (No SP) (Essentials/Standard] (64bit)
- Windows Server 2012 R2 (No SP) (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)

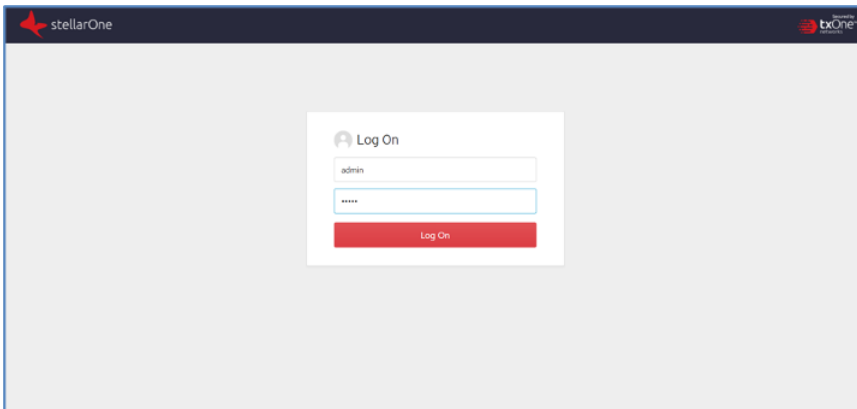
Local Installation

This section mainly explains the steps for installing StellarProtect, including downloading the installation file from StellarOne, running the installer, doing setup, and uninstalling StellarProtect.

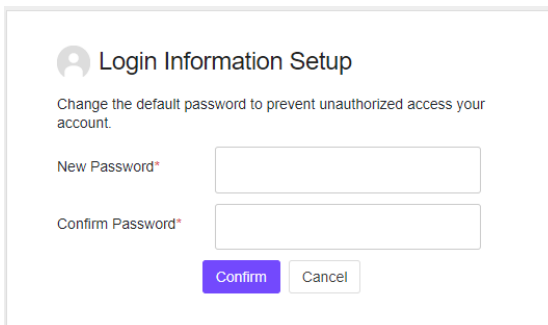
Getting the StellarProtect Agent Package

Procedure

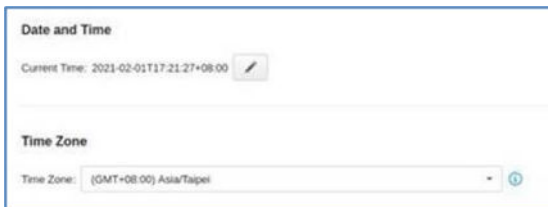
1. First log into StellarOne (default ID and password are admin/txone), the system will guide the user to change their ID and password to ensure account security.



2. Change the administrator password. StellarOne will check the quality of the new login name (ID), and will direct the user to input a strong password twice for confirmation.



3. After first password change on StellarOne, there will be a page for setting Date and Time.

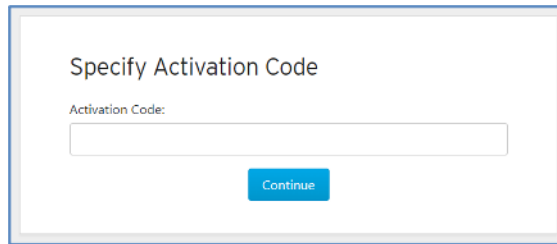


4. The system will ask the user to input an activation code (AC) for StellarOne service activation.



Note

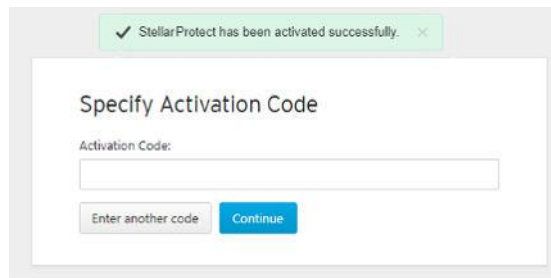
The AC can be provided by the TXOne product center or another authorized agency.



Specify Activation Code

Activation Code:

Continue



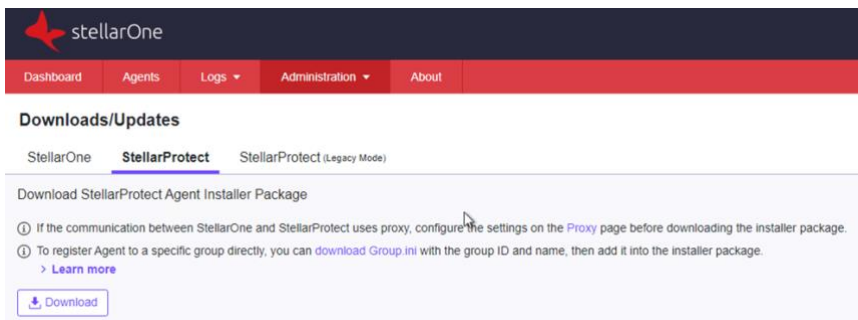
✓ StellarProtect has been activated successfully. ✕

Specify Activation Code

Activation Code:

Enter another code Continue

5. Download the install package from the StellarOne web console. The user can visit **Administration** > **Downloads/Updates** to download the StellarProtect installation package. The downloaded package is packed by StellarOne and can be installed by all agents.



stellarOne

Dashboard Agents Logs Administration About

Downloads/Updates

StellarOne **StellarProtect** StellarProtect (Legacy Mode)

Download StellarProtect Agent Installer Package

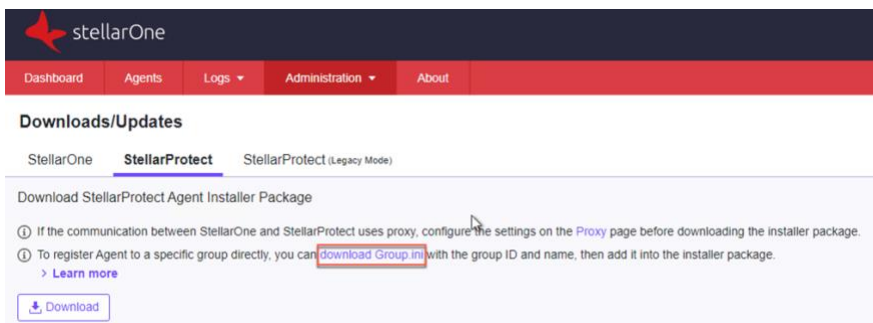
① If the communication between StellarOne and StellarProtect uses proxy, configure the settings on the [Proxy](#) page before downloading the installer package.

① 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.

[Learn more](#)

[Download](#)

6. (Optional) To register StellarProtect agent to a group, The user can visit **Administration > Downloads/Updates** to download `Group.ini` file.



7. (Optional) Select a group for the StellarProtect agent and click **Download**. A file named `Group.ini` is downloaded. Place the `Group.ini` file as the top-level file in the agent's installer package.

The screenshot shows a software installation interface. A central dialog box titled "Select a group" is open, displaying a list of group names with radio buttons. The "AMEA (0)" group is selected. Below the list, it says "1 selected" and there is a "Download" button. To the left, a sidebar contains sections for "Downloads/Updates" and "Patch", each with a "Download" or "Import" button. At the bottom left, a small file explorer snippet shows a file named "Group.ini" with a red border around it.

Dashboard Agent

Downloads/Updates

StellarOne Stellar

Download StellarProte

1 If the communication before downloading t

1 To register Agent to a into the installer pack

Download

Patch

Import

File Name

txone_sp_full_pat

txone_sp_full_pat

Group.ini

Select a group

Select a group and download Group.ini, then add it as the top-level file in the installer package.

Group Name

- All (22)
- AMEA (0)
- Asia (0)
- cccccc (0)
- Europe (0)
- HAWAII (2)
- hello (0)
- L1----- (3)
- Not_exist_agents (3)
- peter (2)
- tc (0)
- tmpr-test-asia (1)
- Z1-L1 (0)
- Z1-L2 (1)
- Z1-L3 (0)
- ZenShareViolate (2)

1 selected

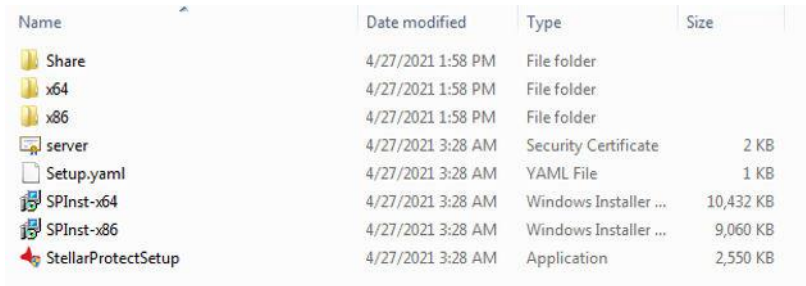
Download

Close

Installing the StellarProtect Agent

Procedure

1. Launch the installer, **StellarProtectSetup.exe**.



| Name | Date modified | Type | Size |
|---------------------|-------------------|-----------------------|-----------|
| Share | 4/27/2021 1:58 PM | File folder | |
| x64 | 4/27/2021 1:58 PM | File folder | |
| x86 | 4/27/2021 1:58 PM | File folder | |
| server | 4/27/2021 3:28 AM | Security Certificate | 2 KB |
| Setup.yaml | 4/27/2021 3:28 AM | YAML File | 1 KB |
| SPInst-x64 | 4/27/2021 3:28 AM | Windows Installer ... | 10,432 KB |
| SPInst-x86 | 4/27/2021 3:28 AM | Windows Installer ... | 9,060 KB |
| StellarProtectSetup | 4/27/2021 3:28 AM | Application | 2,550 KB |

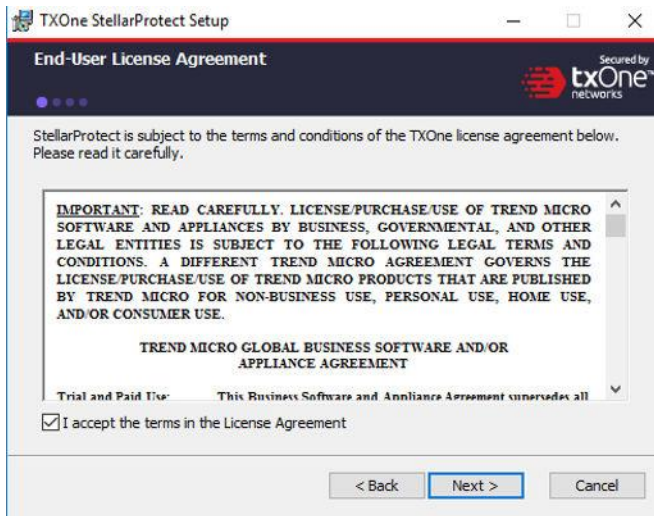
Note

1. To register StellarProtect agent to a specific group via StellarOne console, after downloading the `Group.ini` file to StellarOne console, user must place it in the Installer Package of StellarProtect agent.

-
2. To start the installation, please click **Next**.



3. The End-User License Agreement (EULA) will be shown. Please read the content, then click **I accept the terms of the license agreement** and **Next**.



4. Input your Product Activation Code and choose an administrator password. Please use a strong administrator password with good quality in 8 to 64 alphanumeric characters.

The screenshot shows the 'TXOne StellarProtect Setup' window. The title bar includes the application icon and the text 'TXOne StellarProtect Setup'. The window has a dark header with the text 'Product Activation Code & Administrator Password' and the 'txOne networks' logo. Below the header, there are three progress indicators. The main content area contains two sections: 'Product Activation Code' with an empty text box and a format instruction '(Format: XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX)'; and 'Administrator Password' with instructions 'The password must be 8 to 64 alphanumeric characters. The following characters are not supported: | > < \ ' * spaces.' and two empty text boxes labeled 'Password:' and 'Confirm Password:'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

5. Please input the asset information of the installed device with correct ICS-relative information such as vendor name, model, location and a description.

The screenshot shows the 'TXOne StellarProtect Setup' window. The title bar includes the application icon and the text 'TXOne StellarProtect Setup'. The window has a dark header with the text 'Asset Information' and the 'txOne networks' logo. Below the header, there are three progress indicators. The main content area contains four sections: 'Vendor' with a dropdown menu showing 'GE'; 'Model' with a text box containing 'PC Station'; 'Location' with a text box containing 'taipei'; and 'Description' with an empty text box. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

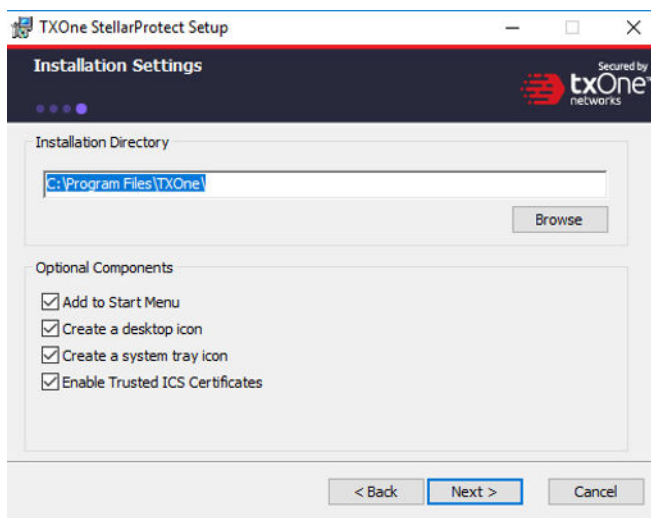
6. Confirm installation settings including installation directory and optional component settings.

**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**

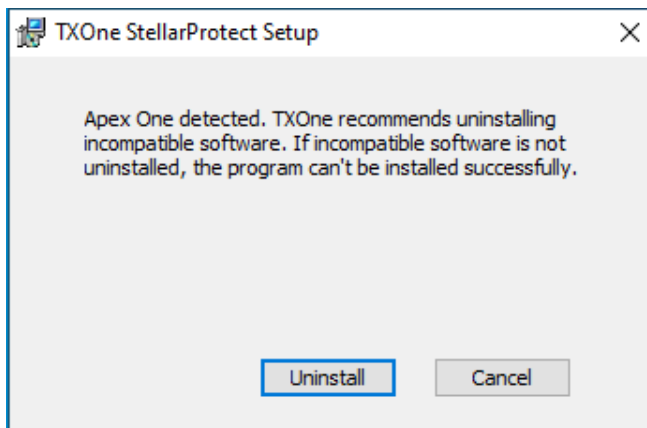
We suggest that users should also check **Enable Trusted ICS Certificates**. This feature ensures that StellarProtect can sync up trusted ICS certificates and enhance ICS applications, and that installers can always be recognized by StellarProtect.



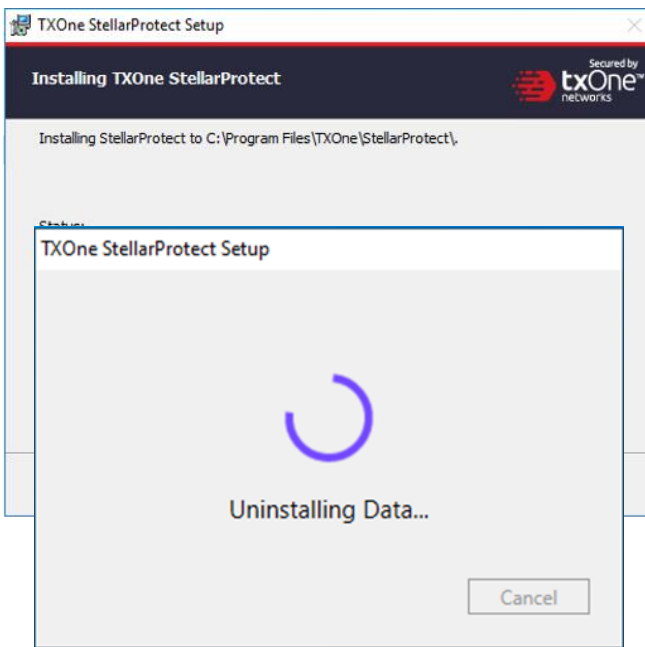
7. If StellarProtect detect the incompatible software on your system. It will display a message shown as below. If not, you will not see this message.
-

 **Note**

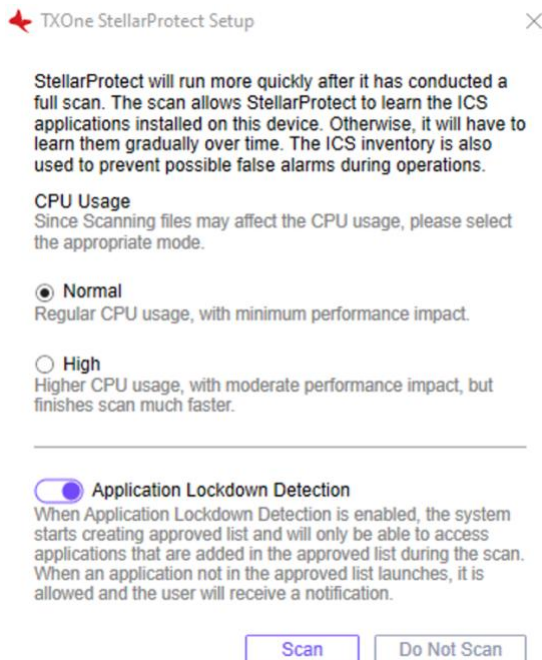
Incompatible software means some TrendMicro product: OfficeScan series, ApexOne, Worry-Free Business Security, Worry-Free Business Security Service. StellarProtect will try to uninstall them to avoid any possible incompatible issue.



8. During the installation, the installer will show the status with a progress bar.



9. Please click the **Scan** button to start the pre-scan task. Please note, this step is extremely important – please agree to allow StellarProtect to scan the ICS device to learn which ICS applications are installed.



Important

If you skip the pre-scan, StellarProtect will not be able to recognize the ICS application before it resumes production, and will need to learn them when as they are executed for the first time. In addition, this may cause delays in ICS applications, so we strongly recommend that you click **Scan** to allow StellarProtect learn about installed ICS applications in advance.

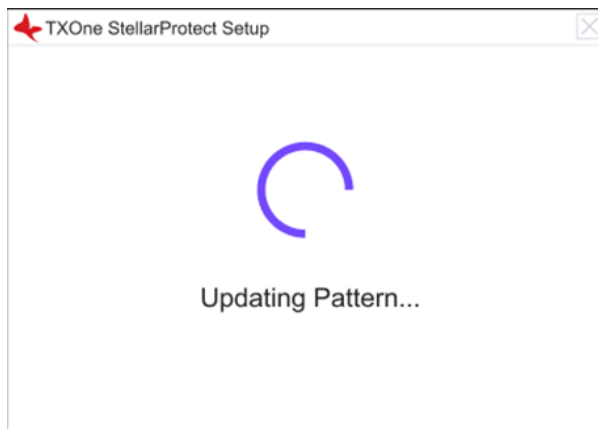
StellarProtect provided a more efficient option HIGH. Option HIGH significantly reduced scanning time but consumed more CPU resources. If no other vital applications are running on the system, you can select option HIGH to reduce scan time furthermore.

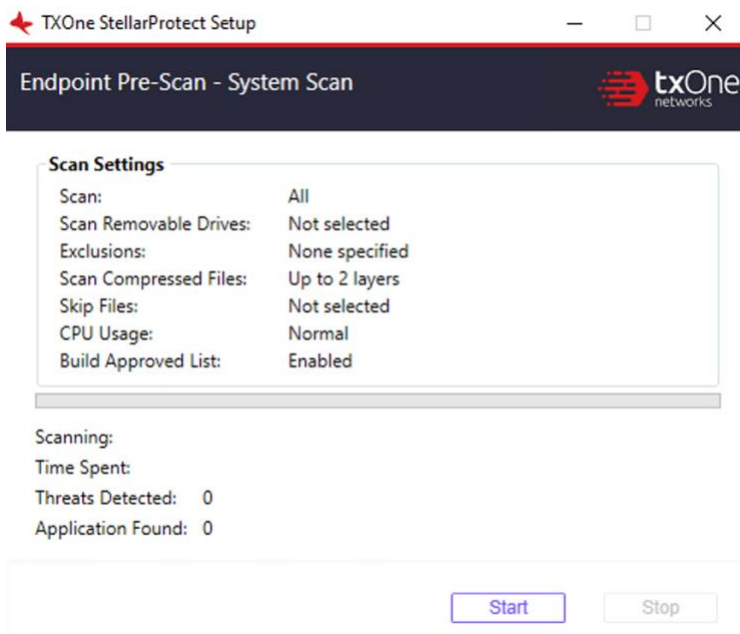
10. To detect potential pre-existing issues, users should run an Endpoint pre-scan. You can view the scan settings and click the Start button to launch the StellarProtect Endpoint pre-scan task.

 **Note**

Before the pre-scan starts, the installer will perform a component update based on the chosen configuration. For the standalone agent installer package, connecting to the Trend Micro Active Update server will be necessary to perform the update, so internet access is required.

The update process will display a message as shown below. Please note that there is no need for concern when you see this window.

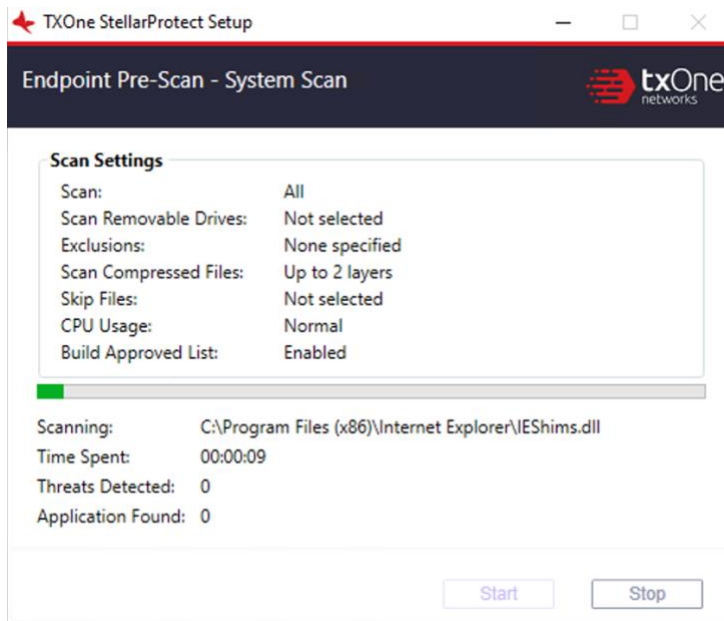




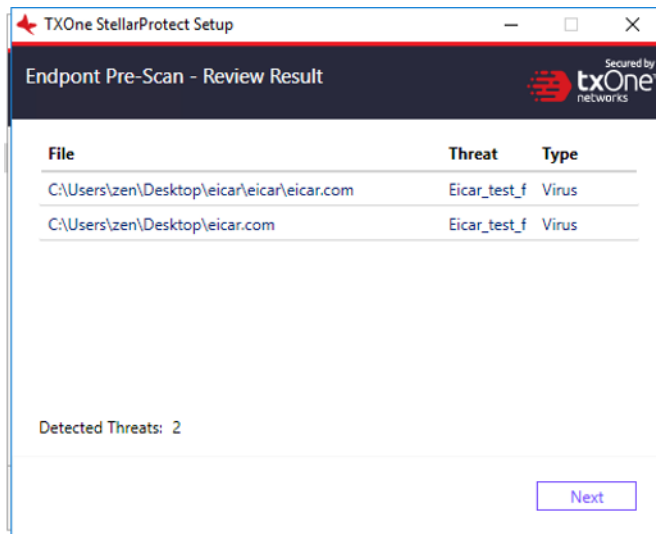
Scan settings are described as follows:

- **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

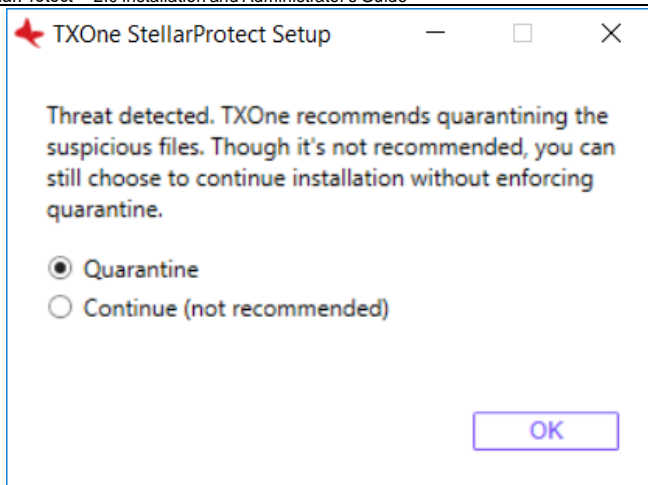
The progress bar shows the status of the prescan.



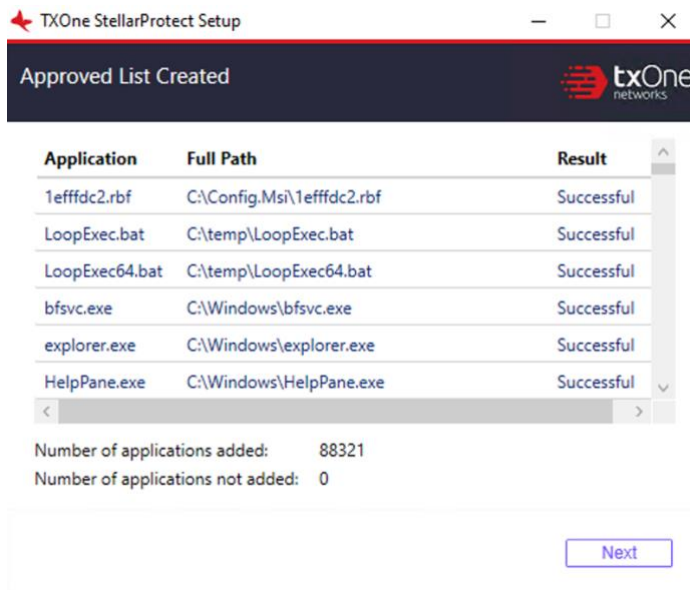
11. After the prescan, results will be shown for review.



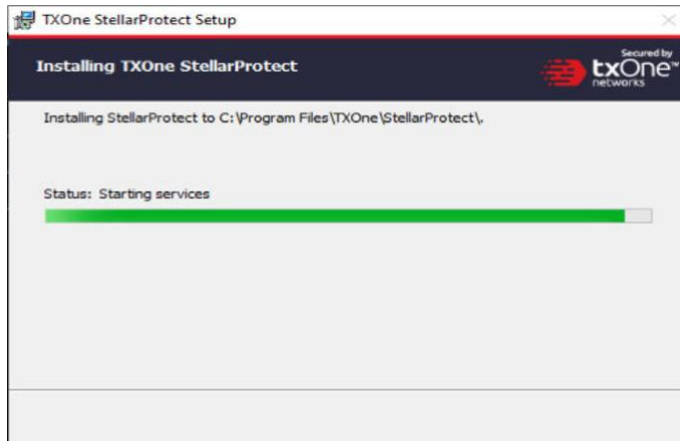
12. If a threat is detected, the user can choose from two options:
 - a. **Quarantine:** Quarantine the threat.
 - b. **Continue:** Take no action at this time.



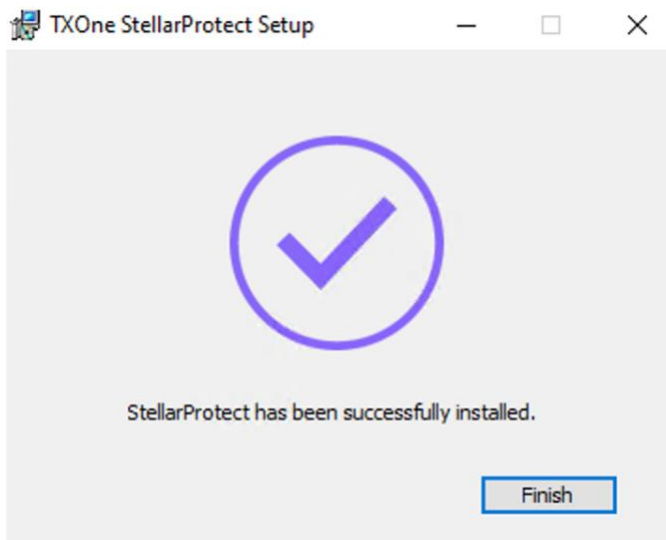
13. The results of adding applications in the Approved List will be shown for review.



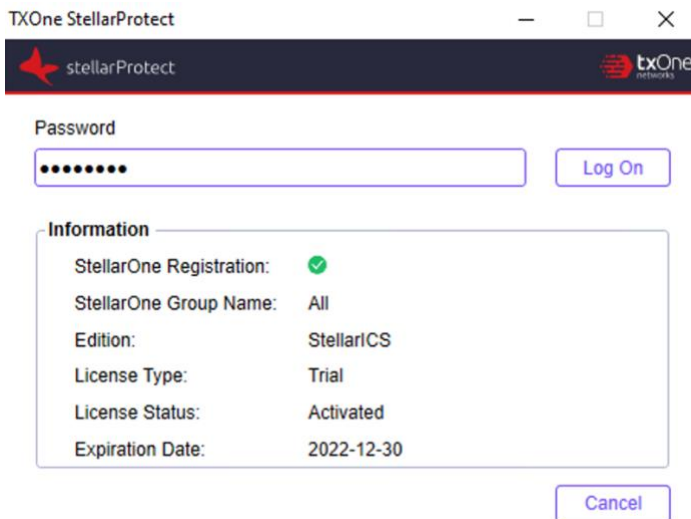
14. After the prescan and the creation of Approved List are complete, the StellarProtect application will be installed.



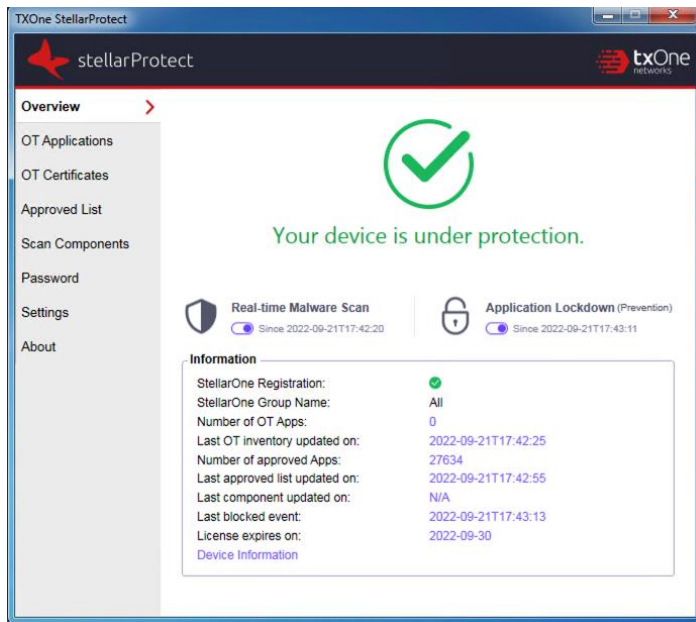
15. When the installation is complete, you will see the window below.



16. Run TXOne StellarProtect and log in with your password.



17. Upon logging into StellarProtect successfully, this window will display.



Silent Installation

StellarProtect provides silent installation based on a pre-defined configuration file. User can use the Configuration session to enable silent installation based on the `Setup.yaml`, then execute `StellarProtectSetup.exe` in silent mode.

Configuring Silent Installation

Users can pre-define the setup configuration for installation. The name is fixed to `Setup.yaml`.

The launcher will parse `Setup.yaml` while executing.

You can find `Setup.yaml` in the installation folder as shown below:

| | | | |
|---------------------|-------------------|-----------------------|-----------|
| Share | 2/26/2021 3:11 PM | File folder | |
| x64 | 2/26/2021 3:11 PM | File folder | |
| x86 | 2/26/2021 3:11 PM | File folder | |
| server | 2/24/2021 6:52 PM | Security Certificate | 2 KB |
| Setup.yaml | 3/2/2021 4:46 PM | Text Document | 0 KB |
| SPInst-x64 | 2/24/2021 7:16 PM | Windows Installer ... | 10,616 KB |
| SPInst-x86 | 2/24/2021 7:16 PM | Windows Installer ... | 9,208 KB |
| StellarProtectSetup | 2/24/2021 7:16 PM | Application | 1,013 KB |

- *Client:*
 - *import_source:* <IMPORT_SOURCE>
- *install:*
 - *activation_code:* <ACTIVATION_CODE>
 - *asset_description:* <ASSET_DESCRIPTION>
 - *asset_location:* <ASSET_LOCATION>
 - *asset_model:* <ASSET_MODEL>

- *asset_vendor*: <ASSERT_VENDOR>
- *enable_desktop_icon*: <ENABLE_DESKTOP_ICON>
- *enable_lockdown_al_building*: <ENABLE_LOCKDOWN_AL_BUILDING>
- *enable_lockdown_detection*: <ENABLE_LOCKDOWN_DETECTION>
- *enable_prescan*: <ENABLE_PRESCAN>
- *enable_silent_install*: <ENABLE_SILENT_INSTALL>
- *enable_start_menu*: <ENABLE_START_MENU>
- *enable_systray_icon*: <ENABLE_SYSTRAY_ICON>
- *enable_trusted_ics_cert*: <ENABLE_TRUSTED_ICS_CERT>
- *install_location*: <INSTALL_PATH>
- *password*: <PASSWORD>
- *prescan*:
 - *action*: <PRESCAN_ACTION>
 - *cpu_usage_mode*: <PRESCAN_CPU_MODE>
- *proxy*:
 - *default*:
 - *host*: <DEFAULT_PROXY_SERVER_HOST>
 - *password*: < DEFAULT_PROXY_SERVER_PASSWORD>
 - *port*: < DEFAULT_PROXY_SERVER_PORT>
 - *username*: < DEFAULT_PROXY_SERVER_USERNAME>
- *server*:

- *cert*: <SERVER_CERT>
- *host*: <SERVER_HOST>
- *listen*: <LISTEN_PORT>
- *port*: <SERVER_PORT>

 **Note**

Please refer to below table for details about a hidden parameter.

- *bypass_windefend_check*: <BYPASS_WINDEFEND_CHECK>
-

The following table lists parameters for `Setup.yaml` along with the details of their use:

| Parameter | Type | Default Value | Description |
|---------------------|---------|---------------|--|
| IMPORT_SOURCE | string | empty string | This is the path to the folder containing the config to be imported |
| ACTIVATION_CODE | string | empty string | The StellarProtect Activation Code (AC) used for license activation. |
| ASSET_DESCRIPTION | string | empty string | The ICS asset description. |
| ASSET_LOCATION | string | empty string | The physical location of the ICS asset. |
| ASSET_MODEL | string | empty string | The model name of the ICS asset. |
| ASSET_VENDOR | string | empty string | The vendor's name of the ICS asset. |
| ENABLE_DESKTOP_ICON | boolean | true | Enable StellarProtect icon to |

| | | | |
|----------------------------------|---------|--|---|
| | | | be placed on the desktop. |
| ENABLE_LOCKDOWN_ALLOWED_BUILDING | boolean | true | Enable the building of Approved List for Application Lockdown. |
| ENABLE_LOCKDOWN_DETECTION | boolean | true | Enable the detect mode of Application Lockdown. |
| ENABLE_PRESCAN | boolean | true | Enable virus scan during installation. |
| ENABLE_SILENT_INSTALL | boolean | false | Hide the installation UI. ACTIVATION_CODE and PASSWORD must be given during silent installation. |
| ENABLE_START_MENU | boolean | true | Enable StellarProtect in the Windows start menu. |
| ENABLE_SYSTRAY_ICON | boolean | true | Enable StellarProtect icon in the Windows system tray. |
| ENABLE_TRUSTED_ICSCERT | boolean | true | Allow the installer to install ICS code signing certificates during installation. |
| INSTALL_PATH | string | empty string → default install path C:\Program Files\TXOne (default install path is decided in MSI installer) | The installation path of the StellarProtect installer. |

| | | | |
|-------------------------------|--------|--------------|---|
| PASSWORD | string | empty string | Administrator's password. The Password will be required by specific functions, including uninstall, the command line interface, and support tools. |
| PRESCAN_ACTION | int | 1 | 0: None 1: Quarantine |
| PRESCAN_CPU_MODE | int | 0 | 0: NORMAL (Single thread scan) 1: HIGH (Multi thread scan) |
| DEFAULT_PROXY_SERVER_HOST | string | empty string | FQDN, hostname or IP address of Intranet proxy server |
| DEFAULT_PROXY_SERVER_PASSWORD | string | empty string | Password of Intranet proxy server, required only when the proxy server is configured to authenticate by username and password |
| DEFAULT_PROXY_SERVER_PORT | int | -1 | Port number of Intranet proxy server |
| DEFAULT_PROXY_SERVER_USERNAME | string | empty string | Username of Intranet proxy server, required only when the proxy server is configured to authenticate by username and password |
| SERVER_CERT | string | server.crt | The certificate filename for communicating with StellarOne |
| SERVER_HOST | string | empty string | StellarOne hostname or IP |
| LISTEN_PORT | int | 14336 | The client listening port for StellarOne |

| | | | |
|------------------------|---------|-------|--|
| SERVER_PORT | int | 9443 | StellarOne's port for connecting to the client |
| BYPASS_WINDEFEND_CHECK | boolean | false | Bypass checking Windows Defender status. |

**Note**

1. When `ENABLE_PRESCAN` is set to `false`, `ENABLE_LOCKDOWN_AL_BUILDING` and `ENABLE_LOCKDOWN_DETECTION` will be automatically set to `false`.
2. `BYPASS_WINDEFEND_CHECK` is a hidden parameter in `setup.yaml`, designed for Windows 7 and Windows Server 2016+ platforms, on which the installation of StellarProtect requires disabling Windows Defender. When the parameter's value is set `true`, the endpoint will bypass Windows Defender check to get the StellarProtect installed without disabling Windows Defender. Please refer to below section for how to use it.

Silent Installation of the StellarProtect Agent

Procedure

1. Please input the activation code and password, then enable silent installation by changing the *enable_silent_install* value to *true* 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.

Please refer to the text below for an example silent installation configuration file:

```
client:
  import_source: C:\txsp_config
install:
  activation_code: TE-XXXXX-SAMPL-EXXXX-CODES-XXXXX-TXONESP
  asset_description: This is a machine
  asset_location: Factory1 North Area
  asset_model: ABB-1X2Y
  asset_vendor: ABB
  enable_desktop_icon: true
  enable_lockdown_al_building: true
  enable_lockdown_detection: true
  enable_prescan: true
  enable_silent_install: true
  enable_start_menu: true
  enable_systray_icon: true
  enable_trusted_ics_cert: true
  install_location: C:\test
  password: 11111111
prescan:
  action: 1
  cpu_usage_mode: 0
proxy:
  default:
    host:
    password:
```



```

port:
username:
server:
cert: server.crt
host: 10.1.195.100
listen: 14336
port: 9443

```

**Note**

(Optional) Insert a line under install section, type:

```
bypass_windefend_check: true
```

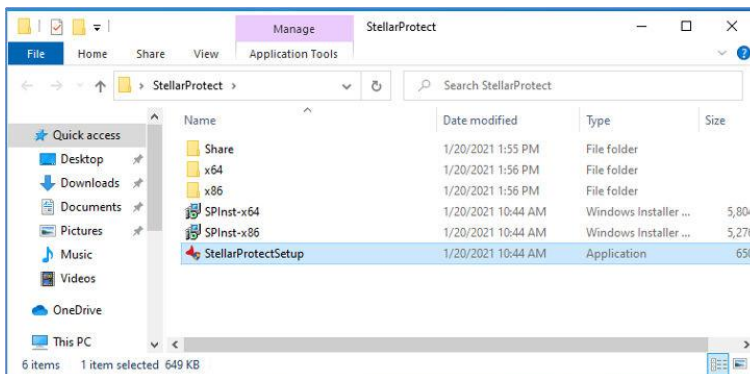
The endpoint will bypass checking Windows Defender status to get the StellarProtect installed without disabling Windows Defender.

2. Double-click the installer, StellarProtectSetup.exe.
-

**Note**

Please note that there are two methods for beginning the silent installation.

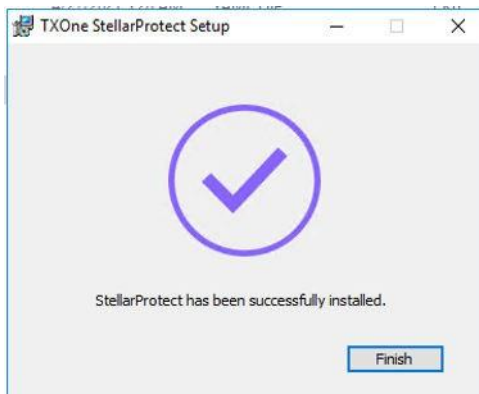
- For a silent installation with a GUI, double-click the installer StellarProtectSetup.exe.



- For a silent installation without any GUI, instead of double-clicking the executable in step 2, instead use the command prompt to execute `StellarProtectSetup.exe` with the argument `-s`. Please note that with this method, pop-up windows mentioned in the following steps will not be shown. To view information related to the installation, check logs filed under `C:\Windows\Temp\StellarProtect`.

```
C:\package>StellarProtectSetup.exe -s
```

3. After the installation is complete, this message box will appear.



4. Run StellarProtect and log in with the configured password.

5. After successfully logging into StellarProtect, the **Overview** window will be displayed.

Encrypting Configuration for Installation (Setup.yaml)

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

Procedure

1. Prepare your `Setup.yaml` as mentioned in *Silent Installation on page 2-21*.
 2. Encrypt `Setup.yaml` by using the command prompt: `StellarProtectSetup.exe -e <CONFIG_FILE>`. The parameter `-e` is used for encrypting the configuration file and generating `Setup.bin` file in the working directory.
 3. After the `Setup.bin` file is generated, place it in the installer package.
 4. The installation with encrypted configuration can now be executed.
-

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

The latest updates can be downloaded from the StellarProtect Software Download Center at <http://downloadcenter.trendmicro.com/>.



Important

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

Table 2-3. 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 | Manually uninstall | No settings retained |
| Local installation using command line interface installer | StellarProtect 1.0/1.1/1.2/1.2 Patch 1 | Manually uninstall | No settings retained |

Table 2-4. 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 | No preparation needed | Compatible settings retained |
| Remote Installation | StellarProtect 1.1/1.2/1.2 Patch 1 Note: StellarProtect 1.0 supports only local installation. | StellarOne 2.0 console or above | Compatible settings retained |

Chapter 3

Uninstalling 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

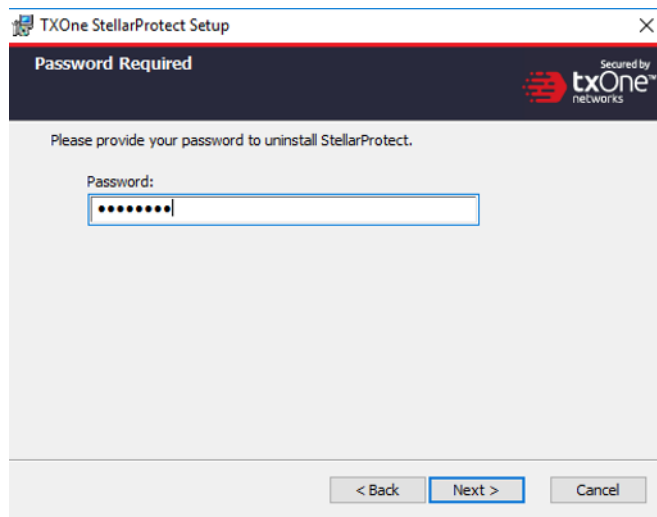
1. On an endpoint with the StellarProtect agent installed, launch StellarProtect Setup.
2. Follow the steps listed here according to your operating system:

| Operating System | Procedure |
|--|---|
| <ul style="list-style-type: none">• Windows 10 Enterprise• Windows 10 IoT Enterprise• Windows 10 Professional• Windows 10 Fall Creators Update (Redstone 3)• Windows 10 April 2018 Update (Redstone 4)• Windows 10 October 2018 Update (Redstone 5)• Windows 11 Professional | <ol style="list-style-type: none">a. Go to Start > Settings.b. Depending on your version of Windows 10, locate the Apps & Features section under one of the following categories:<ul style="list-style-type: none">• System• Appsc. On the left pane, click Apps & Features.d. In the list, click StellarProtect.e. Click Uninstall. |
| <ul style="list-style-type: none">• Windows Server 2022• Windows Server 2016• Windows Server 2012• Windows Storage Server 2016• Windows 8• Windows 7 | <ol style="list-style-type: none">a. Go to Start > Control Panel > Programs and Features.b. In the list, double-click TXOne StellarProtect. |

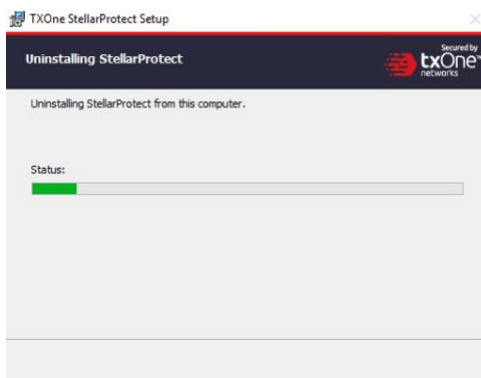
3. After the StellarProtect Setup opens, click **Next**.



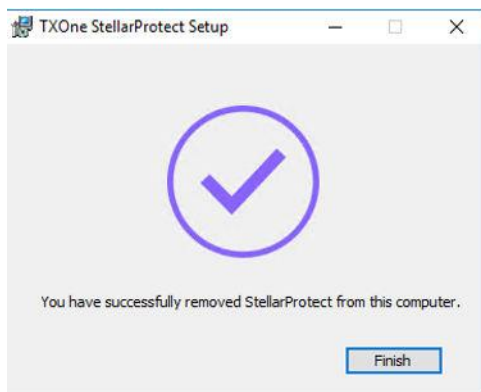
4. Enter in the StellarProtect administrator password, and click **Next**.



5. Make sure StellarProtect's UI is completely closed before you click **OK**.



6. After the software is finished uninstalling, click **Finish**.



Important

For Windows 7 and Windows Server 2016+ platforms, the installation of StellarProtect requires disabling Windows Defender first. After uninstalling StellarProtect, it is suggested to manually enable Windows Defender for security reasons.

Chapter 4

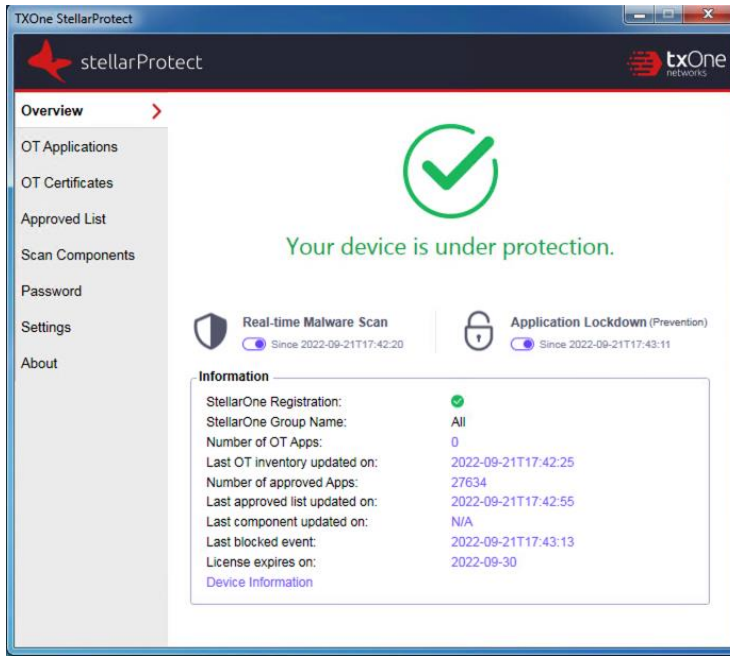
Using the Agent Console

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

Topics in this chapter include:

- *Overview on page 4-2*
- *Settings on page 4-10*

Overview



Overview is a description of the current status of the StellarProtect system. The green check indicates the endpoint is under the protection of Real-time Malware Scan and/or Application Lockdown, while the red cross indicates the endpoint is at risk.

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 function is enabled.

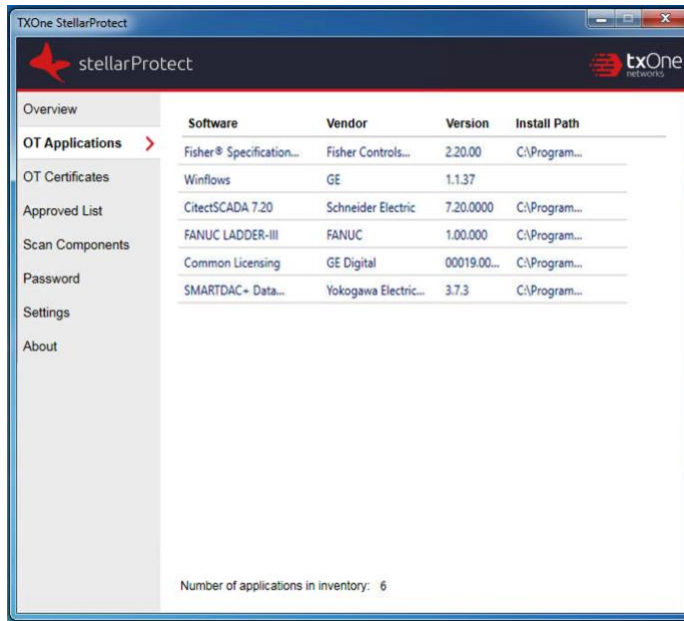
For StellarProtect agent with StellarKiosk license edition, below the green check or red cross icon, a shield-shape icon with the toggle indicates whether the endpoint is currently protected by StellarProtect's Real-time Malware Scan.

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 function 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 console; red cross indicates registration to certain group is failed.
- **StellarOne group name:** shows the group name to which 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:** How many OT applications are in the endpoint
- **Last OT inventory updated on:** The date and time the OT Inventory was last updated on this endpoint
- **Number of approved Apps:** 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:** 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



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... |

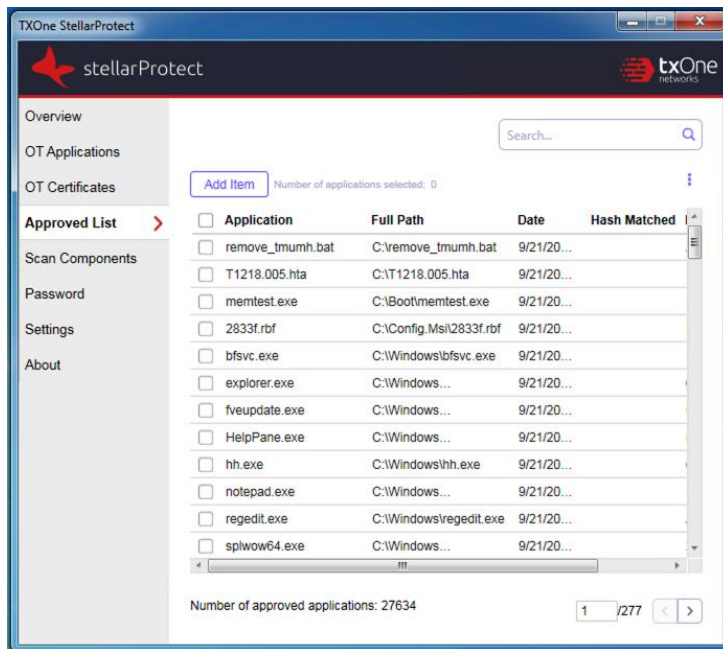
Number of certifications: 5

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 increase with updates from the OT/ICS Application Inventory. This inventory is produced by the TXOne research laboratory and based on OT/ICS product analysis.

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

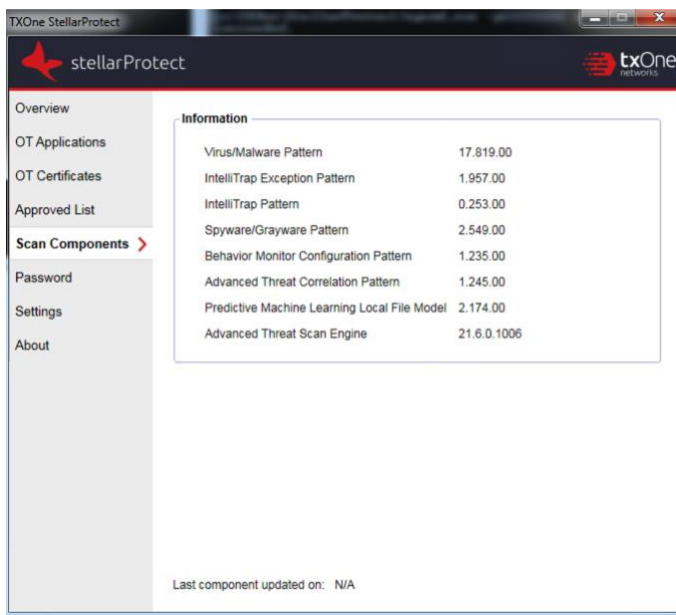
Approved List



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

List all critical scan engines and patterns with versions used by StellarProtect.



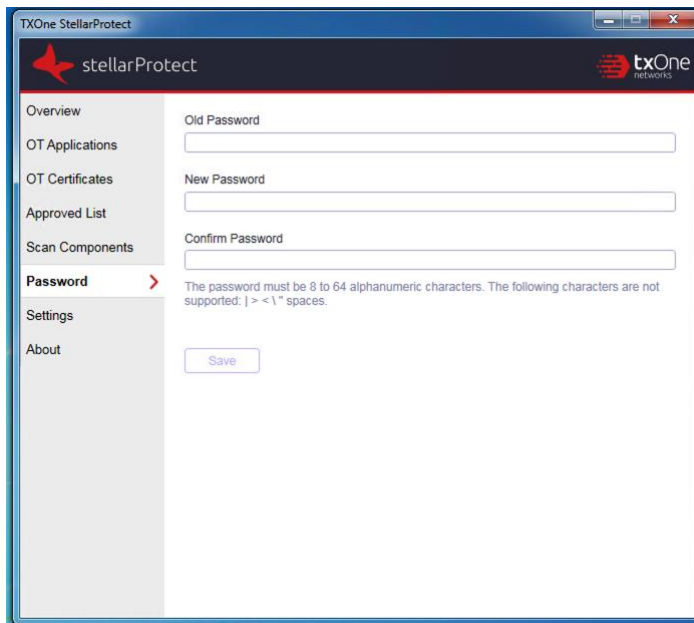
The screenshot displays the TXOne StellarProtect Agent Console interface. The left sidebar contains navigation options: Overview, OT Applications, OT Certificates, Approved List, Scan Components (highlighted with a red arrow), Password, Settings, and About. The main content area shows the 'Information' section for Scan Components, listing various patterns and engines with their respective versions.

| Component | Version |
|--|-------------|
| 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

Password

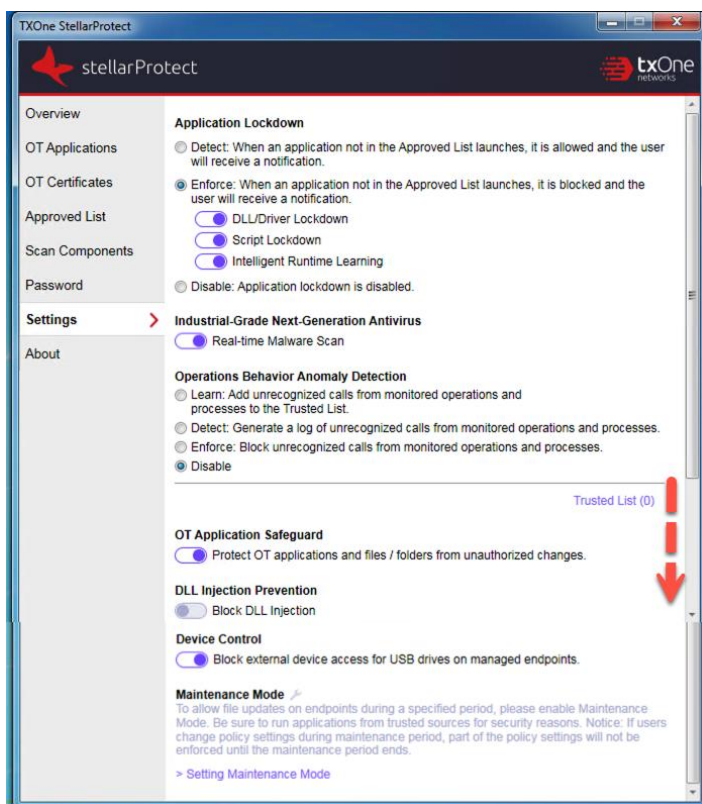
This is the StellarProtect administrator password change function. The user must enter the correct old password, then enter the same new password twice, confirm that the length of the new password meets the requirements, and press **Save** to complete the change.



The screenshot shows a web browser window titled "TXOne StellarProtect". The interface has a dark header with the "stellarProtect" logo on the left and the "txOne networks" logo on the right. A left-hand navigation menu lists several options: Overview, OT Applications, OT Certificates, Approved List, Scan Components, **Password** (which is highlighted with a red arrow), Settings, and About. The main content area is titled "Old Password" and contains three text input fields labeled "Old Password", "New Password", and "Confirm Password". Below these fields is a text-based instruction: "The password must be 8 to 64 alphanumeric characters. The following characters are not supported: | > < \ " spaces." At the bottom of the form is a "Save" button.

Settings

This section mainly describes the StellarProtect settings. Description of the seven main protection functions will be provided later. Each function has a switch that can be turned on or off.



Application Lockdown

This feature prevents malware attacks and increases protection level by locking down files defined in an Application List. 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 enable the **Detect** or **Enforce** function, three more protection options are available:

1. **DLL/Driver Lockdown:** DLL/Driver Lockdown prevents unapproved DLLs or drivers from being loaded into the memory of protected endpoints.
2. **Script Lockdown:** Script Lockdown prevents unapproved script files from being run on protected endpoints.
3. **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 mode can also be disabled in case users may have the needs, but it is recommended 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. We integrate 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 on the StellarOne web console.

This function has four modes, including:

- **Learn Mode**

After activating this function, StellarProtect will monitor unrecognized program calls and add them to the trusted list to learn more about OT/ICS-related program call behaviors.

- **Detect Mode**

After activating this function, StellarProtect will monitor unrecognized program calls and log them for future analysis.

- **Enforce Mode**

After activating this function, StellarProtect will monitor unrecognized program calls and block them to secure the endpoint.

- **Disable Mode**

When Operations Behavior Anomaly Detection is set to Disable, 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 applicationsystem 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 user on StellarOne 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.



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 has a one-time allow function to approve USB storage access after administrator authentication. When an unauthorized USB storage device is inserted into the endpoint for 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. Windows will show a pop-up requiring users to enter the administrator password.
4. The USB device can be allowed access until unplugged.



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.

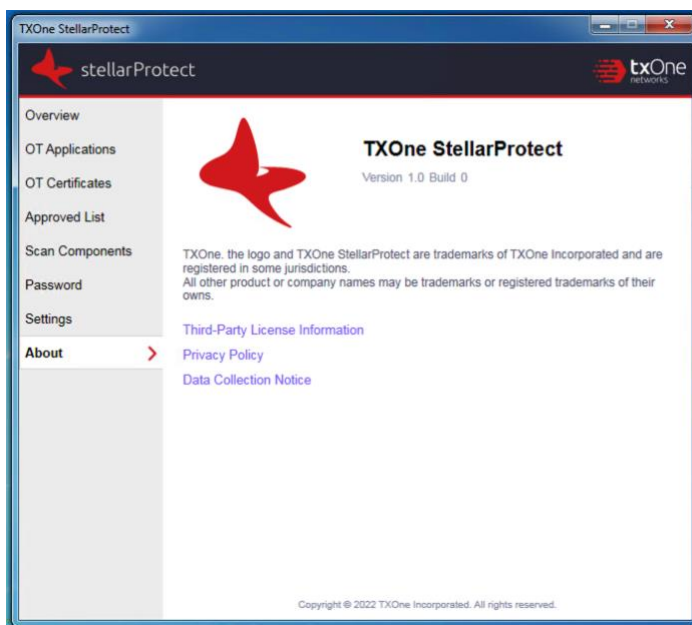


Note

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.

About

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



Proxy

StellarProtect use a proxy for both communication with StellarOne and scan component updates.

It is configurable using `Setup.yaml` before installation and the command line interface afterwards.

- For more information about configuring the proxy before installation using `Setup.yaml`, please see [Configuring Silent Installation on page 2-25](#).
- For more information about configuring the proxy after configuration via the command line interface, please see [List of All Commands on page 5-4](#).

Chapter 5

Using the Agent Command Line Interface (CLI)

This 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) on page 5-2*
- *List of All Commands on page 5-4*

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**.
-

Overview

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

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

Separate long option and argument with an equal sign.

```
-o<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.



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 accidentally, use `-p` without argument to avoid the shell (`cmd.exe`) from recording your password in the command history.

Argument: Optional. Password in plaintext.

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

Description: Show CLI program version.

Argument: No

List of All Commands

| Command | Description | Options |
|---|---|---------|
| <code>opcnd.exe about components</code> | You can browse versions of components from the GUI program, or you can get the list in YAML format with this command. | None |
| <code>opcnd.exe -p appinv make</code> | 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 |
| <code>opcnd.exe appinv list</code> | You can browse the list of detected OT/ICS applications from the GUI program or use this command to get the list in YAML format. | None |

| Command | Description | Options |
|---|---|---|
| opcnd.exe -p config decrypt [-i INPUT- FILE] [-o OUTPUT-FILE] | Decrypt an encrypted configuration file, output decrypted plaintext. Please note that 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: Required argument. Specifies the filename of an input file. If omitted, will read from standard input. -o, --output OUTPUT - FILE: Required argument. Specifies filename of output file. If omitted, write to standard output. |
| opcnd.exe -p config encrypt [-i INPUT- FILE] [-o OUTPUT-FILE] | Encrypt a plaintext configuration file, output encrypted ciphertext. Please note 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: Required argument. Specifies the filename of input file. If filename is omitted, will read from standard input. -o, --output OUTPUT- FILE: Required argument. Specifies filename of output file. If omitted, will write to standard output. |
| opcnd.exe -p config export OUTPUT-FOLDER | Exports product configuration settings to the specified folder. | None |
| opcnd.exe -p config import INPUT-FOLDER | Imports product configuration settings from the specified folder. | -n, --no_ptn Do not import pattern files |
| opcnd.exe -p dip disable | Disables the DLL Injection Prevention function. | None |
| opcnd.exe -p dip enable | Enables the DLL Injection Prevention function. | None |
| opcnd.exe -p lock appinv disable | Disables OT/ICS Application Inventory protection. | None |

| Command | Description | Options |
|---|---|---|
| opcnd.exe -p lock appinv enable | Enables OT/ICS Application Inventory protection. | None |
| opcnd.exe -p lock disable [-d DURATION] [-s START-TIME] | <p>Disables the Change Control module to allow file changes on protected files. You can also specify a duration and start-time to schedule a maintenance mode that allows file changes and enable protection automatically.</p> <p>If -d is not specified, the Change Control module is disabled until it is enabled.</p> <p>If -s is not specified, the Change Control module is disabled immediately. Only one maintenance mode can be scheduled at a time, and new settings from the CLI or policy settings will always overwrite previous settings.</p> | <p>-d, --duration DURATION: Required argument. Specifies the duration of maintenance mode. The Change Control module is restored to its current setting after the duration has elapsed. A duration can be specified in hours, minutes, or both. (ex. -d 30m, -d 2h, -d 2h30m) The letter 'm' can be omitted when specifies a duration only in minutes.</p> <p>-s, --start START-TIME: Required argument. Specifies starting time of maintenance mode. The START-TIME is in ISO8601 format without time zone. (ex. -s 2021-04-14T18:00:00)</p> |
| opcnd.exe -p lockdown approvedlist info | Shows Application Lockdown Approved List information. | None |
| opcnd.exe -p lockdown approvedlist init [-- overwrite] | Initialize Application Lockdown Approved List. | <p>-o, --overwrite: Overwrite the existing Application Lockdown Approved List.</p> <p>If -o is not specified, detected applications will be appended to the existing Application Lockdown Approved List.</p> |

| | | |
|---|---|---|
| <code>opcmd.exe -p lockdown approvedlist add -p PATH [--recursive]</code> | Add the specified file to the Application Lockdown Approved List. | -p, --path PATH: Add the specified file to the Application Lockdown Approved List. -r, --recursive: Includes the specified folder and related subfolders. |
| <code>opcmd.exe -p lockdown enable -m MODE</code> | Enables Application Lockdown. | -m, --mode MODE: Specifies enable mode (detect, enforce). |
| <code>opcmd.exe -p lockdown disable</code> | Disables Application Lockdown. | None |
| <code>opcmd.exe -p lockdown exceptionpath -t TYPE -p PATH (--add --remove)</code> | Add or remove an Application Lockdown exception path. | -t, --type TYPE: Specifies type of exception path (file, folder, folder_and_subfolder, ecmaascript_regexp). -p, --path PATH: Specifies exception path or regexp. |
| <code>opcmd.exe -p lockdown info</code> | Shows Application Lockdown information. | None |
| <code>opcmd.exe -p lockdown script info</code> | Display all Application Lockdown script rules. | None |
| <code>opcmd.exe -p lockdown script add -e EXTENSION -p INTERPRETER [-p INTERPRETER2] ...</code> | Add the specified script extension and the interpreter required to execute the script. | -e, --ext EXTENSION: Specifies script extension. -p, --proc INTERPRETER: Specifies name of script interpreter. |
| <code>opcmd.exe -p lockdown script remove -e EXTENSION [-p INTERPRETER] ...</code> | Remove the specified script extension and the interpreter required to execute the script. | -e, --ext EXTENSION: Specifies script extension. -p, --proc INTERPRETER: Specifies name of script interpreter. |
| <code>opcmd.exe -p lockdown subfeature -f SUB-FEATURE (--enable --disable)</code> | Toggle sub-feature of Application Lockdown. | -f, --feature SUB-FEATURE: Specifies sub-feature (dll_driver, script, intelligent_runtime_learning) |

| | | |
|--|---|--|
| opcmd.exe -p lockdown trustedhash -h HASH (--add --remove) | Add or remove an Application Lockdown trusted hash. | -h, --hash HASH: Specifies trusted hash, 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 ends the maintenance mode immediately. | None |
| opcmd.exe -p maintenance start | Start or schedule maintenance mode. You can specify a duration and start-time to schedule maintenance mode that allows file changes and restore 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 when specifies a duration only in minutes. -s, --start START-TIME: Specifies starting time of maintenance mode. The START-TIME is in ISO8601 format without time zone (for example, -s 2021-04-14T18:00:00). -r, --activate-rts ACTIVATE-REALTIME-SCAN: Enable real-time scan during maintenance mode. |
| opcmd.exe -p maintenance stop | Stop running maintenance mode or cancel 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 |
|--|--|--|
| opcmod.exe -p oad enable -m MODE [-l LEVEL] | Enables Operations Behavior Anomaly Detection. | -m, --mode MODE: Required argument. Enables Operations Behavior Anomaly Detection into a specific mode (learn, detect, enforce). -l, --level LEVEL Required argument. Sets the scan to be normal or aggressive. |
| opcmod.exe -p oad info | Shows information about Operations Behavior Anomaly Detection. | None |
| opcmod.exe -p oad remove -i ID | Removes approved operations from Operations Behavior Anomaly Detection. | -i, --id ID: Required argument. Integer operation ID. |
| opcmod.exe password | Allows administrator to change the administrator password from command line. You are required to enter the old password before setting a new password. | None |
| opcmod.exe -p proxy get | Shows proxy server settings. | None |

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

| Command | Description | Options |
|--|--|---|
| <code>opcnd.exe -p service start</code> | After installation, the StellarProtect service will automatically start when your system is powered on. If your StellarProtect service was stopped for some reason, you can use this command to start the StellarProtect service manually. | None |
| <code>opcnd.exe -p service stop</code> | 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 |
| <code>opcnd.exe update [-s SOURCE]</code> | Updates product components. | <code>-s, --source</code> : Required argument. URL Specifies the update source URL, ex: <code>-s http://tmut.contoso.com / iau_server</code> |
| <code>opcnd.exe -p update stop</code> | Stops the currently running update. | None |
| <code>opcnd.exe -p usb add [-v VID -p PID -s SN] [-o]</code> | Adds a trusted USB device. | <p><code>-v, --vid VID</code>: Required argument. Specifies Vendor ID by hexadecimal string.</p> <p><code>-p, --pid PID</code>: Required argument. Specifies Product ID by hexadecimal string.</p> <p><code>-s --sn SN</code>: Required argument. Specifies serial number.</p> <p><code>-o, --onetime</code>: Grants one-time access to a USB device.</p> |

| Command | Description | Options |
|--|--|--|
| <code>opcnd.exe -p usb enable</code> | Enables USB Vector Control. | None |
| <code>opcnd.exe -p usb disable</code> | Disables USB Vector Control. | None |
| <code>opcnd.exe -p usb info -d DRIVE</code> | Show USB information of the specified drive. | -d, --drive DRIVE: Required argument. Specifies the drive path (ex. E:). |
| <code>opcnd.exe -p usb list</code> | Lists trusted USB devices. | None |
| <code>opcnd.exe -p usb remove [-v VID -p PID -s SN]</code> | Removes a trusted USB device. | -v, --vid VID: Required argument. Specifies Vendor ID by hexadecimal string. -p, --pid PID: Required argument. Specifies Product ID by hexadecimal string. -s --sn SN: Required argument. Specifies serial number. |
| <code>opcnd.exe -p usb status</code> | Shows USB Vector Control status. | None |
| <code>opcnd.exe -p quarantine show</code> | Shows the list of quarantined files. | None |
| <code>opcnd.exe -p quarantine restore [QUARANTINE-NAME]</code> | Restores the specified quarantined file. | None |
| <code>opcnd.exe -p udso list</code> | List user-defined suspicious objects. | -a, --all: List all types of suspicious objects. -p, --file-path: List file path suspicious objects. -h, --file-sha1: List file SHA1 suspicious objects. -H, --file-sha2: List file SHA2 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. |
| opcmd.exe -p update-task | Schedules a recurring update at specified time. | <p>--time, START-TIME: Specifies starting time (HH:MM) of scheduled update.</p> <p>--daily: Specifies the scheduled update to run daily.</p> <p>--weekly DAY-OF-WEEK: Specifies the scheduled update to run weekly on given day of week. Only Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday are valid.</p> <p>--monthly DAY-OF-MONTH: Specifies the scheduled update to run monthly on given day of month (1-31). Specifies -1 to run on the last day of month.</p> <p>--remove: Remove the scheduled update</p> |

Chapter 6

Events

This chapter describes events as they will be recorded within the TXOne StellarProtect Agent.

Topics in this chapter include:

- *Overview of StellarProtect Events on page 6-2*
- *Agent Event Log Descriptions on page 6-2*
- *Agent Event List on page 6-4*

Overview of StellarProtect Events

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 turn on or off.

Agent Event Log Descriptions

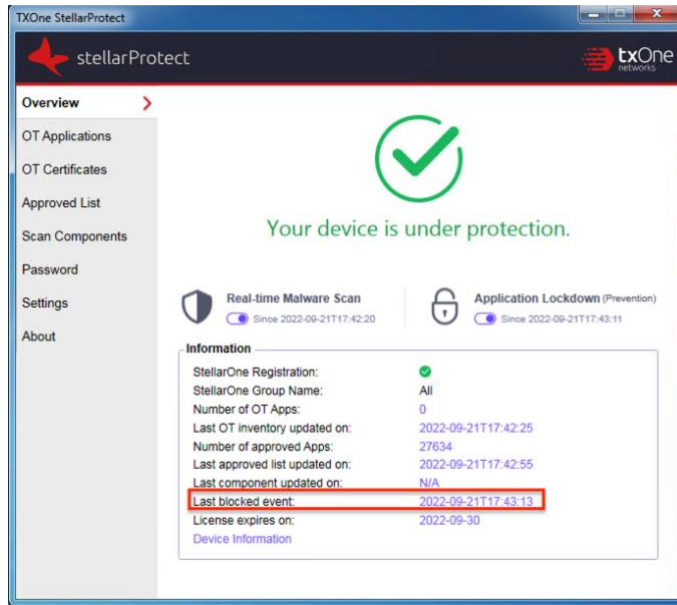
TXOne StellarProtect leverages the Windows™ Event Viewer to display the **ALL** StellarProtect event log. Access the Event Viewer at **Start > Control Panel > Administrative Tools**.

The screenshot shows the Windows Event Viewer window. The left pane displays the event log hierarchy, with 'StellarProtect' selected under 'Applications and Services Logs'. The main pane shows a table of StellarProtect events with the following data:

| Level | Date and Time | Source | Event ID | Task Ca... |
|-------------|-----------------------|----------------|----------|------------|
| Information | 3/28/2022 3:00:07 PM | StellarProtect | 257 | None |
| Warning | 3/28/2022 2:49:23 PM | StellarProtect | 4864 | None |
| Information | 3/28/2022 2:48:56 PM | StellarProtect | 768 | None |
| Information | 3/28/2022 2:47:35 PM | StellarProtect | 768 | None |
| Information | 3/28/2022 2:46:59 PM | StellarProtect | 768 | None |
| Information | 3/28/2022 2:46:48 PM | StellarProtect | 768 | None |
| Information | 3/28/2022 2:45:31 PM | StellarProtect | 768 | None |
| Information | 3/28/2022 2:19:59 PM | StellarProtect | 257 | None |
| Warning | 3/28/2022 2:19:59 PM | StellarProtect | 4864 | None |
| Information | 3/28/2022 2:18:00 PM | StellarProtect | 768 | None |
| Information | 3/28/2022 2:17:58 PM | StellarProtect | 768 | None |
| Information | 3/28/2022 1:59:54 PM | StellarProtect | 257 | None |
| Information | 3/28/2022 12:39:41 PM | StellarProtect | 257 | None |
| Information | 3/28/2022 12:39:41 PM | StellarProtect | 1280 | None |
| Information | 3/28/2022 12:39:41 PM | StellarProtect | 519 | None |
| Information | 3/28/2022 12:39:37 PM | StellarProtect | 256 | None |
| Information | 3/28/2022 12:39:37 PM | StellarProtect | 514 | None |
| Warning | 3/25/2022 2:34:29 PM | StellarProtect | 4352 | None |

The bottom pane shows details for event 257, StellarProtect, with tabs for General and Details.

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



Event Log

| Date | Description | File | Full Path |
|---------------------|-------------------------------|-------------------|---|
| 2022-03-28 17:49:20 | ICS file change blocked by... | TuneMasterApp.exe | C:\Program Files (x86)\ABB\TuneMaster\TuneMasterApp.exe |
| 2022-03-28 17:49:20 | ICS file change blocked by... | TuneMasterApp.exe | C:\Program Files (x86)\ABB\TuneMaster\TuneMasterApp.exe |
| 2022-03-28 17:49:19 | ICS file change blocked by... | TuneMasterApp.exe | C:\Program Files (x86)\ABB\TuneMaster\TuneMasterApp.exe |
| 2022-03-28 17:49:19 | ICS file change blocked by... | TuneMasterApp.exe | C:\Program Files (x86)\ABB\TuneMaster\TuneMasterApp.exe |
| 2022-03-28 17:49:18 | ICS file change blocked by... | TuneMasterApp.exe | C:\Program Files (x86)\ABB\TuneMaster\TuneMasterApp.exe |
| 2022-03-28 17:49:18 | ICS file change blocked by... | TuneMasterApp.exe | C:\Program Files (x86)\ABB\TuneMaster\TuneMasterApp.exe |
| 2022-03-28 17:49:17 | ICS file change blocked by... | TuneMasterApp.exe | C:\Program Files (x86)\ABB\TuneMaster\TuneMasterApp.exe |
| 2022-03-28 17:49:17 | ICS file change blocked by... | TuneMasterApp.exe | C:\Program Files (x86)\ABB\TuneMaster\TuneMasterApp.exe |
| 2022-03-28 17:49:17 | ICS file change blocked by... | TuneMasterApp.exe | C:\Program Files (x86)\ABB\TuneMaster\TuneMasterApp.exe |
| 2022-03-28 17:49:17 | ICS file change blocked by... | TuneMasterApp.exe | C:\Program Files (x86)\ABB\TuneMaster\TuneMasterApp.exe |
| 2022-03-28 17:49:17 | ICS file change blocked by... | TuneMasterApp.exe | C:\Program Files (x86)\ABB\TuneMaster\TuneMasterApp.exe |
| 2022-03-28 17:49:17 | ICS file change blocked by... | TuneMasterApp.exe | C:\Program Files (x86)\ABB\TuneMaster\TuneMasterApp.exe |

Numbers of events 74

Close

Agent Event List

| Event ID | Level | Category | Event Content | Event Details |
|----------|-----------------|----------------|---|--|
| 256 | Information (0) | system (1) | Service started | The service has started. |
| 257 | Information (0) | system (1) | Policy applied successfully (Version: %version%) | Policy has been applied successfully. |
| 258 | Information (0) | system (1) | Patch applied. File Name: %file_name% | Patch has been applied successfully. |
| 259 | Information (0) | system (1) | Patching in progress | Patching in progress. After the earlier-applied patch is completed, the system will automatically try to apply this patch: %deferred_file_name% |
| 513 | Information (0) | intelli_av (2) | ICS Inventory List Update Succeeded | The ICS Inventory List has been updated successfully. |
| 514 | Information (0) | intelli_av (2) | Real Time Scan Enabled | The real-time scan is enabled. |
| 515 | Information (0) | intelli_av (2) | Scheduled Scan Start | A scheduled scan has started. |
| 516 | Information (0) | intelli_av (2) | Scheduled Scan End | A scheduled scan has ended. |

| | | | | |
|-----|-----------------|--------------------|--|---|
| 517 | Information (0) | intelli_av (2) | On-Demand Scan Start | A manually launched scan has started. |
| 518 | Information (0) | intelli_av (2) | On-Demand Scan End | A manually launched scan has ended. |
| 519 | Information (0) | intelli_av (2) | Scheduled Scan Enabled | Scheduled scan has been enabled. Next scan will be on %NextScan%. |
| 520 | Information (0) | intelli_av (2) | Scheduled Scan Disabled | Scheduled scan has been disabled. |
| 768 | Information (0) | anomaly_detect (3) | Operations Behavior Anomaly Detection Enabled | Mode: %Mode% Level: %Level% |
| 769 | Information (0) | anomaly_detect (3) | Added Operations Behavior Anomaly Detection Approved Operation | Access User: %USERNAME% % Id: %ID% Target Process: %PATH% %ARGUMENT% Parent Process 1: %PATH% %ARGUMENT% Parent Process 2: %PATH% %ARGUMENT% Parent Process 3: %PATH% %ARGUMENT% Parent Process 4: %PATH% %ARGUMENT% |
| 770 | Information (0) | anomaly_detect (3) | Removed Operations Behavior Anomaly Detection Approved Operation | Id: %ID% Target Process: %PATH% %ARGUMENT% Parent Process 1: %PATH% |

| | | | | |
|------|-----------------|-----------------------|--|---|
| | | | | %ARGUMENT% Parent Process 2: %PATH% %ARGUMENT% Parent Process 3: %PATH% %ARGUMENT% Parent Process 4: %PATH% %ARGUMENT% |
| 784 | Information (0) | anomaly_detect (3) | DLL Injection Prevention Enabled | The DLL Injection Prevention has been enabled. |
| 1280 | Information (0) | device_control (5) | Device Control Enabled | The Device Control has been enabled. |
| 1281 | Information (0) | device_control (5) | Trusted USB Device Added | Vendor ID: %HEX % Product ID: %HEX% Serial Number: %STRING% Type: permanent or onetime |
| 1282 | Information (0) | device_control (5) | Trusted USB Device Removed | Vendor ID: %HEX % Product ID: %HEX% Serial Number: %STRING% |

| | | | | |
|------|-----------------|----------|--|--|
| 1792 | Information (0) | Lockdown | File access allowed: %PATH% | Access Image Path: %PATH% Access User: %USERNAME% Mode: %MODE% List: %LIST% |
| 1793 | Information (0) | Lockdown | Added to Approved List in Maintenance Mode | Path: %PATH% Hash: %SHA256_HEX STR% |
| 1794 | Information (0) | Lockdown | Approved List updated in Maintenance Mode | Path: %PATH% Hash: %SHA256_HEX STR% |
| 1795 | Information (0) | Lockdown | Approved List initialization started | Approved List initialization started |
| 1796 | Information (0) | Lockdown | Approved List initialization completed | Approved List initialization completed Count: %COUNT% |
| 1797 | Information (0) | Lockdown | Application Lockdown enabled | Application Lockdown enabled Mode: %MODE% |
| 1798 | Information (0) | Lockdown | DLL/Driver Lockdown enabled | DLL/Driver Lockdown enabled |
| 1799 | Information (0) | Lockdown | Script Lockdown enabled | Script Lockdown enabled |
| 1800 | Information (0) | Lockdown | Intelligent Runtime Learning enabled | Intelligent Runtime Learning enabled |
| 2048 | Information (0) | Update | Component update has started. | Component update has started. |

| | | | | |
|------|-----------------|----------------|---|---|
| 2049 | Information (0) | Update | Component update has ended. | Component update has ended. |
| 2050 | Information (0) | Update | Scheduled component update has been 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 (0) | Update | Scheduled component update has been disabled. | Scheduled component update has been disabled. |
| 4352 | Warning (1) | system (1) | Service stopped | The service has stopped. |
| 4353 | Warning (1) | system (1) | Unable to apply policy (Version: %version%) | The policy cannot be applied. |
| 4354 | Warning (1) | system (1) | Unable to update file: %dst_path% | Unable to update file. Source Path: %src_path% Destination Path: %dst_path% Error Code: %err_code% |
| 4355 | Warning (1) | system (1) | Unable to apply patch. File Name: %file_name% | Unable to apply patch. File Name: %file_name% Error Code: %err_code% |
| 4609 | Warning (1) | intelli_av (2) | Incoming Files Scanned, Action Taken by Antivirus: | Incoming files were scanned by antivirus. Actions were taken |

| | | | | |
|------|-------------|----------------|--|--|
| | | | %PATH% | <p>according to settings.</p> <p>File Path: %PATH %</p> <p>File Hash: %STRING%</p> <p>Threat Type: %STRING%</p> <p>Threat Name: %STRING%</p> <p>Action Result: %INTEGER%</p> <p>Quarantine Path: %PATH%</p> |
| 4610 | Warning (1) | intelli_av (2) | <p>Incoming Files Scanned, Action Taken by Next-Generation Antivirus: %PATH%</p> | <p>Incoming files were scanned by next-generation antivirus. Actions were taken according to settings.</p> <p>File Path: %PATH %</p> <p>File Hash: %STRING%</p> <p>Threat Type: %STRING%</p> <p>Threat Name: %STRING%</p> <p>Action Result: %INTEGER%</p> <p>Quarantine Path: %PATH%</p> |
| 4611 | Warning (1) | intelli_av (2) | <p>Local Files Scanned, Action Taken by Antivirus: %PATH%</p> | <p>Local files were scanned by antivirus. Actions were taken according to settings.</p> <p>File Path: %PATH %</p> |

| | | | | |
|------|-------------|----------------|---|--|
| | | | | File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING% Action Result: %INTEGER% Quarantine Path: %PATH% |
| 4612 | Warning (1) | intelli_av (2) | Local Files Scanned, Action Taken by Next- Generation Antivirus: %PATH% | Local files were scanned by next-generation antivirus. Actions were taken according to settings. File Path: %PATH % File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING% Action Result: %INTEGER% Quarantine Path: %PATH% |
| 4613 | Warning (1) | intelli_av (2) | Suspicious Program Execution Blocked: %PATH% | Suspicious program execution was blocked. File Path: %PATH % File Hash: %STRING% |

| | | | | |
|------|-------------|--------------------|---|--|
| 4614 | Warning (1) | intelli_av (2) | Suspicious Program Currently Running: %PATH% | Suspicious program is currently running. Process Id: %PID% File Path: %PATH% File Hash: %STRING% File Credibility: %STRING% |
| 4615 | Warning (1) | intelli_av (2) | Application Execution Blocked by Antivirus: %PATH% | Application execution was blocked by antivirus. Target Process: %PATH% File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING% |
| 4617 | Warning (1) | intelli_av (2) | Application Execution Blocked by Next-Generation Antivirus: %PATH% | Application execution was blocked by next-generation antivirus. Target Process: %PATH% File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING% |
| 4864 | Warning (1) | anomaly_detect (3) | Operations Behavior Anomaly Detection Disabled | Operations Behavior Anomaly Detection has been disabled. |

| | | | | |
|------|-------------|-----------------------|--|--|
| 4865 | Warning (1) | anomaly_detect (3) | Process Allowed by Operations Behavior Anomaly Detection: %PATH% %ARGUMENT% | Access User: %USERNAME% Parent Process 1: %PATH% %ARGUMENT% Parent Process 2: %PATH% %ARGUMENT% Parent Process 3: %PATH% %ARGUMENT% Parent Process 4: %PATH% %ARGUMENT% Mode: %Mode% |
| 4866 | Warning (1) | anomaly_detect (3) | Process Blocked by Operations Behavior Anomaly Detection: %PATH% %ARGUMENT% | Access User: %USERNAME% Parent Process 1: %PATH% %ARGUMENT% Parent Process 2: %PATH% %ARGUMENT% Parent Process 3: %PATH% %ARGUMENT% Parent Process 4: %PATH% %ARGUMENT% Mode: %Mode% |
| 4880 | Warning (1) | anomaly_detect (3) | DLL Injection Prevention Disabled | DLL Injection Prevention has been disabled. |
| 5120 | Warning (1) | change_control (4) | ICS File Change Blocked by SafeGuard: %PATH% | Changes to an ICS file were blocked by SafeGuard. Blocked Process: %PATH% |

| | | | | |
|------|-------------|-----------------------|---|---|
| | | | | Target File: %PATH% |
| 5121 | Warning (1) | change_control (4) | ICS Process Manipulation Blocked by SafeGuard: %PATH% | ICS Process Manipulation was blocked by SafeGuard. Blocked Process: %PATH% Target Process: %PATH% |
| 5376 | Warning (1) | device_control (5) | Device Control Disabled | Device Control has been disabled. |
| 5377 | Warning (1) | device_control (5) | USB Access Blocked: %PATH % | Access Image Path: %PATH% Access User: %USERNAME% Vendor ID: %HEX % Product ID: %HEX% Serial Number: %STRING% |
| 5888 | Warning (1) | Lockdown | File access allowed: %PATH% | Access Image Path: %PATH% Access User: %USERNAME% Mode: %MODE% Reason: %ALLOWED_RE ASON% File hash allowed: %SHA256_HEX STR%%THROTTLI NG_INFO_MSG% |

| | | | | |
|------|--------------|----------------|--|---|
| 5889 | Warning (1) | Lockdown | File access blocked: %PATH% | Access Image Path: %PATH% Access User: %USERNAME% Mode: %MODE% Reason: %BLOCKED_REASON% File hash blocked: %SHA256_HEXSTR%%THROTTLING_INFO_MSG% |
| 5890 | Warning (1) | Lockdown | Unable to add to or update Approved List: %PATH% | Unable to add to or update Approved List: %PATH% |
| 5891 | Warning (1) | Lockdown | Application Lockdown disabled | Application Lockdown disabled |
| 5892 | Warning (1) | Lockdown | DLL/Driver Lockdown disabled | DLL/Driver Lockdown disabled |
| 5893 | Warning (1) | Lockdown | Script Lockdown disabled | Script Lockdown disabled |
| 5894 | Warning (1) | Lockdown | Intelligent Runtime Learning disabled | Intelligent Runtime Learning disabled |
| 5895 | Warning (1) | Lockdown | Approved List initialization canceled | Approved List initialization canceled |
| 8706 | Critical (2) | intelli_av (2) | Real Time Scan Disabled | The Real-Time Scan has been disabled. |

| Event ID | Level | Category | Event Content | Event Details |
|-----------------|--------------|-----------------------|---------------------------|--------------------------------------|
| 9216 | Critical (2) | change_control (4) | Maintenance Mode Start | The Maintenance Mode has started. |
| 9217 | Critical (2) | change_control (4) | Maintenance Mode End | The Maintenance Mode has ended. |

Chapter 7

Technical Support

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

Learn about the following topics:

- *[Troubleshooting Resources on page 7-2](#)*
- *[Contacting Trend Micro and TXOne on page 7-3](#)*
- *[Sending Suspicious Content to Trend Micro on page 7-4](#)*
- *[Other Resources on page 7-5](#)*

Troubleshooting Resources

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

Using the Support Portal

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

Procedure

1. Go to <https://success.trendmicro.com>.
2. Select from the available products or click the appropriate button to search for solutions.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Contact Support** and select the type of support needed.



Tip

To submit a support case online, visit the following URL:

<https://success.trendmicro.com/sign-in>

A Trend Micro support engineer investigates the case and responds in 24 hours or less.

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro 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 phone or email:

Table 6-1. Trend Micro Contact Information

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

Table 6-2. TXOne Contact Information

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

- Worldwide support offices:
<https://www.trendmicro.com/us/about-us/contact/index.html>
<https://www.txone.com/contact/>
- Trend Micro product documentation:
<https://docs.trendmicro.com>

Speeding Up the Support Call

To improve problem resolution, have the following information available:

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

Sending Suspicious Content to Trend Micro

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

Email Reputation Services

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

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

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

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

File Reputation Services

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

A

agents

- features and benefits, 1-3
- system requirements, 2-2

D

- documentation, v
- documentation feedback, 7-6

E

- events, 6-2

L

- local installation, 2-1, 2-4

O

- OPCmd Program
 - using, 5-2

R

- requirements, 2-2

S

- silent installation, 2-1, 2-18
- StellarEnforce, 1-2
- StellarOne, 1-2
- StellarProtect, 1-2
- Stellar series, 1-2
- support
 - resolve issues faster, 7-4
- system requirements, 2-2

U

- uninstallation, 3-1
- upgrade, 2-26



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: APEM29618/221104