



1.0 TXOne StellarEnforce™ Installation Guide

The trust list-based solution for locking down fixed-function computers

Windows



Endpoint Security

TXOne Networks StellarEnforce™ 1.0 Agent Installation 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, StellarEnforce, 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.: SLEM18967/200414

Release Date: March 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 Trend Micro Knowledge Base.

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

Evaluate this documentation on the following site:

<http://docs.txone-networks.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 StellarEnforce 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	iii
About the Documentation	iii
Audience	iv
Document Conventions	iv

Chapter 1: Introduction

About TXOne StellarEnforce	1-2
What's New	1-2
Agent Features and Benefits	1-3
System Requirements	1-5
Agent Use Overview	1-13

Chapter 2: Local Agent Installation

Local Installation Overview	2-2
Installing from Windows	2-3
Setting Up the Approved List	2-10
Installation Using the Command Line	2-13
Installer Command Line Interface Parameters	2-14
Customizing Installation Parameters	2-17
Setup.ini File Arguments	2-18

Chapter 3: Agent Configuration File Deployment

Deployment for Standalone Agents	3-2
Exporting or Importing a Configuration File	3-2
Deployment using StellarOne	3-3
Remotely Exporting Agent Settings	3-3
Remotely Importing Agent Settings	3-4

Chapter 4: Local Agent Uninstallation

Uninstalling Agents from Windows	4-2
--	-----

Chapter 5: Technical Support

Troubleshooting Resources	5-2
Using the Support Portal	5-2
Threat Encyclopedia	5-2
Contacting Trend Micro	5-3
Speeding Up the Support Call	5-4
Sending Suspicious Content to Trend Micro	5-4
Email Reputation Services	5-4
File Reputation Services	5-5
Web Reputation Services	5-5
Other Resources	5-5
Download Center	5-5
Documentation Feedback	5-6

Index

Index	IN-1
-------------	------

Preface

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

Topics in this chapter include:

- *[About the Documentation on page iii](#)*
- *[Audience on page iv](#)*
- *[Document Conventions on page iv](#)*

About the Documentation

TXOne StellarEnforce documentation includes the following:

TABLE 1. TXOne StellarEnforce Documentation

DOCUMENTATION	DESCRIPTION
Installation Guide	A PDF document that discusses requirements and procedures for installing StellarEnforce.
Administrator's Guide	A PDF document that discusses getting started information and StellarEnforce 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 StellarEnforce documentation is intended for administrators responsible for StellarEnforce management, including agent installation. These users are expected to have advanced networking and server management knowledge.

Document Conventions

The following table provides the official terminology used throughout the TXOne StellarEnforce 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

CONVENTION	DESCRIPTION
 Important	Information regarding required or default configuration settings and product limitations
 WARNING!	Critical actions and configuration options

Chapter 1

Introduction

TXOne StellarEnforce 1.0 delivers a simple, no-maintenance solution to lock down and protect fixed-function computers, helping protect businesses against security threats and increase productivity.

Topics in this chapter include:

- *About TXOne StellarEnforce on page 1-2*

About TXOne StellarEnforce

TXOne StellarEnforce protects fixed-function computers like Industrial Control Systems (ICS), Point of Sale (POS) terminals, and kiosk terminals from malicious software and unauthorized use. By using fewer resources and without the need for regular software or system updates, StellarEnforce can reliably secure computers in industrial and commercial environments with little performance impact or downtime.

What's New

TXOne StellarEnforce 1.0 includes the following new features and enhancements.

TABLE 1-1. What's New in TXOne StellarEnforce 1.0

FEATURE	DESCRIPTION
Agent event aggregation	StellarEnforce agent generates a large volume of event logs about activities and incidents, which will now aggregate with better efficiency.
Central console support for agents with dynamic IPs	Agent information (IP address, MAC address, system info, and version info) will be updated periodically during this sync period.
Maintenance Mode now has a summary event	When Maintenance Mode finishes its tasks, it will now have a summary log with final file counts of success or failure to add to the trust list, as well as failed or succeeded actions with infected files.
AU security improved	The AU client is updated with: <ul data-bbox="537 1149 1059 1291" style="list-style-type: none">• Enable HTTPS connection• Disable TLS 1.0/1.1 for HTTPS connection• Enable digital signature checking for downloading from the Global AU server

FEATURE	DESCRIPTION
Intelligent Runtime Learning	If this function is turned on, the Agent will allow run-time execution files that are generated by applications on the Trust List.
Maintenance Mode time sync improved	Maintenance Mode now starts based on specific time periods, measured in 0 to 999 hours.

Agent Features and Benefits

StellarEnforce includes the following features and benefits.

Application Lockdown

By preventing programs, DLL files, drivers, and scripts not specifically on the Approved List of applications from running (also known as application trust listing), StellarEnforce provides both improved productivity and system integrity by blocking malicious software and preventing unintended use.

StellarEnforce write protection blocks modification and deletion of files, folders, and registry entries.

Exploit Prevention

Known targeted threats like Downad and Stuxnet, as well as new and unknown threats, are a significant risk to ICS and kiosk computers. Systems without the latest operating system updates are especially vulnerable to targeted attacks.

StellarEnforce provides both intrusion prevention, which helps prevent threats from spreading to the endpoint, and execution prevention, which helps prevent threats from spreading to the endpoint or from running.

Approved List Management

When software needs to be installed or updated, you can use one of the following methods to make changes to the endpoint and automatically add

new or modified files to the Approved List, all without having to unlock TXOne StellarEnforce:

- Maintenance Mode
- Trusted Updater
- Predefined Trusted Updater List
- Command Line Interface (CLI):
 - Trusted hash
 - Trusted certification

Small Footprint

Compared to other endpoint security solutions that rely on large pattern files that require constant updates, application lockdown uses less memory and disk space, without the need to download updates.

Role Based Administration

TXOne StellarEnforce provides a separate administrator and Restricted User account, providing full control during installation and setup, as well as simplified monitoring and maintenance after deployment.

Graphical and Command Line Interfaces

Anyone who needs to check the software can use the console, while system administrators can take advantage of the command line interface (CLI) to access all of the features and functions available.

Self Protection

Self Protection provides ways for TXOne StellarEnforce to defend its processes and resources, required to function properly, from being disabled by programs or actual users.

Self Protection blocks all attempts to terminate the following services:

- Trend Micro Unauthorized Change Prevention Service (TMBMSRV.exe)
- Trend Micro Personal Firewall (TmPfw.exe)
- TXOne StellarEnforce Service (WkSrv.exe)

System Requirements

This section introduces StellarEnforce system requirements.

Hardware Requirements

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

TABLE 1-2. Required Hardware for StellarEnforce

HARDWARE/SOFTWARE	DESCRIPTION
Available disk space	200MB minimum 300MB recommended
Monitor resolution	640x480



Important

StellarEnforce cannot be installed on a system that already runs one of the following:

- Trend Micro OfficeScan
- Trend Micro Titanium
- Other Trend Micro endpoint solutions

Operating Systems



Important

Ensure that the following root certification authority (CA) certificates are installed with intermediate CAs, which are found in `WKSrv.exe`. These root CAs should be installed on the StellarEnforce agent environment to communicate with StellarOne.

- Intermediate_Symantec Class 3 SHA256 Code Signing CA
- Root_VeriSign Class 3 Public Primary Certification Authority - G5
- DigiCert Assured ID Root CA

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

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



Note

- Memory Randomization, API Hooking Prevention, and DLL Injection Prevention are not supported on 64-bit platforms.
 - See the latest StellarEnforce readme file for the most up-to-date list of supported operating systems for agents.
-

Windows clients:

- Windows 2000 SP4 (32-bit)

**Note**

StellarEnforce installed on Windows 2000 SP4 (without update rollup) or Windows XP SP1 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, Maintenance Mode, and Predefined Trusted Updater.

To support these features, install Filter Manager:

- For Windows 2000 Service Pack 4, apply the update KB891861 from the Microsoft Update Catalog website.
- For Windows XP SP1, upgrade to Windows XP SP2.

-
- Windows XP SP1*/SP2/SP3 (32-bit) (except Starter and Home editions)

**Note**

- StellarEnforce installed on Windows 2000 SP4 (without update rollup) or Windows XP SP1 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, Maintenance Mode, and Predefined Trusted Updater.
- StellarEnforce does not support a custom action of “quarantine” on Windows XP.

-
- Windows Vista No-SP/SP1/SP2 (32-bit) (except Starter and Home editions)
 - Windows 7 No-SP/SP1 (32-bit and 64-bit) (except Starter and Home editions)
 - Windows 8 No-SP (32-bit and 64-bit)
 - Windows 8 No-SP (Professional/Enterprise) (32-bit and 64-bit)
 - Windows 8.1 No-SP (Professional/Enterprise with Bing) (32-bit and 64-bit)
 - Windows 8.1 No-SP (32-bit and 64-bit)

- Windows 10 (Professional/Enterprise/IoT Enterprise) (32-bit and 64-bit)
 - Anniversary Update (Redstone 1)
 - Creators Update (Redstone 2)
 - Fall Creators Update (Redstone 3)
 - April 2018 Update (Redstone 4)
 - October 2018 Update (Redstone 5)
 - May 2019 Update (19H1)
 - November 2019 Update (19H2)
 - May 2020 Update (20H1)
 - Oct 2020 Update (20H2)

**Note**

- Unlock the endpoint before updating your Windows 10 operating system to the Anniversary Update, Creators Update, Fall Creators Update, April 2018 Update, October 2018 Update, or later versions.
 - OneDrive integration in Windows 10 Fall Creators Update, Spring Creators Update, or later versions is not supported. Ensure that OneDrive integration is disabled before installing StellarEnforce.
 - To improve performance, disable the following Windows 10 components:
 - Windows Defender Antivirus. This may be disabled via group policy.
 - Window Update. Automatic updates may require the download of large files which may affect performance.
 - Windows Apps (Microsoft Store) auto-update. Checking for frequent updates may cause performance issues.
 - In Windows 10 April 2018 Update (Redstone 4) and later, StellarEnforce has the following limitations when working with folders where the `case sensitive` attribute has been enabled:
 - Enabling the `case sensitive` attribute for a folder may prevent StellarEnforce from performing certain actions (eg. `prescan`, custom actions) on that folder. Folders that do not have the attribute enabled are not affected.
 - StellarEnforce blocks all processes started from folders where the `case sensitive` attribute is enabled. Additionally, StellarEnforce is unable to provide any information for the blocked processes, except for file path.
 - The StellarEnforce agent cannot verify file signatures of files saved in folders where the `case sensitive` attribute is enabled. As a result, DAC exceptions related to signatures cannot work.
-

Windows Server:

- Windows 2000 Server SP4* (32-bit)

**Note**

StellarEnforce installed on Windows 2000 SP4 (without update rollup) or Windows XP SP1 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, Maintenance Mode, and Predefined Trusted Updater.

- Windows Server 2003 SP1/SP2 (32-bit)
-

**Note**

- StellarEnforce installed on Windows 2000 SP4 (without update rollup) or Windows XP SP1 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, Maintenance Mode, and Predefined Trusted Updater.
-

- Windows Server 2003 R2 No-SP/SP2 (Standard/Enterprise/Storage) (32-bit)
-

**Note**

- StellarEnforce installed on Windows 2000 SP4 (without update rollup) or Windows XP SP1 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, Maintenance Mode, and Predefined Trusted Updater.
-

- Windows Server 2008 SP1/SP2 (32-bit and 64-bit)
- Windows Server 2008 R2 No-SP/SP1 (64-bit)
- Windows Server 2012 No-SP (64-bit)
- Windows Server 2012 R2 No-SP (64-bit)
- Windows Server 2016 (Standard) (64-bit)
- Windows Server 2019 (Standard) (64-bit)

Windows Embedded Standard:

- Windows (Standard) XP Embedded SP1*/SP2 (32-bit)

**Note**

- StellarEnforce installed on Windows 2000 SP4 (without update rollup) or Windows XP SP1 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, Maintenance Mode, and Predefined Trusted Updater.
- StellarEnforce does not support a custom action of “quarantine” on Windows XP.

-
- Windows Embedded Standard 2009 (32-bit)
 - Windows Embedded Standard 7 (32-bit and 64-bit)
 - Windows Embedded Standard 8 (32-bit and 64-bit)
 - Windows Embedded 8 Standard No-SP (32-bit and 64-bit)
 - Windows Embedded Standard 8.1 (32-bit and 64-bit)
 - Windows Embedded 8.1 Standard (Professional/Industry Pro) (32-bit and 64-bit)

Windows Embedded POSReady:

- Windows Embedded POSReady (32-bit)
- Windows Embedded POSReady 2009 (32-bit)
- Windows Embedded POSReady 7 (32-bit and 64-bit)

Windows Embedded Enterprise:

- Windows Embedded Enterprise XP SP1*/SP2/SP3 (32-bit)



- StellarEnforce installed on Windows 2000 SP4 (without update rollup) or Windows XP SP1 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, Maintenance Mode, and Predefined Trusted Updater.
-

- Windows Embedded Enterprise Vista (32-bit)
- Windows Embedded Enterprise 7 (32-bit and 64-bit)

Windows Embedded Server:

- Windows Embedded Server 2003 SP1/SP2 (32-bit)
-



- StellarEnforce installed on Windows 2000 SP4 (without update rollup) or Windows XP SP1 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, Maintenance Mode, and Predefined Trusted Updater.
-

- Windows Embedded Server 2003 R2 (32-bit)
-



- StellarEnforce installed on Windows 2000 SP4 (without update rollup) or Windows XP SP1 does not support the following functions: DLL/Driver Lockdown, Script Lockdown, Integrity Monitoring, USB Malware Protection, Storage Device Blocking, Maintenance Mode, and Predefined Trusted Updater.
-

- Windows Embedded Server 2008 (32-bit and 64-bit)
- Windows Embedded Server 2008 R2 (64-bit)
- Windows Embedded Server 2012 (64-bit)

- Windows Embedded Server 2012 R2 (64-bit)

Windows Storage Server

- Windows Storage Server 2012 Standard (64-bit)
- Windows Storage Server 2012 R2 Standard (64-bit)
- Windows Storage Server 2016

Agent Use Overview

TXOne StellarEnforce is a trust list-based solution that locks down computers, preventing all applications not on the Approved List from running. StellarEnforce can be configured and maintained using the graphical user interface (GUI) agent console or the command line interface (CLI). System updates can be applied without turning off Application Lockdown at the endpoint through Maintenance Mode, trust hash, trust certification, predefined trusted updater list or by using the Trusted Updater.

Consider this typical use case scenario:

1. Set up the Approved List and turn on Application Lockdown on the endpoint so that unapproved applications cannot be run.
2. Use Maintenance Mode, trust hash, trust certification, predefined trusted updater list or by using the Trusted Updater to update or install software.
3. Configure and enable the Restricted User account for later maintenance.

If someone tries to run an application not specifically on the Approved List, the following message displays:



FIGURE 1-1. TXOne StellarEnforce blocking message

Chapter 2

Local Agent Installation

This chapter describes local TXOne StellarEnforce agent installation and setup procedures.

Topics in this chapter include:

- *Local Installation Overview on page 2-2*
- *Installing from Windows on page 2-3*
- *Setting Up the Approved List on page 2-10*
- *Installation Using the Command Line on page 2-13*
- *Customizing Installation Parameters on page 2-17*

Local Installation Overview

Procedure

1. Verify that the endpoint meets the TXOne StellarEnforce system requirements.

For details, see [System Requirements on page 1-5](#).

2. Install TXOne StellarEnforce using your preferred installation method.

TXOne StellarEnforce can be installed using either the Windows Installer or the command line interface (CLI) installer.

TABLE 2-1. StellarEnforce Local Installation Methods

INSTALLATION METHOD	BENEFITS
Windows Installer	The Windows Installer provides simplified step-by-step installation wizard for first-time or single installation and is also suitable for preparing for mass deployment for cloned endpoint systems. For details, see Installing from Windows on page 2-3 .
Command line interface installer	The command line interface (CLI) installer provides silent installation and can be integrated into a batch file for mass deployment. For details, see Installation Using the Command Line on page 2-13 .



Note

To customize installations using either the Windows Installer or the command line interface (CLI) installer, modify the `Setup.ini` file.

For details, see [Customizing Installation Parameters on page 2-17](#).

3. Configure the new installation.

- a. Open the TXOne StellarEnforce console and set up the Approved List.

Before TXOne StellarEnforce can protect the endpoint, it must check the endpoint for existing applications and files necessary for the system to run correctly.

For details, see [Setting Up the Approved List on page 2-10](#).

- b. Modify the TXOne StellarEnforce settings.
- c. (Optional) Deploy the updated settings to multiple agents.

To deploy settings to multiple TXOne StellarEnforce agents, use an agent configuration file.

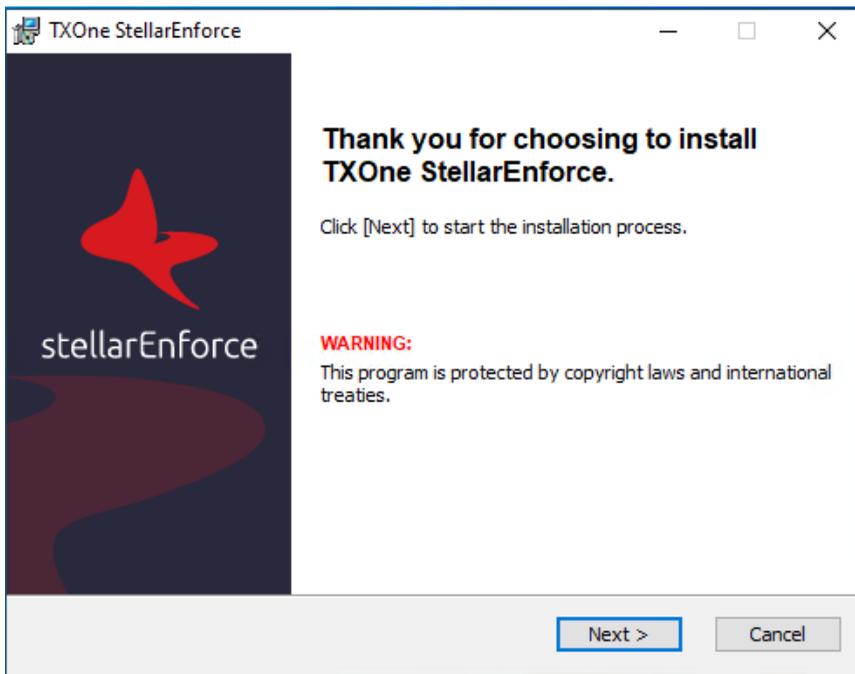
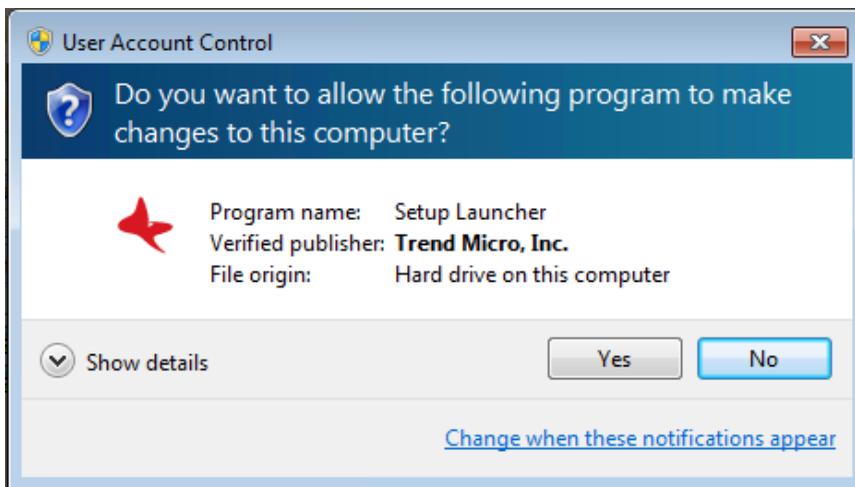
Installing from Windows

To install TXOne StellarEnforce, you must log on using an account with administrator privileges.

Procedure

1. Double-click `SL_Install.exe`.

If a **User Account Control** warning from Windows appears, click **Yes**.

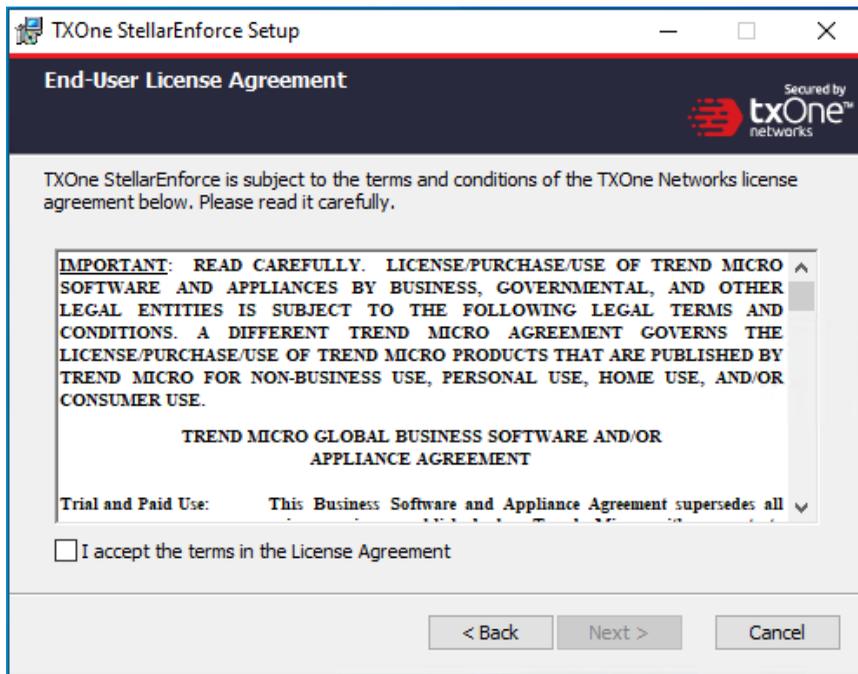


2. When the installation wizard opens, click **Next**.

**Note**

If there is another version of StellarEnforce on the endpoint, the installer will remove it before installing the latest version.

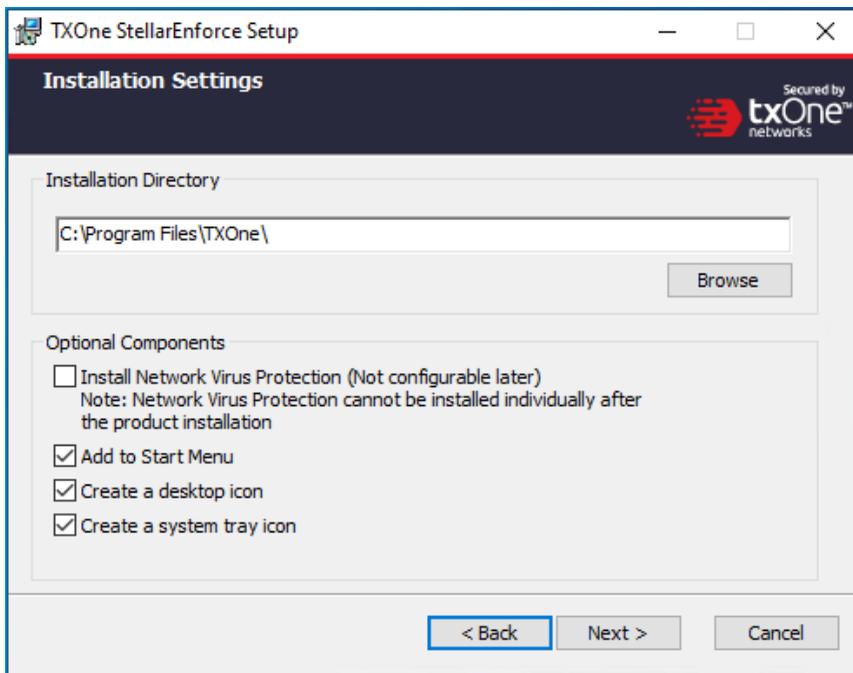
3. Read the license agreement, select **I accept the terms in the License Agreement**, and click **Next**.



4. Make any necessary changes to the installation options, and click **Next**.

**Important**

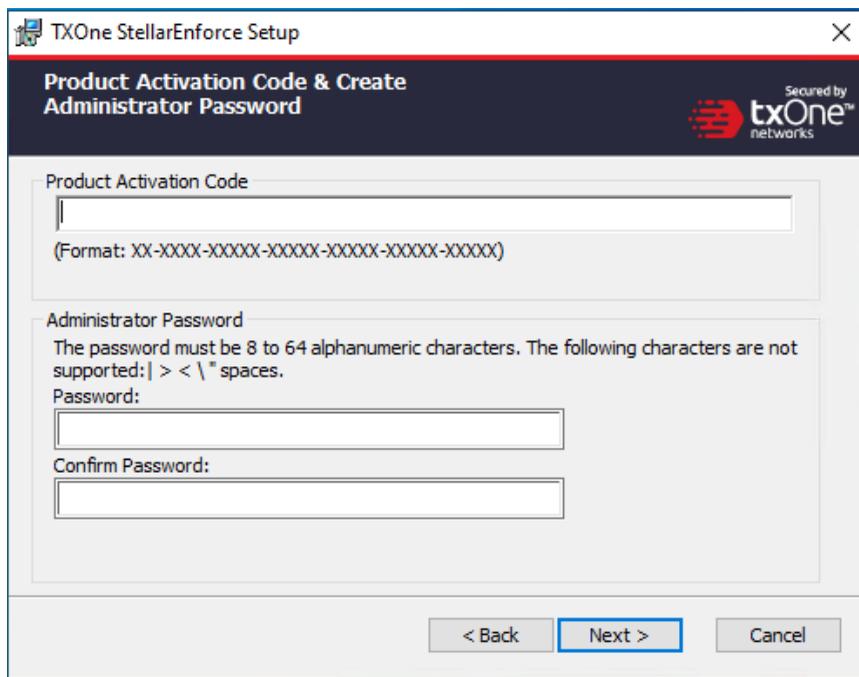
Network Virus Protection can only be installed during the initial program installation, but it can be disabled after installation, if necessary. See *Exploit Prevention Settings* in the Administrator's Guide for more information.



5. Provide the Activation Code and specify an administrator password for TXOne StellarEnforce.

**Note**

The password must be 8 to 64 alphanumeric characters. The following characters are not supported: | > < \ " spaces. The StellarEnforce administrator password is unrelated to the Windows administrator password.



The screenshot shows a window titled "TXOne StellarEnforce Setup" with a close button in the top right corner. The window has a dark blue header with the text "Product Activation Code & Create Administrator Password" and the TXOne Networks logo on the right, which includes the text "Secured by txOne networks".

The main content area is divided into two sections:

- Product Activation Code:** A text input field with a placeholder "(Format: XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX)".
- Administrator Password:** A section with the text "The password must be 8 to 64 alphanumeric characters. The following characters are not supported: | > < \ " * spaces." Below this are two text input fields labeled "Password:" and "Confirm Password:".

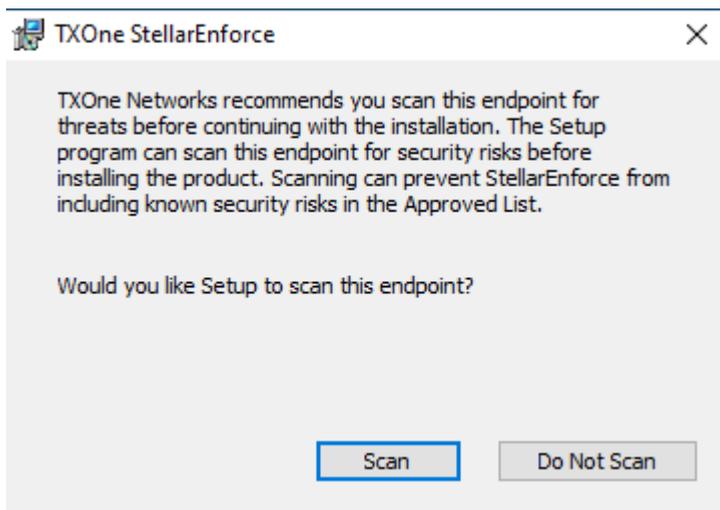
At the bottom of the window, there are three buttons: "< Back", "Next >" (which is highlighted with a blue border), and "Cancel".

**WARNING!**

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

6. Click **Next**.

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



7. (Optional) Scan the endpoint for threats before continuing with the installation. TXOne Networks recommends you perform this scan.
 - To scan the endpoint for threats, click **Scan**.
 - a. The **Endpoint Prescan** window appears.
 - b. To customize the scan settings, click **Edit Scan Settings**.
 - c. Click **Scan Now**.

If Endpoint Prescan detects security risks, TXOne Networks recommends canceling the installation. Remove threats from the endpoint and try again. If critical programs are detected as threats, confirm that the endpoint is secure and that the versions of the programs installed do not contain threats. Ignore detected threats only if you are absolutely certain that they are false positives.

**Note**

You cannot stop a scan process when you set the PRESCANCLEANUP and FORCE_PRESCAN options in the Setup.ini file.

For more information, see [Prescan Section on page 2-37](#).

**Tip**

Perform a manual scan to detect and remove threats on endpoints. For more information, see *Manual Scan Commands* in the Administrator's Guide.

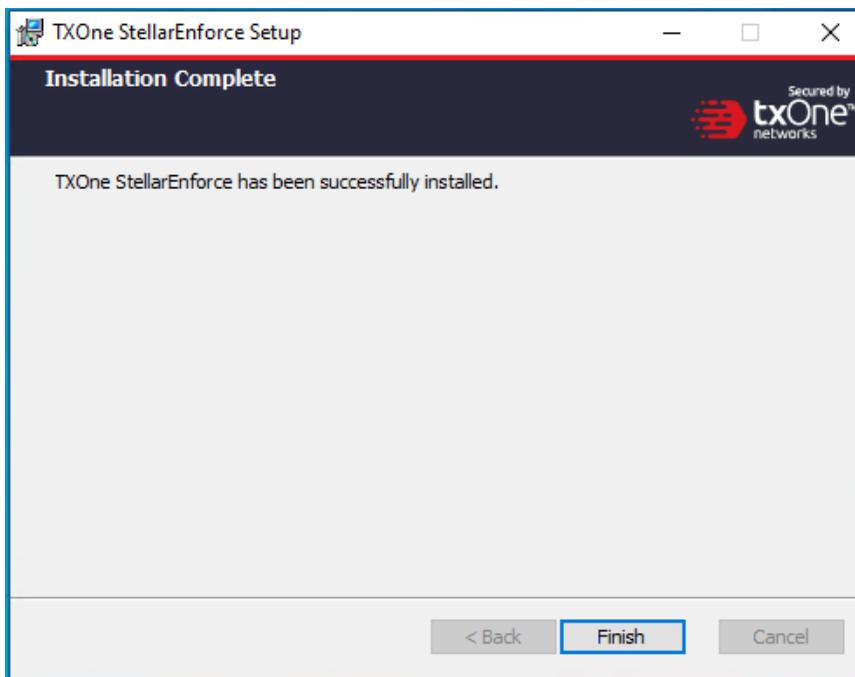
- To skip scanning, click **Do Not Scan**.

**Note**

The **Do Not Scan** and close buttons are not applicable when you set the PRESCANCLEANUP and FORCE_PRESCAN options in the Setup.ini file.

For more information, see [Prescan Section on page 2-37](#).

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

**Note**

Optionally enable memory randomization on older operating systems such as Windows XP or Windows Server 2003, which may lack or offer limited Address Space Layout Randomization (ASLR) support. See *Exploit Prevention Settings* in the Administrator's Guide for more information.

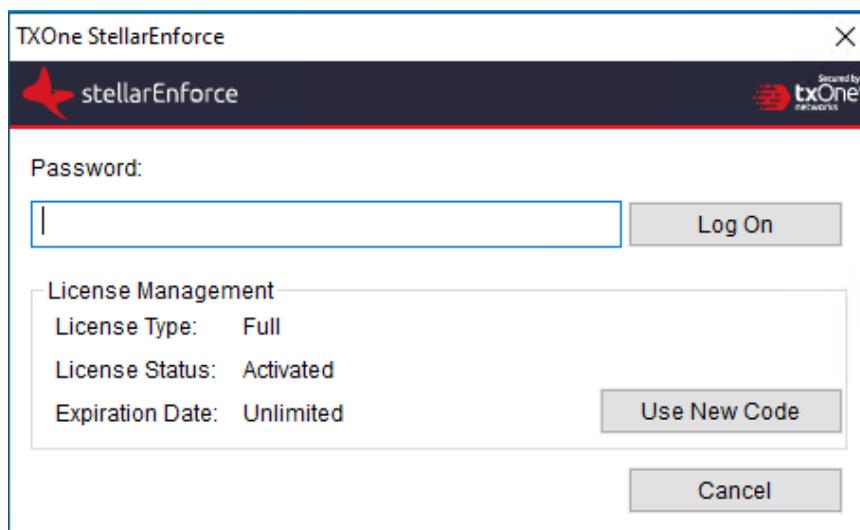
Setting Up the Approved List

Before TXOne StellarEnforce can protect the endpoint, it must check the endpoint for existing applications and files necessary for the system to run correctly.

Procedure

1. Open the StellarEnforce console.

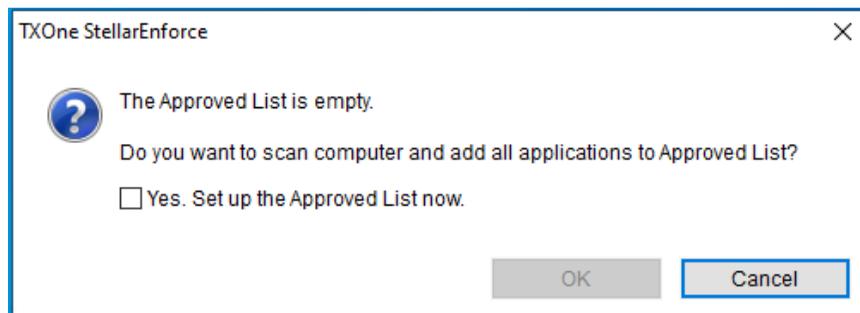
The StellarEnforce log on screen appears.



The screenshot shows the TXOne StellarEnforce login window. The title bar reads "TXOne StellarEnforce". The window features the StellarEnforce logo on the left and the "Secured By txOne" logo on the right. Below the logos, there is a "Password:" label followed by a text input field. To the right of the input field is a "Log On" button. Below the input field is a "License Management" section with the following details: "License Type: Full", "License Status: Activated", and "Expiration Date: Unlimited". To the right of these details is a "Use New Code" button. At the bottom right of the window is a "Cancel" button.

2. Provide the password and click **Login**.

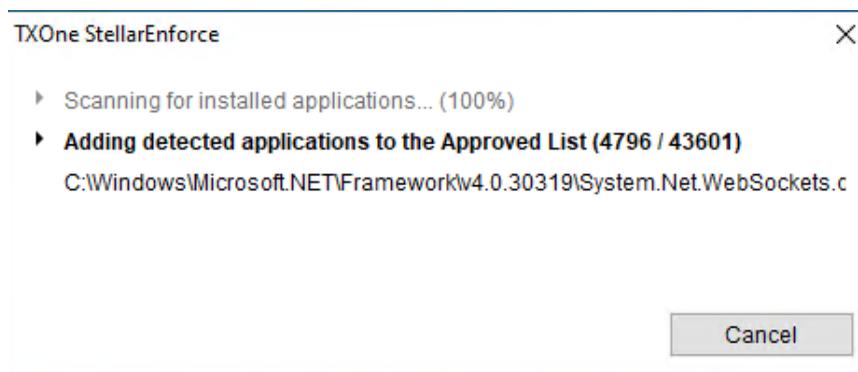
StellarEnforce asks if you want to set up the Approved List now.



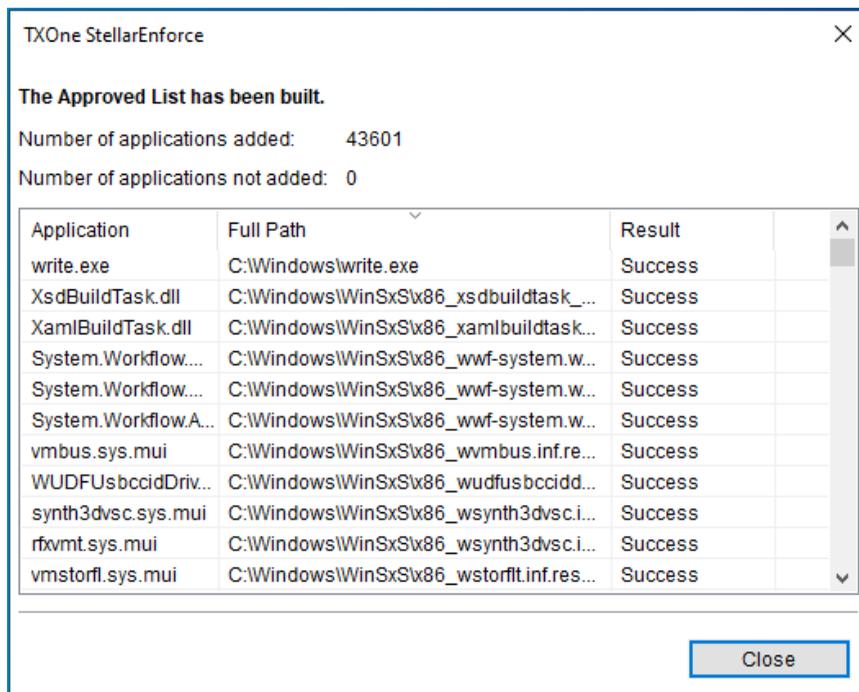
The screenshot shows a dialog box titled "TXOne StellarEnforce". It contains a question mark icon and the text: "The Approved List is empty. Do you want to scan computer and add all applications to Approved List?". Below this text is a checkbox labeled "Yes. Set up the Approved List now.". At the bottom right of the dialog box are two buttons: "OK" and "Cancel".

3. At the notification window, select **Yes. Set up the Approved List now** and click **OK**.

StellarEnforce scans the endpoint and adds all applications to the Approved List.



StellarEnforce displays the Approved List Configuration Results.



Note

When TXOne StellarEnforce Application Lockdown is on, only applications that are in the Approved List will be able to run.

4. Click **Close**.

Installation Using the Command Line

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

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

**WARNING!**

- Please store your StellarEnforce administrator password carefully. If you lose your StellarEnforce administrator password, please contact TXOne Networks support.
 - Make sure to enable memory randomization on older operating systems such as Windows XP or Windows Server 2003, which may lack or offer limited Address Space Layout Randomization (ASLR) support. See *Exploit Prevention Settings* in the Administrator's Guide for more information.
-

**Important**

Network Virus Protection can only be installed during the initial program installation, but it can be disabled after installation, if necessary. See *Exploit Prevention Settings* in the Administrator's Guide for more information.

**Note**

The password must be 8 to 64 alphanumeric characters. The following characters are not supported: | > < \ " spaces. The StellarEnforce administrator password is unrelated to the Windows administrator password.

Installer Command Line Interface Parameters

The following table lists the commands available for `SL_Install.exe`.

TABLE 2-2. StellarEnforce Installer Command Line Options

PARAMETER	VALUE	DESCRIPTION
-q		<p>Run the installer silently</p> <hr/> <p> Note</p> <p>During the installation process, you can view the following log files in the folder C:\windows\temp to check the status of the the prescan and initial approved process:</p> <ul style="list-style-type: none"> • Prescan process: YYYYMMDDHHMMSS_wk_PreScanProgress.log • Initial approved process: YYYYMMDDHHMMSS_wk_InitListProgress.log
-p	<administrator_password>	Specify the administrator password
-d	<path>	Specify the installation path
-ac	<activation_code>	Specify the activation code
-nd		Do not create a desktop shortcut
-fw		Enable Network Virus Protection
-ns		Do not add a shortcut to the Start menu
-ni		Hide the task tray icon
-cp	<path>	<p>Specify the StellarEnforce configuration file</p> <hr/> <p> Note</p> <p>The StellarEnforce configuration file can be exported after installing StellarEnforce.</p>

PARAMETER	VALUE	DESCRIPTION
-lp	<path>	Specify the Approved List <hr/>  Note After installing StellarEnforce and creating the Approved List, the list can be exported.
-qp	<path>	Specify the folder path for quarantined files when custom action is set to “quarantine” mode
-nps		Do not execute Prescan
-ips		Do not cancel installation when Prescan detects threats

An example command line interface (CLI) install would look like this:

```
SL_Install.exe -q -ac XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX -p  
P@ssW0Rd -nd
```

**Important**

An administrator password and Activation Code must be specified for the installation to continue.

Customizing Installation Parameters



Note

The installer applies the specified arguments in the following order:

- Encrypted `setup.bin`
- Command line interface (CLI)
- `setup.ini`

If `setup.bin` exists, the installer applies the configuration in `setup.bin` takes precedence and ignores settings from the CLI and `setup.ini` file.

For example, if the switch `-nd` is added to `SL_Install.exe`, and `setup.ini` contains `NO_DESKTOP=0`, the switch will take precedence, and a StellarEnforce desktop shortcut will not be created.

To change the default installation parameters using a `Setup.ini` file, follow the steps below.

Procedure

1. Locate the `Setup.ini` file in the installation folder.
2. Customize the installation parameters as required.

For information on installation parameters and their possible values, see [Setup.ini File Arguments on page 2-18](#).

3. Optionally encrypt the `Setup.ini` file to prevent unauthorized access to important settings.
 - a. From the installation folder, copy the `Setup.ini` file and the `WKSupportTool.exe` file to your desktop.
 - b. Run a command prompt window as administrator.
 - c. Navigate to the desktop and type `WKSupportTool.exe encryptsetupini Setup.ini Setup.bin` to encrypt the `Setup.ini` file and name the encrypted file as "Setup.bin".

- d. Save the Setup.bin file in the installation folder and remove the Setup.ini file.

Setup.ini File Arguments



Note

The installer applies the specified arguments in the following order:

- Encrypted setup.bin
- Command line interface (CLI)
- setup.ini

If setup.bin exists, the installer applies the configuration in setup.bin takes precedence and ignores settings from the CLI and setup.ini file.

For example, if the switch `-nd` is added to `SL_Install.exe`, and `setup.ini` contains `NO_DESKTOP=0`, the switch will take precedence, and a StellarEnforce desktop shortcut will not be created.

The following tables list the commands available for `setup.ini`. If no value is specified in the setup file, the default value will be used.

Property Section

The following table lists the commands available for `setup.ini`. If no value is specified in the setup file, the default value will be used.

TABLE 2-3. Setup.ini File [PROPERTY] Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
ACTIVATION_CODE	Activation Code	<activation_code>	<empty>	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
NO_DESKTOP	Create a shortcut on desktop	<ul style="list-style-type: none"> • 0: Create shortcut • 1: Do not create shortcut 	0	No
NO_STARTMENU	Create a shortcut in the Start menu	<ul style="list-style-type: none"> • 0: Create shortcut • 1: Do not create shortcut 	0	No
NO_SYSTRAY	Display the system tray icon and Windows notifications	<ul style="list-style-type: none"> • 0: Create system tray icon • 1: Do not create system tray icon 	0	No
NO_NSC	Install firewall for network virus protection	<ul style="list-style-type: none"> • 0: Create firewall • 1: Do not create firewall 	1	No
CONFIG_PATH	Configuration file path	<path>	<empty>	No
LIST_PATH	Approved List path for import	<path>	<empty>	No
APPLICATION FOLDER	Installation path for agent program	<path>	<empty>	No
PASSWORD	Password which is used for SLCmd.exe and StellarOne	<password>	<empty>	No
CUSTOM_ACTION	Custom action for blocked events	<ul style="list-style-type: none"> • 0: Ignore • 1: Quarantine • 2: Ask server 	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
QUARANTINE_FOLDER_PATH	Quarantine path for agent program	<path>	<empty>	No
INTEGRITY_MONITOR	Enable Integrity Monitor	<ul style="list-style-type: none"> 0: Disable 1: Enable 	0	No
PREDEFINED_TRUSTED_UPDATER	Enable Predefined Trusted Updater	<ul style="list-style-type: none"> 0: Disable 1: Enable 	0	No
WINDOWS_UPDATE_SUPPORT	Enable Window Update Support	<ul style="list-style-type: none"> 0: Disable 1: Enable 	0	No
PRESCAN	Prescan the endpoint before installing StellarEnforce	<ul style="list-style-type: none"> 0: Do not prescan the endpoint 1: Prescan the endpoint 	1	No
MAX_EVENT_DATABASE_SIZE	Maximum database file size (MB)	Positive integer	1024	No
WEL_SIZE	Windows Event Log size (KB)	Positive integer <hr/>  Note Default value for new installations. Upgrading StellarEnforce does not change any user-defined WEL_SIZE values set in the previous installation.	10240	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
WEL_RETENTION	Windows Event Log option when maximum event log size is reached on Windows Event Log	<p>For Windows XP or earlier platforms:</p> <ul style="list-style-type: none"> 0: Overwrite events as needed 1 - 365: Overwrite events older than (1-365) days -1: Do not overwrite events (Clear logs manually) <p>For Windows Vista or later platforms:</p> <ul style="list-style-type: none"> 0: Overwrite events as needed (oldest events first) 1: Archive the log when full, do not overwrite events -1: Do not overwrite events (Clear logs manually) 	0	No
WEL_IN_SIZE	Windows Event Log size for Integrity Monitor events (KB)	Positive integer	10240	No
WEL_IN_RETENTION	Windows Event Log option for when maximum event log size for Integrity Monitor events is reached in the	<p>For Windows XP or earlier platforms:</p> <ul style="list-style-type: none"> 0: Overwrite events as needed 	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
	Windows Event Log	<ul style="list-style-type: none"> 1 - 365: Overwrite events older than (1-365) days -1: Do not overwrite events (Clear logs manually) <p>For Windows Vista or later platforms:</p> <ul style="list-style-type: none"> 0: Overwrite events as needed (oldest events first) 1: Archive the log when full, do not overwrite events -1: Do not overwrite events (Clear logs manually) 		
USR_DEBUGLOG_ENABLE	Enable debug logging for user sessions	<ul style="list-style-type: none"> 0: Do not log 1: Log 	0	No
USR_DEBUGLOG_LEVEL	The number of debug log entries allowed for user sessions	<ul style="list-style-type: none"> 256 	256	No
SRV_DEBUGLOG_ENABLE	Enable debug logging for service sessions	<ul style="list-style-type: none"> 0: Do not log 1: Log 	0	No
SRV_DEBUGLOG_LEVEL	The number of debug log entries allowed	<ul style="list-style-type: none"> 256 	256	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
	for service sessions			
SILENT_INSTALL	Execute installation in silent mode	<ul style="list-style-type: none"> 0: Do not use silent mode 1: Use silent mode 	0	No
	 Important To use silent mode, you must also specify the ACTIVATION_CODE and PASSWORD keys and values. For example: [PROPERTY] ACTIVATION_CODE=XX-XXXXX-XXXXX-XXXXX-XXXXX PASSWORD=P@ssw0rd SILENT_INSTALL=1			
STORAGE_DEVICE_BLOCKING	Blocks storage devices, including CD/DVD drives, floppy disks, and USB devices, from accessing managed endpoints	<ul style="list-style-type: none"> 0: Allow access from storage devices 1: Block access from storage devices 	0	No
INIT_LIST	Initialize the Approved List during installation	<ul style="list-style-type: none"> 0: Do not initialize the Approved List during installation 1: Initialize the Approved List 	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		during installation		
	 Note LIST_PATH has priority over INIT_LIST. For example: [PROPERTY] LIST_PATH=liststore.db INIT_LIST=1 In this case, liststore.db is imported and INIT_LIST is ignored.			
INIT_LIST_PATH	A folder path to be traversed for the Approved List initialization Each local disk's root directory will be traversed if empty	<folder path>	<empty>	No
INIT_LIST_PATH_OPTIONAL	A folder path to be traversed for the Approved List initialization Each local disk's root directory will be traversed if empty	<folder path>	<empty>	No
INIT_LIST_EXCLUDED_FOLDER	An absolute folder path to exclude from automatic file	<folder path>	<empty>	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
	<p>enumeration for Approved List initialization</p> <p>The configuration applies to the Approved List first initialized and all subsequent Approved List updates</p> <p>Specify multiple folders by creating new entries with names that start with</p> <p>INIT_LIST_EXCLUDED_FOLDER. Ensure each entry name is unique. For example:</p> <p>INIT_LIST_EXCLUDED_FOLDER= c:\folder1</p> <p>INIT_LIST_EXCLUDED_FOLDER2= c:\folder2</p> <p>INIT_LIST_EXCLUDED_FOLDER3= c:\folder3</p>	<p> Note</p> <ul style="list-style-type: none"> Folder path supports a maximum length of 260 characters. Folder paths that do not exist may be specified. The exclusion applies to subfolders. 		
INIT_LIST_EXCLUDED_EXTENSION	A file extension to exclude from automatic file enumeration for	<file extension>	<empty>	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
	<p>Approved List initialization</p> <p>The configuration applies to the Approved List first initialized and all subsequent Approved List updates</p> <p>Specify multiple extensions by creating new entries with names that start with</p> <p>INIT_LIST_EXCLUDED_EXTENSION, while ensuring that each entry name is unique. For example:</p> <p>INIT_LIST_EXCLUDED_EXTENSION=bmp</p> <p>INIT_LIST_EXCLUDED_EXTENSION2=png</p>	<p> Note</p> <p>Specifying file extensions of executable files (e.g. exe, dll and sys) may cause issues with Application Lockdown.</p>		
LOCKDOWN	Turn Application Lockdown on after installation	<ul style="list-style-type: none"> • 0: Turn off Application Lockdown • 1: Turn on Application Lockdown 	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
FILELESS_ATTACK_PREVENTION	Enable the Fileless Attack Prevention feature	<ul style="list-style-type: none"> 0: Disable feature 1: Enable feature 	0	No
SERVICE_CREATION_PREVENTION	Enable the Service Creation Prevention feature	<ul style="list-style-type: none"> 0: Disable feature 1: Enable feature 	0	No
	<div style="border: 1px solid black; padding: 5px;">  Note StellarEnforce temporarily disables the Service Creation Prevention feature under the following conditions: <ul style="list-style-type: none"> Updating or installing new applications using installers allowed by Trusted Updater. The feature is automatically re-enabled after the Trusted Updater process is complete Enabling Windows Update Support Disabling Windows Update Support automatically re-enables the feature </div>			
USR_DEBUGLOG_ENABLE	Enable debug log in user session	<ul style="list-style-type: none"> 0: Disable debug log 1: Enable debug log 	0	No
USR_DEBUGLOG_LEVEL	Debug level in user session	273	273	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
SRV_DEBUGLOG_ENABLE	Enable debug log in service session	<ul style="list-style-type: none"> 0: Disable debug log 1: Enable debug log 	0	No
SRV_DEBUGLOG_LEVEL	Debug level in service session	<ul style="list-style-type: none"> 273 	273	No
FW_USR_DEBUGLOG	Enable debug log in user session of firewall	<ul style="list-style-type: none"> 0: Disable debug log 1: Enable debug log 	0	No
FW_USR_DEBUGLOG_LEVEL	Debug level in user session of firewall	number	273	No
FW_SRV_DEBUGLOG_ENABLE	Enable debug log in service session of firewall	<ul style="list-style-type: none"> 0: Disable debug log 1: Enable debug log 	0	No
FW_SRV_DEBUGLOG_LEVEL	Debug level in service session of firewall	number	273	No
BM_SRV_DEBUGLOG_ENABLE	Enable debug log of Behavior Monitoring Core service	<ul style="list-style-type: none"> 0: Disable debug log 1: Enable debug log 	0	No
BM_SRV_DEBUGLOG_LEVEL	Debug level of Behavior Monitoring Core service	<ul style="list-style-type: none"> 51 	51	No
INTELLIGENT_RUNTIME_LEARNING	The agent will allow runtime execution files	<ul style="list-style-type: none"> 0: Disable 1: Enable 	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
	that are generated by applications on the Approved List			

EventLog Section

The following table lists the commands available for `setup.ini`. If no value is specified in the setup file, the default value will be used.

TABLE 2-4. Setup.ini File [EVENTLOG] Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
ENABLE	Log events related to StellarEnforce	<ul style="list-style-type: none"> • 1: Log • 0: Do not log 	1	No
LEVEL_WARNINGLOG	Log “Warning” level events related to StellarEnforce	<ul style="list-style-type: none"> • 1: Log • 0: Do not log 	1	No
LEVEL_INFORMATIONLOG	Log “Information” level events related to StellarEnforce	<ul style="list-style-type: none"> • 1: Log • 0: Do not log 	0	No
BLOCKEDACCESSLOG	Log files blocked by StellarEnforce	<ul style="list-style-type: none"> • 1: Log • 0: Do not log 	1	No
APPROVEDACCESSLOG	Log files approved by StellarEnforce	<ul style="list-style-type: none"> • 1: Log • 0: Do not log 	1	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
APPROVEDACCESSLOG_TRUSTEDUPDATER	Log Trusted Updater approved access	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
APPROVEDACCESSLOG_TRUSTEDHASH	Log Trusted Hash approved access	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
APPROVEDACCESSLOG_DLLDRIVER	Log DLL/Driver approved access	<ul style="list-style-type: none"> 1: Log 0: Do not log 	0	No
APPROVEDACCESSLOG_EXCEPTIONPATH	Log Application Lockdown exception path approved access	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
APPROVEDACCESSLOG_TRUSTEDCERT	Log Trusted Certifications approved access	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
APPROVEDACCESSLOG_WRITEPROTECTION	Log Write Protection approved access	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
SYSTEMEVENTLOG	Log events related to the system	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
SYSTEMEVENTLOG_EXCEPTIONPATH	Log exceptions to Application Lockdown	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
SYSTEMEVENTLOG_WRITEPROTECTION	Log Write Protection events	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
LISTLOG	Log events related to the Approved list	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
USBMALWAREPROTECTIONLOG	Log events that trigger USB Malware Protection	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
EXECUTIONPREVENTIONLOG	Log events that trigger Execution Prevention	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
NETWORKVIRUSPROTECTIONLOG	Log events that trigger Network Virus Protection	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
INTEGRITYMONITORINGLOG_FILECREATED	Log file and folder created events	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
INTEGRITYMONITORINGLOG_FILEMODIFIED	Log file modified events	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
INTEGRITYMONITORINGLOG_FILEDELETED	Log file and folder deleted events	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
INTEGRITYMONITORINGLOG_FILERENAMED	Log file and folder renamed events	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
INTEGRITYMONITORINGLOG_REGVALUEMODIFIED	Log registry value modified events	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
INTEGRITYMONITORINGLOG_REGVALUEDELETED	Log registry value deleted events	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
INTEGRITYMONITORINGLOG_REGKEYCREATED	Log registry key created events	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
INTEGRITYMONITORINGLOG_REGKEYDELETED	Log registry key deleted events	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
INTEGRITYMONITORINGLOG_REGKEYRENAMED	Log registry key renamed events	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No
DEVICECONTROLLOG	Log events related to device access control	<ul style="list-style-type: none"> 1: Log 0: Do not log 	1	No

Server Section

The following table lists the commands available for `setup.ini`. If no value is specified in the setup file, the default value will be used.

TABLE 2-5. Setup.ini File [SERVER] Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
HOSTNAME	Server host name	<host_name>	<empty>	No
PORT_FAST	Server listen port for fast lane	1 - 65535	<empty>	No
CERT	Certificate file name	<certificate_file_name>	<empty>	No

Agent Section

The following table lists the commands available for `setup.ini`. If no value is specified in the setup file, the default value will be used.

TABLE 2-6. Setup.ini File [AGENT] Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
PORT	Agent listening port	1 - 65535	<empty>	No
FIXED_IP	Set the agent IP address to communicate with the StellarEnforce server	<ul style="list-style-type: none"> • A.B.C.D/E • A,B,C,D: 0~255 • E: 1~32 	<empty>	No

Maintenance Mode Section

The following table lists the commands available for `setup.ini`. If no value is specified in the setup file, the default value will be used.

TABLE 2-7. Setup.ini File [MAINTENANCEMODE] Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
ENABLE_DURATION	Start maintenance mode with this duration immediately after the install process is finished	0 - 999 Unit: Hours	0	No
SCAN	Enable file scanning after	<ul style="list-style-type: none"> • 0: No scan (default) • 1: Quarantine 	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
	the maintenance period	<p>StellarEnforce scans files that are created, executed, or modified during the maintenance period and quarantine detected files</p> <ul style="list-style-type: none"> 2: al <p>StellarEnforce scans files that are created, executed, or modified during the maintenance period and adds these files (including files that are detected as malicious) to the Approved List</p>		

Message Section

The following table lists the commands available for `setup.ini`. If no value is specified in the setup file, the default value will be used.

TABLE 2-8. Setup.ini File [MESSAGE] Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
INITIAL_RETRY_INTERVAL	Starting interval, in seconds, between attempts to	<ul style="list-style-type: none"> 0 ~ 2147483647 	120	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
	<p>resend an event to StellarOne</p> <p>This interval doubles in size for each unsuccessful attempt, until it exceeds the MAX_RETRY_INTERVAL value</p>			
MAX_RETRY_INTERVAL	<p>Maximum interval, in seconds, between attempts to resend events to StellarOne</p>	<ul style="list-style-type: none"> 0 ~ 2147483647 	7680	No
REGULAR_STAT US_UPDATE	<p>Agent information will be updated periodically during this sync period:</p> <ul style="list-style-type: none"> IP address & MAC address System info Version info <p>The sync group policy timer default value is 20 minutes</p>	<p>0 : Disable</p> <p>1 : Enable</p>	0	No

MessageRandomization Section



Note

StellarEnforce agents respond as soon as possible to direct requests from StellarOne. For details, refer to Applying Message Time Groups in the StellarEnforce Administrator's Guide.

The following table lists the commands available for `setup.ini`. If no value is specified in the setup file, the default value will be used.

TABLE 2-9. Setup.ini File [MESSAGERANDOMIZATION] Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
TOTAL_GROUP_NUM	Number of groups controlled by the server	0 - 2147483646	0	No
OWN_GROUP_IN_DEX	Index of group which this agent belongs to	0 - 2147483646	0	No
TIME_PERIOD	Maximum amount of time agents have to upload data (in seconds)	0 - 2147483647	0	No

Proxy Section

The following table lists the commands available for `setup.ini`. If no value is specified in the setup file, the default value will be used.

TABLE 2-10. Setup.ini File [PROXY] Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
MODE	Proxy mode	<ul style="list-style-type: none"> • 0: No proxy used • 1: Proxy used with manual settings • 2: Proxy used with settings retrieved from Internet Explorer automatically 	0	No
HOSTNAME	Proxy host name	<host_name>	<empty>	No
PORT	Proxy port	1 - 65535	<empty>	No
USERNAME	Proxy user name	<user_name>	<empty>	No
PASSWORD	Proxy password	<password>	<empty>	No

Prescan Section

The following table lists the commands available for `setup.ini`. If no value is specified in the setup file, the default value will be used.

TABLE 2-11. Setup.ini File [PRESCAN] Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
IGNORE_THREAT	Cancel installation after detecting malware threat during prescan	<ul style="list-style-type: none"> • 0: Cancel • 1: Continue installation after detecting malware threat during prescan • 2: Continue installation when 	2	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		no malware is detected, or after all detected malware is cleaned, deleted, or quarantined successfully without a system reboot		
REPORT_FOLDER	An absolute folder path where prescan result reports are saved	<ul style="list-style-type: none"> • <folder_path> • <empty>: Defaults to %windir%\temp\prescan\log 	<empty>	No
SCAN_TYPE	<p>The type of scan executed during silent installation</p> <hr/>  Note The selected value is used as the default value for a UI installation.	<ul style="list-style-type: none"> • Full: Scan all folders on the endpoint • Quick: Scans the following folders: <ul style="list-style-type: none"> • Fixed root drives For example: c:\ d:\ • System root folder For example, c:\Windows • System folder	Full	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		<p>For example, c:\Windows\System</p> <ul style="list-style-type: none"> • System32 folder <p>For example, c:\Windows\System32</p> <ul style="list-style-type: none"> • Driver folder <p>For example, c:\Windows\System32\Drivers</p> <ul style="list-style-type: none"> • Temp folder <p>For example, c:\Users\Trend\AppData\Local\Temp</p> <ul style="list-style-type: none"> • Desktop folder including sub folders and files <p>For example, c:\Users\Trend\Desktop</p>		

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		<ul style="list-style-type: none"> Specific: Scan folders specified with SPECIFIC_FOLDER entries 		
COMPRESS_LAYER	The number of compressed layers to scan when a compressed file is scanned	<ul style="list-style-type: none"> 0: Do not scan compressed files 1 - 20: Scan up to the specified number of layers of a compressed file 	2	No
MAX_FILE_SIZE	The largest file allowed for scan	<ul style="list-style-type: none"> 0: Scan files of any sizes 1 - 9999: Only scan files equal to or smaller than the specified size (MB) 	0	No
SCAN_REMOVABLE_DRIVE	Scan removable drives	<ul style="list-style-type: none"> 0: Do not scan removable drives 1: Scan removable drives 	0	No
SPECIFIC_FOLDER	An absolute folder path to scan when the scan type is [Specific]	<p><folder_path></p> <p>Multiple folders can be specified by creating new entries whose name starting with SPECIFIC_FOLDER</p> <p>Every entry name needs to be unique</p> <p>For example:</p>	<empty>	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		SPECIFIC_FOLDER=c: \folder1 SPECIFIC_FOLDER2=c: \folder2 SPECIFIC_FOLDER3=c: \folder3		
EXCLUDED_FILE	An absolute file path to exclude from scanning	<file_path> Multiple files can be specified by creating new entries whose name starting with EXCLUDED_FILE Every entry name needs to be unique For example: EXCLUDED_FILE=c:\file1.exe EXCLUDED_FILE2=c:\file2.exe EXCLUDED_FILE3=c:\file3.exe	<empty>	No
EXCLUDED_FOLDER	An absolute folder path to exclude from scanning	<folder_path> Multiple folders can be specified by creating new entries whose name starting with EXCLUDED_FOLDER Every entry name needs to be unique For example:	<empty>	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		EXCLUDED_FOLDER=c:\file1 EXCLUDED_FOLDER2=c:\file2 EXCLUDED_FOLDER3=c:\file3		
EXCLUDED_EXTENSION	A file extension to exclude from scanning	<file_extension> Multiple extensions can be specified by creating new entries whose name starting with EXCLUDED_EXTENSION Every entry name needs to be unique For example: EXCLUDED_EXTENSION=bmp EXCLUDED_EXTENSION2=png	<empty>	No
PRESCANCLEANUP	Attempt to clean detected files during prescan	<ul style="list-style-type: none"> 0: No action This is the default setting for installations using the Windows Installer 1: Clean, or delete if the clean action is unsuccessful 	2	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
		<ul style="list-style-type: none"> • 2: Clean, or quarantine if the clean action is unsuccessful • 3: Clean, or ignore if the clean action is unsuccessful 		
FORCE_PRESCAN	Perform a prescan before installation	<ul style="list-style-type: none"> • 0: Disable • 1: Enable 	0	No

BlockNotification Section

The following table lists the notification commands available for `setup.ini`. If no value is specified in the setup file, the default value will be used.

See [Property Section on page 2-18](#) for more information.



Important

To enable the feature, make sure to also enable the display for system tray icons and notifications. See `NO_SYSTRAY` in this table for details.

TABLE 2-12. Setup.ini File [BlockNotification] Section Arguments

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
ENABLE	Display notifications on managed endpoints when StellarEnforce blocks an unapproved file	<ul style="list-style-type: none"> • 0: Disable • 1: Enable 	0	No

KEY	DESCRIPTION	POSSIBLE VALUES	DEFAULT VALUE	ENCRYPTED
ALWAYS_ON_TOP	Display the file blocking notification on top of other screens	<ul style="list-style-type: none">• 0: Disable• 1: Enable	1	No
SHOW_DETAILS	Display file name, file path, and event time in the notification	<ul style="list-style-type: none">• 0: Disable• 1: Enable	1	No
AUTHENTICATE	Authenticate the user by requesting the administrator password when closing a notification	<ul style="list-style-type: none">• 0: Disable• 1: Enable	1	No
TITLE	Notification title	<notification_title>	<empty>	No
MESSAGE	Notification content	<notification_content>	<empty>	No

Chapter 3

Agent Configuration File Deployment

This chapter describes the deployment of settings to multiple TXOne StellarEnforce agents using an Agent Configuration File.

Deployment for Standalone Agents

Agents installed in `Standalone` mode are not managed by a TXOne StellarEnforce Central Console server. To manually deploy a single configuration to multiple `Standalone` agents, use an agent configuration file.

Exporting or Importing a Configuration File

**Note**

TXOne StellarEnforce encrypts the configuration file before export. Users must decrypt the configuration file before modifying the contents.

Procedure

1. Open the TXOne StellarEnforce console using the desktop icon (if available) or the **Start** menu by clicking **All Programs > TXOne StellarEnforce**.
2. Provide the password and click **Login**.
3. Click the **Settings** menu item to access the **Export/Import Configuration** section.

To export the configuration file as a database (.xen) file:

- a. Click **Export**, and choose the location to save the file.
- b. Provide a filename, and click **Save**.

To import the configuration file as a database (.xen) file:

- a. Click **Import**, and locate the database file.
- b. Select the file, and click **Open**.

TXOne StellarEnforce overwrites the existing configuration settings with the settings in the database file.

Deployment using StellarOne

Agents installed in **Managed** mode are managed by a StellarOne server, which can issue remote commands to all managed agents. To deploy agent configuration settings to multiple managed agents, launch the StellarOne web console and use the **Send Command** menu located on the **Agent Management** screen.

Remotely Exporting Agent Settings

You can remotely obtain agent configuration settings and Approved Lists by exporting and downloading them from the StellarOne.

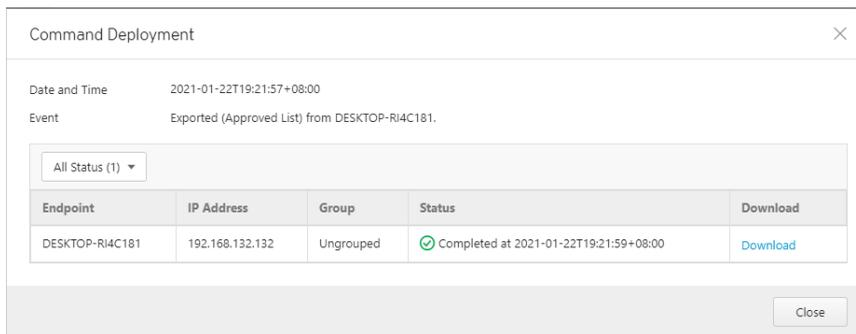
Procedure

1. Click **Agents > StellarEnforce** from the StellarOne.
The **Agent Management** screen appears.
2. Select a target endpoint.
3. Click **Import / Export** and select one of the following:
 - **Import Approved List**
 - **Import Agent Configuration**

The StellarOne will issue the command. Progress can be viewed from the pop-up **Details** window.

4. To export settings, repeat the above steps, instead selecting either **Export Approved List** or **Export Agent Configuration**.

When the exports are complete, you will be confirmed by this message on the top of the screen:



5. Click **View Details** to download the exported settings.

Remotely Importing Agent Settings

You can remotely apply new agent settings to agents from StellarOne. This feature allows you to:

- Remotely overwrite agent configurations
- Remotely overwrite Approved Lists
- Remotely add approved items to Approved Lists

Procedure

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

**Note**

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

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

2. Click **Agents** from the StellarOne console.

The **Agent Management** screen appears.

3. To import the customized file to agents, follow the steps below.

- a. From the Endpoint column, select one or more agents.
- b. Click **Import / Export**.
- c. Select **Import Approved List** or **Import Agent Configuration**

The import dialog will appear.

4. To import the customized file to an agent group, follow the steps below.

- a. From the left panel, select an agent group and go to **Import / Export**.
- b. Select **Import Approved List** or **Import Agent Configuration**.

The import dialog will appear.

5. By default, StellarOne does the following:

- **Approved List:** accumulates items from the customized Approved List to the target Approved Lists. To replace the target Approved Lists with the customized Approved List, select **Overwrite the existing Approved List**.
- **Agent Configuration:** overwrites the target Approved Lists with the customized Approved List.

6. Click **Browse** to select the customized file.

7. Click **OK**.

Chapter 4

Local Agent Uninstallation

This chapter describes TXOne StellarEnforce agent uninstallation procedures.

Topics in this chapter include:

- *[Uninstalling Agents from Windows on page 4-2](#)*

Uninstalling Agents from Windows



Note

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

Procedure

1. On an endpoint with the StellarEnforce agent installed, launch TXOne StellarEnforce Setup.

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

OPTION	DESCRIPTION
<p>If you use one of the following operating systems:</p> <ul style="list-style-type: none"> • Windows 10 Enterprise • Windows 10 IoT Enterprise • Windows 10 Professional 	<ol style="list-style-type: none"> a. Go to Start > Settings. b. Depending on your version of Windows 10, locate the Apps & features section under one of the following categories: <ul style="list-style-type: none"> • System • Apps c. On the left pane, click Apps & features. d. In the list, click TXOne StellarEnforce. e. Click Uninstall.
<p>If you use one of the following operating systems:</p> <ul style="list-style-type: none"> • Windows 7 • Windows 8 • Windows Vista • Windows Server 2008 • Windows Server 2012 • Windows Server 2016 	<ol style="list-style-type: none"> a. Go to Start > Control Panel > Programs and Features. b. In the list, double-click TXOne StellarEnforce.

OPTION	DESCRIPTION
<ul style="list-style-type: none">• Windows Storage Server 2016• Windows Server 2019	
If you use one of the following operating systems: <ul style="list-style-type: none">• Windows Server 2003• Windows XP• Windows 2000	<ol style="list-style-type: none">a. Go to Start > Control Panel > Add or Remove Programs.b. In the list, select TXOne StellarEnforce.c. Click Remove.

StellarEnforce Setup opens in uninstaller mode.

2. After StellarEnforce Setup opens, click **Next**.
3. Provide the StellarEnforce administrator password, and click **Next**.
4. After the software is finished uninstalling, click **Finish**.

Chapter 5

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

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

- agent configuration file
 - exporting or importing, 3-2
- agent installer
 - approved list, 2-10
 - command line interface, 2-13, 2-14
 - overview, 2-2
 - Setup.ini Agent section, 2-33
 - Setup.ini arguments, 2-18
 - Setup.ini BlockNotification section, 2-43
 - Setup.ini EventLog section, 2-29
 - Setup.ini MessageRandomization section, 2-36
 - Setup.ini Message section, 2-34
 - Setup.ini Prescan section, 2-37
 - Setup.ini Property section, 2-18, 2-33
 - Setup.ini Proxy section, 2-36
 - Setup.ini Server section, 2-32
 - Setup.ini use, 2-17
 - Windows Installer, 2-3
- agents, 1-2
 - accounts, 1-4
 - features and benefits, 1-3
 - operating systems, 1-6
 - system requirements, 1-5
 - uninstallation, 4-2
 - use overview, 1-13
- Application Lockdown, 1-3
- Approved List
 - setting up, 2-10, 2-11

D

- documentation, iii
- documentation feedback, 5-6

E

- Exploit Prevention, 1-3

I

- installation
 - customization, 2-17
 - methods, 2-2

N

- Network Virus Protection, 2-6, 2-14

O

- operating systems, 1-6

R

- requirements, 1-5

S

- Self Protection, 1-4
- StellarEnforce, 1-2
- support
 - resolve issues faster, 5-4
- system requirements, 1-5

U

- uninstallation, 4-2



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: SLEM19268/210330