



1.1

TXOne StellarProtect™

Installation and Administrator's Guide

All-terrain protection for mission critical assets

Windows



Endpoint Security

**TXOne Networks StellarProtect™ 1.1 Installation and Administrator's
Guide**

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:

<http://docs.trendmicro.com/en-us/enterprise/txone-stellarenforce.aspx>

© 2021 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.: SLEM19396/210826

Release Date: September 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 Networks Online Help Center and/or the TXOne Networks 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@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 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 Trend Micro Privacy Notice:

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

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	2-4
Getting the StellarProtect Agent Package	2-4
Installing the StellarProtect Agent	2-7
Silent Installation	2-18
Configuring Silent Installation	2-18
Silent Installation of the StellarProtect Agent	2-22
Preparing the Agent for Upgrade to a Later Version	2-26

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
USB Vector Control	4-8
ICS 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	6-2

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
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

CONVENTION	DESCRIPTION
 WARNING!	Critical actions and configuration options

Chapter 1

Introduction

This chapter introduces TXOne StellarProtect 1.1, 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™ on page 1-2*
- *Agent Features and Benefits on page 1-3*

About the TXOne™ Stellar™ Series and StellarProtect™

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

- StellarProtect™, industrial-grade next-generation antivirus endpoint security for modernized ICS endpoints
- StellarEnforce™, for trust list-based application lockdown of legacy and fixed-use ICS endpoints with on-demand AV scan
- StellarOne™, the ONE centralized management console for the Stellar series

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

What's New

TXOne StellarProtect 1.1 includes the following new features and enhancements.

TABLE 1-1. What's New in TXOne StellarProtect 1.1

FEATURE	DESCRIPTION
Compatibility with Trend Micro Portable Security 2 and 3	StellarProtect 1.1 is now compatible with Trend Micro Portable Security products.
Remote patching from StellarOne is now supported	Starting from version 1.1, StellarProtect can be patched from the StellarOne console.
Scan components can now update from StellarOne	For air-gapped environments, StellarProtect now can perform scan component updates from StellarOne.
Scan components now update before prescan	StellarProtect will now update scan components before beginning the prescan.

FEATURE	DESCRIPTION
Silent install has been enhanced	A new silent install method is now available.
Support added to the command line for restoring quarantined files	Users can now restore quarantined files on the standalone agent using the CLI.
New Windows platform support added	StellarProtect 1.1 now officially support Windows Server 2008 and Windows 10 21H1.
Various bug fixes and enhancements	Bugs were fixed and many enhancements were added, including new kinds of event blocking based on user-defined rules.

Agent Features and Benefits

StellarProtect includes the following 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 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 2-4*
- *Silent Installation on page 2-18*

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	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
- 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

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/RS5/20H1/20H2/21H1) [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 SP1/SP2 (32-bit and 64-bit)
- 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)

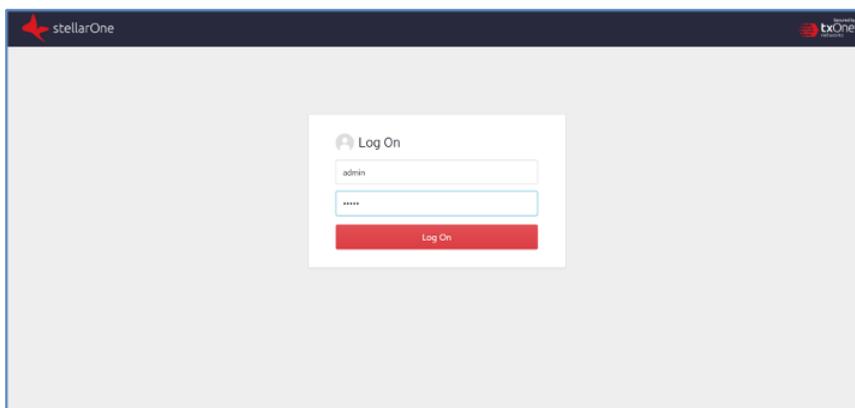
Local Installation

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

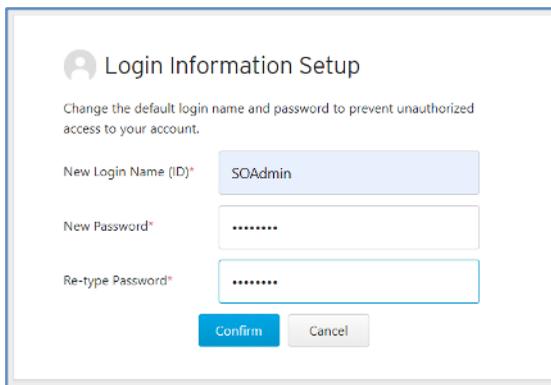
Getting the StellarProtect Agent Package

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.



Login Information Setup

Change the default login name and password to prevent unauthorized access to your account.

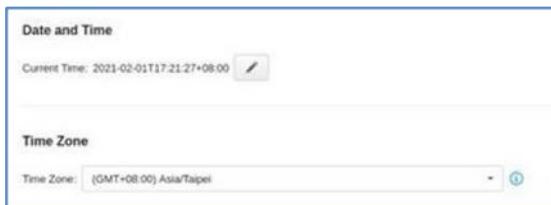
New Login Name (ID)* SOAdmin

New Password* *****

Re-type Password* *****

Confirm Cancel

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



Date and Time

Current Time: 2021-02-01T17:21:27+08:00

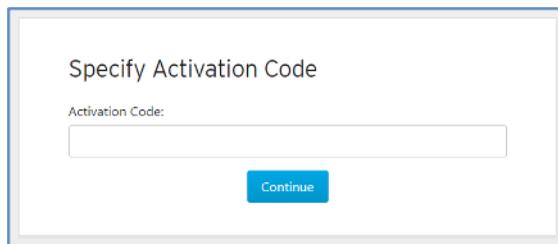
Time Zone

Time Zone: (GMT+08:00) Asia/Taipei

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

**Note**

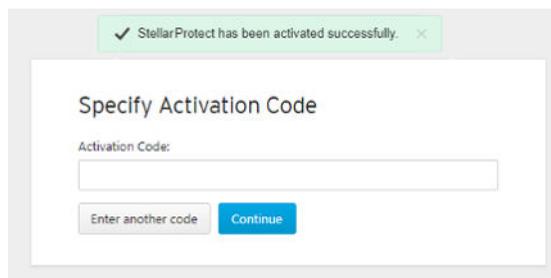
The AC can be provided by the TXOne product center or another authorized agency.



Specify Activation Code

Activation Code:

Continue



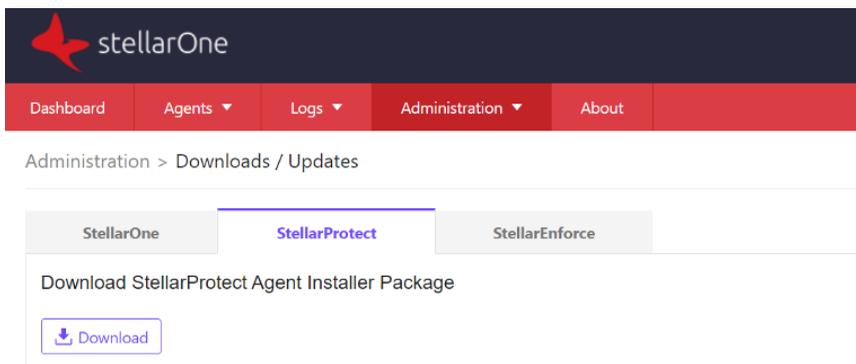
✓ StellarProtect has been activated successfully. ✕

Specify Activation Code

Activation Code:

Enter another code Continue

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



stellarOne

Dashboard Agents Administration About

Administration > Downloads / Updates

StellarOne StellarProtect StellarEnforce

Download StellarProtect Agent Installer Package

Download

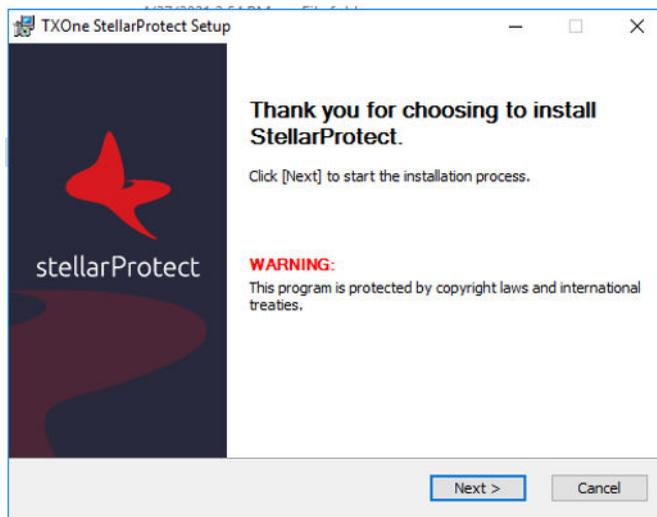
Installing the StellarProtect Agent

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

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 'Product Activation Code & Administrator Password' screen of the TXOne StellarProtect Setup. The window title is 'TXOne StellarProtect Setup'. The header bar is dark blue with the TXOne Networks logo and the text 'Secured by txOne networks'. The main content area is white and contains two sections: 'Product Activation Code' and 'Administrator Password'. The 'Product Activation Code' section has a text box containing 'TE-VRZS-9FTKG-58ZBH-FA43S-ZE47Z-MHZXB' and a note '(Format: XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX)'. The 'Administrator Password' section has a note 'The password must be 8 to 64 alphanumeric characters. The following characters are not supported: | > < \ " * spaces.' and two password input fields, one for 'Password:' and one for 'Confirm Password:', both containing eight dots. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

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

The screenshot shows the 'Asset Information' screen of the TXOne StellarProtect Setup. The window title is 'TXOne StellarProtect Setup'. The header bar is dark blue with the TXOne Networks logo and the text 'Secured by txOne networks'. The main content area is white and contains four input fields: 'Vendor' (a dropdown menu with 'GE' selected), 'Model' (a text box with 'PC Station'), 'Location' (a text box with 'taipei'), and 'Description' (an empty text box). At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

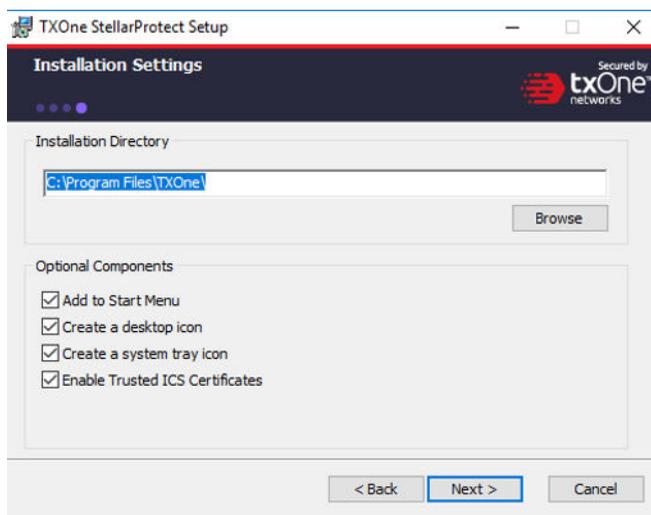
6. Confirm installation settings including installation directory and optional component settings.

**Note**

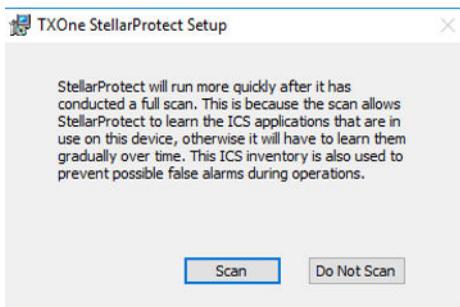
Users can choose to whether or not to add an icon to the start menu, create a desktop icon, or create a system tray icon.

**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.



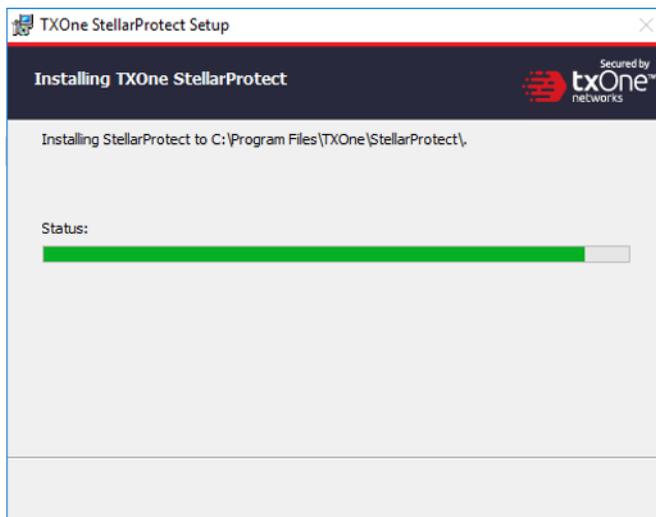
7. Please click the **Scan** button to start the pre-scan task. Please note, this step is extremely important – please agree to allow StellarProtect to scan the ICS device to learn which ICS applications are installed.



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.

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

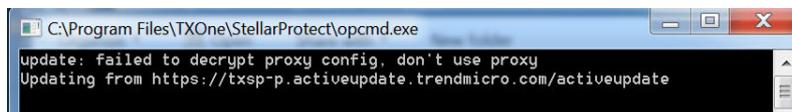


9. To detect potential pre-existing issues, users should run an Endpoint Prescan. You can view the scan settings and click the Start button to launch the StellarProtect Endpoint Prescan task.



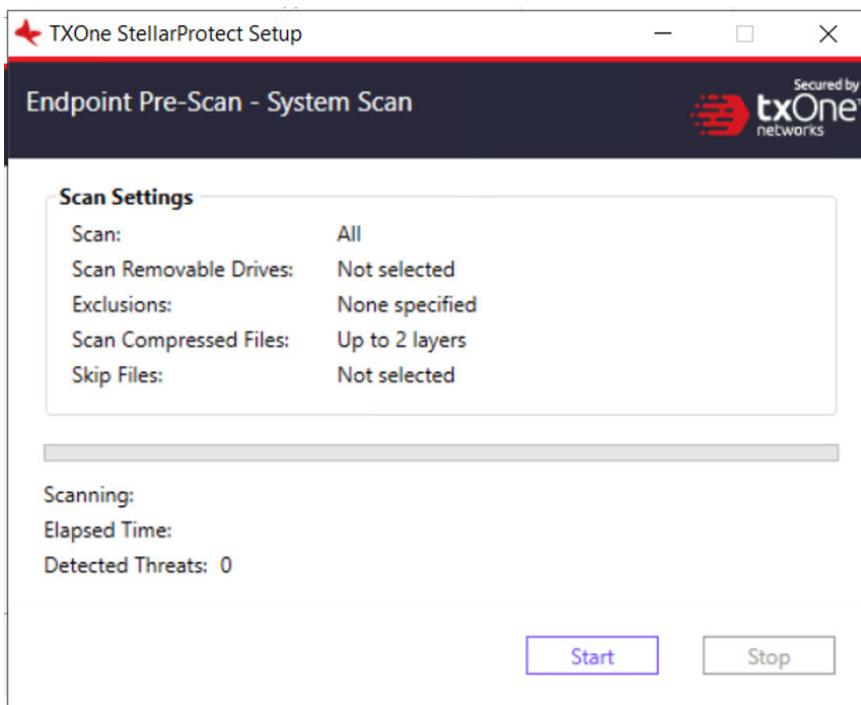
Before the prescan starts, the installer will perform a component update based on the chosen configuration. For the standalone agent installer package, connecting to the Trend Micro Active Update server will be necessary to perform the update, so internet access is required.

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

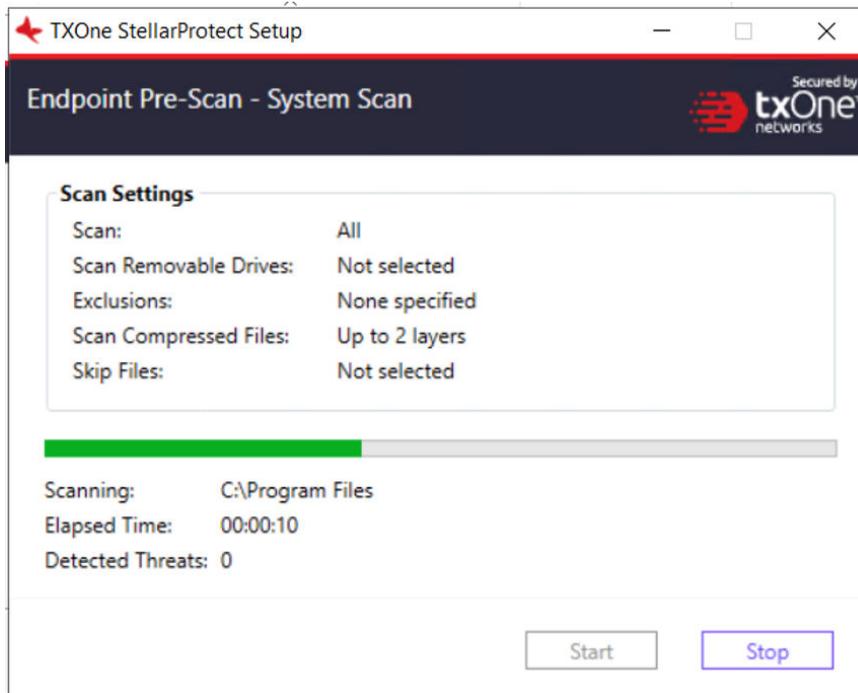


Scan settings are described as follows:

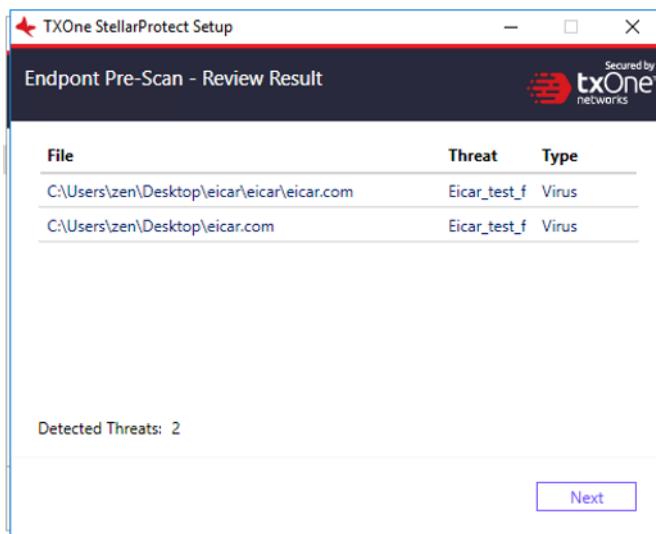
- **Scan:** This is the default anti-virus scan, following our template
- **Scan Removable Drives:** Selected removable drives are scanned
- **Exclusion:** Which files or folders won't be scanned
- **Scan Compressed Files:** Scan up to 20 layers of compression
- **Skip Files:** Specific files that will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



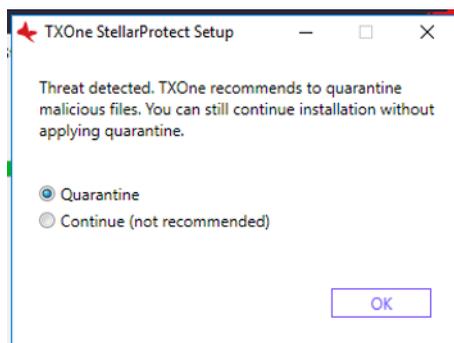
The progress bar shows the status of the prescan.



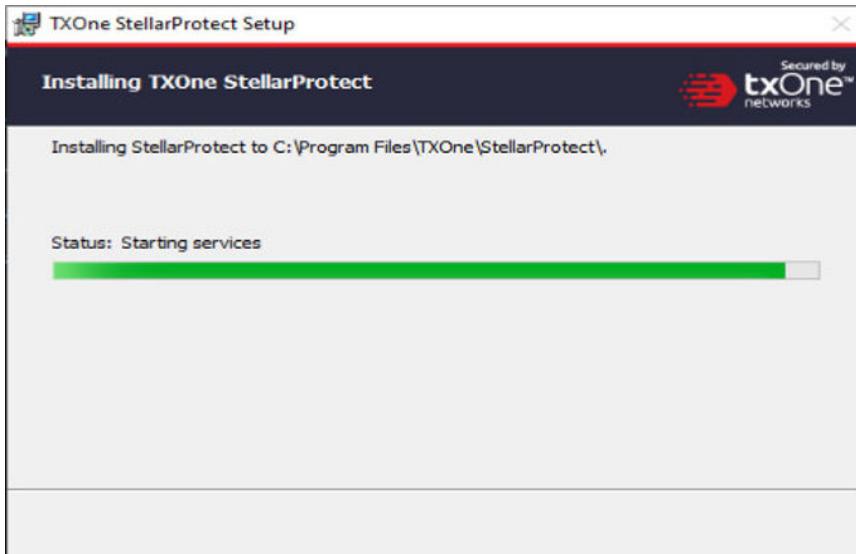
10. After the prescan, results will be shown for review.



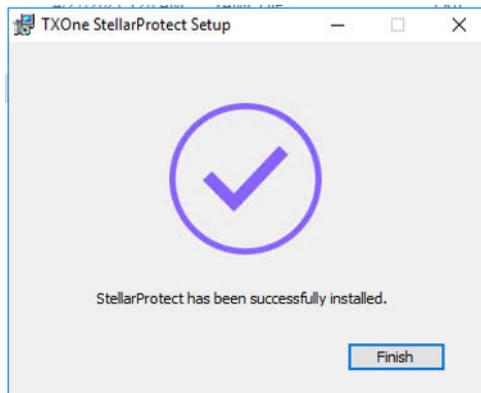
11. If a threat is detected, the user can choose from two options:
 - a. **Quarantine:** Quarantine the threat.
 - b. **Continue:** Take no action at this time.



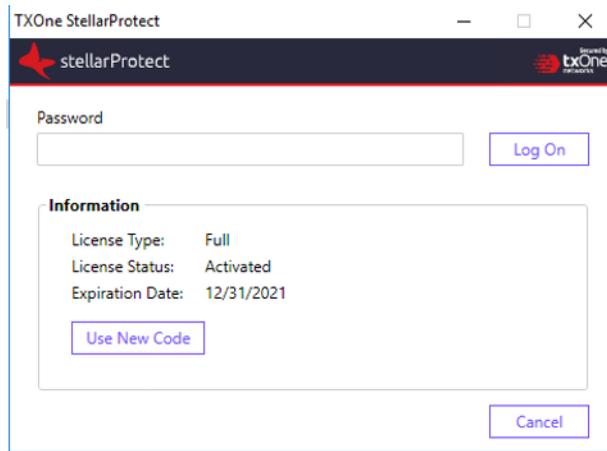
12. After the prescan phase is complete, the StellarProtect application will be installed.



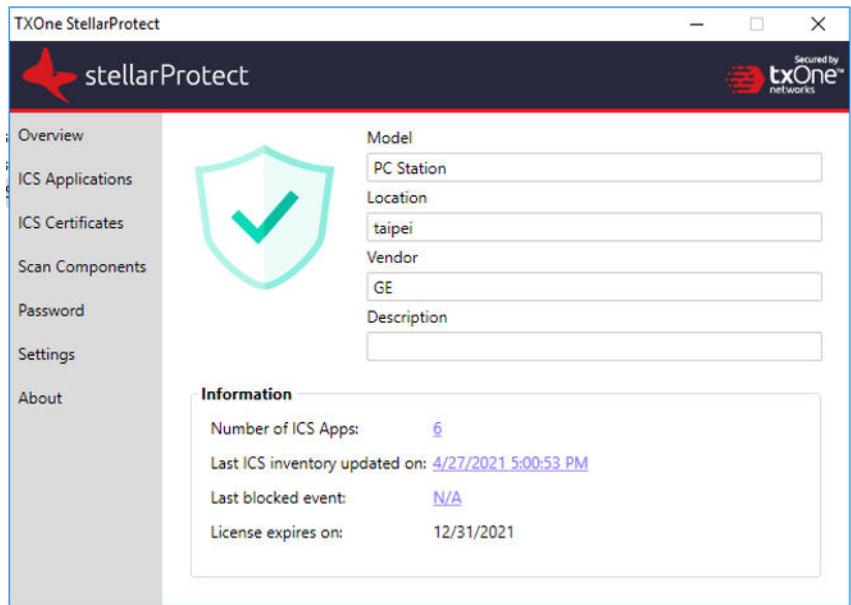
13. When the installation is complete, you will see the window below.



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



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



Silent Installation

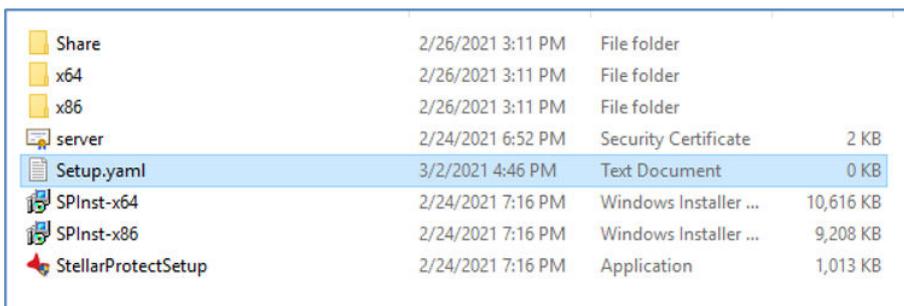
StellarProtect provides silent installation based on a pre-defined configuration file. User can use the Configuration session to enable silent installation based on the `Setup.yaml`, then execute `StellarProtectSetup.exe` in silent mode.

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

- install:
- • activation_code: <ACTIVATION_CODE>
password: <PASSWORD>
asset_vendor: <ASSET_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:
 - • default:
 - • • 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) used for license activation.
PASSWORD	string	empty string	Administrator's password. The Password will be required by specific functions, including uninstall, the command line interface, and 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	string	empty string	The physical 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 the StellarProtect installer.

PARAMETER	TYPE	DEFAULT VALUE	DESCRIPTION
ENABLE_START_MENU	boolean	true	Enable StellarProtect in the Windows start menu.
ENABLE_DESKTOP_ICON	boolean	true	Enable StellarProtect icon to be placed on the desktop.
ENABLE_SYSTRAY_ICON	boolean	true	Enable StellarProtect icon in the Windows system tray.
ENABLE_TRUSTED_ICS_CERT	boolean	true	Allow the installer to install ICS code signing certificates during installation.
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.
PRESCAN_ACTION	int	1	0: None 1: Quarantine
SERVER_HOST	string	empty string	StellarOne hostname or IP
SERVER_PORT	int	9443	StellarOne's port for connecting to the client
SERVER_CERT	string	server.crt	The certificate filename for communicating with StellarOne

PARAMETER	TYPE	DEFAULT VALUE	DESCRIPTION
LISTEN_PORT	int	14336	The client listening port for StellarOne
IMPORT_SOURCE	string	empty string	This is the path to the folder containing the config to be imported
DEFAULT_PROXY_SERVER_HOST	string	empty string	FQDN, hostname or IP address of Intranet proxy server
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
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

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:

- install:
 - activation_code: TE-XXXXX-SAMPL-EXXXX-CODES-XXXXX-TXONESP
 - 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

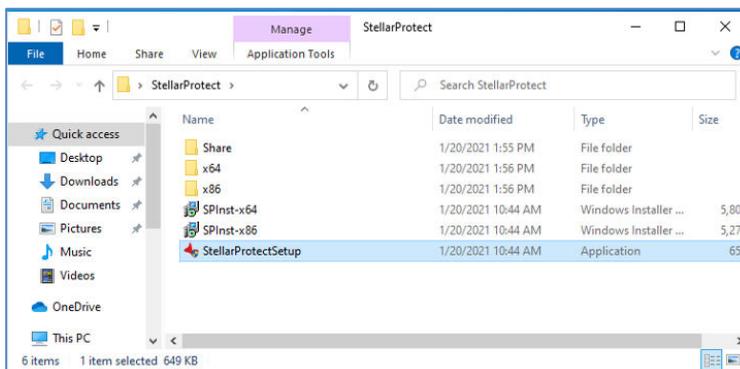
2. Double-click the installer, StellarProtectSetup.exe.



Note

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

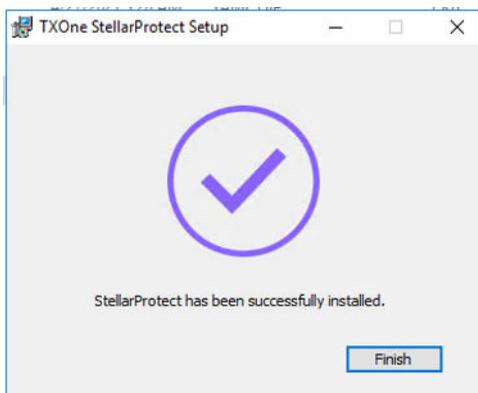
- For a silent installation with a GUI, double-click the installer StellarProtectSetup.exe.



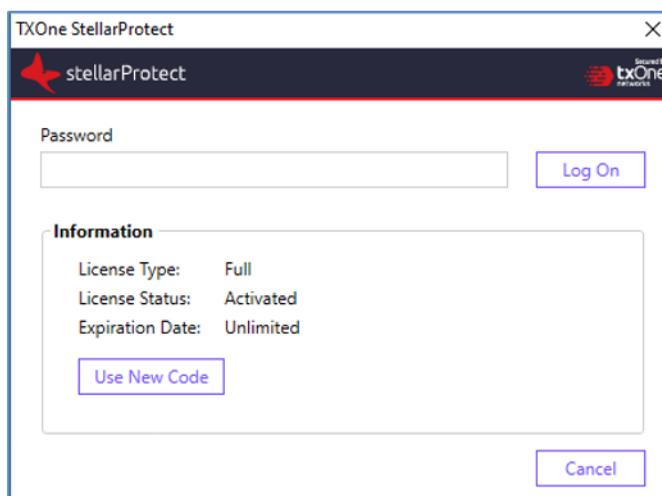
- For a silent installation without any GUI, instead of double-clicking the executable in step 2, instead use the command prompt to execute StellarProtectSetup.exe with the argument -s. Please note that with this method, pop-up windows mentioned in the following steps will not be shown. To view information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

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

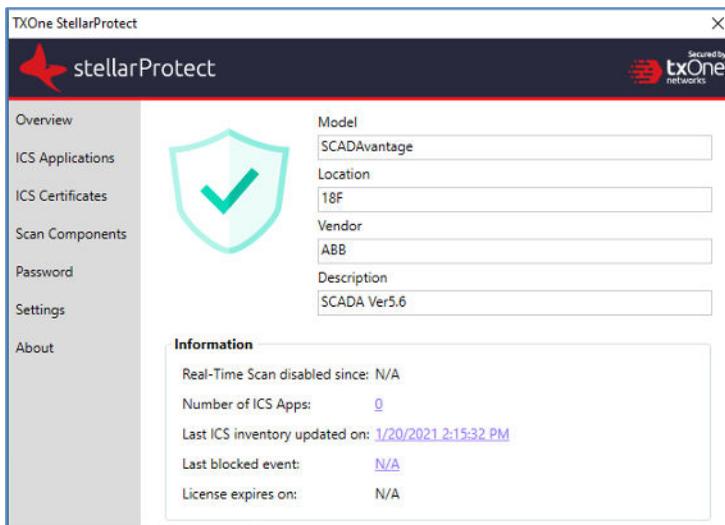
3. After the installation is complete, this message box will appear.



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



5. After successfully logging into StellarProtect, this window will be displayed.



Preparing the Agent for Upgrade to a Later Version

This version of StellarProtect supports upgrade from the following version:

- StellarProtect 1.0

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 StellarEnforce 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	Manually uninstall	No settings retained
Local installation using command line interface installer	StellarProtect 1.0	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	No preparation needed	Compatible settings retained
Remote Installation	Not supported	Not supported	Not supported

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

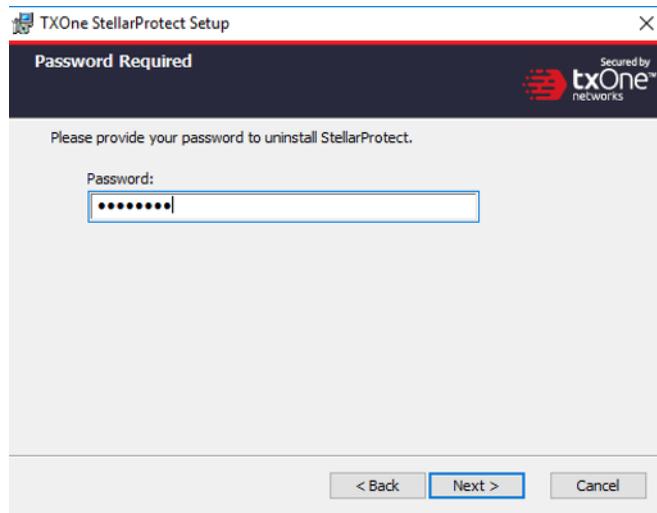
1. On an endpoint with the StellarProtect agent installed, launch StellarProtect Setup.
2. Follow the steps listed here according to your operating system:

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)	<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 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.

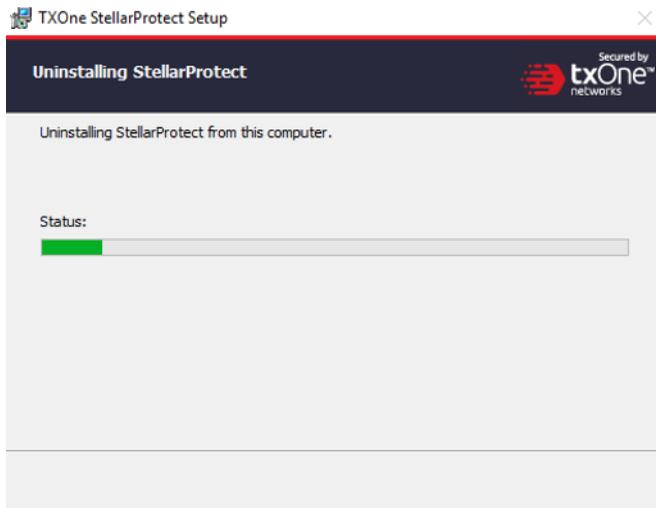
3. After the StellarProtect Setup opens, click **Next**.



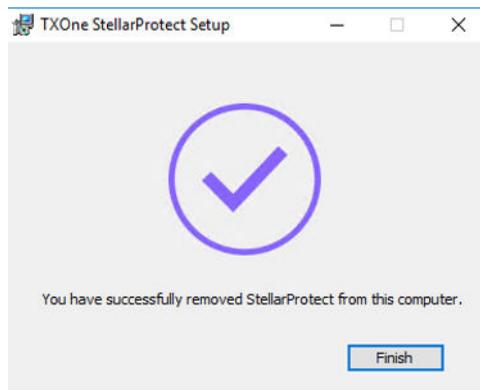
4. Enter in the StellarProtect administrator password, and click **Next**.



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



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



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:

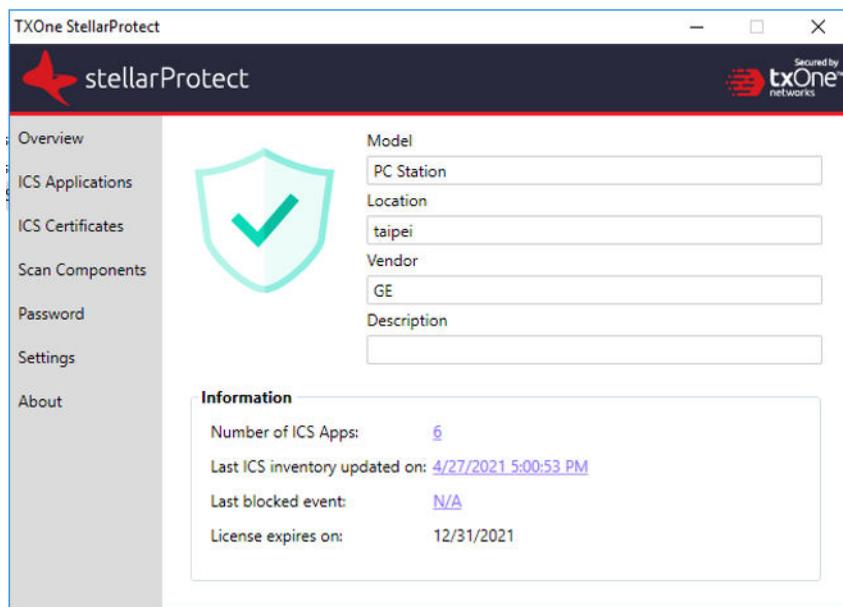
- *Overview on page 4-2*
- *Settings on page 4-10*

Overview

Overview is a description of the current status of the StellarProtect system. The shield shape indicates if the endpoint is currently protected by StellarProtect's Next-Generation Antivirus. The column on the right is the endpoint's ICS asset information including Model, Location, Vendor and Description.

The following current information about endpoint protection 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 shows the most recent blocked events
- **License expires on:** When StellarProtect's current license will expire

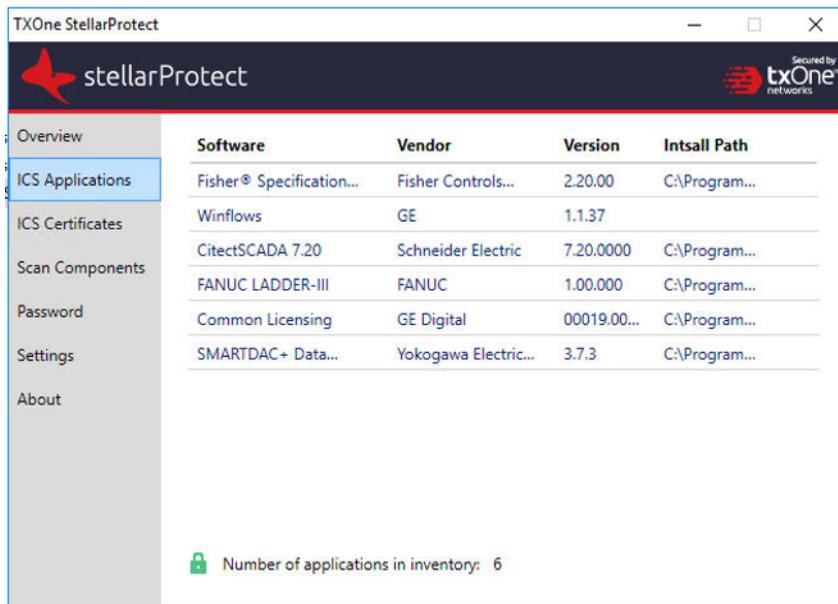


ICS Applications

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.

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

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

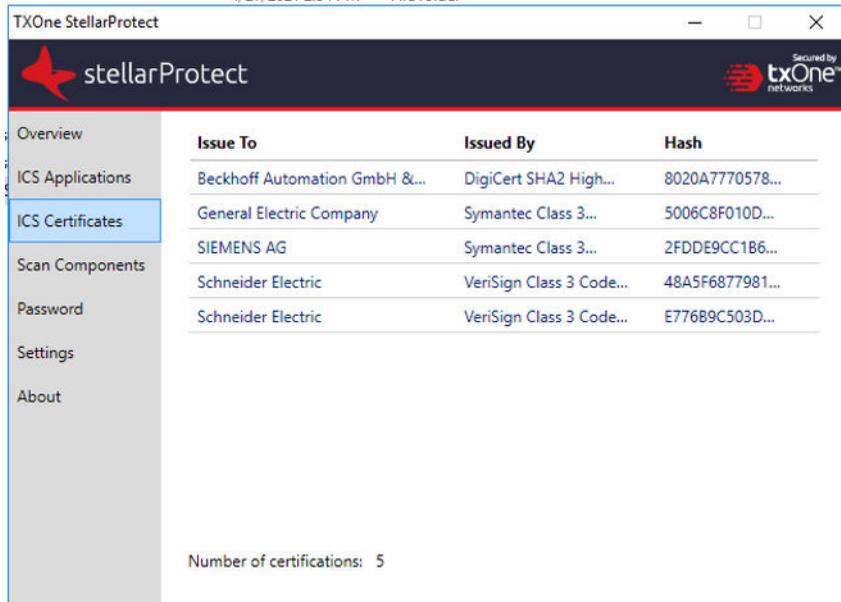


ICS Certificates

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.

The number of ICS certificates that StellarProtect can recognize will increase with 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 for management.



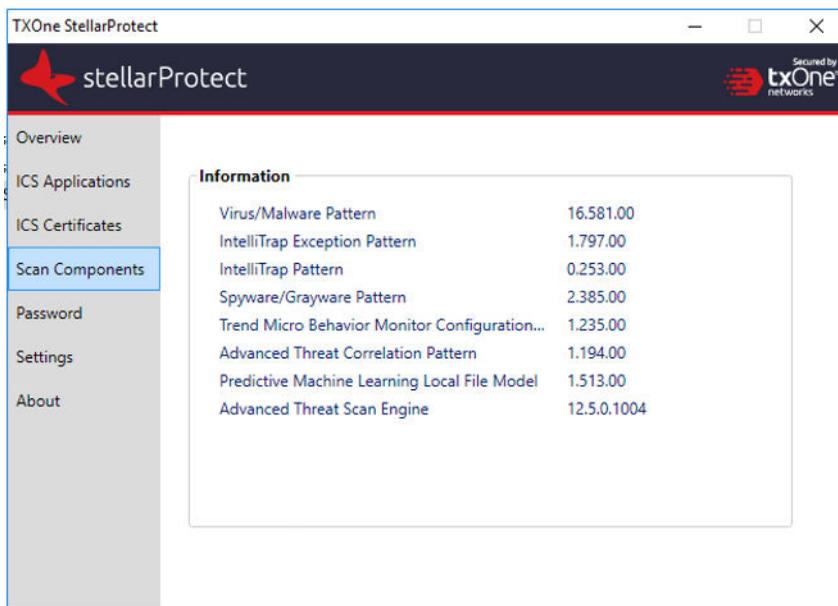
The screenshot shows the TXOne StellarProtect application window. The title bar reads "TXOne StellarProtect". The interface features a dark header with the "stellarProtect" logo and a "Secured by txOne networks" badge. A left-hand navigation menu includes "Overview", "ICS Applications", "ICS Certificates" (highlighted), "Scan Components", "Password", "Settings", and "About". The main content area displays a table of certificates with the following data:

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...

At the bottom of the main content area, it states "Number of certifications: 5".

Scan Components

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

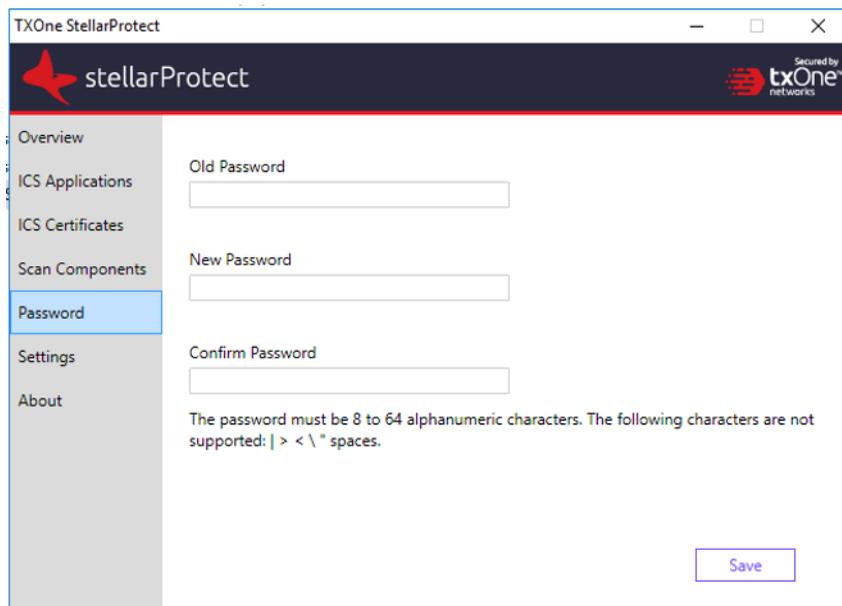


Information	
Virus/Malware Pattern	16.581.00
IntelliTrap Exception Pattern	1.797.00
IntelliTrap Pattern	0.253.00
Spyware/Grayware Pattern	2.385.00
Trend Micro Behavior Monitor Configuration...	1.235.00
Advanced Threat Correlation Pattern	1.194.00
Predictive Machine Learning Local File Model	1.513.00
Advanced Threat Scan Engine	12.5.0.1004

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 the TXOne StellarProtect web interface. The window title is "TXOne StellarProtect". The interface features a dark header with the "stellarProtect" logo and "Secured by txOne networks" branding. A left-hand navigation menu includes "Overview", "ICS Applications", "ICS Certificates", "Scan Components", "Password" (highlighted in blue), "Settings", and "About". The main content area is titled "Password" and contains three input fields: "Old Password", "New Password", and "Confirm Password". Below these fields, a message states: "The password must be 8 to 64 alphanumeric characters. The following characters are not supported: | > < \ " spaces." A "Save" button is located at the bottom right of the form.

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 false alarms.

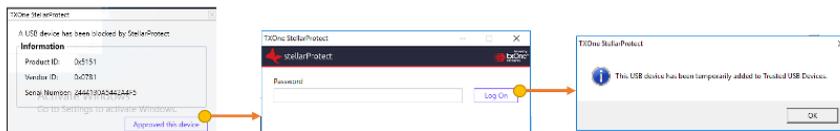
USB Vector Control

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.

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



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

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.

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

DLL Injection Prevention

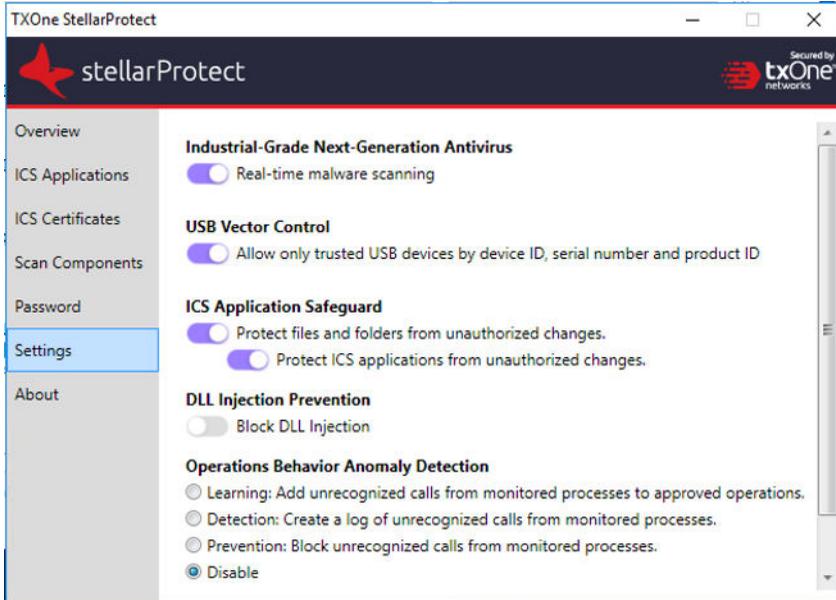
DLL injection is a high-risk attack in the ICS field, and StellarProtect can prevent this type of attack when this feature is enabled.

**Note**

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

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.



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 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.

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

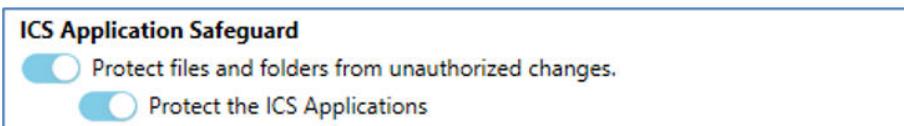


ICS Application SafeGuard

This function 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 monitor and protect the files and folders defined by the user on StellarOne.

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.

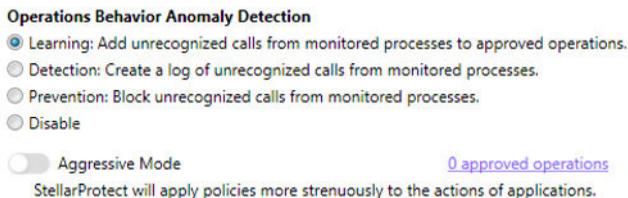
Operations Behavior Anomaly Detection

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 web console.

This function has four modes, including:

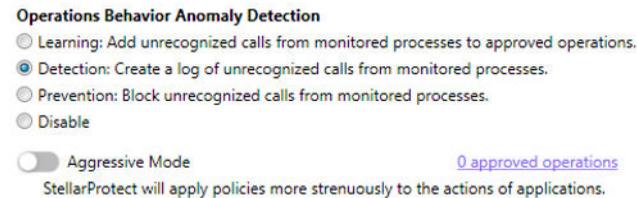
- **Learning Mode**

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.



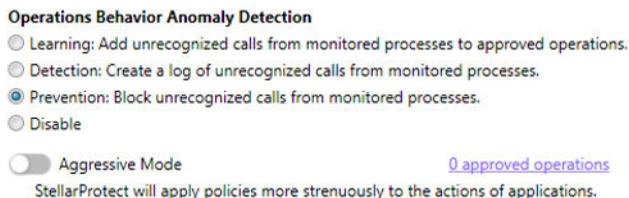
- **Detection Mode**

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



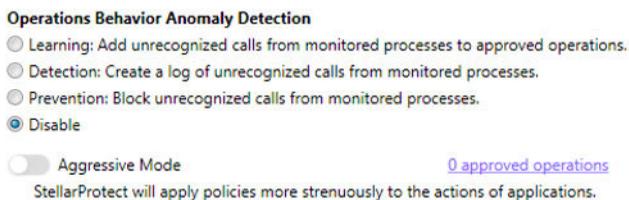
- **Prevention Mode**

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



- **Disabled Mode**

When **Operations Behavior Anomaly Detection** is set to **Disable**, protection is turned off.



The Operations Behavior Anomaly Detection function additionally has an **Aggressive Mode**, and can activate protection through process parameter recognition.

Users can check the process and parameters under monitoring.

DLL Injection Prevention

This feature specifically prevents DLL injection-based attacks.

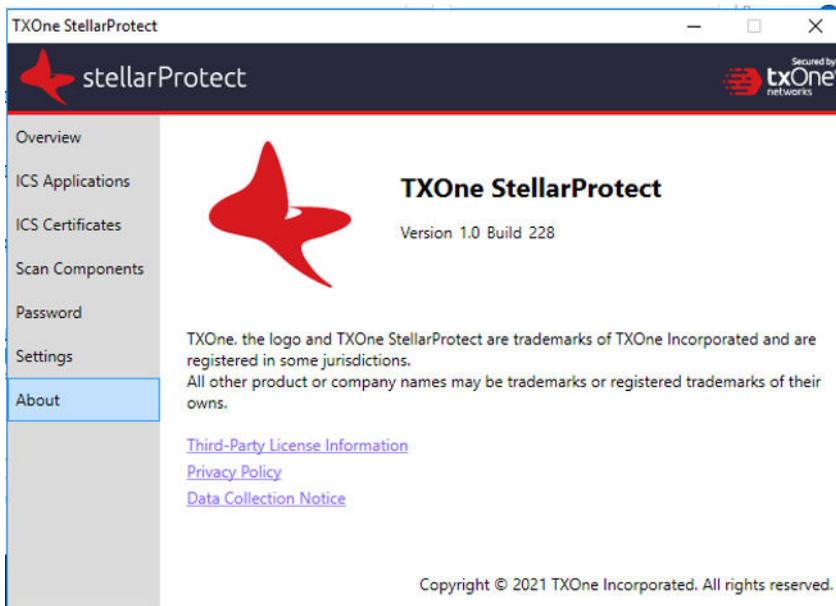


**Note**

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

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 2-18](#).

- 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>opcmd.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>opcmd.exe -p appinv make</code>	The StellarProtect service will re-detect installed ICS applications when your scheduled change window ends. You can also use this command to perform the detection manually at any time.	None
<code>opcmd.exe appinv list</code>	You can browse the list of detected ICS applications from the GUI program or use this command to get the list in YAML format.	None

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

COMMAND	DESCRIPTION	OPTIONS
<code>opcmd.exe -p lock appinv disable</code>	Enables ICS Application Inventory protection.	None
<code>opcmd.exe -p lock disable [-d DURATION] [-s START-TIME]</code>	<p>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.</p> <p>If <code>-d</code> is not specified, ICS application safeguard will be disabled until it is manually enabled. If <code>-s</code> is not specified, the ICS application safeguard is disabled immediately. Only one change window can be scheduled at a time, and new settings from the CLI or policy settings will always overwrite previous settings.</p>	<p><code>-d, --duration DURATION</code>: Required argument. Specifies the duration of a change window. ICS application safeguard is re-enabled after the change window duration has elapsed. Duration is specified in hours, minutes, or both. (ex. <code>-d 30m</code>, <code>-d 2h</code>, <code>-d 2h30m</code>)</p> <p><code>-s, --start START-TIME</code>: Required argument. Specifies starting time of a change window. The <code>START-TIME</code> is in ISO8601 format without time zone. (ex. <code>-s 2021-04-14T18:00:00</code>)</p>
<code>opcmd.exe -p lock enable</code>	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.	None
<code>opcmd.exe -p oad disable</code>	Disables Operations Behavior Anomaly Detection.	None

COMMAND	DESCRIPTION	OPTIONS
<code>opcmd.exe -p oad enable -m MODE [-l LEVEL]</code>	Enables Operations Behavior Anomaly Detection.	<code>-m, --mode MODE</code> : Required argument. Enables Operations Behavior Anomaly Detection into a specific mode (<code>learning</code> , <code>detection</code> , <code>prevention</code>). <code>-l, --level LEVEL</code> Required argument. Sets the scan to be <code>normal</code> or <code>aggressive</code> .
<code>opcmd.exe -p oad info</code>	Shows information about Operations Behavior Anomaly Detection.	None
<code>opcmd.exe -p oad remove -i ID</code>	Removes approved operations from Operations Behavior Anomaly Detection.	<code>-i, --id ID</code> : Required argument. Integer operation ID.
<code>opcmd.exe password</code>	Allows administrator to change the administrator password from command line. You are required to enter the old password before setting a new password.	None
<code>opcmd.exe -p proxy get</code>	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 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>

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.	<code>-v, --vid VID</code> : Required argument. Specifies Vendor ID by hexadecimal string. <code>-p, --pid PID</code> : Required argument. Specifies Product ID by hexadecimal string. <code>-s --sn SN</code> : Required argument. Specifies serial number. <code>-o, --onetime</code> : Grants one time access to a USB device.

COMMAND	DESCRIPTION	OPTIONS
<code>opcmod.exe -p usb enable</code>	Enables USB Vector Control.	None
<code>opcmod.exe -p usb disable</code>	Disables USB Vector Control.	None
<code>opcmod.exe -p usb info -d DRIVE</code>	Show USB information of the specified drive.	<code>-d, --drive DRIVE</code> : Required argument. Specifies the drive path (ex. E:).
<code>opcmod.exe -p usb list</code>	Lists trusted USB devices.	None
<code>opcmod.exe -p usb remove [-v VID -p PID -s SN]</code>	Removes a trusted USB device.	<code>-v, --vid VID</code> : Required argument. Specifies Vendor ID by hexadecimal string. <code>-p, --pid PID</code> : Required argument. Specifies Product ID by hexadecimal string. <code>-s --sn SN</code> : Required argument. Specifies serial number.
<code>opcmod.exe -p usb status</code>	Shows USB Vector Control status.	None
<code>opcmod.exe -p quarantine show</code>	Shows the list of quarantined files.	None
<code>opcmod.exe -p quarantine restore [QUARANTINE-NAME]</code>	Restores the specified quarantined file.	None

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 List on page 6-2](#)*

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 List

EVENT ID	LEVEL	CATEGORY	EVENT CONTENT	EVENT DETAILS
0x0100	Information (0)	system (1)	Service started	
0x1100	Warning (1)	system (1)	Service stopped	
0x0101	Information (0)	system (1)	Policy applied successfully (Version: %version%)	
0x1101	Warning (1)	system (1)	Unable to apply policy (Version: %version%)	
0x0201	Information (0)	intelli_av (2)	ICS Inventory List Update Succeeded	
0x0202	Information (0)	intelli_av (2)	Real Time Scan Enabled	
0x2202	Critical (2)	intelli_av (2)	Real Time Scan Disabled	

EVENT ID	LEVEL	CATEGORY	EVENT CONTENT	EVENT DETAILS
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%

EVENT ID	LEVEL	CATEGORY	EVENT CONTENT	EVENT DETAILS
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%

EVENT ID	LEVEL	CATEGORY	EVENT CONTENT	EVENT DETAILS
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%

EVENT ID	LEVEL	CATEGORY	EVENT CONTENT	EVENT DETAILS
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%

EVENT ID	LEVEL	CATEGORY	EVENT CONTENT	EVENT DETAILS
0x1204	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%
0x1205	Warning (1)	intelli_av (2)	Suspicious Program Execution Blocked: %PATH%	Suspicious program execution was blocked. File Path: %PATH% File Hash: %STRING%
0x0300	Information (0)	anomaly_detect (3)	Operations Behavior Anomaly Detection Enabled	Mode: %Mode% Level: %Level%

EVENT ID	LEVEL	CATEGORY	EVENT CONTENT	EVENT DETAILS
0x1300	Warning (1)	anomaly_detect (3)	Operations Behavior Anomaly Detection Disabled	
0x0301	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%

EVENT ID	LEVEL	CATEGORY	EVENT CONTENT	EVENT DETAILS
0x0302	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%
0x1301	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: Detection

EVENT ID	LEVEL	CATEGORY	EVENT CONTENT	EVENT DETAILS
0x1302	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: 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	Information (0)	device_control (5)	USB Vector Control Enabled	
0x1500	Warning (1)	device_control (5)	USB Vector Control Disabled	

EVENT ID	LEVEL	CATEGORY	EVENT CONTENT	EVENT DETAILS
0x0501	Information (0)	device_control (5)	Trusted USB Device Added	Vendor ID: %HEX% Product ID: %HEX% Serial Number: %STRING% Type: permanent or onetime
0x0502	Information (0)	device_control (5)	Trusted USB Device Removed	Vendor ID: %HEX% Product ID: %HEX% Serial Number: %STRING%
0x1501	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%

EVENT ID	LEVEL	CATEGORY	EVENT CONTENT	EVENT DETAILS
0x1102	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%
0x0102	Information (0)	system (1)	Patch applied. File Name: %file_name%	Patch applied. File Name: %file_name%
0x1103	Warning (1)	system (1)	Unable to apply patch. File Name: %file_name%	Unable to apply patch. File Name: %file_name% Error Code: %err_code%

Chapter 7

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.

Learn about the following topics:

- *[Troubleshooting Resources on page 7-2](#)*
- *[Contacting Trend Micro 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> 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	https://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:
<https://www.trendmicro.com/us/about-us/contact/index.html>
- 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.

Documentation Feedback

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

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

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



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: SLEM19396/210826