TREND MICRO | txOne networks

1.0 TXOne StellarProtect™

Installation and Administrator's Guide

All-terrain protection for mission critical assets

Windows

Endpoint Security

TXOne StellarProtect™

Installation and Administrator's Guide

TXOne Networks Incorporated 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:
http://docs.trendmicro.com/en-us/enterprise/txone-stellarprotect.aspx

Document Part No.: SLEM19272/210330

Release Date: May 4th, 2021

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 Online Help Center and/or the TXOne Knowledge Base.

TXOne always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any TXOne document, please contact us at docs@trendmicro.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 products collect and send feedback regarding product usage and detection information to TXOne. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want TXOne to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that TXOne StellarOne 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 is subject to the conditions stated in the Trend Micro Privacy Notice:

https://www.trendmicro.com/privacy

Table of Contents

Preface

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

Audience

TXOne StellarProtect documentation is intended for administrators responsible for StellarProtect management, including agent installation management and command line interface. These users are expected to have advanced networking and device management knowledge.

Document Conventions

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

Table 1. Document Conventions

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

Terminology

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

Table 2. StellarProtect Terminology

Terminology	Description
server	The StellarOne console server program
server endpoint	The host where the StellarOne server is installed
agents	The hosts running the StellarProtect program
NAT agents	The agents that are built under the routers with the Network Address Translation (NAT) function enabled
managed agents managed endpoints	The hosts running the StellarProtect program that are known to the StellarOne server program
target endpoints	The hosts where the StellarOne managed agents will be installed
administrator (or StellarOne administrator)	The person managing the StellarOne server
web console	The user interface for configuring and managing StellarOne settings and managed agents
CLI	Command Line Interface
license activation	Includes the type of StellarOne server installation and the allowed period of usage that you can use the application

agent installation folder	The folder on the host that contains the StellarProtect agent files. If you accept the default settings during installation, you will find the installation folder at the following location: "C:\Program Files\TXOne\StellarProtect"

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 the TXOne™ Stellar™ Series and StellarProtect™

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

. StellarOne™, the ONE console for Stellar series products

. StellarProtect™, the Industrial-Grade Next-Generation Antivirus

. StellarEnforce™, for application lockdown with on-demand AV scan

StellarProtect™ provides an ICS-compatible, high performance and zero touch endpoint protection solution.

Agent Features and Benefits

TXOne™ StellarProtect™ includes the following features and benefits.

Table 1-1. Features and Benefits

Feature	Benefit
Industrial-Grade Next-Generation Antivirus	ICS root of trust and advanced threat scan secure 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
ICS Application Safeguard	Intelligently locate and secure the integrity of the ICS process from ICS targeted attacks by device
USB Vector Control	Prevent insider threats by only allowing usage of USB ports on a case-by-case administrator-reviewed basis

Chapter 2

Installation

This chapter shows how to install the StellarProtect agent.

Overview

The StellarProtect agent provides several installation types including local installation and silent installation.

System Requirements

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

Hardware Requirements:

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

Software	Description
.NET framework	Ver 3.5 or 4.0 available
Hardware	Description
Available disk space	200MB minimum 300MB 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
- Another Trend Micro endpoint solution
- Other anti-virus 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

Client OS:

- Windows 7 (No SP/SP1) [Professional / Enterprise / Ultimate] (32/64bit)
- Windows 8 (No SP) [Pro/Enterprise] (32/64bit)
- Windows 10 (RS1/RS2/RS3/RS4/RS5/20H1/20H2) [Pro/Enterprise/IoT Enterprise] (32/64bit)
- Windows Embedded 8 Standard (No SP) (32/64bit)
- Windows Embedded 8.1 [Pro/Industry Pro](No SP) (32/64bit)
- Windows Embedded POSReady 7 (32/64bit)

Server OS:

- 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 Storage Server 2012 Standard (64bit)
- Windows Server 2016 (No SP) [Standard] (64bit)
- Windows Server 2019 Standard (64bit)

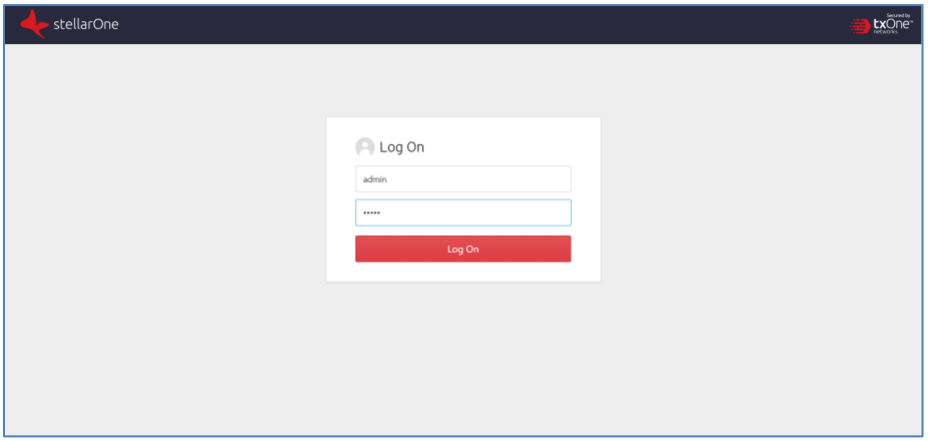
Local Installation

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

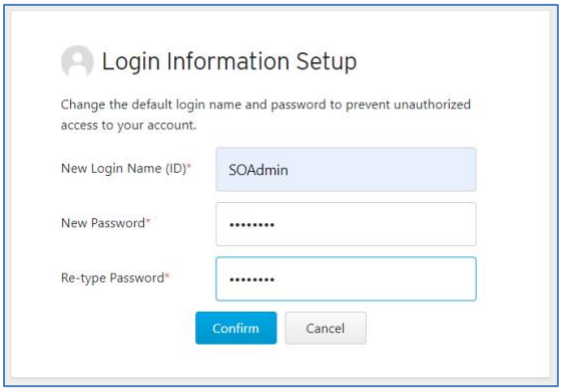
Installation Steps

[Obtaining the StellarProtect Agent installation package]

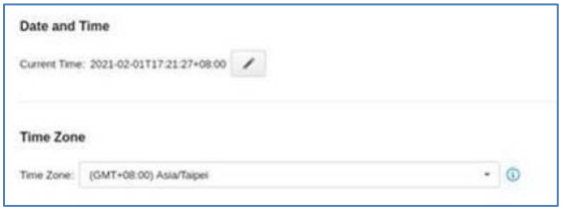
1. First log into StellarOne (default ID and password are admin/txone), the system will guide the user to change their ID and password to ensure account security.



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.

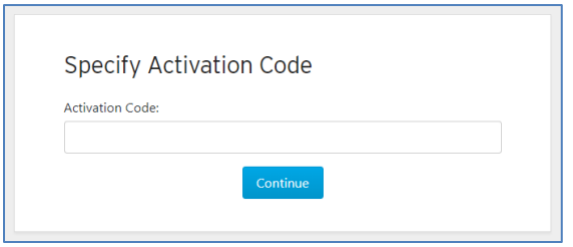


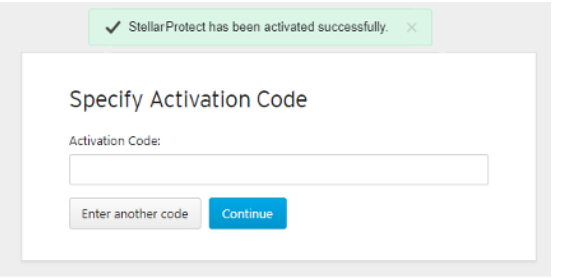
After first password change on StellarOne, there will be a page for setting Date and Time.



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

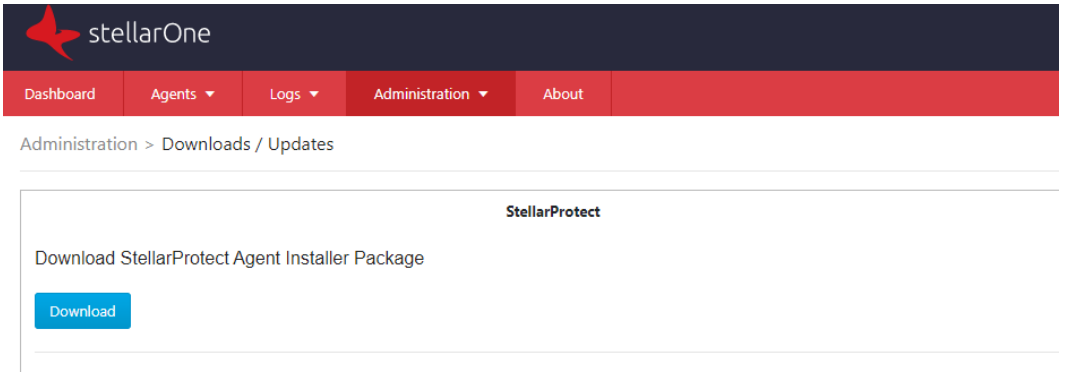
The AC can be provided by the TXOne product center or another authorized agency.





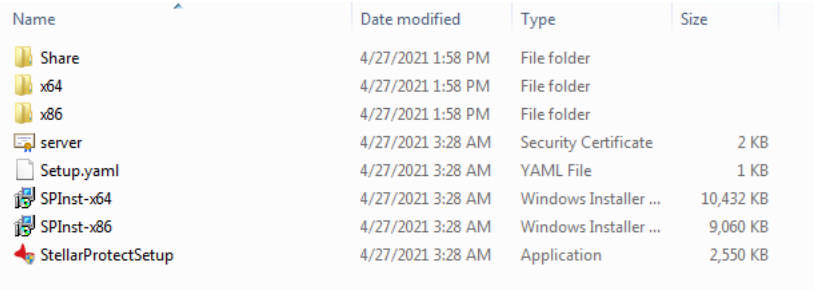
2. Download the install package from the StellarOne website.

The user can visit Administration > Updates to download the StellarProtect installation package. The downloaded package is packed by StellarOne and can be installed by all agents.

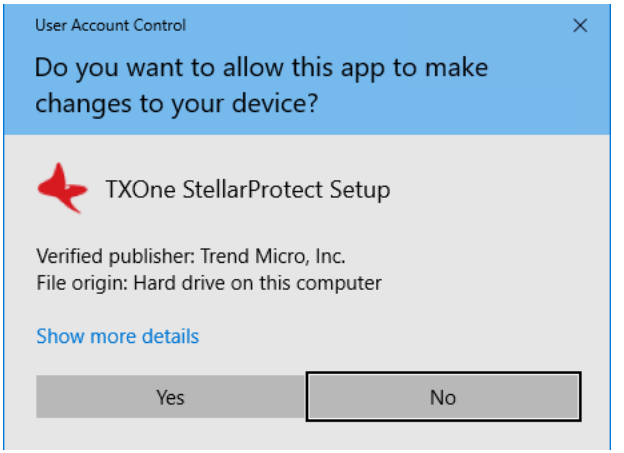


[Starting the StellarProtect Agent installation process]

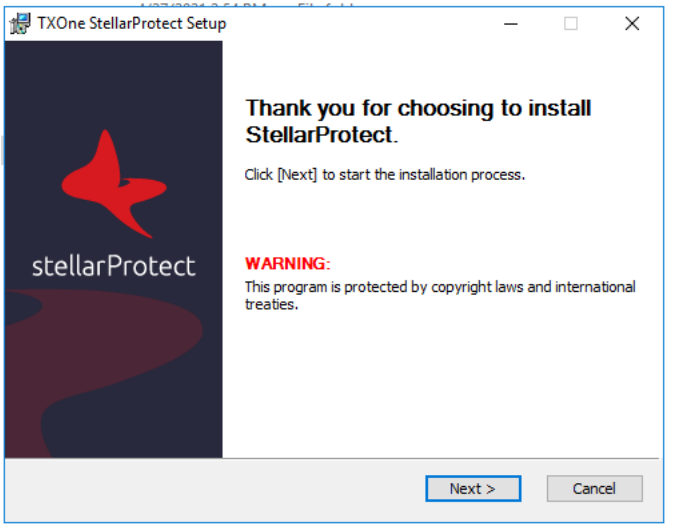
Launch the downloaded installer. Double-click the installer, **StellarProtectSetup.exe**. and follow the steps shown to finish the StellarProtect agent installation, which includes both 32- and 64-bit versions of Windows.



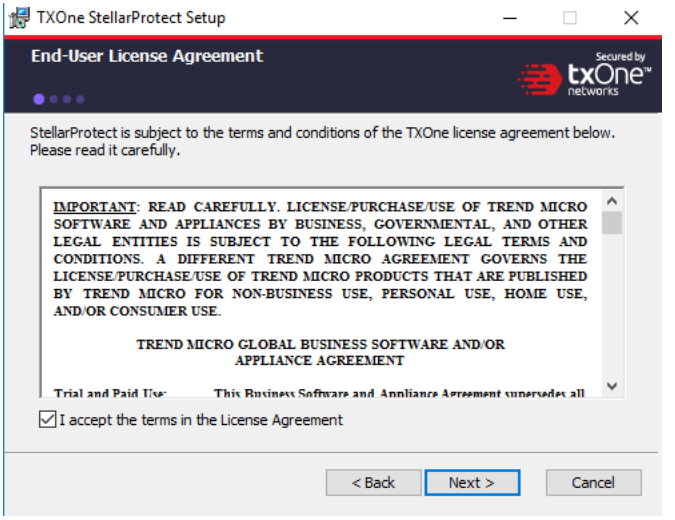
Windows will show User Account Control for user confirmation, please click Yes to start the installation.



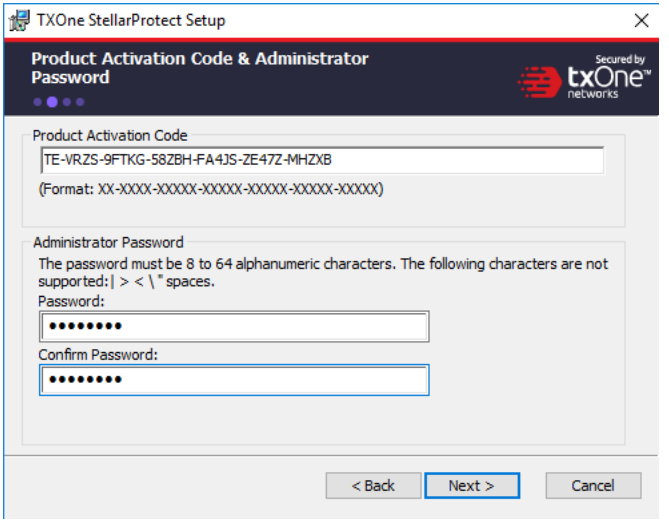
To start the installation, please click Next.



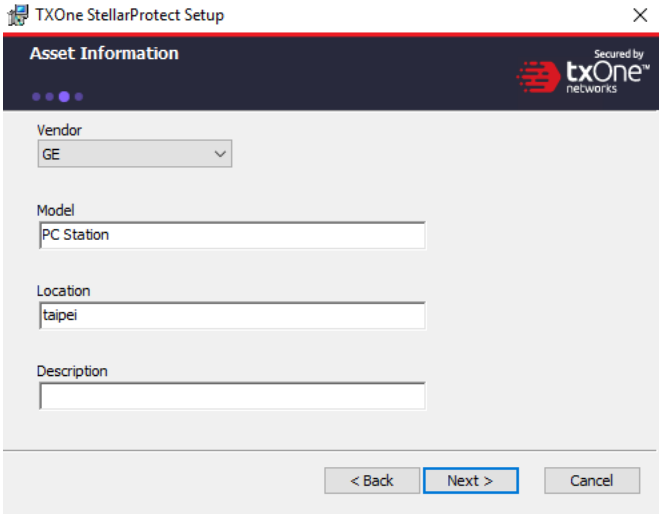
The End-User License Agreement (EULA) will be shown. Please read the content and click “I accept the terms of the license agreement” and Next.



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.



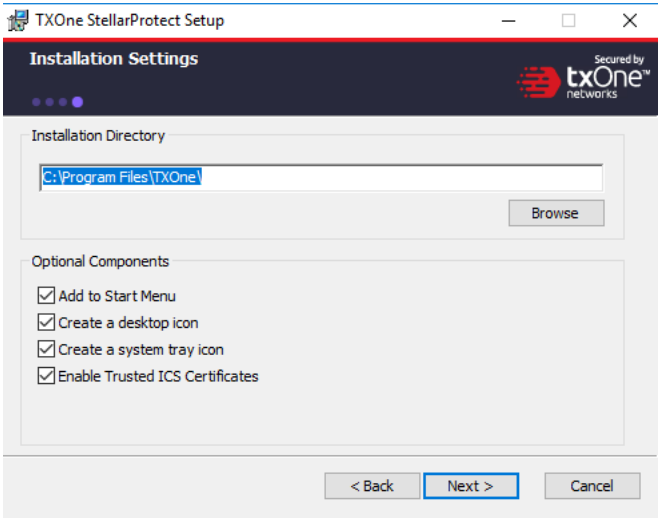
Please input the asset information of the installed device with correct ICS-relative information such as vendor name, model, location and a description.



Confirm installation settings about installation directory and optional component settings.

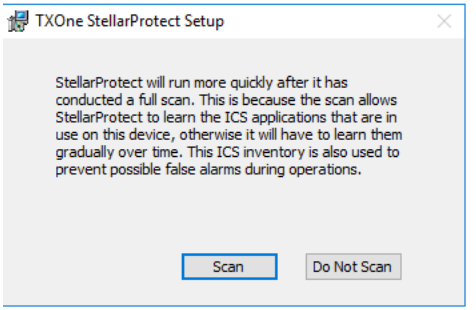
Users can choose to whether or not to add an icon to the start menu, create a desktop icon, or create a system tray icon.

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.


TXOne StellarProtect Setup
Installation Settings
Secured by txOne networks
Installation Directory
C:\Program Files\TXOne\
Browse
Optional Components
Add to Start Menu
Create a desktop icon
Create a system tray icon
Enable Trusted ICS Certificates
< Back
Next >
Cancel

Pre-scan the device.

This step is VERY IMPORTANT. Please agree to allow StellarProtect to scan the ICS device to learn which ICS applications are installed. Please click the Scan button to start the pre-scan task.

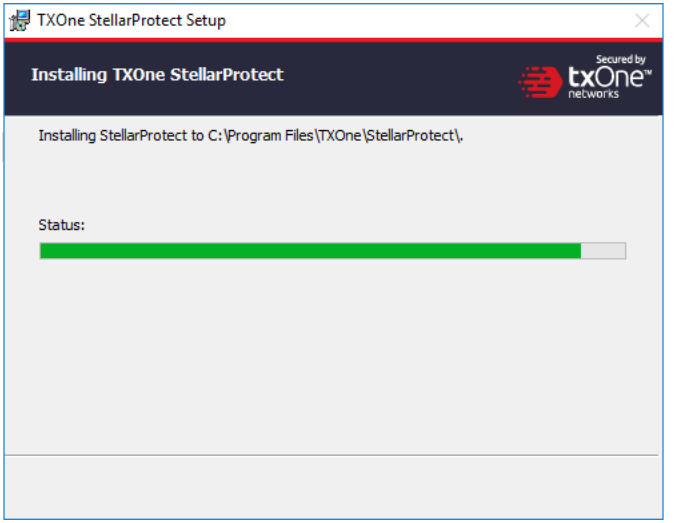


If you skip the pre-scan, StellarProtect will not be able to recognize the ICS application before it resumes production.

But don't worry, StellarProtect will relearn them when ICS applications are executed for the first time.

In addition, this may cause delays in the ICS application, so we strongly recommend that you click "Scan" to learn about the ICS application.

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

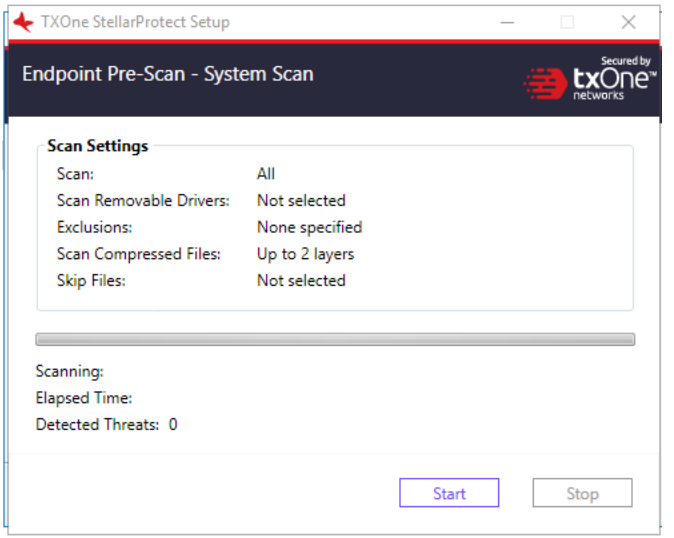


Detect existing problems by conducting an Endpoint Prescan.

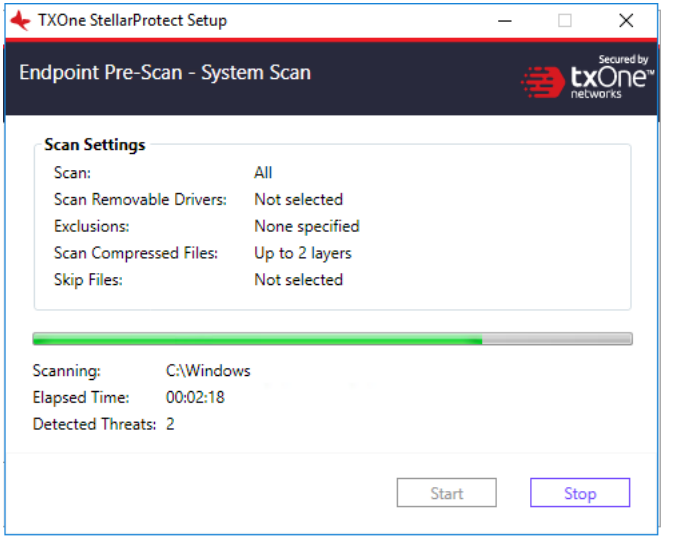
You can view the scan settings and click the Start button to launch the StellarProtect Endpoint Prescan task.

Scan settings are described as follows:

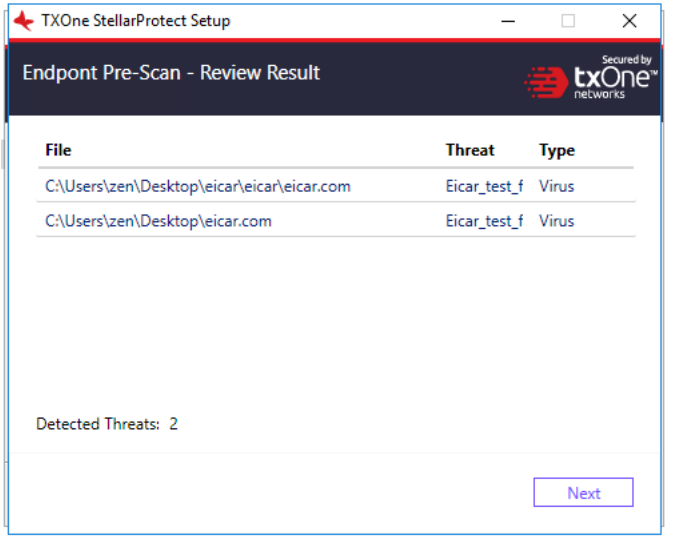
- **Scan:** This is the default anti-virus scan, following our template
- **Scan Removable Drivers:** Selected removable drives are scanned
- **Exclusion:** Which files or folders won't be scanned
- **Scan Compressed Files:** Scan up to 20 layers of compression
- **Skip Files:** Specific files that will be skipped



The progress bar shows the status of the prescan.



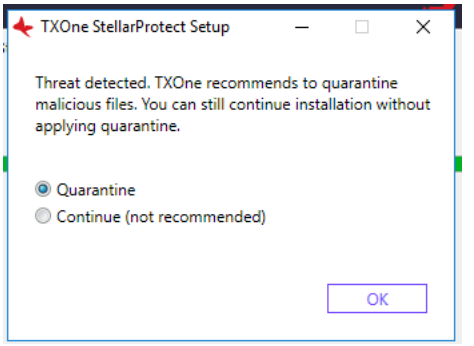
Endpoint Prescan - Review Result



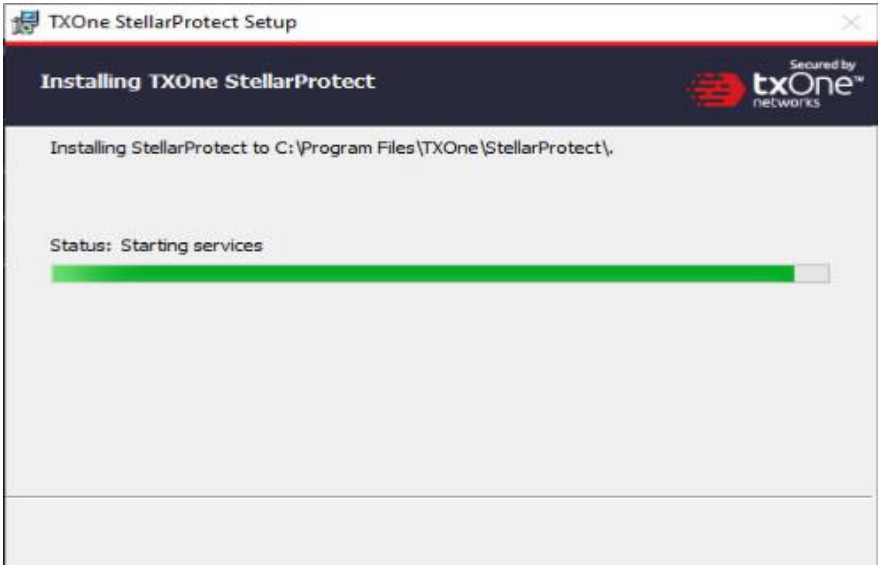
If a threat is detected, the user can choose from two options:

Quarantine: Quarantine the threat.

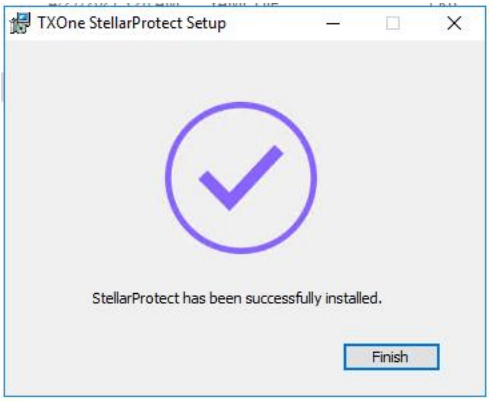
Continue: Take no action at this time.



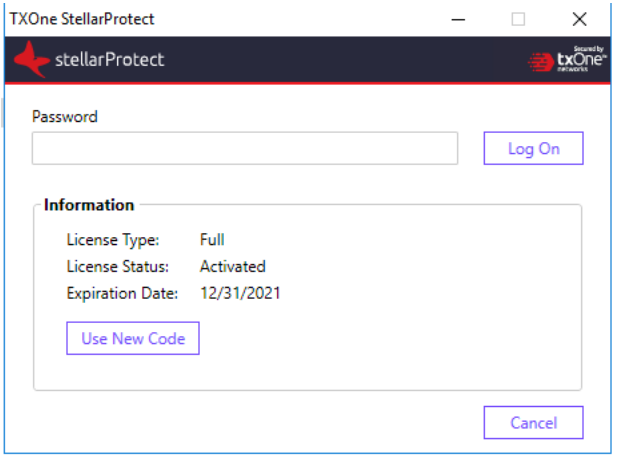
Install StellarProtect programs after the prescan has finished.



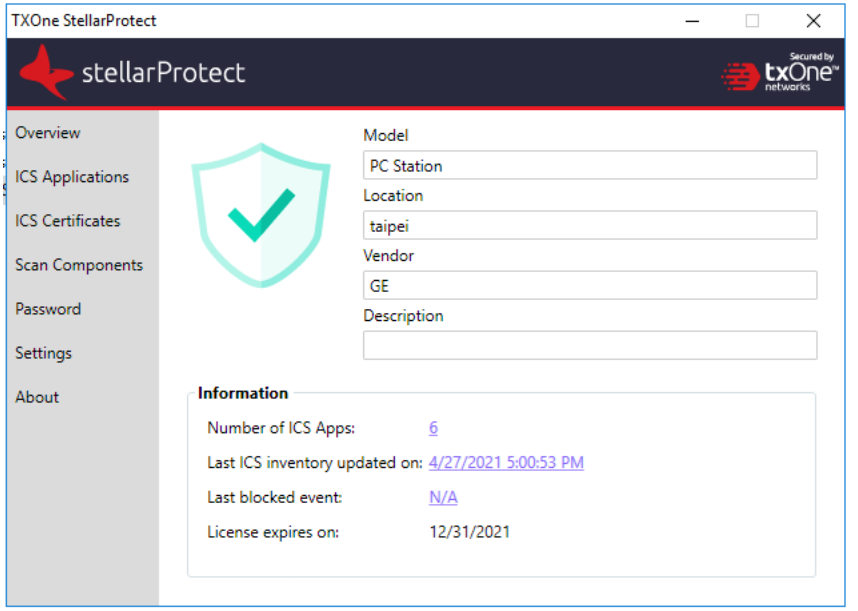
When the installation is complete, you will see this window:



Run TXOne StellarProtect and log in with the correct password.



Upon logging into StellarProtect successfully, this Window will display.



Silent Installation

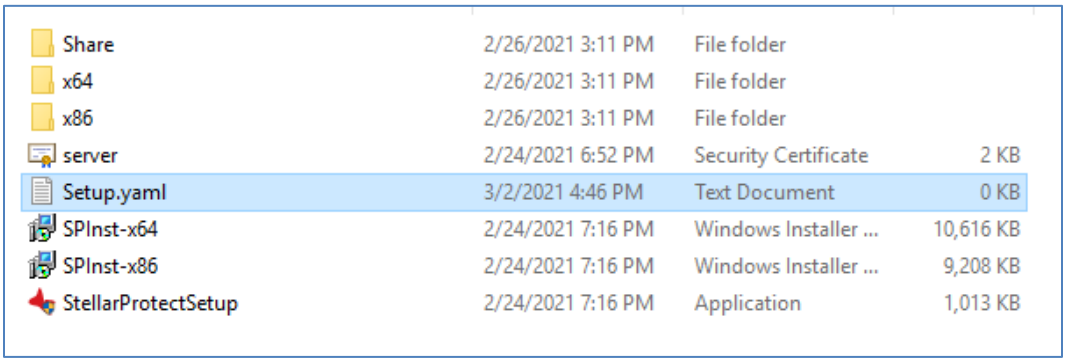
StellarProtect provides slient installation based on a pre-defined configuration file. User can use the Configuration session to enable silent installation based on the Setup.yaml, then execute StellarProtectSetup.exe with silent mode.

Configuration

Users can pre-define the setup configuration which will be applied to the installer. The name is fixed to Setup.yaml.

The launcher will try to parse Setup.yaml while executing.

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



The format and parameter definition for the Setup.yaml is as follows:

```
install:
    activation_code: <ACTIVATION_CODE>
    password: <PASSWORD>
    asset_vendor: <ASSERT_VENDOR>
    asset_model: <ASSET_MODEL>
    asset_location: <ASSET_LOCATION>
    asset_description: <ASSET_DESCRIPTION>
    install_location: <INSTALL_LOCATION>
    enable_start_menu: <ENABLE_START_MENU>
    enable_desktop_icon: <ENABLE_DESKTOP_ICON>
    enable_systray_icon: <ENABLE_SYSTRAY_ICON>
    enable_trusted_ics_cert: <ENABLE_TRUSTED_ICS_CERT>
    enable_prescan: <ENABLE_PRESCAN>
    enable_silent_install: <ENABLE_SILENT_INSTALL>
prescan:
    action: <PRESCAN_ACTION>
server:
    host: <SERVER_HOST>
    port: <SERVER_PORT>
    cert: <SERVER_CERT>
    listen: <LISTEN_PORT>
client:
    import_source: <IMPORT_SOURCE>
proxy:
    intranet:
        host: <INTRANET_PROXY_SERVER_HOST>
        port: <INTRANET_PROXY_SERVER_PORT>
        username: <INTRANET_PROXY_SERVER_USERNAME>
        password: <INTRANET_PROXY_SERVER_PASSWORD>
```

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

Parameter	Type	Default Value	Description
ACTIVATION_CODE	string	empty string	The StellarProtect Activation Code (AC) to activate the product.
PASSWORD	string	empty string	Administrator's password. The Password will be required by specific functions, ex. Uninstall, CLI or support tools.
ASSET_VENDOR	string	empty string	The vendor's name of the ICS asset.
ASSET_MODEL	string	empty string	The model name of the ICS asset.
ASSET_LOCATION	strin	empty	The physical

	g	string	location of the ICS asset.
ASSET_DESCRIPTION	string	empty string	The ICS asset description.
INSTALL_PATH	string	empty string → default install path C:\Program Files\TXOne (default install path is decided in MSI installer)	The installation path of StellarProtect installer.
ENABLE_START_MENU	boolean	true	Enable StellarProtect in Windows start menu.
ENABLE_DESKTOP_ICON	boolean	true	Enable StellarProtect execution icon on desktop.
ENABLE_SYSTRAY_ICON	boolean	true	Enable StellarProtect execution icon on windows system tray.
ENABLE_TRUSTED_ICS_CERT	boolean	true	Allow the installer to

			install ICS code signing certificates during the installation.
ENABLE_PRESCAN	boolean	true	Enable virus scan during the installation.
ENABLE_SILENT_INSTALL	boolean	false	Hide the installation UI. ACTIVATION_CODE and PASSWORD must be given during silent installation.
PRESCAN_ACTION	int	1	0: None 1: Quarantine
SERVER_HOST	string	empty string	StellarOne hostname or IP
SERVER_PORT	int	9443	StellarOne port for client
SERVER_CERT	string	server.crt	The certificate filename for communicating with StellarOne
LISTEN_PORT	int	14336	The client listen port for StellarOne
IMPORT_SOURCE	string	empty	This is the path

		string	to the folder containing the config to be imported
INTRANET_PROXY_SERVER_HOST	string	empty string	FQDN, hostname or IP address of Intranet proxy server
INTRANET_PROXY_SERVER_PORT	int	-1	Port number of Intranet proxy server
INTRANET_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
INTRANET_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

Installation Steps

Step1:

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

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 sample:

==========

install:

activation_code: **TE-GE4E-RMQNA-3VLLR-JBKMK-6YC5A-X887A**

password: **11111111**

asset_vendor: ABB

asset_model: ABB-1X2Y

asset_location: Factory1 North Area

asset_description: This is a machine

install_location: C:\test

enable_start_menu: true

enable_desktop_icon: true

enable_systray_icon: true

enable_trusted_ics_cert: true

enable_prescan: true

enable_silent_install: **true**

prescan:

action: 1

server:

host: **10.1.195.100**

port: 9443

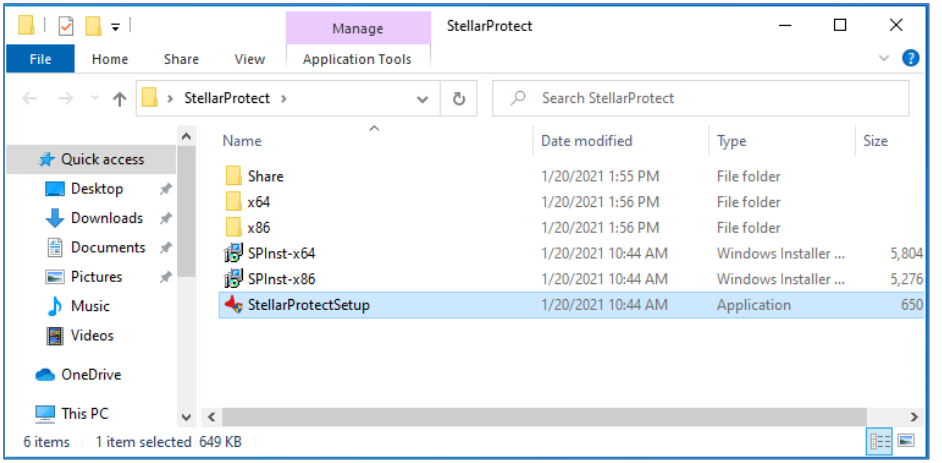
cert: server.crt

listen: 14336

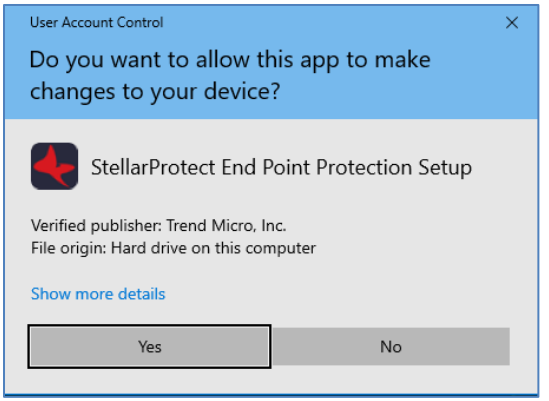
==========

Step2:

Double-click the installer StellarProtectSetup.exe. And wait for the StellarProtect agent installation to complete.

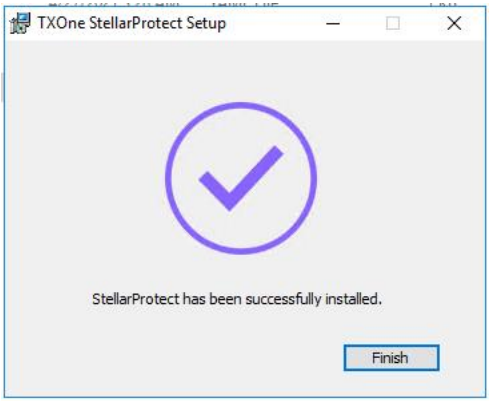


Windows will show User Account Control for user confirmation, please click “Yes” to start the installation.

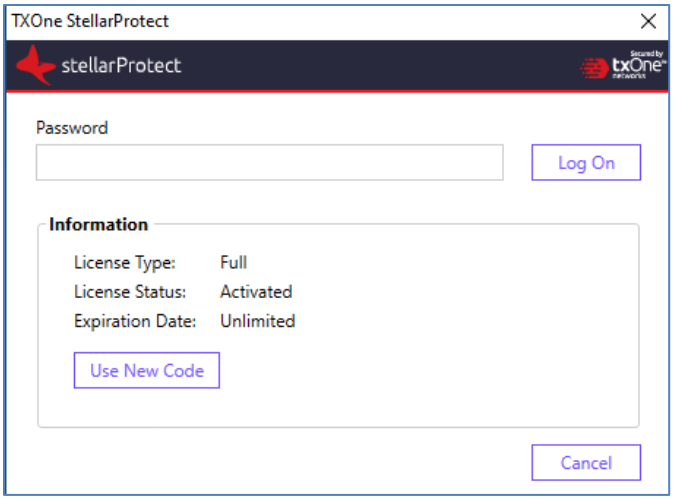


Step3:

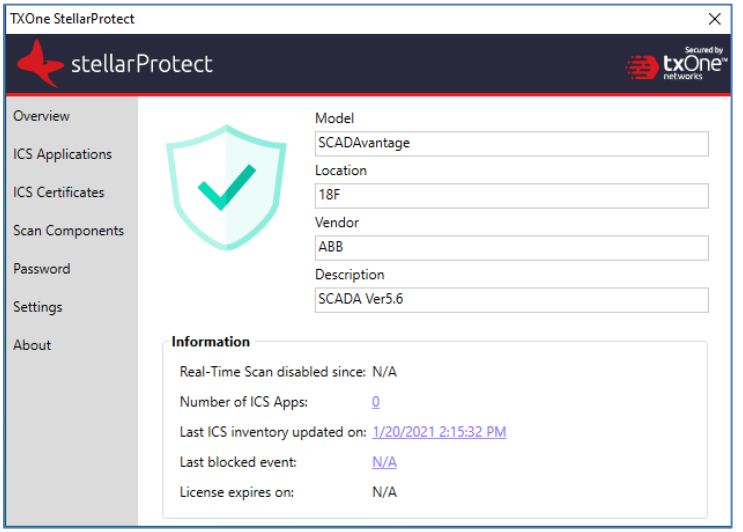
After the installation is complete, this message will be displayed to notify the user.



You can run TXOne StellarProtect and log in with the configured password to confirm StellarProtect is operating normally.



After successfully logging in to StellarProtect, this window will be displayed.



Uninstallation

The chapter will show you how to uninstall StellarProtect.

Note

The StellarProtect administrator password is required to uninstall the software from the endpoint.

Note

Please make sure the StellarProtect UI is not open.

Procedure:

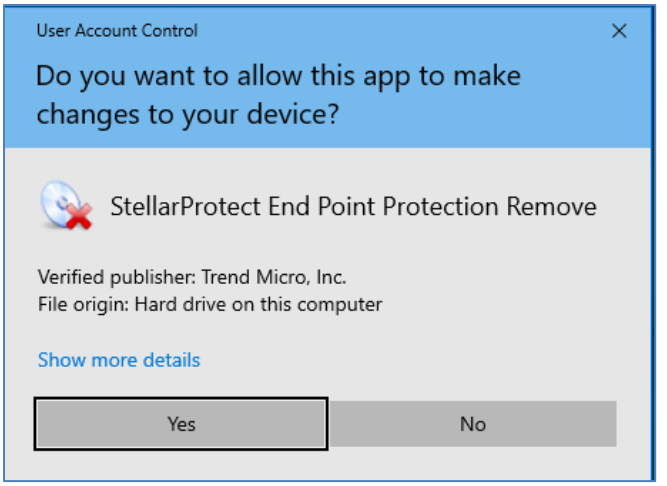
On an endpoint with the StellarProtect agent installed, launch StellarProtect Setup.

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

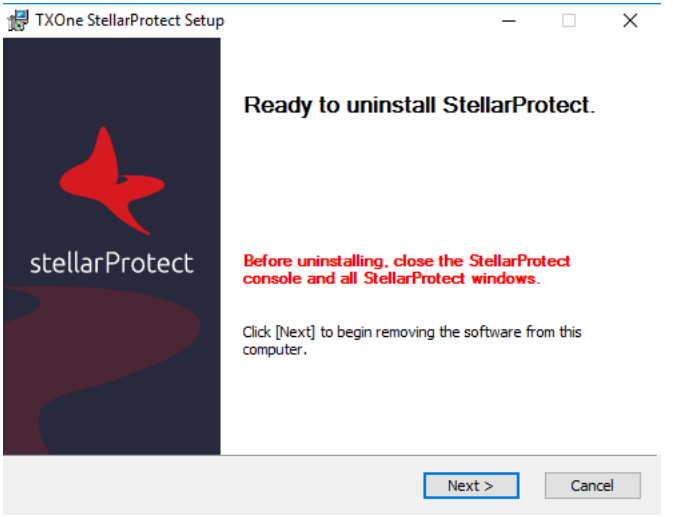
Option	Description
If you use one of the following operating systems: • Windows 10 Enterprise • Windows 10 IoT Enterprise • Windows 10 Professional • Windows 10 Fall Creators Update (Redstone 3) • Windows 10 April 2018 Update (Redstone 4) • Windows 10 October 2018 Update (Redstone 5)	a. Go to Start > Settings. b. Depending on your version of Windows 10, locate the Apps & Features section under one of the following categories: • System • Apps c. On the left pane, click Apps & Features. d. In the list, click StellarProtect. e. Click Uninstall.
If you use one of the following operating systems: • Windows Server 2016 • Windows Server 2012 • Windows Storage Server 2016 • Windows 8 • Windows 7	a. Go to Start > Control Panel > Programs and Features. b. In the list, double-click TXOne StellarProtect.

StellarProtect Setup will open in uninstaller mode.

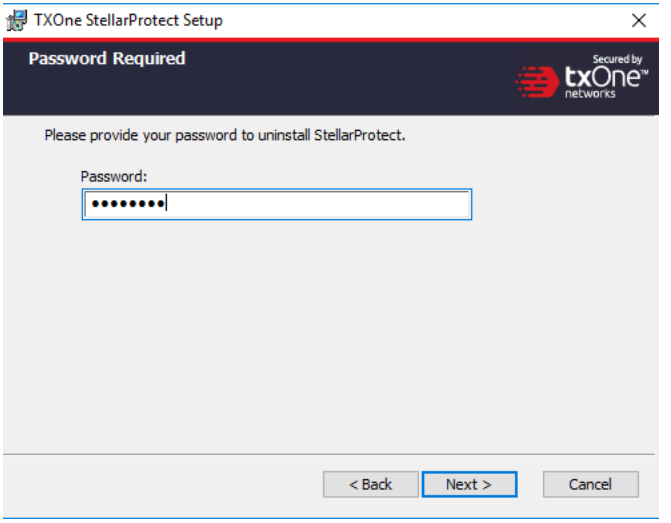
When the User Account Control window opens, click Yes.



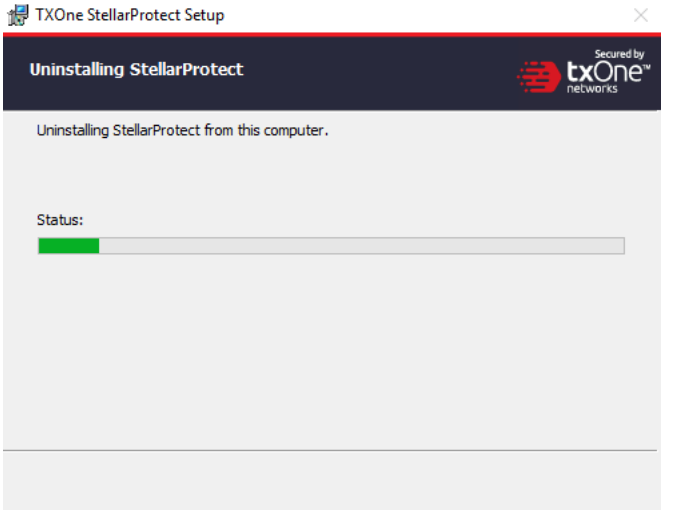
After the StellarProtect Setup opens, click Next.



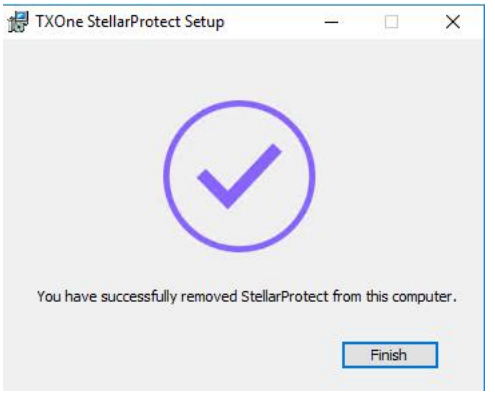
Provide the StellarProect administrator password, and click Next.



Close files that need to be updated are currently in use, click OK.



After the software is finished uninstalling, click Finish.


TXOne StellarProtect Setup
You have successfully removed StellarProtect from this computer.
Finish

Chapter 3

StellarProtect

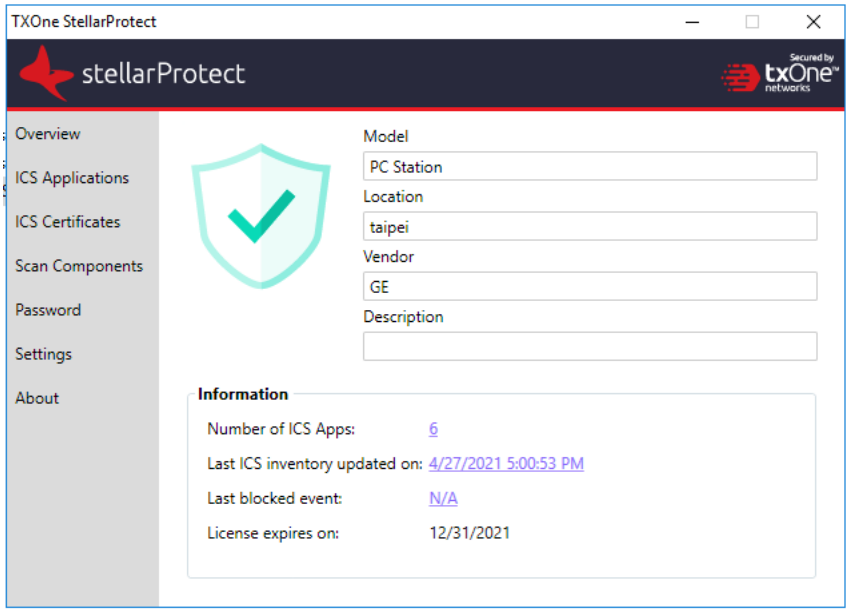
This chapter shows how to operate TXOne StellarProtect's various functions.

Overview

Overview is a description of the current status of the StellarProtect system. The shield shape indicates that the endpoint is currently protected by StellarProtect's NGAV or not. The column on the right is the endpoint ICS asset information, including Model, Location, Vendor and Description.

The following current endpoint protection information will be shown:

- Number of ICS apps: How many ICS applications are in the endpoint
- Last ICS inventory update on: The date and time the ICS Inventory was last updated on this endpoint
- Last blocked event: Clicking the link can show the most recent blocked events
- License expires on: When StellarProtect's current license will expire

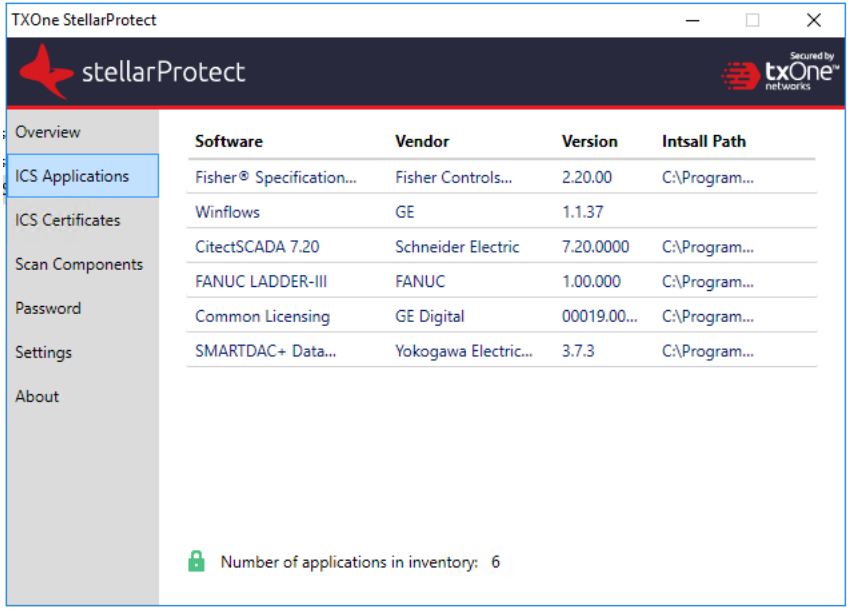


ICS Applications

This function lists all 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.

At present, the number of ICS application systems that StellarProtect can recognize will increase due to the update of the ICS Application Inventory, which is produced by the TXOne research laboratory based on market ICS product analysis.

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

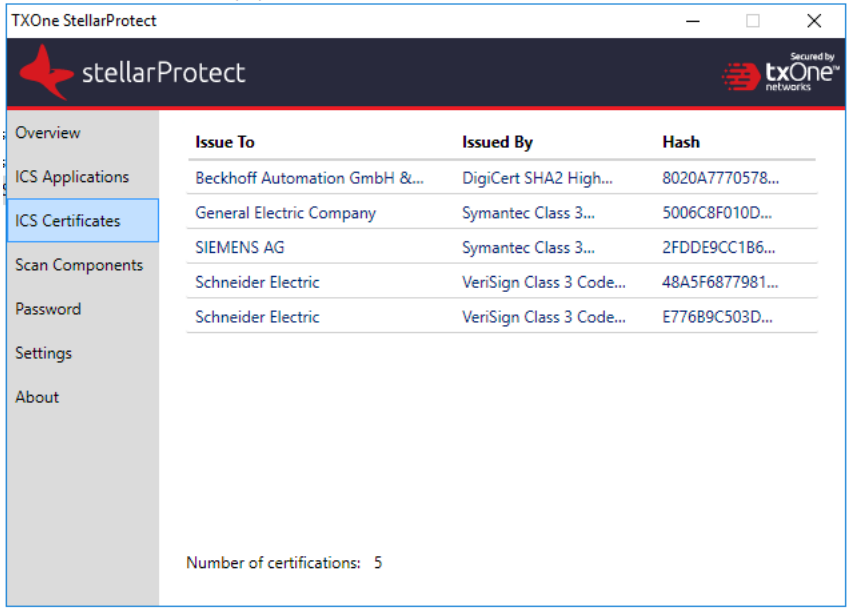


ICS Certificates

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

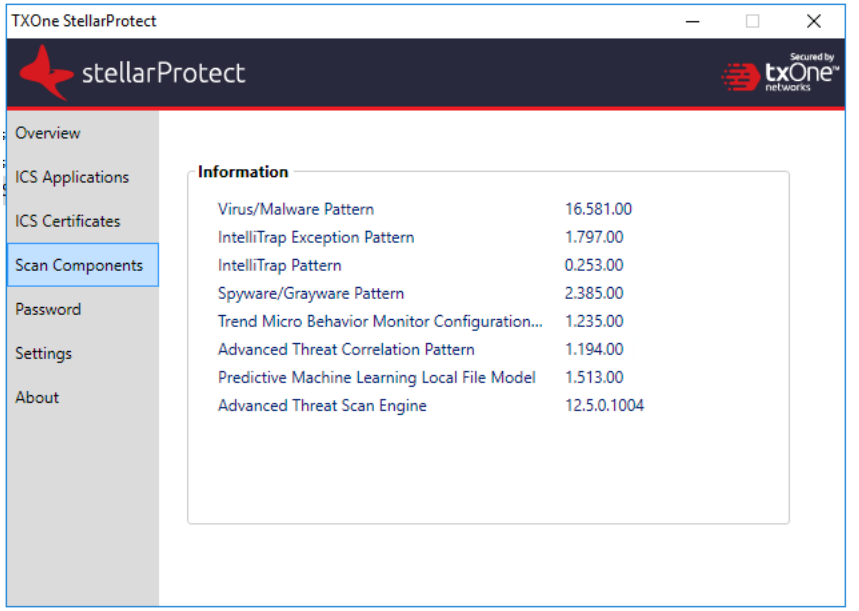
At present, the number of ICS certificates that StellarProtect can recognize will increase due to the updates from the ICS Application Inventory. This inventory is produced by the TXOne research laboratory and based on ICS product analysis.

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



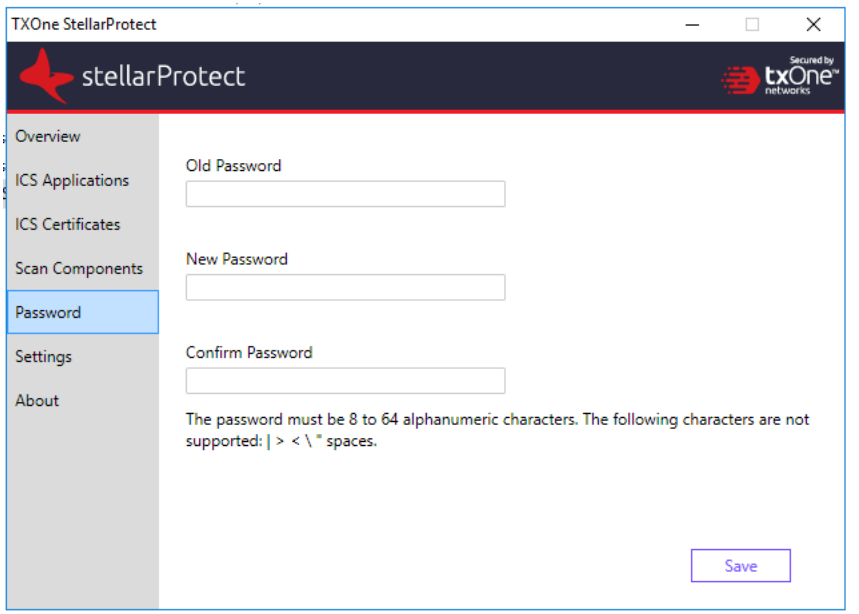
Scan Components

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



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.



USB Vector Control

USB Vector 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.

When an unauthorized USB storage device is inserted into the endpoint device, StellarProtect will send a blocked event to StellarOne, and the administrator can view the blocked event in the StellarOne console and decide to continue blocking or approve access.

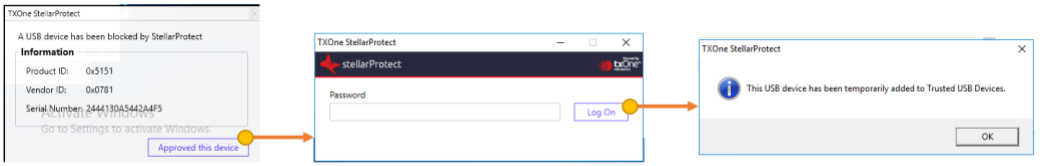
In addition, the USB Vector Control use case is as follows:

1. Plug in the USB

2. The USB will be blocked if USB Vector Control is enabled and the device is untrusted

3. Windows will show a pop-up, as in the screenshots below

4. The USB device can be allowed access until unplugged



Industrial-Grade Next-Generation Antivirus

Industrial-grade next-generation antivirus software 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 has built-in ICS application recognition technology to prevent too many false alarms.

ICS Application SafeGuard

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

Operations Behavior Anomaly Detection

Operational abnormal behavior may be caused by advanced attacks (such as fileless attacks). StellarProtect can detect the behavior of these threats using learning, prevention, or detection, and it can also keep logs for later analysis.

In addition, this function can be applied in aggressive mode to protect the endpoint with high security protection.

DLL Injection Protection

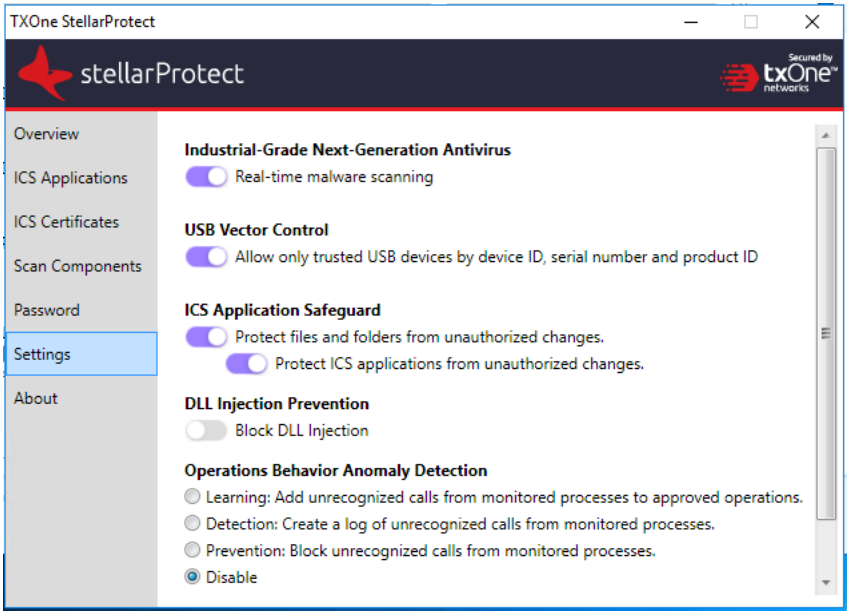
DLL injection is a high-risk attack in the ICS field, and StellarProtect can prevent this type of attack when this feature is enabled.

Note

DLL injection can **ONLY** be enabled in 32-bit Windows OS.

Settings

This section mainly describes the StellarProtect settings, including the aforementioned four main protection functions and DLL Injection Protection. Each function has a switch that can be turned on or off.



The following section describes each setting one-by-one:

Industrial-Grade Next-Generation Antivirus

This function mainly provides real-time NGAV protection. StellarProtect integrates ICS application system recognition technology, which can greatly reduce the occurrence of false alarms.

The user can click the switch to turn the function on or off.

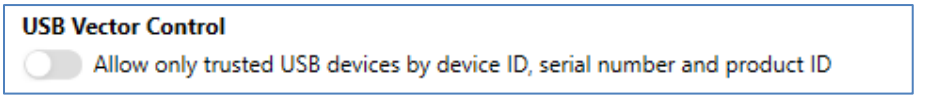
USB Vector Control

This function mainly provides identification and protection of 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.

At present, in addition to adding or deleting the trusted device list from StellarOne, when an unauthorized device is inserted into the device 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.

USB Vector Control has a one-time allow function to approve USB storage access after administrator authentication.

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



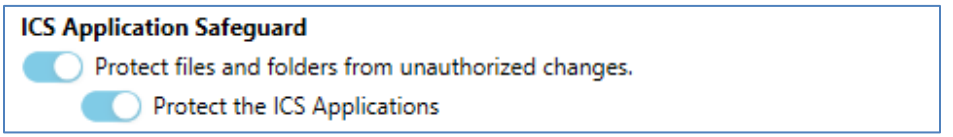
ICS Application SafeGuard

This function mainly supports StellarProtect by identifying ICS

application technology and providing protection that is consistent with ICS application system updates.

After enabling "Protect files and folders from unauthorized changes", StellarProtect will protect the files and folders defined by the user on StellarOne, which will be monitored and protected by StellarProtect.

After enabling "Protect ICS Applications", ICS application executable files will be protected automatically without user definitions.



Administrators can use StellarOne to set related exception files, registry entries, or directories.

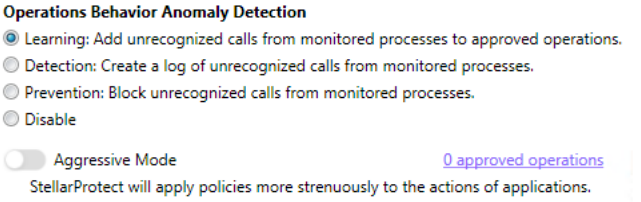
Operations Behavior Anomaly Detection

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 website.

This function has four modes, including:

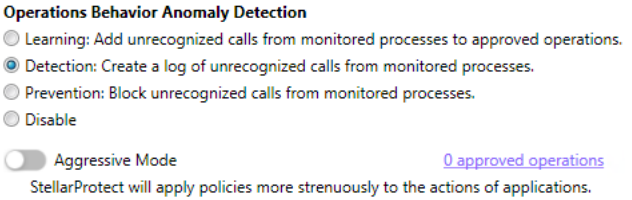
Learning Mode

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



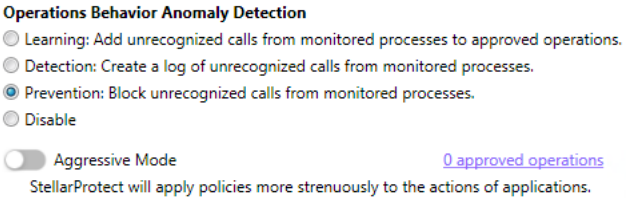
Detection Mode

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



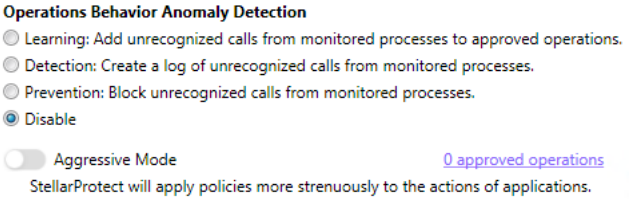
Prevention Mode

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



Disabled Mode

User can set this feature to Disabled Mode to turn off protection.



The Operations Behavior Anomaly Detection function has an **aggressive mode** and can activate protection through process parameter recognition.

Users can check the process and parameters under monitoring.

DLL Injection Protection

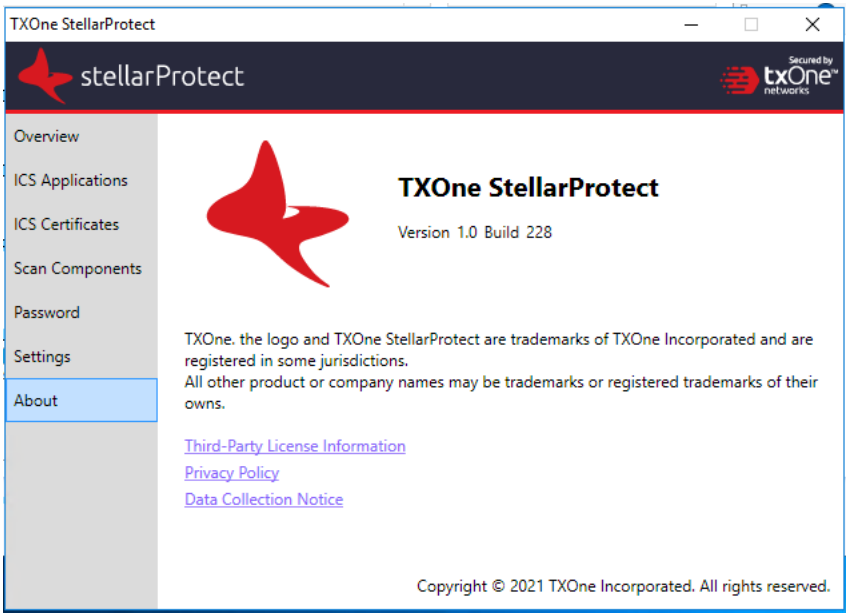
This feature specifically prevents DLL injection-based attacks.

Note

DLL injection can **ONLY** be enabled in 32-bit Windows OS.

About

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



Chapter 4

CLI

This chapter has information about operating TXOne StellarProtect's Command Line Interface.

Overview

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

Procedures:

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.

Synopsis

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

```
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.

Note

All options are optional, including global options and command-specific options.

In below commands, if it says an **argument** is REQUIRED, it means the argument is required when you use that option.

If you have trouble about the difference between an "**option**" and an "**argument**", please read the Synopsis section.

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, show brief CLI usage.

When used with a command, show 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.

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

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.

Argument: Optional. Password in plaintext.

Global Option: -v, --version

Description:
Show CLI program version and exit.

Argument: No

List of All Commands

about components:
usage: opcmd.exe about components

You can browse versions of components from the GUI program,
or you can get the list in YAML format with this command.

appinv make:
usage: opcmd.exe -p appinv make

The StellarProtect service will re-detect installed ICS applications when your schedued change window ends. You can also use this command to perform
the detection manually at any time.

appinv list:
usage: opcmd.exe appinv list

You can browse the list of detected ICS applications from the GUI program.
Or, you can get the list in YAML format with this command.

config decrypt:
usage: opcmd.exe -p config decrypt [-i INPUT-FILE] [-o OUTPUT-FILE]

Decrypt a encrypted configuration file, output decrypted plaintext.

[OPTIONS]
-i, --input INPUT-FILE Specifies the filename of an input file. If omitted, read
from standard input.

-o, --output OUTPUT-FILE Specifies filename of output file. If omitted, write
to standard output.

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 any personal
privacy data.

config encrypt:

usage: opcmd.exe -p config encrypt [-i INPUT-FILE] [-o OUTPUT-FILE]

Encrypt a plaintext configuration file, output encrypted ciphertext.

[OPTIONS]
-i, --input INPUT-FILE Specifies the filename of input file. If filename is
omitted, will read from standard input.
-o, --output OUTPUT-FILE Specifies filename of output file. If omitted, will
write to standard output.

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.

config export:

usage: opcmd.exe -p config export OUTPUT-FOLDER

Exports product configuration settings to the specified folder.

dip disable:

usage: opcmd.exe -p dip disable

Disables the DLL Injection Prevention function.

dip enable:
usage: opcmd.exe -p dip enable

Enables the DLL Injection Prevention function.

lock appinv disable:
usage: opcmd.exe -p lock appinv disable

Disables ICS Application Inventory protection.

lock appinv enable:
usage: opcmd.exe -p lock appinv disable

Enables ICS Application Inventory protection.

lock disable:
usage: opcmd.exe -p lock disable [-d DURATION] [-s START-TIME]

Disables ICS application safeguard to allow file changes on protected files.
You can also specify a duration and start-time to schedule a Change Window
that allows file changes and enable protection automatically.

[OPTIONS]
-d, --duration DURATION Specifies duration of a Change Window. The ICS
application safeguard is re-enabled after the
duration elapsed. Duration is specified in hours,

minutes, or both. (ex. -d 30m, -d 2h, -d 2h30m)
-s, --start START-TIME Specifies starting time of a Change Window. The
START-TIME is in ISO8601 format without time zone. (ex. -s 2021-04-14T18:00:00)

If -d is not specified, the ICS application safeguard is disabled until it is enabled. If -s is not specified, the ICS application safeguard is disabled immediately. Only one Change Window can be scheduled, and new settings (from the CLI or policy settings) will always overwrite previous settings.

lock enable:

usage: opcmd.exe -p lock enable

Enables ICS application safeguard to prevent file changes on protected files.
If ICS application safeguard is disabled by a scheduled Change Window, this command ends the Change Window immediately.

oad disable:

usage: opcmd.exe -p oad disable

Disables Operations Behavior Anomaly Detection.

oad enable:

usage: opcmd.exe -p oad enable -m MODE [-l LEVEL]

Enables Operations Behavior Anomaly Detection.

[OPTIONS]

-m, --mode MODE Specifies enable mode (learning, detection, prevention).
-l, --level LEVEL Specifies level (normal, aggressive).

oad info:
usage: opcmd.exe -p oad info

Shows Operations Behavior Anomaly Detection information.

oad remove:
usage: opcmd.exe -p oad remove -i ID

Removes approved operations from Operations Behavior Anomaly Detection.

[OPTIONS]
-i, --id ID Integer operation ID.

password:
usage: opcmd.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.

proxy get:
usage: opcmd.exe -p proxy get

Shows proxy server settings.

proxy set:

usage: opcmd.exe -p proxy set [-h HOST -p PORT [-u USERNAME] [-P PASSWORD]]

Sets proxy server settings.

[OPTIONS]
-h, --host HOST Specifies FQDN, hostname, or IP address of proxy server.
-p, --port PORT Specifies port number of proxy server.
-u, --username USERNAME Specifies username for proxy server authentication.
-P, --password PASSWORD Specifies password for proxy server authentication.

To disable proxy use, use this command without any options.

scan task:
usage: opcmd.exe -p scan task -s START-TIME --daily --weekly --monthly

Schedules a recurring scan task at specified start time.

[OPTIONS]
-s, --start START-TIME Specifies starting time of a Change Window. The
START-TIME is in ISO8601 format without time zone.
(ex. -s 2021-04-14T18:00:00)
--daily Specifies the scheduled scan to run daily.
--weekly Specifies the scheduled scan to run weekly.
--monthly Specifies the scheduled scan to run monthly.

service start:
usage: opcmd.exe -p service start

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.

service stop:

usage: opcmd.exe -p service stop

This sets StellarProtect service to stop until the system is powered off. If you need to stop StellarProtect service for some reason, you can use this command to stop StellarProtect service manually.

update:

usage: opcmd.exe update [-s SOURCE]

Updates product components.

[OPTIONS]
-s, --source URL Specifies the update source URL.
Ex. -s http://tmut.contoso.com/iau_server

update-stop:

usage: opcmd.exe -p update stop

Stops the currently running update.

usb add:

usage: opcmd.exe -p usb add [-v VID -p PID -s SN] [-o]

Adds a trusted USB device.

[OPTIONS]
-v, --vid VID Specifies Vendor ID in hexadecimal string.
-p, --pid PID Specifies Product ID in hexadecimal string.
-s --sn SN Specifies serial number.
-o, --onetime Grants access to a USB device one time only.

usb disable:
usage: opcmd.exe -p usb disable

Disables USB Vector Control.

usb enable:
usage: opcmd.exe -p usb enable

Enables USB Vector Control.

usb info:
usage: opcmd.exe -p usb info -d DRIVE

Show USB information of the specified drive.

[OPTIONS]
-d, --drive DRIVE Specifies the drive path (ex. E:).

usb list:
usage: opcmd.exe -p usb list

Lists trusted USB devices.

usb remove:
usage: opcmd.exe -p usb remove [-v VID -p PID -s SN]

Removes a trusted USB device.

[OPTIONS]
-v, --vid VID Specifies Vendor ID in hexadecimal string.
-p, --pid PID Specifies Product ID in hexadecimal string.
-s --sn SN Specifies serial number.

usb status:

usage: opcmd.exe -p usb status

Shows USB Vector Control status.

Chapter 5

Events

This chapter introduces the TXOne StellarProtect Agent Events description.

Overview

StellarProtect agent can generate events when some important tasks (level 0, Information), incidences (level 1, Warning) or critical functions turn on or off (level 2, Critical) issues happened.

Agent Event List

Event ID	Level	Category	Event Content	Event Detail
0x0100	info (0)	system (1)	Service started	
0x1100	warning (1)	system (1)	Service stopped	
0x0101	info (0)	system (1)	Policy applied successfully (Version: %version%)	
0x1101	warning (1)	system (1)	Unable to apply policy (Version: %version%)	
0x0201	info (0)	intelli_av (2)	ICS Inventory List Update Succeeded	
0x0202	info (0)	intelli_av (2)	Real Time Scan Enabled	
0x2202	critical (2)	intelli_av (2)	Real Time Scan Disabled	

0x1207	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%
0x1209	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%

0x1201	warning (1)	intelli_av (2)	Incoming Files Scanned, Action Taken by Antivirus: %PATH%	Incoming files were scanned by antivirus. Action were taken according to settings. File Path: %PATH% File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING% Action Result: %INTEGER% Quarantine Path: %PATH%

0x1202	warning (1)	intelli_av (2)	Incoming Files Scanned, Action Taken by Next-Generation Antivirus: %PATH%	Incoming 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%

0x1203	warning (1)	intelli_av (2)	Local Files Scanned, Action Taken by Antivirus: %PATH%	Local files were scanned by 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%

0x1204	warning (1)	intelli_av (2)	Local Files Scanned, Action Taken by Next-Generation Antivirus: %PATH%	Local files were scanned by next-generation antivirus. Action**s** were taken according to settings. File Path: %PATH% File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING% Action Result: %INTEGER% Quarantine Path: %PATH%
0x1205	warning (1)	intelli_av (2)	Suspicious Program Execution Blocked: %PATH%	Suspicious program execution was blocked. File Path: %PATH% File Hash: %STRING%
0x0300	info (0)	anomaly_detect (3)	Operations Behavior Anomaly Detection **E**nabled	Mode: %Mode% Level: %Level%

0x1300	warning (1)	anomaly_detect (3)	Operations Behavior Anomaly Detection **D**isabled	
0x0301	info (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%

0x0302	info (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%

0x1301	warning (1)	anomaly_detect (3)	Process **A**llowed 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: Detection

0x1302	warning (1)	anomaly_detect (3)	Process **B**locked 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: Protection
0x2400	critical (2)	change_control (4)	Change Window Start	
0x2401	critical (2)	change_control (4)	Change Window End	

0x1400	warning (1)	change_control (4)	ICS File Change Blocked by SafeGuard: %PATH%	ICS File change to executable file were blocked by SafeGuard. Blocked Process: %PATH% Target File: %PATH%
0x0500	info (0)	device_control (5)	USB Vector Control **E**nabled	
0x1500	warning (1)	device_control (5)	USB Vector Control **D**isabled	
0x0501	info (0)	device_control (5)	Trusted USB Device Added	Vendor ID: %HEX% Product ID: %HEX% Serial Number: %STRING% Type: permanent or onetime
0x0502	info (0)	device_control (5)	Trusted USB Device Removed	Vendor ID: %HEX% Product ID: %HEX% Serial Number: %STRING%

0x1501	warning (1)	device_control (5)	USB **A**ccess **B**locked: %PATH%	Access Image Path: %PATH% Access User: %USERNAME% Vendor ID: %HEX% Product ID: %HEX% Serial Number: %STRING%

Glossary

Acronym/Term	Definition
OBAD	Operations Behavior Anomaly Detection

Chapter 6

Technical Support

TXOne Networks is a joint venture of Trend Micro and Moxa, and support for TXOne Networks products is provided by Trend Micro. All technical support goes through Trend Micro engineers.

This chapter includes information about troubleshooting, contacting Trend Micro, sending suspicious content to Trend Micro, and other resources.

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 24/7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

1. Go to http://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 will investigate the case and respond in 24 hours or less.

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro and TXOne combat 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 http://about-threats.trendmicro.com/us/threatencyclopedia#malware 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

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

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	http://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:

  http://www.trendmicro.com/us/about-

  us/contact/index.html

- TXOne product documentation:
  http://docs.trendmicro.com

Speeding Up the Support Call

To improve problem resolution, have the following information available:

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

Sending Suspicious Content to Trend Micro

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

Email Reputation Services

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

https://ers.trendmicro.com/

Refer to the following Knowledge Base entry to send message samples to TXOne:

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

File Reputation Services

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

http://esupport.trendmicro.com/solution/en-us/1059565.aspx

Please 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):

http://global.sitesafety.trendmicro.com/

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

Other Resources

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

Download Center

From time to time, TXOne 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:

http://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.

Documentation Feedback

TXOne always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any TXOne document, please go to the following site:

http://www.trendmicro.com/download/documentation/rating.asp

TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: SLEM19272/210330