txOne networks | Keep the Operation Running

3.0

TXOne StellarProtect

Administrator's Guide

Unified agent providing asset lifetime all-terrain protection

Windows

Document Part No.: APEM39735/230619

Release Date: July 2023

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

Privacy and Personal Data Collection Disclosure

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

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

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

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

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

Table of Contents

Chapter 4: Using the Agent Command Line Interface (CLI)

Chapter 5: Working with the Agent Configuration File

Chapter 6: Agent Event Logs

Chapter 7: Troubleshooting Resources

Chapter 8: Technical Support

Appendix A: StellarProtect (Legacy Mode) Limitations by Operating Systems

Index

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

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

Preface

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

Topics in this chapter include:

About the Documentation

TXOne Networks StellarProtect documentation includes the following:

Documentation	Description
Readme file	Contains a list of known issues and basic installation steps. It may also contain late-breaking product information not found in the other documents.
Installation Guide	A PDF document that discusses requirements and procedures for installing and managing StellarProtect.
Administrator's Guide	A PDF document that discusses StellarProtect agent installation, getting started information, and server and agent management
Knowledge Base	An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following websites: https://kb.txone.com/ http://success.trendmicro.com

Audience

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

Document Conventions

The documentation uses the following conventions.

Table 1. Document Conventions

Convention	Description
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard

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

Terminology

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

Terminology	Description
server	The StellarOne console server program
agents	The host running the StellarProtect program

Terminology	Description
managed agents managed endpoints	The hosts running the StellarProtect program that are known to the StellarOne server program
target endpoints	The hosts where the StellarProtect ™ managed agents will be installed
Administrator (or StellarProtect administrator)	The person managing the StellarProtect agents
StellarProtect console	The user interface for configuring and managing StellarProtect settings
StellarOne (management) console	The user interface for configuring and managing the StellarProtect agents managed by StellarOne
CLI	Command Line Interface
license activation	Includes the type of StellarProtect agent installation and the allowed period of usage that you can use the application

agent installation folder	The folder on the host that contains the StellarProtect agent files. If you accept the default settings during installation, you will find the installation folder at one of the followinglocations:
	
	`C:\Program Files\TXOne\StellarProtect`
	
	`C:\Program Files\TXOne\StellarProtect (Legacy Mode)`

Chapter 1

Introduction

This section introduces TXOne StellarProtect the unified agent, and gives an overview of its functions.

Topics in this chapter include:

About TXOne Stellar

TXOne Stellar provides a context-focused security solution for OT endppoints and cyber-physical systems (CPS), aiming to defend operation stability with continuous detection and response aligned to the specific requirements of the OT domain.

TXOne Stellar platform is composed of the centralized menagement console server and unified agents apt for legacy OT devices and modern cyber-physical systems.

- StellarOne™ , designed to streamline administration of the agents installed on modernized systems and legacy systems, along with its intuitive centralized management, consistent policy enforcement, and action-oriented alerts that empower security teams of all sizes and skill levels to successfully mature their organization's security posture.
- StellarProtect ™ / StellarProtect (Legacy Mode), using the single-agent design that delivers seamless asset-centric protection and ensures coverage for modern CPS and legacy OT devices throughout their entire asset lifecycle. The lightweight unified agent simplifies security by combining CPS Detection and Response (CPSDR), threat prevention, operations lockdown, and device control.
    - CPSDR: Embodied within the advanced Operations Behavior Anomaly Detection feature, which establishes a unique baseline fingerprint of each agent-device during practicable operating states and performs fingerprint deviation analysis by means of an expansive industrial application repository and ransomware detection engine to defend against unexpected changes that may impact stability.

      Moreover, TXOne Stellar brings the contextualization of security into an operation-led view to allow both the operation and security teams to achieve their goals without needing to compromise. To illustrate, if a device suddenly tried to start launching different applications, it would be blocked from doing so.

      From the operation view, this may be an unplanned auto-update that, if run, would take the device offline to reboot. From a security

view, this could be an attempt to access an encryption library that is about to be used to execute ransomware. By applying the operation context, both security and operation-initiated changes can be detected, and appropriate responses are taken.

In both cases, CPSDR stopped the event before it could occur. The security team followed up and resolved the ransomware infection in a different part of the environment. The operation team scheduled the required update for during an upcoming planned maintenance window.

- Multi-Method Threat Prevention: Provides advanced threat scan on the basis of ICS root of trust and operations-focused machine learning to secure the agent-devices against known and unknown malware threats without compromising operational availability.
- Operations Lockdown: For fixed-function and devices with limited patching availability,operations lockdown enforcement prohibits unauthorized changes, including alterations to registry and function parameters.
- Trusted Peripheral Control: Unauthorized access from external sources, such as USB devices, is configurable and controlled to reduce physical access threats.

Leveraging an expansive ICS application and certificate library and exclusive ransomware detection engine, TXOne Stellar maintains CPS operational integrity through behavioral anomaly detection and eliminates configuration drift for legacy and fixed-use assets with device lockdown. Security teams can confidently deliver detection and response outcomes across the OT terrain, with TXOne Stellar effectively secure organization's security posture while maintaining its business operations stability.

Key Features and Benefits

The StellarProtect provides following features and benefits.

TABLE 1-1. Features and Benefits

FEATURE	BENEFIT
Cyber-Physical System Detection and Response (CPSDR)	The CPSDR requires a deep understanding of what the expected behaviors for each device are. Embodied within the advanced Operations Behavior Anomaly Detection feature, which primarily defends against unexpected changes that may impact operational stability by comparing daily operation processes and behaviors with a unique baseline of each agent-device and performing comprehensive behavioral analysis not only via identifying baseline deviation but also using TXOne Networks' exclusive industrial application repository and ransomware detection engine.
One unified agent	TXOne StellarProtect simplifies security by combining multi-method threat prevention, operations lockdown, and OT anomaly detection. The unified agent provides long-term support throughout the asset life cycle from modern to legacy.
Scan functions for modern and legacy systems	For modern systems, the StellarProtect provides **Multi-Method Threat Prevention**; the OT/ICS root of trust and advanced threat scan secure OT/ICS assets with no interruption to operations. This feature is the core protection of StellarProtect. TXOne Networks integrates signature-based and AI-based malware detection engine to provide real-time scanning of any file or process activity. Meanwhile, the StellarProtect (Legacy Mode) offers **Threat Prevention** that persistently scan new and changed files, along with system memory, to provide security assessment for maximum protection against malware in fixed-use and legacy systems.
Application Lockdown	This operations lockdown feature prevents malware attacks and increases protection level by allowing only the files defined in an Approved List to be executed. By preventing programs, DLL files, drivers, and scripts not specified on the Approved List of applications from running (also known as application trust listing), StellarProtect and StellarProtect (Legacy Mode) provide both improved productivity and system integrity by blocking malicious software and preventing unintended use. Furthermore, to ensure operational integrity, Intelligent Runtime Learning allows runtime executable files that are generated by applications in the Approved List to run smoothly.

Feature	Benefit
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 that automatically adds new or modified files to the Approved List, all without having to unlock TXOne StellarProtect or StellarProtect (Legacy Mode): • Maintenance Mode • Trusted Updater (Legacy Mode only) • Predefined Trusted Updater List (Legacy Mode only) • Command Line Interface (CLI) • Trusted hash • Trusted certificate
DLL Injection Prevention	This feature detects and blocks API call behaviors used by malicious software. Blocking these threats helps prevent malicious processes from running.
Device Control	This feature prevents insider threats by only allowing usage of USB ports on a case-by-case administrator reviewed basis. **Note** For StellarProtect (Legacy Mode), Device Control is included as one of the features of *Exploit Prevention* settings.
Maintenance Mode	To perform file updates on endpoints, users can configure Maintenance Mode settings to define a period when StellarProtect or StellarProtect (Legacy Mode) allows all file executions and adds all files that are created, executed, or modified to the Approved List.
Role Based Administration	TXOne StellarProtect and StellarProtect (Legacy Mode) both provide a separate Administrator and User account, providing full control during installation and setup, as well as simplified monitoring and maintenance after deployment.
Self Protection	With self protection features, StellarProtect/StellarProtect (Legacy Mode) are capable of defending its processes and resources, required to function properly, from being disabled by programs or actual users.

Feature	Benefit
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.
Features designed specifically for modernized assets: • OT Application Safeguard • Operations Behavior Anomaly Detection	For modernized assets, StellarProtect offers features such as **OT Application Safeguard** and **Operations Behavior Anomaly Detection** that detect behavioral anomalies and quickly determine operational credibility using an expansive library of OT/ICS applications and certificates. **OT Application Safeguard** intelligently locates and secures the operational integrity of the critical OT/ICS applications by preventing the un-authorized changes. TXOne Networks continuously builds up the only OT/ICS context-focused database that can identify thousands of applications and certificates to ensure undisturbed operations. Meanwhile, **Operations Behavior Anomaly Detection** detects abnormal operations and exercises least privilege-based control to prevent malware-free attacks by means of its auto-learn runtime behavior to adapt to the dynamic needs of autonomous operations.
Features designed specifically for legacy assets: • Write Protection • Fileless Attack Prevention • Exploit Prevention settings	For fixed-use and legacy systems, StellarProtect (Legacy Mode) provides more options available from Application Lockdown settings. **Write Protection** blocks modification and deletion of files, folders, and registry entries; **Fileless Attack Prevention** detects and blocks unapproved process chains and arguments that may lead to a fileless attack event. For advanced threat prevention, StellarProtect (Legacy Mode) *Exploit Prevention* settings includes Intrusion Prevention, Execution Prevention, and Device Control to stop threats from spreading to the endpoint or executing.

What's New

TXOne StellarProtect 3.0 provides following new features and enhancements.

TABLE 1-2. What's New in TXOne StellarProtect 3.0

FEATURE	BENEFIT
Cyber-Physical System Detection and Response (CPSDR)	Embodied within the advanced Operations Behavior Anomaly Detection feature, which establishes a unique baseline fingerprint of each agent-device during practicable operating states and performs fingerprint deviation analysis by means of an expansive industrial application repository and exclusive ransomware detection engine to defend against unexpected changes that may impact stability. Since every agent continuously analyzes its host device to establish and maintain a unique baseline fingerprint, in real-time, unexpected behaviors and deviations from this fingerprint can be detected at the individual agent level and then secondarily at the centralized control level to inform wider instability issues and prompt preventative actions to be taken.

System Requirements

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

Software and Hardware Requirements

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

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

HARDWARE	DESCRIPTION

Available free disk space	400MB
	
	Note
	• Recommended free disk space for StellarProtect Single Installer required during the installation process: 1.5GB
	• Minimum memory usage required when Application Lockdown and Real-Time Scan are both enabled:
	  • StellarProtect: 350MB
	  • StellarProtect (Legacy Mode): 300MB
	• Minimum memory usage required when Application Lockdown is enabled and Real-Time Scan is disabled:
	  • StellarProtect: 120MB
	  • StellarProtect (Legacy Mode): 100MB

Monitor and resolution	VGA (640 x 480), 16 colors

TABLE 1-4. Required Software for StellarProtect

SOFTWARE	DESCRIPTION
.NET framework	Version 3.5 SP1 or 4.0 available

Note

StellarProtect (Legacy Mode) does not have the software requirement for .NET framework.

By default, StellarProtect/StellarProtect (Legacy Mode) uses port 14336 as the listening port for StellarOne, which is sometimes blocked by firewalls. Please make sure this port is kept open for StellarProtect's use.

The Active Update server link for StellarProtect/StellarProtect (Legacy Mode) has been changed to **https://ttau.cs.txone.com**. Please ensure that you whitelist this URL in your firewall.

Important

- StellarProtect/StellarProtect (Legacy Mode) cannot be installed on a system that already runs one of the following:
  - Trend Micro OfficeScan
  - Trend Micro Titanium
  - Other Trend Micro endpoint solutions
  - Other antivirus products
- Ensure that the following root certification authority (CA) certificates are installed with intermediate CAs, which are found in `StellarSetup.exe`. These root CAs should be installed on the StellarProtect/StellarProtect (Legacy Mode) 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 (Legacy Mode only)
  - DigiCert Trusted Root G4 (Legacy Mode only)

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

Note

Memory Randomization (Legacy Mode only), API Hooking Prevention (Legacy Mode only), and DLL Injection Prevention are not supported on 64-bit platforms.

Operating Systems

Windows Client:

- Windows 2000 (SP4) [Professional] (32bit)
- Windows XP (SP1/SP2/SP3) [Professional/Professional for Embedded Systems] (32bit)
- Windows Vista (NoSP/SP1/SP2) [Business/Enterprise/Ultimate] (32bit)
- Windows 7 (NoSP/SP1) [Professional/Enterprise/Ultimate/Professional for Embedded Systems/Ultimate for Embedded Systems] (32/64bit)
- Windows 8 (NoSP) [Pro/Enterprise] (32/64bit)
- Windows 8.1 (NoSP) [Pro/Enterprise/with Bing] (32/64bit)
- Windows 10 [Pro/Enterprise/IoT Enterprise] (32/64bit), LTSC 2015, Anniversary Update, LTSC 2016, Creators Update, Fall Creators Update, April 2018 Update, October 2018 Update*, LTSC 2019, May 2019 Update, November 2019 Update, May 2020 Update, October 2020 Update, May 2021 Update, November 2021 Update, LTSC 2021, 2022 Update
- Windows 11 (NoSP) [Pro/Enterprise] (64bit) 2022 Update
- Windows Embedded POSReady 2009 (32bit)
- Windows Embedded Standard 7 (NoSP/SP1) (32/64bit)
- Windows Embedded POSReady 7 (NoSP) (32/64bit)
- Windows Embedded 8 Standard (NoSP) (32/64bit)
- Windows Embedded 8 Industry (NoSP) [Pro/Enterprise] (32/64bit)
- Windows Embedded 8.1 Industry (NoSP) [Pro/Enterprise/Sideloading] (32/64bit)

Note

Windows 10 October 2018 Update is also known as version 1809, of which Microsoft resumed the public rollout on November 13, 2018.

Windows Server:

- Windows Server 2000 (SP4) (32bit)
- Windows Server 2003 (SP1/SP2) [Standard/Enterprise/Storage] (32bit)
- Windows Server 2003 R2 (NoSP/SP2) [Standard/Enterprise/Storage] (32bit)
- Windows Server 2008 (SP1/SP2) [Standard/Enterprise/ Storage] (32/64bit)
- Windows Server 2008 R2 (NoSP/SP1) (Standard/Enterprise/Storage] (64bit)
- Windows Server 2012 (NoSP) (Essentials/Standard] (64bit)
- Windows Server 2012 R2 (NoSP) (Essentials/Standard] (64bit)
- Windows Server 2016 (NoSP) [Standard] (64bit)
- Windows Server 2019 (NoSP) [Standard] (64bit)
- Windows Server 2022 (NoSP) [Standard] (64bit)
- Windows Storage Server 2012 (NoSP) [Standard] (64bit)
- Windows Storage Server 2012 R2 (NoSP) [Standard] (64bit)
- Windows Storage Server 2016 (NoSP) (64bit)

Note

- See the latest StellarProtect readme file for the most up-to-date list of supported operating systems for agents.
- See *StellarProtect (Legacy Mode) Limitations by Operating Systems on page A-1* for the limitations of the StellarProtect (Legacy Mode) installed on certain operating systems.

Chapter 2

Setting Up the Approved List

This chapter describes how to set up the Approved List for StellarProtect/ StellarProtect (Legacy Mode).

Setting Up the Approved List

Before TXOne StellarProtect or StellarProtect (Legacy Mode) Application Lockdown feature can protect the endpoint, it must check the endpoint for existing applications and files necessary for the system to run correctly.

The following instructions take StellarProtect (Legacy Mode) as an example for how to set up the Approved List for StellarProtect (Legacy Mode) or StellarProtect agent. StellarProtect would require you to follow similar procedures with slight differences in the GUI.

Note

If you choose not to create the Approved List during the StellarProtect installation process, refer to the following procedures to perform the task.

Procedure

1. Open the StellarProtect (Legacy Mode) console. The StellarProtect (Legacy Mode) log on screen appears.
2. Provide the password and click **Log On**.

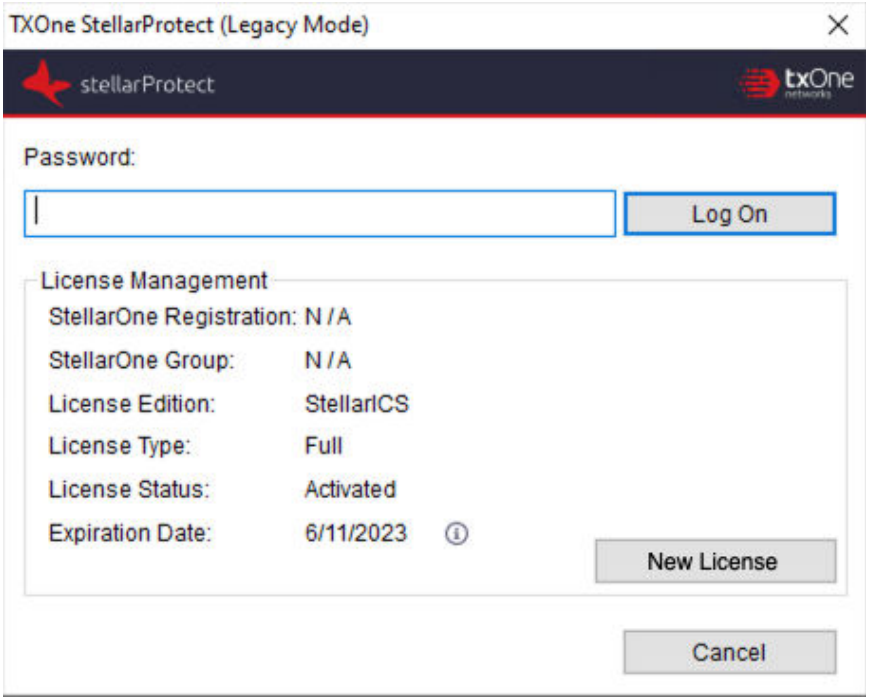

FIGURE 2-1. StellarProtect (Legacy Mode) Log On Screen

3. StellarProtect (Legacy Mode) asks if you want to set up the Approved List now.

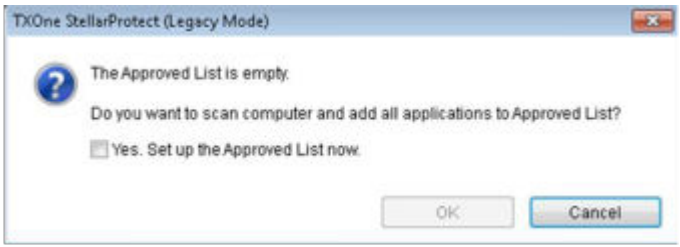

FIGURE 2-2. The Approved List is Empty

4. At the notification window, select **Yes. Set up the Approved List now** and click **OK**. StellarProtect (Legacy Mode) scans the endpoint and adds all applications to the Approved List.

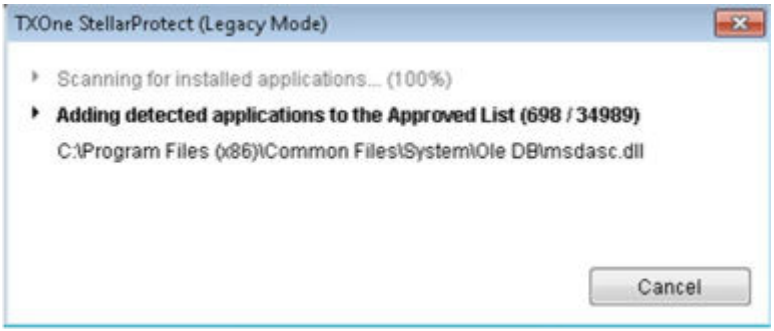

FIGURE 2-3. Scanning for Creating Approved List

5. StellarProtect (Legacy Mode) displays the Approved List Configuration Results.

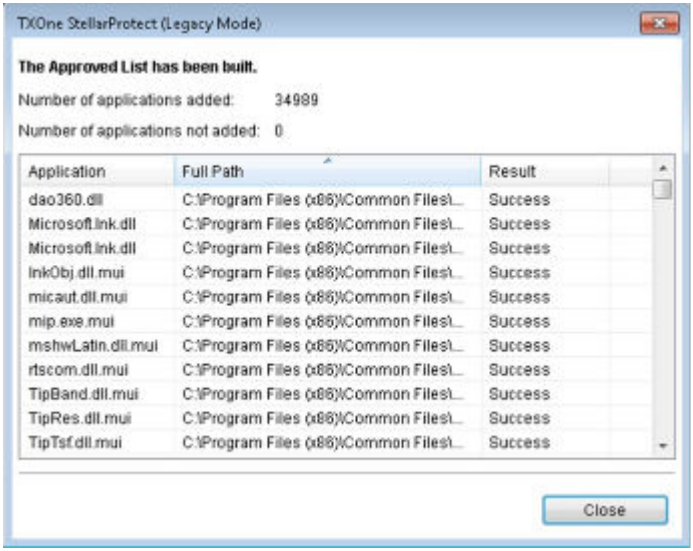

FIGURE 2-4. Approved List Created

Note

- When TXOne StellarProtect/StellarProtect (Legacy Mode) Application Lockdown is enabled, only applications that are in the Approved List will be able to run.
- When the endpoint is creating or updating its Approved List, no policy settings can be deployed.

6. Click **Close**.

Chapter 3

Using the Agent Console

This chapter describes how to operate TXOne StellarProtect's/StellarProtect (Legacy Mode)'s various functions using the agent console on the endpoint.

Topics in this chapter include:

Using the StellarProtect Agent Console

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

Topics include:

Overview

The agent console provides easy access to commonly used features in TXOne StellarProtect.

The **Overview** serves as the portal as well as one of the side navigation options on StellarProtect console. It displays the current status of the StellarProtect system.

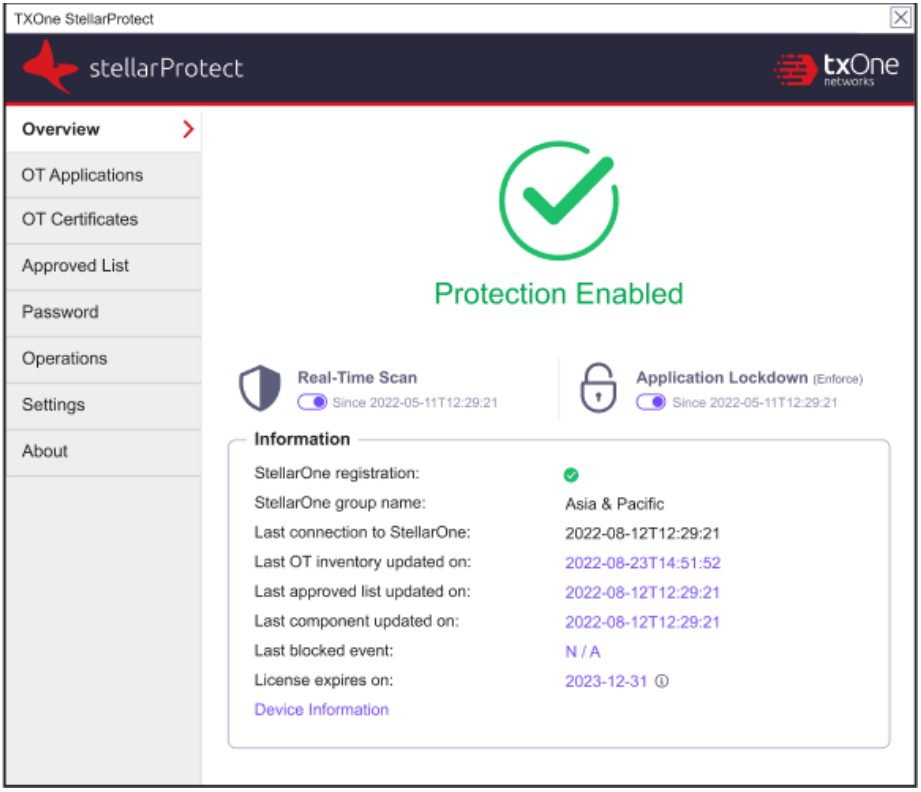

FIGURE 3-1. Overview of StellarProtect Console - Protection Enabled

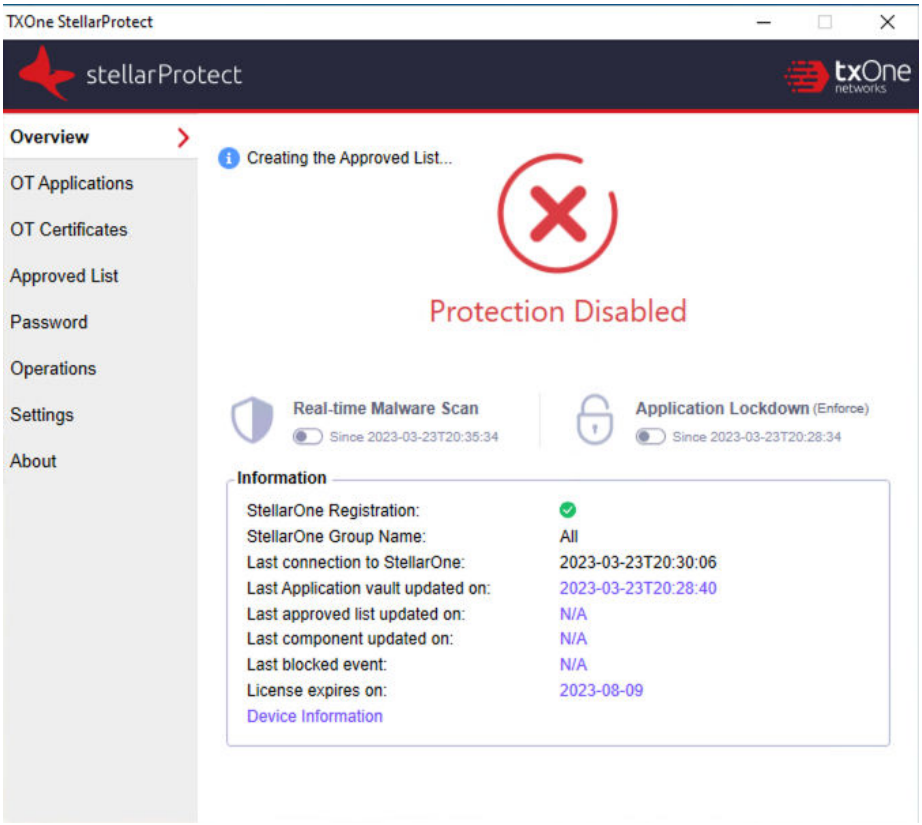

FIGURE 3-2. Overview of StellarProtect Console - Protection Disabled

The following table describes the features available on the **Overview** of the agent console:

TABLE 3-1. Overview Item Descriptions

ITEM	FUNCTION	DESCRIPTION
Side Navigation Menu	**Overview**	Displays the current status of the StellarProtect software.
	OT Applications	Lists all OT/ICS application systems recognized by StellarProtect on this endpoint, and lists

Item	Function	Description
		the software name, vendor name, product version and installation path of each application system.
	OT Certificates	Lists all OT/ICS certificates recognized by StellarProtect on this endpoint, and lists the receiver, issuer, and hash value of each certificate.
	Approved List	Displays applications allowed to run and lets users manage the list.
	Password	Enables administrator to change the StellarProtect Administrator or User passwords. **Note** Only users logged in as the administrator can change the passwords.
	Operations	Provides options to perform tasks such as on-demand scan, policy sync, connection check, and maintenance mode setting.
	Settings	Enables or disables vulnerability protection settings.
	About	Displays the product information and component version numbers
Status Information		Indicates the Real-time Scan and/or Application Lockdown are/is enabled.
		Indicates the main protection features have been turned off and the endpoint may be vulnerable to security threats.
	Real-Time Scan	Enables users to toggle on the **Real-Time Scan** function, which provides persistent and ongoing file scan for the endpoints when a file

Item	Function	Description
		is received, opened, downloaded, copied, or modified. **Tip** The date and time the Real-Time Scan was last turned on or off are displayed next to the toggle switch.
	Application Lockdown	Enables users to toggle on the **Application Lockdown (Enforce)** function, which locks down the system, blocking applications not on the Approved List from running. **Note** After disabling **Application Lockdown (Enforce)** mode, StellarProtect switches to a "Detect" mode. In this mode, StellarProtect does not block any applications from running, but logs when applications that are not in the Approved List run. You can use these logs to check if the Approved List contains all the applications required on the endpoint. **Tip** The date and time the Application Lockdown was last turned on or off are displayed next to the toggle switch.

Item	Function	Description
StellarOne registration		Indicates the StellarProtect agent is successfully registered to a designated StellarOne web console.
		Indicates the registration to a StellarOne web console has failed.
	N/A	Indicates the agent was installed in standalone mode and has not registered to any StellarOne web console.
StellarOne group name		Displays the name of the group the agent belongs to. When you mouse over the displayed name, information about the group name, group ID, and policy version will appear. **Note** • If the agent does not belong to any group, the group name displayed should be **All**. • For standalone agents, the group name displayed should be **N/A**.
Last connection to StellarOne		Indicates the last time the agent was connected with StellarOne console.
Last application vault updated on		Displays the last time the application vault was updated. By clicking the link, you will be directed to the **OT Applications** tab page for viewing the details and number of the OT applications installed on the endpoint.
Last approved list updated on		Displays the last time the approved list was updated. By clicking the link, you will be directed to the **Approved List** tab page for viewing the details and number of the applications added into the approved list on this endpoint.

Item	Function	Description
Last component updated on		Displays the last time the components were updated. By clicking the link, you will be directed to the **About** tab page for viewing the details of the components updated on this endpoint.
Last blocked event		Clicking the link shows the most recent blocked events.
License expires on		Displays the date and time the software expires. Clicking the link shows more license information such as license edition, type, and status.
Device Information		Clicking the link shows device information about the endpoint, such as Vendor, Model, Location, and Remark.

Note

The Overview displays different protection features depending on different license editions:

License Edition	Main Protection Features
StellarICS	• Real-Time Scan • Application Lockdown
StellarKiosk	Real-Time Scan
StellarOEM	Application Lockdown

OT Applications

This option lists all the OT/ICS application systems recognized by StellarProtect on this endpoint and displays the associated software name, vendor name, product version and installation path.

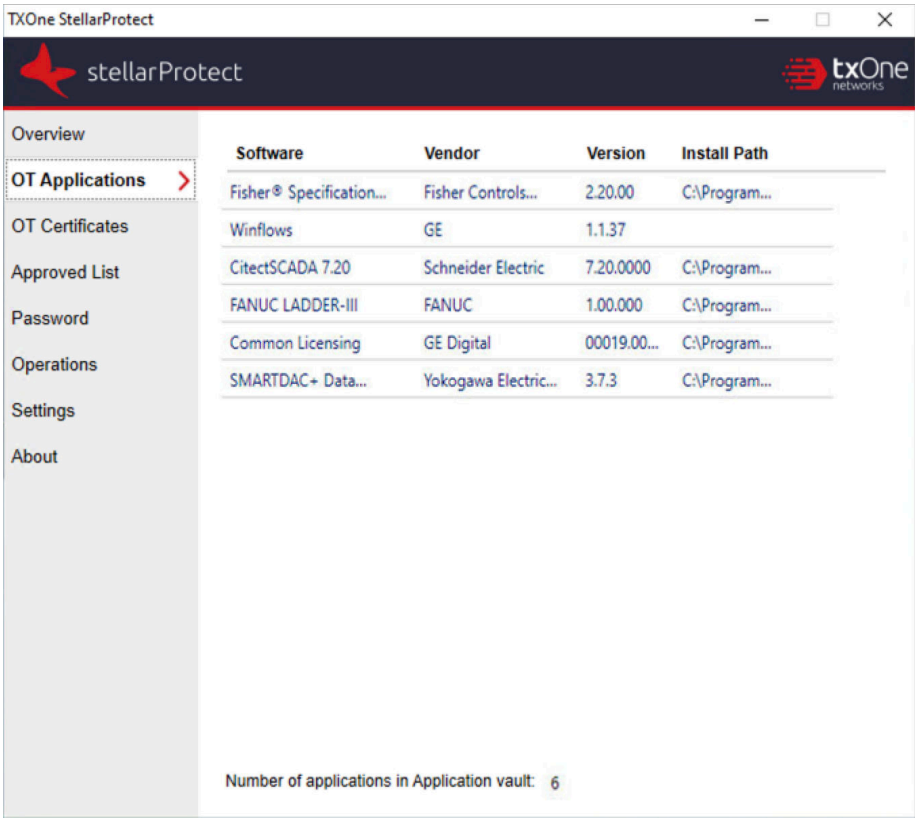

FIGURE 3-3. StellarProtect OT Applications

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

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

OT Certificates

The 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.

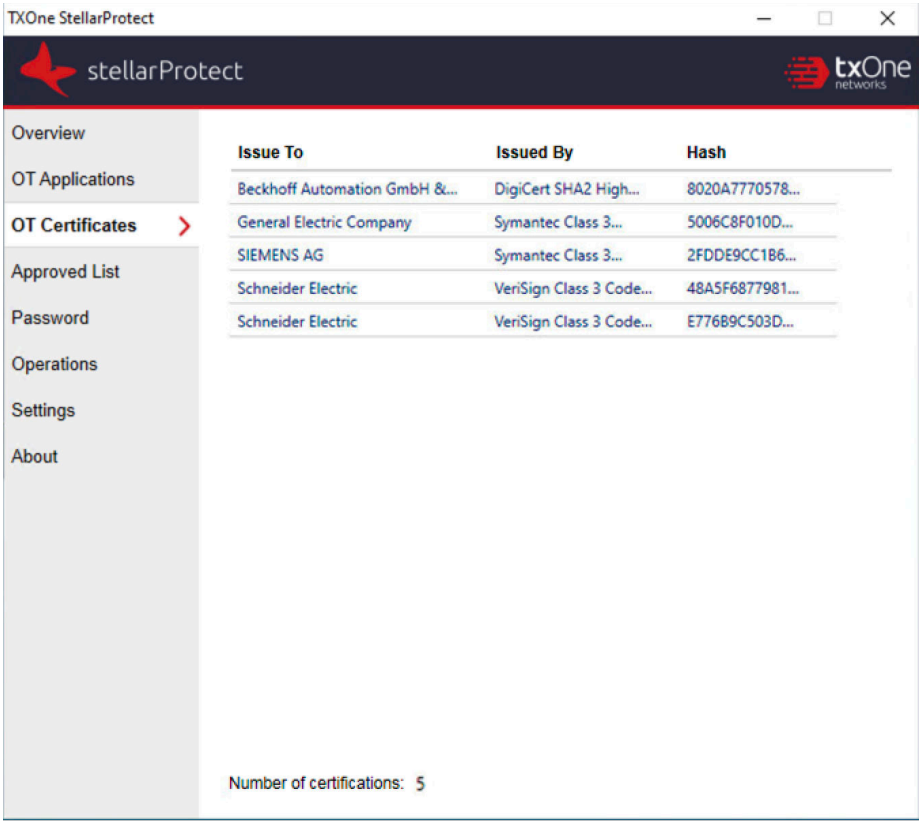

FIGURE 3-4. StellarProtect OT Certificates

The number of OT/ICS certificates that StellarProtect can recognize will increase with updates from the application vault, which is producedby the TXOne research laboratory and based on OT/ICS product analysis.

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

Approved List

If you enabled **Creating Approved List** during the installation, applications found would be added to and shown on the **Approved List** page. The following table describes the features available on the **Approved List**.

Note

If you choose not to create the Approved List during the StellarProtect installation process, you can choose to set up the Approved List at the notification window that appears after logging on the agent console, or through the StellarOne web console.

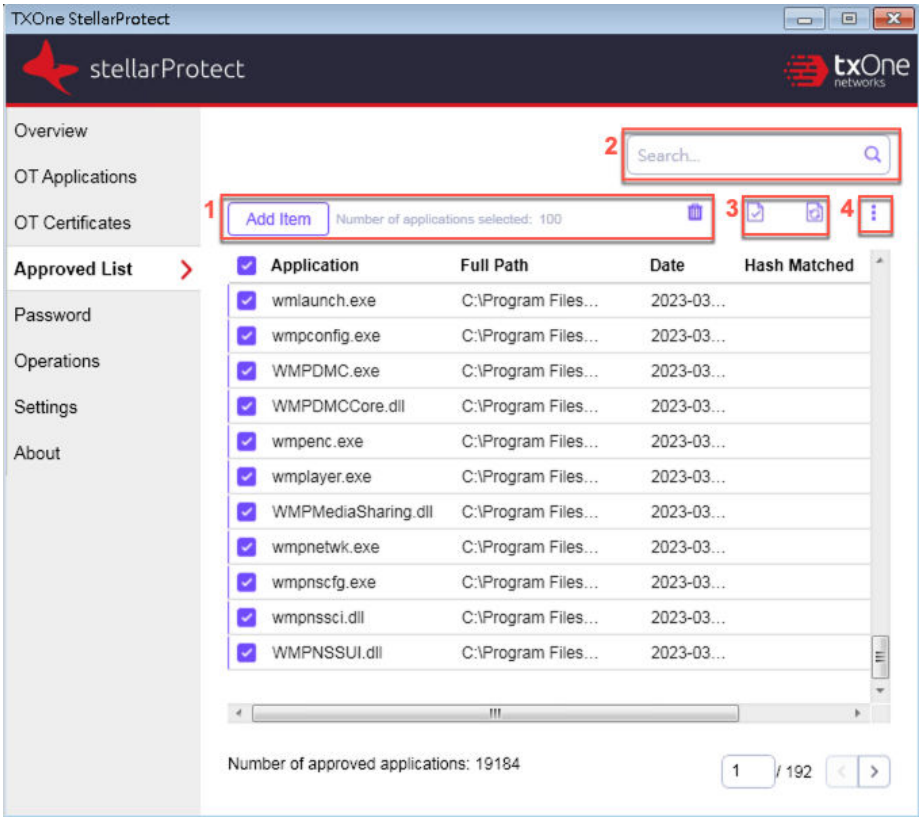

FIGURE 3-5. StellarProtect Approved List

TABLE 3-2. Approved List Item Descriptions

#	ITEM	DESCRIPTION
1	**Add Item/Delete**	Adds or removes selected items to or from the Approved List See *Adding or Removing Files on page 3-17* for instructions. **Note** The **Delete** icon will appear after you select the checkbox(es) next to the target application(s).
2	**Search Bar**	Searches the Application and Full Path columns
3	**Check Hash/Update Hash**	Checks or updates the hash values for applications in the Approved List. See *About Hashes on page 3-14* for more details and *Checking or Updating Hashes on page 3-14* for instructions. **Note** The **Check Hash** and **Update Hash**icons will appear after you select the checkbox(es) next to the target application(s).
4	**Import All Hash / Export All Hash** **Note** Click **More actions** and the menu items will appear.	Imports trusted file hashes to the Approved List or exports all the existing file hashes. See *Exporting or Importing the File Hashes on page 3-18*for instructions.

About Hashes

StellarProtect calculates a unique hash value for each file in the Approved List. This value can be used to detect any changes made to a file, since any change results in a different hash value. Comparing current hash values to previous values can help detect file changes.

The following table describes the hash check status icons.

Icon	Description
	The calculated hash value matches the stored value.
	The calculated hash value does not match the stored value.
	There was an error calculating the hash value.

Moving or overwriting files manually can result in the hash values not matching, but a mismatch could also result from other applications (including malware) altering or overwriting existing files. If it is unsure why a hash value mismatch has occurred, scan the endpoint for potential security threats.

Checking or Updating Hashes

Checking the hash value of files in the Approved List can help verify the integrity of files currently permitted to run.

Procedure

1. Open the TXOne StellarProtect console using the desktop icon (if available) or the Start menu by clicking **All Programs** > **TXOne StellarProtect**.
2. Provide the password and click **Log On**.
3. Click the **Approved List** on the **Side Navigation Menu**.
    - To check the file hash values:

a. Select the target file(s). To check all files, select the check box at the top of the Approved List.

b. Click the **Check Hash** icon that appears at the upper right hand.

- To update the file hash values:

  a. Select the target file(s). To check all files, select the check box at the top of the Approved List.

  b. Click the **Update Hash** icon that appears at the upper right hand.

The Hash Matched column shows the hash checking or updating result.

Important

If it is unsure why a hash value mismatch has occurred, scan the endpoint for potential security threats.

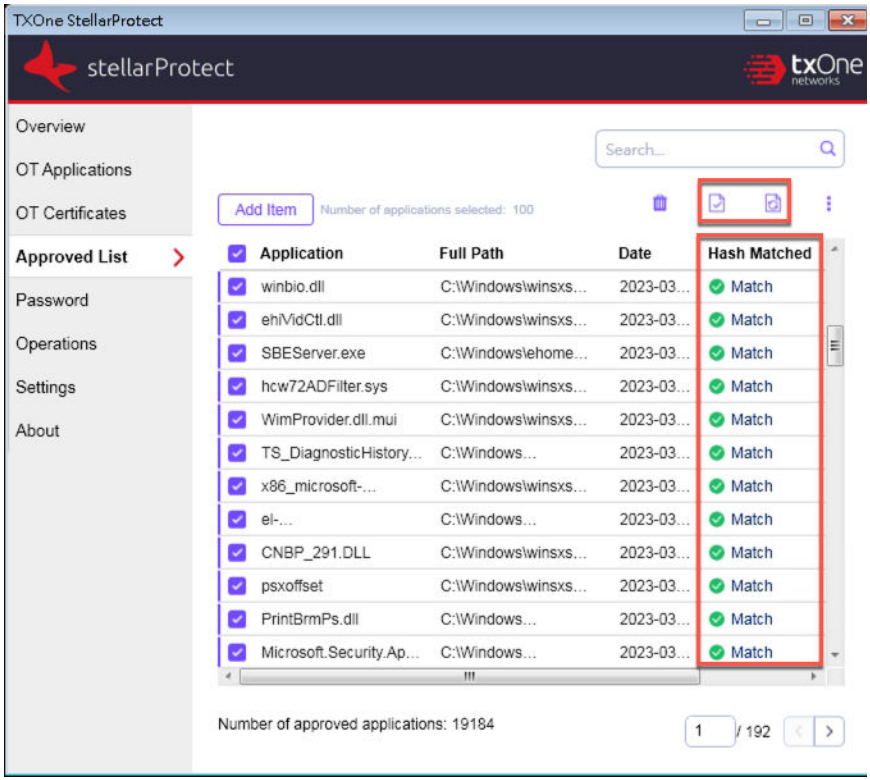

FIGURE 3-6. Hash Values Matched

Configuring the Approved List

After setting up the Approved List, you can manually add new programs by clicking **Add Item** and select the software that already exists on the endpoint. Adding a file grants permission to run the file, but it does not alter the file or the system.

For example, if Windows Media Player (`wmplayer.exe`) is not in the Approved List after initial setup, you can add it to the list using the console.

Note

Moving or overwriting files manually may result in the hash values not matching. See *Checking or Updating Hashes on page 3-14* for how to keep the hash values up to date.

Adding or Removing Files

Procedure

1. Open the TXOne StellarProtect console using the desktop icon (if available) or the **Start** menu by clicking **All Programs** > **TXOne StellarProtect**.
2. Provide the password and click **Log On**.
3. Click the **Approved List** on the **Side Navigation Menu**.
   - To add an item:
     a. Click **Add Item**.
     b. A pop-up window appears. Click the **Select** drop-down menu and choose **Specific applications**, **All applications in selected folders**, or **All applications in a specified path**.
     c. A selection window appears.
        - If you choose **Specific applications**, select the desired application and click **Open**.
        - If you choose **All applications in selected folders**, select the desired application or folder to add and click **OK**.
        - If you choose **All applications in a specified path**, specify the file or folder path in the text field displayed and click **OK**.

Note

If you want to include the subfolders under the specified folder, check **include all the subfolders**.

d. The selected applications will be listed and displayed for double-check. Confirm the items to be added, and click **Add**.

e. After adding the desired items to the Approved List, click **Finish**.

- To remove an item:

a. Search the Approved List for the application to remove.

b. Select the checkbox next to the file name to be removed, and click the **Delete** icon.

c. When asked to remove the item, click **Yes**.

d. Click **OK** to close the confirmation window.

Exporting or Importing the File Hashes

You can export or import the file hashes of an Approved List as a `.csv` file for reuse in mass deployment situations.

WARNING!

The operating system files used by the exporting and importing endpoints must match exactly. Any difference between the operating system files on the endpoints can lead to operating system malfunctions or system lock-out after importing.

Procedure

1. Open the TXOne StellarProtect console using the desktop icon (if available) or the **Start** menu by clicking **All Programs** > **TXOne StellarProtect**.
2. Provide the password and click **Log On**.
3. Click the **Approved List** on the **Side Navigation Menu**.
   - To export file hashes from the existing Approved List on the endpoint:

a. Search and select the applications, or check the check box next to the **Application** header to select all files.

b. Click **More actions** icon at the upper right hand, and then choose **Export All Hash**.

c. Provide a filename and specify where to save the file.

d. Click **Save**.

e. A success message appears. Click **OK**.

- To import file hashes from an Approved List:

a. Click **More actions** icon at the upper right hand, and then choose **Import All Hash**.

b. A notification window appears. Read the message carefully and determine if you want to overwrite the existing hash values with the imported hash values generated from the same applications. Click **Continue**.

Note

By default, overwriting existing hash with the imported hash is disabled.

c. Locate the file (a `.csv` file) to import.

d. Select the file, and click **Open**.

e. A success message appears. Click **OK**.

Password and Account Types

TXOne Networks StellarProtect provides role-based administration, allowing Administrator to grant the User account access to limited features on the main console.

StellarProtect Administrator can choose one of the ways listed below to enable or disable the User account:

- GUI: See *Account Settings on page 3-20*
- CLI: See *OPCmd Program Commands on page 4-4*

The following table show privileges available with the two account types. To sign in with a specific account, specify the password for that account.

TABLE 3-3. StellarProtect Account Types

ACCOUNT	DETAILS
Administrator	• Default account • Full access to StellarProtect functions • Can use both the console GUI and command line interface (CLI)
User	• Secondary maintenance account • Limited access to StellarProtect functions • Can only use the console GUI

Account Settings

Only the Administrator can change the passwords of StellarProtect **Administrator** and **User** accounts via the console,. To log on the console as the administrator account, provide the administrator password when launching the console.

Important

The StellarProtect Administrator and User passwords cannot be the same.

Procedure

1. Open the TXOne console using the desktop icon (if available) or the **Start** menu by clicking **All Programs** > **TXOne StellarProtect**.
2. Provide the StellarProtect **Administrator** password and click **Log On**.
3. Click the **Password** on the **Side Navigation Menu** to display the **Administrator** password page.

- To change the StellarProtect Administrator password:
  a. Provide the current password, specify and confirm the new password, and click **Save**.

  WARNING!

  Please treat your StellarProtect administrator password with care. If you lose it, please contact TXOne Networks support.

- To create a User password:
  a. Click the tab to switch to the **User** page
  b. Click **Enable User account** to turn it on.
  c. Specify and confirm the password, and click **Save**.
- To change an existing User password:
  a. Specify and confirm the new password, and click **Save**.

Operations

The **Operations** page provides options to perform tasks such as on-demand scan, policy sync, connection check, and maintenance mode setting.

Note

Both the Administrator and User accounts are allowed to access the functions available on the **Operations** page.

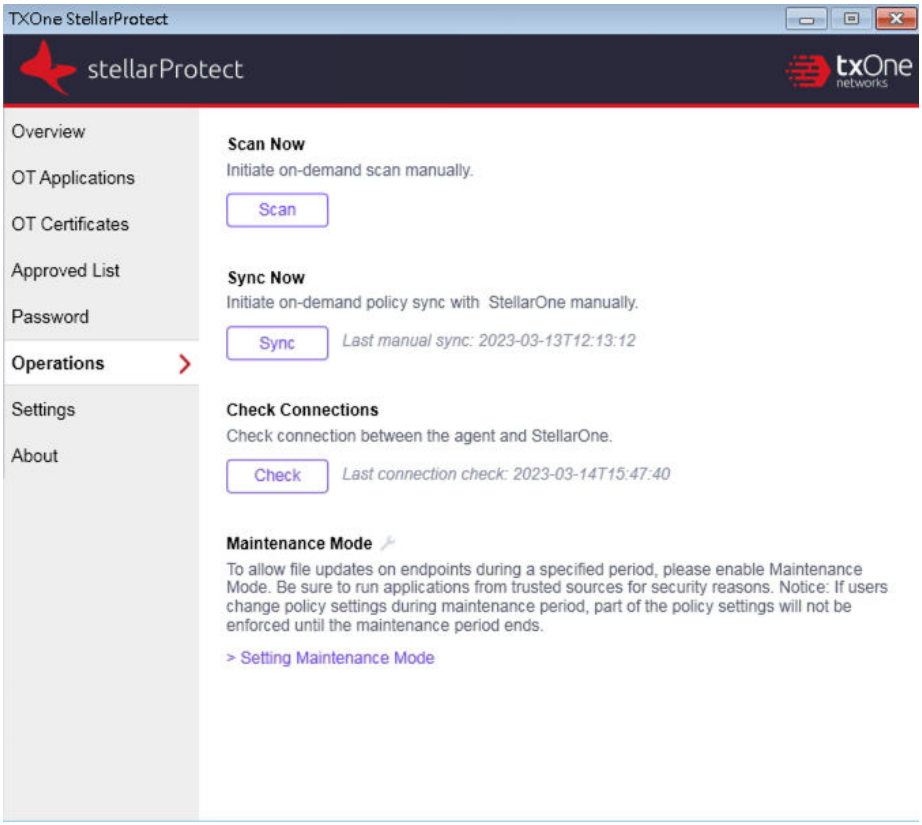

FIGURE 3-7. StellarProtect Operations Page

The following table describes the features available on the **Operations** page.

ITEM	DESCRIPTION
Scan Now	Click the **Scan** button to initiate on-demand scanning. See *Scan Now on page 3-23* for more details.
Sync Now	Click the **Sync** button to synchronize policy with StellarOne server. See *Sync Now on page 3-24* for more details.

Item	Description
Check Connection	Click the **Check** button to check if the agent is properly connected with the StellarOne server. See *Check Connection on page 3-24* for more details.
Maintenance Mode	Read the description of the Maintenance Mode carefully and click **Setting Maintenance Mode** to enable or disable it. See *Setting Maintenance Mode on page 3-25* for more details.

Scan Now

The **Scan** button on the **Operations** page enables both the Administrator and User accounts to manually initiate on-demand scan when needed.

Procedure

1. Open the TXOne console using the desktop icon (if available) or the **Start** menu by clicking **All Programs** > **TXOne StellarProtect**.
2. Provide the StellarProtect Administrator or User password and click **Log On**.
3. Click **Operations** on the **Side Navigation Menu**.
4. Find the **Scan Now** section and click the **Scan** button.
5. The **Scan Settings** window appears. Click **Start** to initiate the scan.

   Note

   - Only the StellarOne administrator can configure the scan settings. See *Advanced Settings for Scheduled Scan* section in the *StellarOne Administrator's Guide* for more details.
   - It may take a while to complete the scanning.

6. A scan result appears indicating threats detected. Click **OK** to complete the scan task.

Sync Now

The **Sync** button on the **Operations** page enables both the Administrator and User accounts to manually initiate on-demand policy sync with StellarOne when needed.

Procedure

1. Open the TXOne console using the desktop icon (if available) or the **Start** menu by clicking **All Programs** > **TXOne StellarProtect**.
2. Provide the StellarProtect Administrator or User password and click **Log On**.
3. Click **Operations** on the **Side Navigation Menu**.
4. Find the **Sync Now** section and click the **Sync** button.
5. A successful message appears. The **Last manual sync** next to the **Sync** button indicates the last time the policy sync has been manually initiated and succesfully completed.

Check Connection

The **Check** button on the **Operations** page enables both the Administrator and User accounts to manually initiate connection check to see if the agent is properly connected with StellarOne.

Procedure

1. Open the TXOne console using the desktop icon (if available) or the **Start** menu by clicking **All Programs** > **TXOne StellarProtect**.
2. Provide the StellarProtect Administrator or User password and click **Log On**.
3. Click **Operations** on the **Side Navigation Menu**.
4. Find the **Check Connection** section and click the **Check** button.

5. A successful message appears. The **Last connection check** next to the **Check** button indicates the last time the connection check has been manually initiated and succesfully completed.

Setting Maintenance Mode

To perform approved file updates or system maintenance on endpoints, you can configure Maintenance Mode for a specified period of time. During the Maintenance Mode, StellarProtect allows all file executions and adds all files that are created, executed, or modified to the Approved List.

Besides, StellarProtect can ensure the execution of these applications are under the protected conditions by performing malware scanning before adding new or changed files to the Approved List.

Note

If you change the settings of Application Lockdown, real-time scan (Multi-Method Threat Prevention), or OT Application Safeguard during maintenance period, the settings will not be implemented until the maintenance period ends.

Procedure

1. Open the TXOne console using the desktop icon (if available) or the **Start** menu by clicking **All Programs** > **TXOne StellarProtect**.
2. Provide the StellarProtect Administrator or User password and click **Log On**.
3. Click **Operations** on the **Side Navigation Menu**.
4. Find the **Maintenance Mode** section and read the description carefully.

Note

To know whether the agent is currently in maintenance mode, check the **Overview** page or the **Maintenance Mode** section on the **Operations** page.

- : Indicates the agent is in maintenance mode. A timestamp appears near the icon indicating the maintenance start time (only available on **Overview** page) and end time.
- : Indicates the agent is not in maintenance mode

5. Click **Setting Maintenance Mode** at the bottom.
6. The configuration window appears.
   - Click **Disable** to end Maintenance Mode.

     Important

     If the Maintenance Mode is ended, the endpoint will start blocking the execution of files that are not recognized by the Application Lockdown and OT Application Safeguard.

   - Click **Enable** to start the Maintenance Mode settings.
     a. Specify the duration of the maintenance period in **Maintenance Mode will be ended after ... hour (s)**.
     b. (Optional) If real-time scan is disabled, the **Perform real-time scan during the maintenance period** toggle appears at the bottom of this window and is set **enabled** by default.

        Note

        TXOne Networks suggests you keep this toggle turned on to ensure all the new or changed files go through the malware scanning before they're added to the Approved List.

     c. Click **OK** to complete the settings.

Important

To reduce risk of infection, run only applications from trusted sources on endpoints during the maintenance period.

About Feature Settings

StellarProtect offers the following protection features.

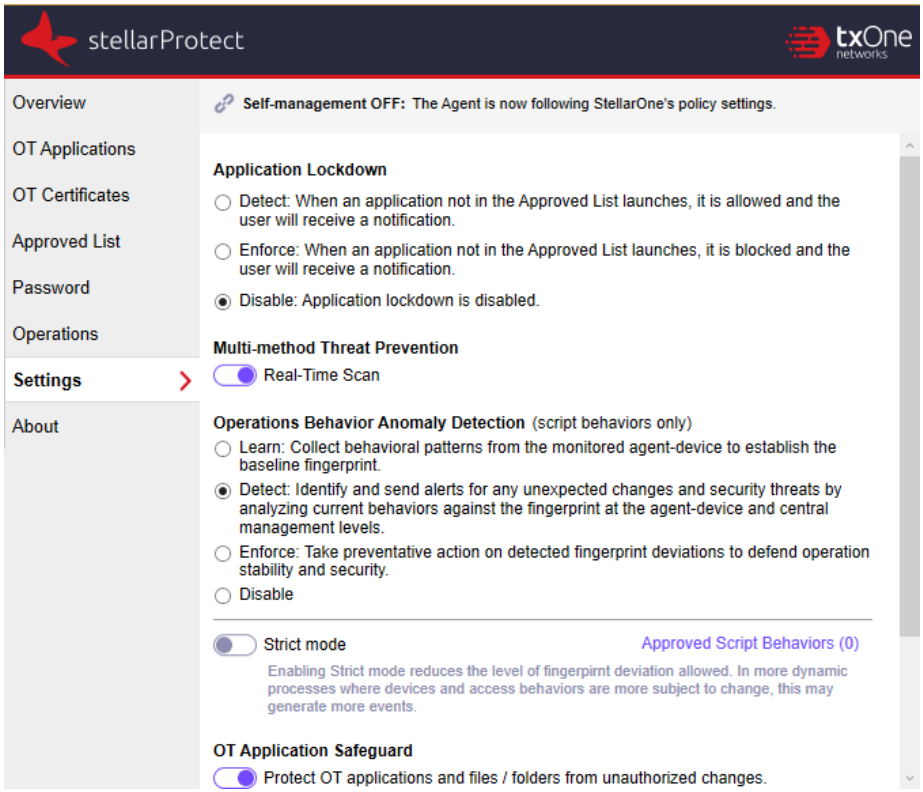

FIGURE 3-8. StellarProtect Settings Screen

Application Lockdown

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

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

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

When **Detect** or **Enforce** mode is selected, three more protection options become available:

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

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

Multi-Method Threat Prevention

Multi-Method Threat Prevention (real-time scan) is the core protection of StellarProtect. TXOne integrates signature-based and AI-based antivirus software to provide real-time scanning of any file or process activity.

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

You can toggle the **Real-Time Scan** on or off to enable or disable this security option.

Operations Behavior Anomaly Detection

The **Operations Behavior Anomaly Detection** strengthens security resilience and operation stability by leveraging Cyber-Physical System Detection and Response (CPSDR). It collects behavioral patterns in the OT environment and identifies any unexpected changes or abnormal behaviors that could impact the operation.

This function mainly allows StellarProtect to protect the endpoints against script-based of fileless attacks when enabled. By comparing the list of script behaviors and monitored process in the baseline with those running for daily operations, unrecognized monitored process or unexpected script behaviors will be detected as anomalies and trigger event notifications or be blocked.

By default, StellarProtect monitors specific high-risk applications such as `Powershell.exe`, `wscript.exe`, `cscript.exe`, `mshta.exe`, and `psexec.exe` to stop legitimate programs from being misused when the **Operations Behavior Anomaly Detection Detect** or **Enforce** is enabled. You can also manually add commonly-abused applications used in operations and processes via the StellarOne web console for strengthening security monitoring.

The **Operations Behavior Anomaly Detection** for StellarProtect provides four normal modes. In addition, there is a special mode under two of the normal modes. See the details below for more information.

- **Learn**: In this mode, StellarProtect collects behavioral patterns from the monitored agent-devices to establish baseline fingerprints.

  Important

  TXOne Networks recommends you set the target agents to the **Learn mode** first to establish their own baseline fingerprints before they can perform automated behavioral analysis in the **Detect** or **Enforce** mode.

- **Detect**: In this mode, StellarProtect identifies and sends alerts for any unexpected changes and security threats by analyzing current behaviors against the fingerprints at the agent-device and central management levels.

    - **Strict mode**: This special mode appears when you select the **Detect** mode. Enabling the **Strict mode** reduces the level of the fingerprint deviation allowed; in other words, it performs stricter comparison between the established baseline and currently-running operational behaviors. In more dynamic operating environments where devices and access behaviors are more subject to change, this may generate more events.

- **Enforce**: In this mode, StellarProtect takes preventative action on detected fingerprint deviations to defend operation stability and security.

    - **Strict mode**: This special mode appears when you select the **Enforce** mode. Enabling the **Strict mode** reduces the level of the fingerprint deviation allowed; in other words, it performs stricter comparison between the established baseline and currently-running operational behaviors. In more dynamic operating environments where devices and access behaviors are more subject to change, this may generate more events and require more preventative actions to be taken.

- **Disable**: The Operations Behavior Anomaly Detection can also be disabled if needed, but it is recommended to have this function enabled to maintain security against behavior anomalies.

OT Application Safeguard

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

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

After enabling **Protect OT application and files/folders from unauthorized changes**, ICS application executable files will be protected automatically without user definition. An administrator may also manually define additional files and folders to be protected via the StellarOne web console.

DLL Injection Prevention

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

Note

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

Device Control

StellarProtect will control access to external USB storage devices to ensure that only authorized USB devices can be used.

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

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

StellarProtect will send a blocked event notification to StellarOne. The StellarOne administrator can view the blocked event and can approve access or maintain the block.

The Device Control use case is as follows:

1. Plug in the USB.
2. The USB will be blocked if Device Control is enabled and the device is untrusted.
3. A pop-up window appears to require users to enter the administrator password.

4. After granted access permission, the USB device can be allowed access until unplugged.

FIGURE 3-9. Use Case of Device Control

You can toggle the **Device Control** on or off to enable or disable this security option.

Enabling or Disabling Feature Settings

Follow the procedures to enable or disable feature settings for StellarProtect agents.

Note

By default, TXOne StellarProtect enables DLL/Driver Lockdown, Script Lockdown, and Intelligent Runtime Learning features if the Application Lockdown is set to "Detect" or "Enforce" mode.

Procedure

1. Open the TXOne console using the desktop icon (if available) or the **Start** menu by clicking **All Programs** > **TXOne StellarProtect**.
2. Provide the Administrator password and click **Log On**.
3. Click the **Settings** on the **Side Navigation Menu** to configure the feature settings.
4. Check or uncheck to enable or disable the desired features.
5. Click **Save**.

About StellarProtect

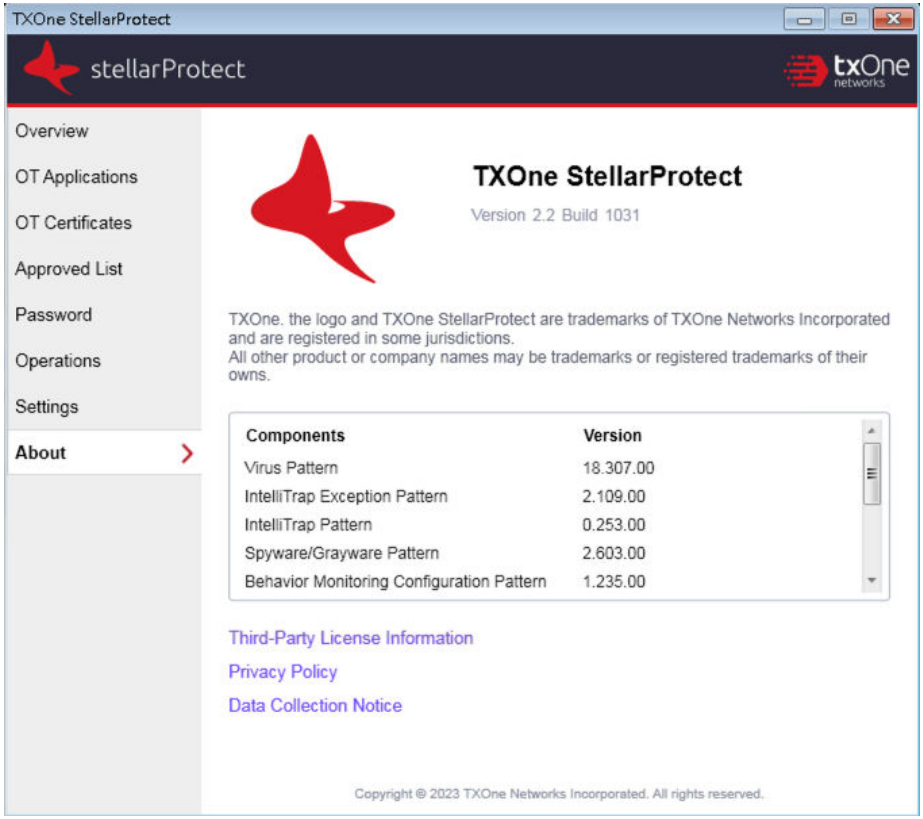

FIGURE 3-10. About StellarProtect

You can find StellarProtect product information, version and build number, scan components, third-party license information, as well as privacy policy and data collection notice on this page.

Using the StellarProtect (Legacy Mode) Agent Console

This section describes how to operate TXOne StellarProtect (Legacy Mode)'s various functions using the agent console on the endpoint.

Topics include:

Overview

The agent console provides easy access to commonly used features in TXOne StellarProtect (Legacy Mode).

The **Overview** serves as the portal as well as one of the side navigation options on StellarProtect (Legacy Mode) console. It displays the current status of the StellarProtect (Legacy Mode) system.

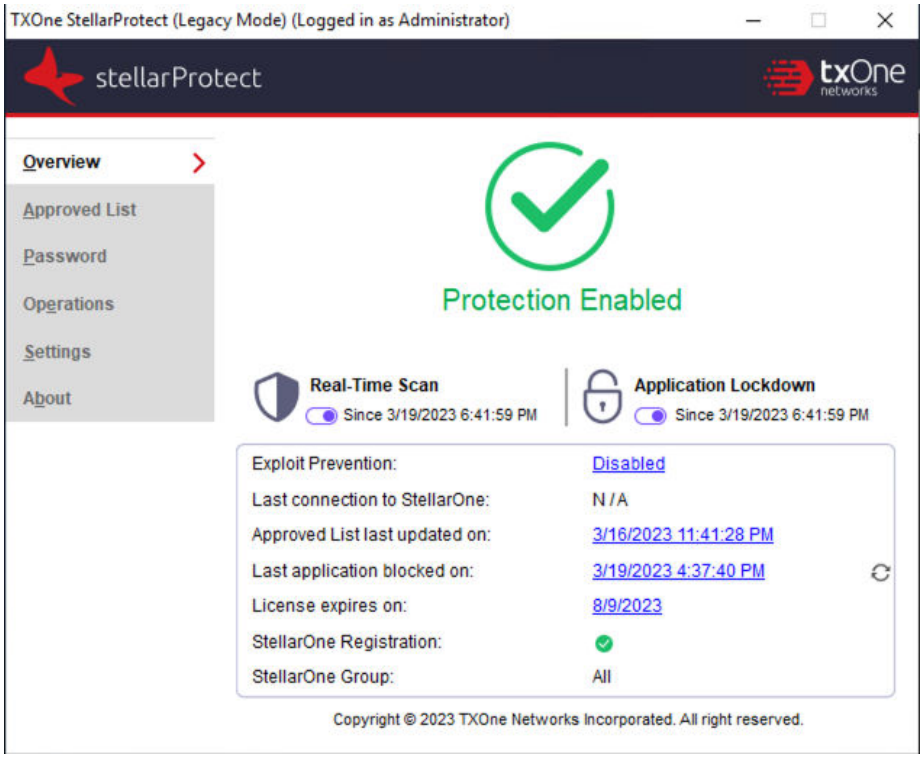

FIGURE 3-11. Overview of StellarProtect (Legacy Mode) Console - Protection Enabled

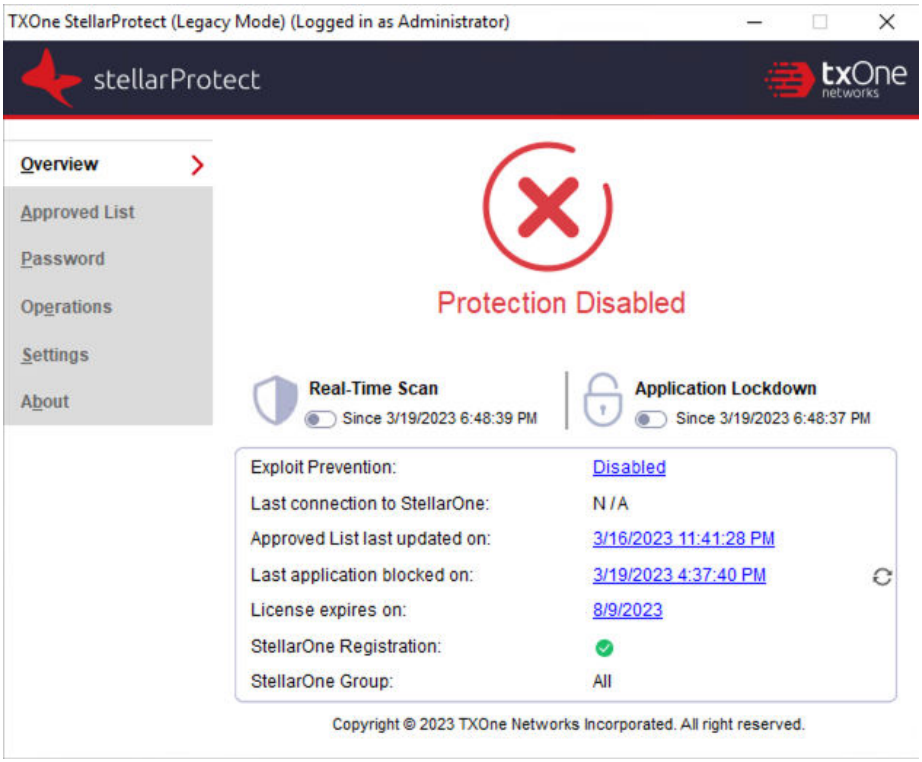

FIGURE 3-12. Overview ofStellarProtect (Legacy Mode) Console - Protection Disabled

The following table describes the features available on the **Overview** of the agent console:

TABLE 3-4. Overview Item Descriptions

ITEM	FUNCTION	DESCRIPTION
Side Navigation Menu	**Overview**	Displays the current status of the StellarProtect (Legacy Mode) software.
	Approved List	Displays applications allowed to run and lets users manage the list.

ITEM	FUNCTION	DESCRIPTION
	Password	Enables administrators to change the StellarProtect (Legacy Mode) Administrator or User passwords. **Note** Only users logged in as the administrator can change the passwords.
	Operations	Provides options to perform tasks such as on-demand scan, policy sync, connection check, and maintenance mode setting.
	Settings	Enables or disables vulnerability protection settings and exports or imports the system configuration.
	About	Displays the product information and component version numbers
Status Information	**Protection Check**	• The green check indicates the Real-time Scan and/or Application Lockdown are/is enabled • The red cross indicates main protection features have been turned off and the endpoint may be vulnerable to security threats
	Real-Time Scan	Enables users to toggle on the **Real-Time Scan** function, which provides persistent and ongoing file scan for the endpoints when a file is received, opened, downloaded, copied, or modified. **Tip** The date and time that the Real-Time Scan was last turned on or off are shown next to the toggle switch.

Item	Function	Description
	Application Lockdown	Enables users to toggle on the **Application Lockdown** function, which locks down the system, blocking applications not on the Approved List from running. **Note** After disabling Lockdown mode, StellarProtect (Legacy Mode) switches to a “unlock” mode. In this mode, StellarProtect (Legacy Mode) does not block any applications from running, but logs when applications that are not in the Approved List run. You can use these logs to check if the Approved List contains all the applications required on the endpoint. **Tip** The date and time that the Application Lockdown was last turned on or off are shown next to the toggle switch.
Exploit Prevention		• **Enabled:** All Exploit Prevention features are enabled. Click the status to open the settings screen. • **Enabled (Partly):** Some Exploit Prevention features are enabled. Click the status to open the settings screen. • **Disabled:** No Exploit Prevention features are enabled. Click the status to open the settings screen.

Item	Function	Description
Last connection to StellarOne		Indicates the last time the agent was connected with StellarOne console
Approved List status	**Approved List last updated on**	Click the corresponding last updated date to open the **Approved List** and view details.
	Last application blocked on	Click the corresponding last application blocked date to open the **Blocked Application Event Log** and view details.
License expires on		The time and date that the software expires. Click the corresponding date to view the current license status and activate/renew the license if needed.
StellarOne registration		The green check indicates the StellarProtect (Legacy Mode) agent is successfully registered to a group via StellarOne console; the N/A indicates the agent is not registered to any group; the red cross indicates registration to certain group is failed.
StellarOne group		Shows the group name to which the agent belongs to. When user hovers mouse over the group name, information about group name, group ID, and policy version will appear.

Note

The Overview displays different protection features depending on different license editions:

License Edition	Main Protection Features
StellarICS	• Real-Time Scan • Application Lockdown
StellarKiosk	• Real-Time Scan • Application Lockdown
StellarOEM	Application Lockdown

Approved List

Use the Approved List to display the files that StellarProtect (Legacy Mode) allows to run or make changes to the endpoint.

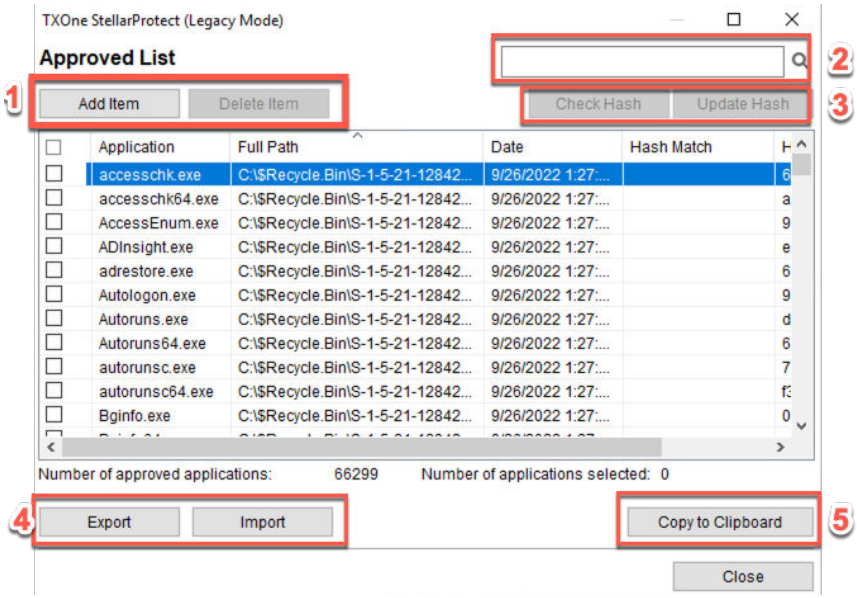

FIGURE 3-13. The StellarProtect (Legacy Mode) Approved List

The following table describes the features available on the **Approved List**.

TABLE 3-5. Approved List Item Descriptions

#	ITEM	DESCRIPTION
1	**Add Item / Delete Itme**	Adds or removes selected items to or from the Approved List
2	**Search Bar**	Searches the Application and File Path columns
3	**Check Hash / Update Hash**	Checks or updates the hash values for applications in the Approved List For more details, see: • *About Hashes on page 3-42* • *Checking or Updating Hashes on page 3-42*

#	Item	Description
4	**Export / Import**	Exports or imports the Approved List using a SQL database (.db) file
5	**Copy to Clipboard**	Copies the Approved List to the clipboard with comma separated values (CSV) format for easy review or reporting

About Hashes

StellarProtect (Legacy Mode) calculates a unique hash value for each file in the Approved List. This value can be used to detect any changes made to a file, since any change results in a different hash value. Comparing current hash values to previous values can help detect file changes.

The following table describes the hash check status icons.

Icon	Description
	The calculated hash value matches the stored value.
	The calculated hash value does not match the stored value.
	There was an error calculating the hash value.

Moving or overwriting files manually (without using the Trusted Updater) can result in the hash values not matching, but a mismatch could also result from other applications (including malware) altering or overwriting existing files. If it is unsure why a hash value mismatch has occurred, scan the endpoint for potential security threats.

Checking or Updating Hashes

Checking the hash value of files in the Approved List can help verify the integrity of files currently permitted to run.

Procedure

1. Open the TXOne StellarProtect (Legacy Mode) console using the desktop icon (if available) or the Start menu by clicking **All Programs** > **TXOne StellarProtect (Legacy Mode)**.
2. Provide the password and click **Log On**.
3. Click the **Approved List** on the **Side Navigation Menu**.
   - To check the file hash values:
     a. Select the target file(s). To check all files, select the check box at the top of the Approved List.
     b. Click **Check Hash**.
   - To update the file hash values:
     a. Select the target file(s). To check all files, select the check box at the top of the Approved List.
     b. Click **Update Hash**.

   The Hash Match column shows the hash checking or updating result.

Important

If it is unsure why a hash value mismatch has occurred, scan the endpoint for potential security threats.

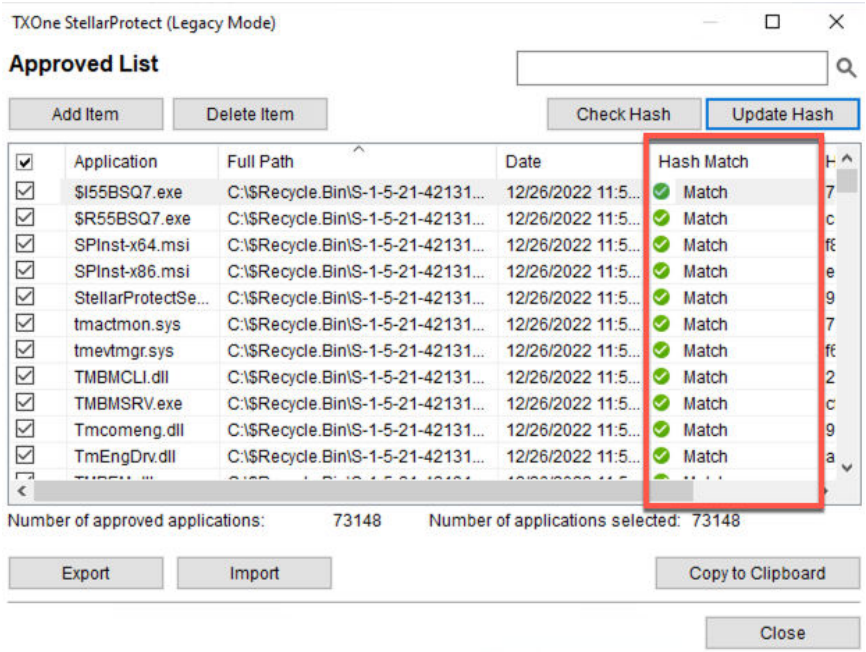

FIGURE 3-14. Hash Values Matched

Configuring the Approved List

After setting up the Approved List, you can add new programs by clicking **Add Item**, which displays the options in the following table.

TABLE 3-6. Methods for Adding Applications to the Approved List

OPTION	WHEN TO USE
Manually browse and select files	Choose this option when the software already exists on the endpoint and is up to date. Adding a file grants permission to run the file, but it does not alter the file or the system. For example, if Windows Media Player (`wmplayer.exe`) is not in the Approved List after initial setup, users can add it to the list using the console.

Option	When to Use
Automatically add files created or modified by the selected application installer (using the Trusted Updater)	Choose this option when you need to update or install new applications to your managed endpoint without having to unlock TXOne StellarProtect (Legacy Mode). TXOne StellarProtect (Legacy Mode) will add any new or modified files to the Approved List. For example, if Mozilla Firefox needs to be installed or updated, select this option to allow the installation or update to launch, and also add any files created or modified in the process to the Approved List.

Note

Moving or overwriting files manually (without using the Trusted Updater) can result in the hash values not matching.

Adding or Removing Files

Procedure

1. Open the TXOne StellarProtect (Legacy Mode) console using the desktop icon (if available) or the **Start** menu by clicking **All Programs** > **TXOne StellarProtect (Legacy Mode)**.
2. Provide the password and click **Log On**.
3. Click the **Approved List** on the **Side Navigation Menu**.
   - To add an item:
     a. Click **Add Item**, select **Manually browse and select files**, and click **Next**.
     b. A pop-up window appears. Click the **Select one** drop-down menu and choose **Specific applications**, **All applications in selected folders**, or **All applications in a specified path**.
     c. A selection window appears.

- If you choose **Specific applications**, select the desired application and click **Open**.
- If you choose **All applications in selected folders**, select the desired application or folder to add, a or **OK**.
- If you choose **All applications in a specified path**, specify the file or folder path in the text field displayed, and click **OK**.

Note

If you want to include the subfolders under the specified folder, check **include all the subfolders**.

d. Click **OK**.

e. The selected applications will be listed and displayed for double-check. Confirm the items to be added, and click **Approve**.

f. After adding the desired items to the Approved List, click **Close**.

- To remove an item:

a. Search the Approved List for the application to remove.

b. Select the check box next to the file name to be removed, and click **Delete Item**.

c. When asked to remove the item, click **OK**.

d. Click **OK** again to close the confirmation window.

Updating or Installing Using the Trusted Updater

StellarProtect (Legacy Mode) automatically adds applications to the Approved List after the Trusted Updater adds or modifies the program files.

Procedure

1. Open the TXOne StellarProtect (Legacy Mode) console using the desktop icon (if available) or the **Start** menu by clicking **All Programs** > **TXOne StellarProtect (Legacy Mode)**.
2. Provide the password and click **Log On**.
3. Click the **Approved List** on the **Side Navigation Menu**.
4. To install or update an application, select the installer that the Trusted Updater should temporarily allow to run:
   a. Click **Add Item**, select **Automatically add files created or modified by the selected application installer**, and click **Next**.
   b. A pop-up window appears. Click the **Select one** drop-down menu and choose **Specific installers**, **All installers in folders and subfolders**, or **All installers in a folder**.
   c. Select the desired installation package or folder to add, and then click **Open** or **OK**.

      Note

      Only existing `EXE`, `MSI`, `BAT`, and `CMD` files can be added to the Trusted Updater.

   d. Check that the correct items appear on the list, and click **Start**.

      The StellarProtect (Legacy Mode) **Trusted Updater** window displays.
5. Install or update the program as usual. When finished, click **Stop** on the **Trusted Updater** window.
6. Check that the correct items appear on the Approved List, and click **Approve**, and then click **Close**.

Exporting or Importing the Approved List

Users can export or import the Approved List as a database (`.db`) file for reuse in mass deployment situations. **Copy to Clipboard** creates a `CSV` version of the list on the Windows clipboard.

WARNING!

The operating system files used by the exporting and importing endpoints must match exactly. Any difference between the operating system files on the endpoints can lead to operating system malfunctions or system lock-out after importing.

Procedure

1. Open the TXOne StellarProtect (Legacy Mode) console using the desktop icon (if available) or the **Start** menu by clicking **All Programs** > **TXOne StellarProtect (Legacy Mode)**.
2. Provide the password and click **Log On**.
3. Click the **Approved List** on the **Side Navigation Menu**.
   - To export the Approved List:
     a. Click **Export**, and choose where to save the file.
     b. Provide a filename, and click **Save**.

        The exported file includes the following information:

        - File full path
        - File hash value
        - Additional notes
        - Last update time
   - To import an Approved List:
     a. Click **Import**, and locate the database file

b. Select the file, and click **Open**.

Password and Account Types

TXOne Networks StellarProtect (Legacy Mode) provides role-based administration, allowing Administrator to grant certain User account access to limited features on the main console.

StellarProtect (Legacy Mode) Administrator can choose one of the ways listed below to enable or disable the User account:

- GUI: See *Account Settings on page 3-51*

- CLI: See *Using SLCmd at the Command Line Interface (CLI) on page 4-16*

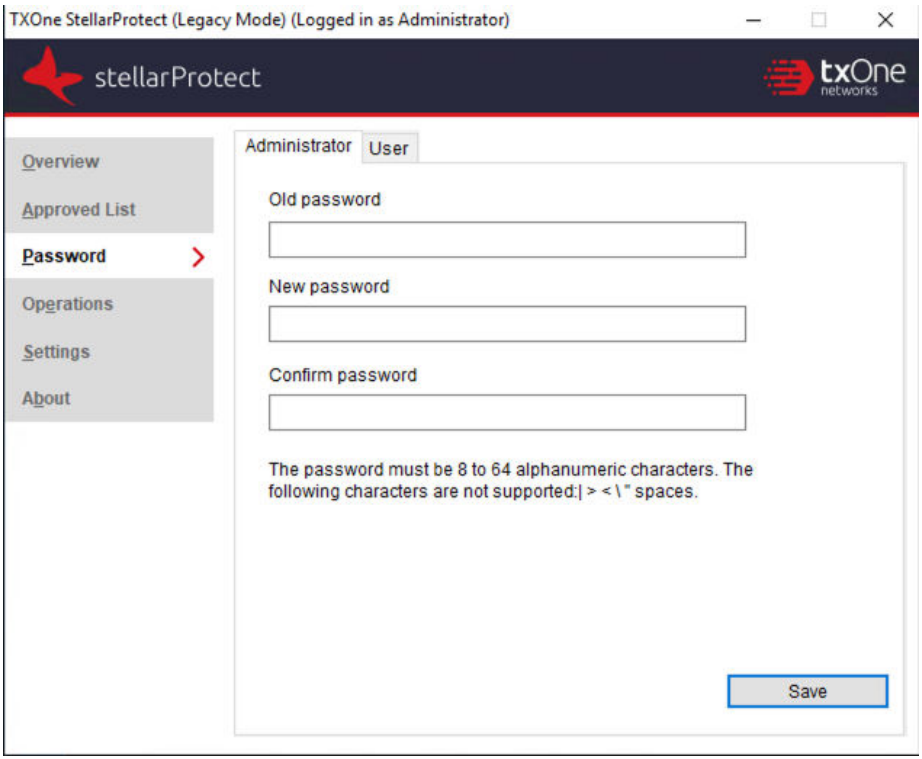

FIGURE 3-15. Password Screen

The following table show privileges available with the two account types. To sign in with a specific account, specify the password for that account.

TABLE 3-7. StellarProtect (Legacy Mode) Account Types

ACCOUNT	DETAILS
Administrator	• Default account • Full access to StellarProtect (Legacy Mode) functions • Can use both the console GUI and command line interface (CLI)
User	• Secondary maintenance account • Limited access to StellarProtect (Legacy Mode) functions • Can only use the console GUI

Account Settings

Only the Administrator can change the passwords of StellarProtect (Legacy Mode) **Administrator** and **User** accounts via the console,. To log on the console as the administrator account, provide the administrator password when launching the console.

Important

The StellarProtect (Legacy Mode) Administrator and User passwords cannot be the same.

Procedure

1. Open the TXOne console using the desktop icon (if available) or the **Start** menu by clicking **All Programs** > **TXOne StellarProtect (Legacy Mode)**.
2. Provide the StellarProtect (Legacy Mode) administrator password and click **Log On**.
3. Click the **Password** on the **Side Navigation Menu** to display the **Administrator** password page.
    - To change the StellarProtect (Legacy Mode) administrator password:

a. Provide the current password, specify and confirm the new password, and click **Save**.

WARNING!

Please treat your StellarProtect (Legacy Mode) administrator password with care. If you lose it, please contact TXOne Networks support.

- To create a User password:
  a. Click the tab to switch to the **User** page
  b. Select the **Enable User** check box.
  c. Specify and confirm the password, and click **Save**.
- To change an existing User password:
  a. Specify and confirm the new password, and click **Save**.

Operations

he **Operations** page provides options to perform tasks such as on-demand scan, policy sync, connection check, and maintenance mode setting.

Note

Both the Administrator and User accounts are allowed to access the functions available on the **Operations** page.

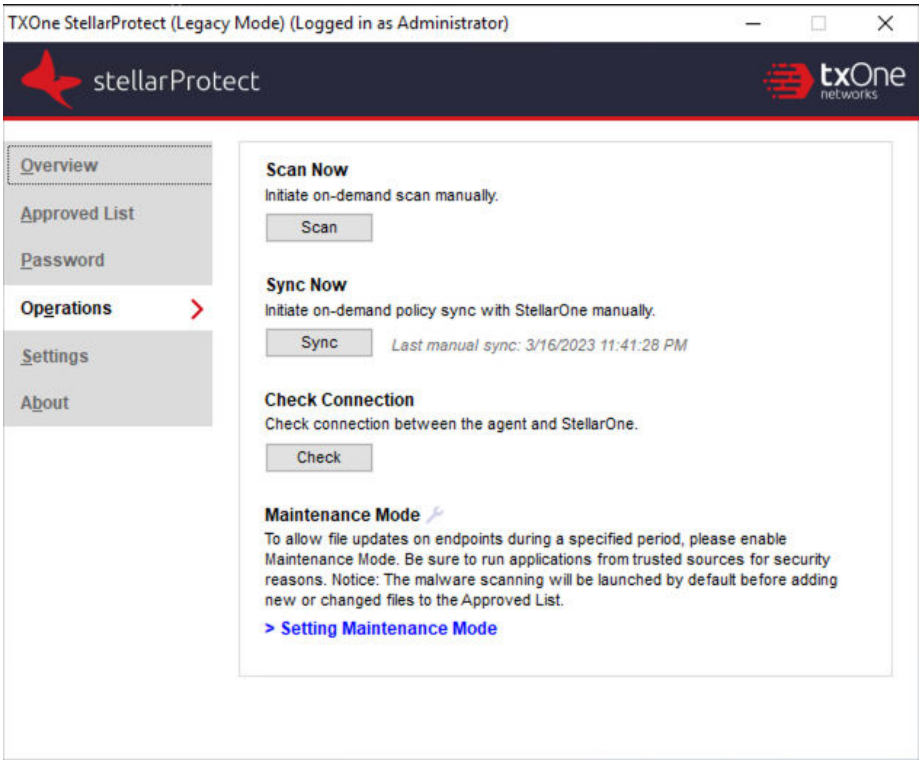

FIGURE 3-16. StellarProtect (Legacy Mode) Operations Page

The following table describes the features available on the **Operations** page.

ITEM	DESCRIPTION
Scan Now	Click the **Scan** button to initiate on-demand scanning. See *Scan Now on page 3-54* for more details.
Sync Now	Click the **Sync** button to synchronize policy with StellarOne server. See *Sync Now on page 3-55*for more details.
Check Connection	Click the **Check** button to check if the agent is properly connected with the StellarOne server. See *Check Connection on page 3-55*for more details.

Item	Description
Maintenance Mode	Read the description of the Maintenance Mode carefully and click **Setting Maintenance Mode** to enable or disable it. See *Setting Maintenance Mode on page 3-56* for more details.

Scan Now

The **Scan** button on the **Operations** page enables both the Administrator and User accounts to manually initiate on-demand scan when needed.

Procedure

1. Open the TXOne console using the desktop icon (if available) or the **Start** menu by clicking **All Programs** > **TXOne StellarProtect (Legacy Mode)**.
2. Provide the StellarProtect (Legacy Mode) Administrator or User password and click **Log On**.
3. Click **Operations** on the **Side Navigation Menu**.
4. Find the **Scan Now** section and click the **Scan** button.
5. The **Scan Settings** window appears. Click **Start** to initiate the scan.

   Note

   - Only the StellarOne administrator can configure the scan settings. See *Advanced Settings for Scheduled Scan* section in the *StellarOne Administrator's Guide* for more details.
   - It may take a while to complete the scanning.

6. A scan result appears indicating threats detected. Click **OK** to complete the scan task.

Sync Now

The **Sync** button on the **Operations** page enable both the Administrator and User accounts to manually initiate on-demand policy sync with StellarOne when needed.

Procedure

1. Open the TXOne console using the desktop icon (if available) or the **Start** menu by clicking **All Programs** > **TXOne StellarProtect (Legacy Mode)**.
2. Provide the StellarProtect (Legacy Mode) Administrator or User password and click **Log On**.
3. Click **Operations** on the **Side Navigation Menu**.
4. Find the **Sync Now** section and click the **Sync** button.
5. A successful message appears. The **Last manual sync** next to the **Sync** button indicates the last time the policy sync has been manually initiated and succesfully completed.

Check Connection

The **Check** button on the **Operations** page enable both the Administrator and User accounts to manually initiate connection check to see if the agent is properly connected with StellarOne.

Procedure

1. Open the TXOne console using the desktop icon (if available) or the **Start** menu by clicking **All Programs** > **TXOne StellarProtect (Legacy Mode)**.
2. Provide the StellarProtect (Legacy Mode) Administrator or User password and click **Log On**.
3. Click **Operations** on the **Side Navigation Menu**.
4. Find the **Check Connection** section and click the **Check** button.

5. A successful message appears. The **Last connection check** next to the **Check** button indicates the last time the connection check has been manually initiated and succesfully completed.

Setting Maintenance Mode

To perform approved file updates or system maintenance on endpoints, you can configure Maintenance Mode for a specified period of time. During the Maintenance Mode, StellarProtect (Legacy Mode) allows all file executions and adds all files that are created, executed, or modified to the Approved List.

Besides, StellarProtect (Legacy Mode) can ensure the execution of these applications are under the protected conditions by performing malware scanning before adding new or changed files to the Approved List.

Important

Before using Maintenance Mode, apply the required updates on the following supported platforms for StellarProtect (Legacy Mode) agents:

- 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.

Note

- If you change the settings of Application Lockdown or Threat Prevention during maintenance period, the settings will not be implemented until the maintenance period is ended.
- During the maintenance period, StellarProtect (Legacy Mode)does not support Windows updates that require restarting an endpoint.
- To run an installer that deploys files to a network folder during the maintenance period, StellarProtect (Legacy Mode) must have access permission to the network.

Procedure

1. Open the TXOne console using the desktop icon (if available) or the **Start** menu by clicking **All Programs** > **TXOne StellarProtect (Legacy Mode)**.
2. Provide the StellarProtect (Legacy Mode) Administrator or User password and click **Log On**.
3. Click **Operations** on the **Side Navigation Menu**.
4. Find the **Maintenance Mode** section and read the description carefully.

Note

To know whether the agent is currently in maintenance mode, check the **Overview** page or the **Maintenance Mode** section on the **Operations** page.

- : Indicates the agent is in maintenance mode. A timestamp appears near the icon indicating the maintenance start time (only available on **Overview** page) and end time.
- : Indicates the agent is not in maintenance mode

5. Click **Setting Maintenance Mode** at the bottom.
6. The configuration window appears.
   - Click **Disable** to end Maintenance Mode.

Important

If the Maintenance Mode is ended, the endpoint will start blocking the execution of files that are not recognized by the Application Lockdown.

   - Click **Enable** to start the Maintenance Mode settings.
     a. Specify the duration of the maintenance period in **Maintenance Mode will be ended after ... hour (s)**.

b. (Optional) If Real-Time Scan is disabled, the **Scan the endpoint before adding new or changed files to the Approved List** toggle appears at the bottom of this window and is set **enabled** by default.

Note

- TXOne Networks suggests you keep this toggle turned on to ensure all the new or changed files go through the malware scanning before they're added to the Approved List.
- When the agent is about to leave Maintenance Mode, restarting the endpoint prevents StellarProtect (Legacy Mode) from adding files in the queue to the Approved List.

c. Click **OK** to complete the settings.

Important

To reduce risk of infection, run only applications from trusted sources on endpoints during the maintenance period.

About Feature Settings

StellarProtect (Legacy Mode) offers the following protection features.

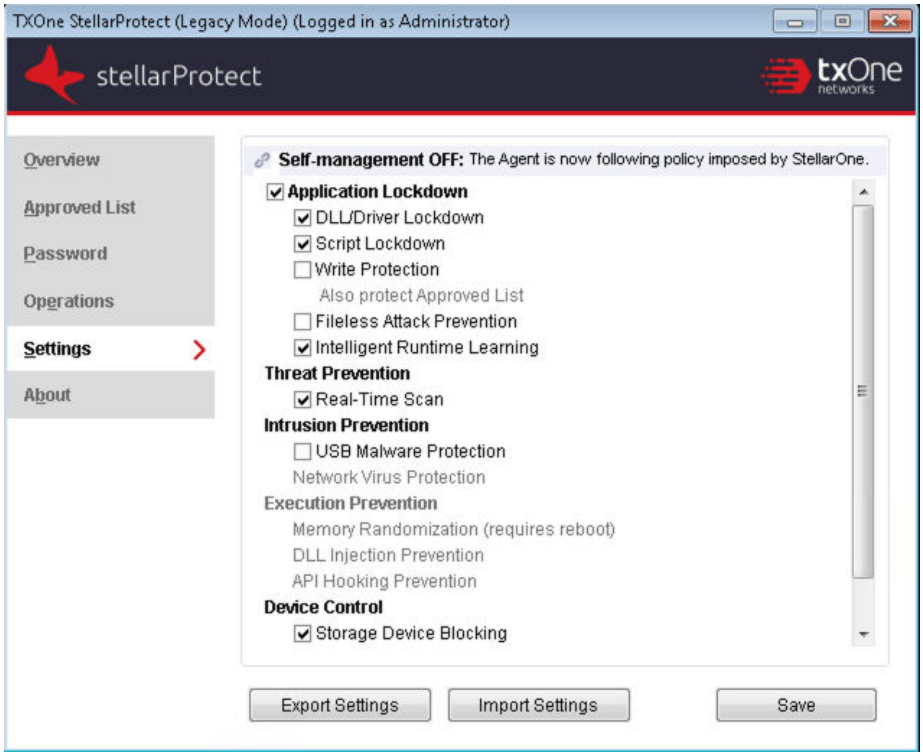

FIGURE 3-17. StellarProtect (Legacy Mode) Settings Screen

TABLE 3-8. Application Lockdown

SETTING	DESCRIPTION	
Application Lockdown	When Application Lockdown is turned on, the agent will only be able to access applications that are in the Approved List; the applications not in the Approved List will be blocked.	
DLL/Driver Lockdown	DLL/Driver Lockdown prevents unapproved DLLs or drivers from being loaded into the memory of protected endpoints.	**Important** To enable DLL/Driver Lockdown, Script Lockdown, Write Protection, or Fileless Attack Prevention, ensure that Application Lockdown is also enabled on the managed endpoint.
Script Lockdown	Script Lockdown prevents unapproved script files from being run on protected endpoints.	
Write Protection	Write Protection prevents write access to objects (files, folders, and registry entries) in the Write Protection List and optionally prevents write access to files in the Approved List.	
Fileless Attack Prevention	Fileless Attack Prevention detects and blocks unapproved process chains and arguments that may lead to a fileless attack event.	
Intelligent Runtime Learning	Intelligent Runtime Learning allows runtime executable files that are generated by applications in the Approved List.	

TABLE 3-9. Threat Prevention

SETTING	DESCRIPTION
Real-Time Scan	Real-time Scan provides persistent and ongoing file scan for the endpoints. Each time a file is received, opened, downloaded, copied, or modified, Real-Time Scan always scans the file for security assessment. If a security risk or possible virus/malware has been detected during the scanning, a notification message appears indicating the name of the infected file and the specific security risk. Moreover, a persistent scan cache is maintained and reloaded each time the Real-time Scan is executed. The Real-time Scan tracks any changes made to files or folders that have occurred until the function is disabled and the files are unloaded and removed from the scan cache.

TABLE 3-10. Execution Prevention

SETTING	DESCRIPTION
Memory Randomization	Address Space Layout Randomization (ASLR) helps prevent shellcode injection by randomly assigning memory locations for important functions, forcing an attacker to guess the memory location of specific processes. Enable this feature on older operating systems such as Windows XP or Windows Server 2003, which may lack or offer limited Address Space Layout Randomization support. **Note** The endpoint must be restarted to enable or disable Memory Randomization.

Setting	Description
DLL Injection Prevention	DLL Injection Prevention detects and blocks API call behaviors used by malicious software. Blocking these threats helps prevent malicious processes from running. Never disable this feature except in troubleshooting situations since it protects the system from a wide variety of serious threats.
API Hooking Prevention	API Hooking Prevention detects and blocks malicious software that tries to intercept and alter messages used in critical processes within the operating system. Never disable this feature except in troubleshooting situations since it protects the system from a wide variety of serious threats.

Table 3-11. Device Control & Other

Setting	Description
Storage Device Blocking	Blocks storage devices, including USB drives, CD/DVD drives, and floppy disks from accessing the managed endpoint.
Integrity Monitoring	Integrity Monitoring logs events related to changes for files, folders, and the registry on the managed endpoint. **Note** To view Integrity Monitoring logs on the managed endpoint, go to **Start** > **Control Panel** > **Administrative Tools** and access Event Viewer.

See *Enabling or Disabling Feature Settings on page 3-63* for how to enable or disable the feature settings.

Enabling or Disabling Feature Settings

Follow the procedures to enable or disable feature settings for StellarProtect (Legacy Mode) agents.

Note

By default, TXOne StellarProtect (Legacy Mode) enables the DLL/Driver Lockdown and Script Lockdown features under the Application Lockdown.

Procedure

1. Open the TXOne console using the desktop icon (if available) or the **Start** menu by clicking **All Programs** > **TXOne StellarProtect (Legacy Mode)**.
2. Provide the Administrator password and click **Log On**.
3. Click the **Settings** on the **Side Navigation Menu** to configure the feature settings.
4. Check or uncheck to enable or disable the desired features.
5. Click **Save**.

About StellarProtect (Legacy Mode)

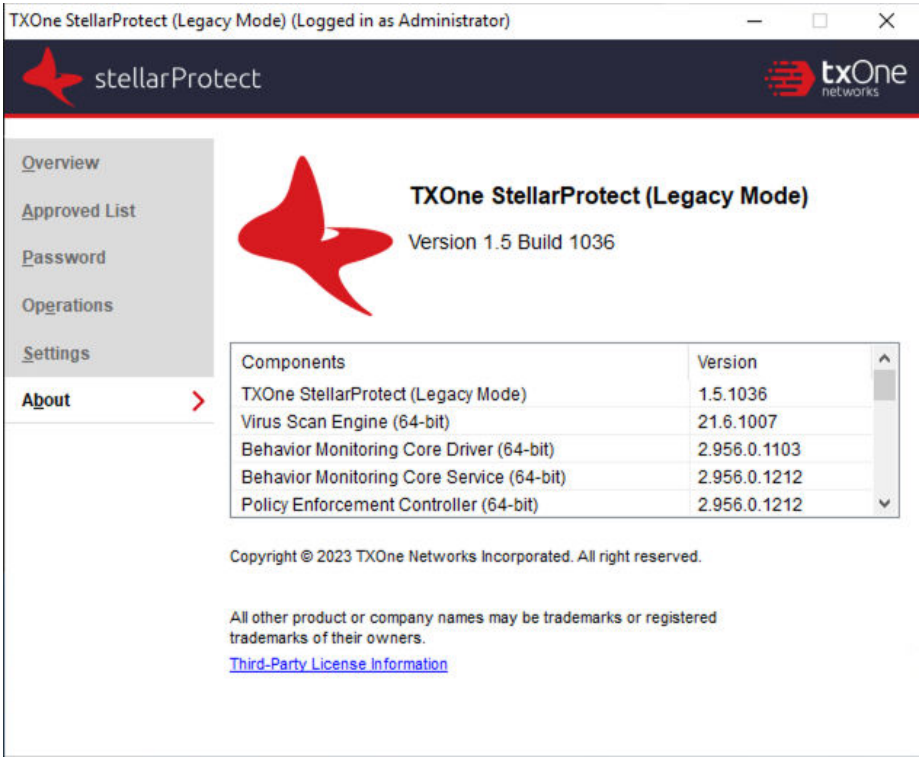

FIGURE 3-18. About StellarProtect (Legacy Mode)

You can find StellarProtect (Legacy Mode) product information, version and build number, scan components, and third-party license information on this page.

Chapter 4

Using the Agent Command Line Interface (CLI)

This chapter describes how to configure and use TXOne StellarProtect/ StellarProtect (Legacy Mode) using the command line interface (CLI).

Topics in this chapter include:

Using StellarProtect Command Line Interface (CLI)

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

Topics include:

Using OPCmd at the Command Line Interface (CLI)

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

Procedure

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

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

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

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

Overview of StellarProtect CLI

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

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

The global-options are options that affect all commands, and must come before the command. A command consists of one or more words, followed

by any options that are specific to that command. If an option requires an argument, you may specify the argument in one of the following syntaxes:

Options

Separate long option and argument with an equal sign:

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

Argument follows the option character immediately:

```
-o<argument>
```

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

```
-o <argument>
```

Important

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

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

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

Global Options

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

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

Argument: No

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

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

  

  Note

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

  Argument: Optional. Password in plain text.

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

  Description: Show CLI program version.

  Argument: No

OPCmd Program Commands

TABLE 4-1. List of All Commands

COMMAND	DESCRIPTION	OPTIONS
`opcmd.exe about components`	You can browse versions of components from the GUI program, or you can get the list in YAML format with this command.	None

Command	Description	Options
`opcmd.exe -p appinv make`	The StellarProtect service will re-detect installed OT/ICS applications when your scheduled maintenance mode ends. You can also use this command to perform the detection manually at any time.	None
`opcmd.exe appinv list`	You can browse the list of detected OT/ICS applications from the GUI program or use this command to get the list in YAML format.	None
`opcmd.exe -p config decrypt [-i INPUT-FILE] [-o OUTPUT-FILE]`	Decrypts an encrypted configuration file and outputs decrypted plaintext. **Note** The data security of this command is designed for the protection of configuration files. Do not rely on this command to protect personal privacy data.	`-i, --input INPUT - FILE`: The required argument to specify the filename of an input file. If it's omitted, the program will read from standard input. `-o, --output OUTPUT - FILE`: The required argument to specify the filename of an output file. If it's omitted, the program will write to standard output.

Command	Description	Options
`opcmd.exe -p config encrypt [-i INPUT-FILE] [-o OUTPUT-FILE]`	Encrypts a plaintext configuration file and outputs encrypted ciphertext. **Note** The data security of this command is designed for protection of configuration files. Do not rely on this command to protect any personal privacy data.	`-i, --input INPUT-FILE`: The required argument to specify the filename of an input file. If it's omitted, the program will read from standard input. `-o, --output OUTPUT-FILE`: The required argument to specify the filename of an output file. If it's omitted, the program will write to standard output.
`opcmd.exe -p config export OUTPUT-FOLDER`	Exports product configuration settings to the specified folder.	None
`opcmd.exe -p config import INPUT-FOLDER`	Imports product configuration settings from the specified folder.	`-n, --no_ptn` **Note** Do not import pattern files.
`opcmd.exe -p dip disable`	Disables the DLL Injection Prevention function.	None
`opcmd.exe -p dip enable`	Enables the DLL Injection Prevention function.	None
`opcmd.exe -p lock appinv disable`	Disables OT Application Safeguard	None
`opcmd.exe -p lock appinv enable`	Enables OT Application Safeguard	None

Command	Description	Options
`opcmd.exe -p lock disable`	Disables the Change Control module to allow file changes on protected files.	None
`opcmd.exe -p lockdown approvedlist info`	Shows Application Lockdown Approved List information.	None
`opcmd.exe -p lockdown approvedlist init [--overwrite]`	Initializes Appplication Lockdown Approved List.	`-o`, `--overwrite`: This command is used to overwrite existing Application Lockdown Approved List. If `-o` is not specified, detected applications will be added to existing Appplication Lockdown Approved List.
`opcmd.exe -p lockdown approvedlist add -p PATH [--recursive]`	Adds the specified file to the Application Lockdown Approved List	`-p`, `--path PATH`: Adds the specified file to the Application Lockdown Approved List `-r`, `--recursive`: Includes the specified folder and related subfolders
`opcmd.exe -p lockdown enable -m MODE`	Enables Application Lockdown	`-m`, `--mode MODE`: Specifies the mode (Detect or Enforce) for Application Lockdown
`opcmd.exe -p lockdown disable`	Disables Application Lockdown	None
`opcmd.exe -p lockdown exceptionpath -t TYPE -p PATH (--add|--remove)`	Adds or removes an Application Lockdown exception path	`-t`, `--type TYPE`: Specifies type of exception path (file, folder, folder and subfolder, ecmascript_regexp). `-p`, `--path PATH`: Specifies exception path or regexp.
`opcmd.exe -p lockdown info`	Shows Application Lockdown information	None

Command	Description	Options
`opcmd.exe -p lockdown script info`	Display all Application Lockdown script rules	None
`opcmd.exe -p lockdown script add -e EXTENSION -p INTERPRETER [-p INTERPRETER2] ...`	Adds the specified script extension and the interpreter required to execute the script	`-e, --ext EXTENSION`: Specifies script extension `-p, --proc INTERPRETER`: Specifies name of script interpreter
`opcmd.exe -p lockdown script remove -e EXTENSION [-p INTERPRETER] ...`	Removes the specified script extension and the interpreter required to execute the script	`-e, --ext EXTENSION`: Specifies script extension `-p, --proc INTERPRETER`: Specifies name of script interpreter
`opcmd.exe -p lockdown subfeature -f SUB-FEATURE (--enable|--disable)`	Toggles sub-feature of Application Lockdown	`-f, --feature SUB-FEATURE`: Specifies sub-feature (dll_driver, script, intelligent_runtime_learning)
`opcmd.exe -p lockdown trustedhash -h HASH (--add|--remove)`	Adds or removes an Application Lockdown trusted hash	`-h, --hash HASH`: Specifies trusted hash **Note** Only `SHA-256` is supported.
`opcmd.exe -p lock enable`	Enables Change Control module to prevent file changes on protected files. If Change Control module is disabled by a scheduled maintenance mode, this command will end the maintenance mode immediately.	None

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

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

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

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

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

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

Command	Description	Options
`opcmd.exe -p update-task`	Schedules a recurring update task at specified start time and interval	`--time START-TIME`: Specifies the start time (HH:MM) of scheduled update. `--daily`: Specifies the scheduled update to run daily. `--weekly DAY-OF-WEEK`: Specifies the scheduled update to run weekly on a given day of a week. Only Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday are valid. `--monthly DAY-OF-MONTH`: Specifies the scheduled update to run monthly on a given day of a month (1-31). Specifies `-1` to run the update on the last day of a month. `--remove`: Removes the scheduled update
`opcmd.exe -p user enable`	Enable the User account and specify User password if needed	`-p --password`: Specifies the User password
`opcmd.exe -p user disable`	Disable the User account	None
`opcmd.exe -p user info`	Show status of the User account	None
`opcmd.exe -p rts start`	Enable Real-Time Scan	None
`opcmd.exe -p rts stop`	Disable Real-Time Scan	None

Using StellarProtect (Legacy Mode) Command Line Interface (CLI)

This section describes how to configure and use TXOne StellarProtect (Legacy Mode) using the command line interface (CLI).

Topics include:

Using SLCmd at the Command Line Interface (CLI)

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

Procedure

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

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

   `cd /d "c:\Program Files\TXOne\`StellarProtect (Legacy Mode)
3. Type `SLCmd.exe -h` to get usage information for an individual command.

SLCmd Program and Console Function Comparison

The following table lists the TXOne StellarProtect (Legacy Mode) features available in SLCmd program and the StellarProtect (Legacy Mode) console program.

Function	SLCmd Program at the Command Line Interface (CLI)	Console
Account Management	Yes	Yes
Agent Event Aggregation	No	No
Approved List Management	Yes	Yes
Decrypt/Encrypt configuration file	Yes	No
Display the blocked log	Yes	Yes
Export/Import Approved List	Yes	Yes
Export/Import configuration	Yes	Yes
Group Policy/Global Policy	No	No
Install	Yes	Yes
Intelligent Runtime Learning	Yes	Yes
Windows Update Support	Yes	No
Application Lockdown	Yes	Yes
Write Protection	Yes	Yes
Write Protection Exceptions	Yes	No
Integrity Monitoring	Yes	Yes
Exception Paths	Yes	No
License Management	Yes	Yes
Administrator password	Yes	Yes
Turn on/off Application Lockdown	Yes	Yes
Enable/disable pop-up notifications for blocked files	Yes	No

Function	SLCmd Program at the Command Line Interface (CLI)	Console
Start/Stop Trusted Updater	Yes	Yes
Trusted Hash List	Yes	No
Start/Stop the service	Yes	No
Uninstall	No	No
Storage Device Control	Yes	Yes
Fileless Attack Prevention	Yes	Yes
Add Trusted USB Device	Yes	No
Configure Maintenance Mode	Yes	No
On-demand Scan	Yes	No
Real-Time Scan	Yes	Yes

Not all settings are available through the command line interface (CLI) or console. Refer to *Working with the Agent Configuration File on page 4-2 on page 5-2* for information about modifying the system configuration.

Overview of StellarProtect (Legacy Mode) CLI

The following tables list summary commands available using the `SLCmd` program at the command line interface (CLI). To use the program, type `SLCmd` and the desired command. Type `SLCmd` and press ENTER to display the list of available commands

Note

Only a StellarProtect (Legacy Mode) administrator with Windows administrator privileges can use `SLCmd` at the command line interface (CLI). `SLCmd` will prompt for the administrator password before running certain commands.

The following is a full list of commands available using the `SLCmd` program.

General Commands

Perform general actions using the Command Line Interface.

The following table lists the available abbreviated forms of parameters.

TABLE 4-2. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
`adminpassword`	`ap`	Manage the StellarProtect (Legacy Mode) admistrator password
`lock`	`lo`	Manage Application Lockdown status
`blockedlog`	`bl`	Manage the applications blocked by StellarProtect (Legacy Mode)
`license`	`lc`	Manage the StellarProtect (Legacy Mode) license
`settings`	`set`	Manage the StellarProtect (Legacy Mode) settings
`service`	`srv`	Manage the StellarProtect (Legacy Mode) service

SLCmd Program Commands

The following table lists the commands, parameters, and values available.

TABLE 4-3. General Commands

COMMAND	PARAMETER	DESCRIPTION
`help`		Display a list of StellarProtect (Legacy Mode) commands For example, type: `SLCmd.exe help`
`activate`	`<license_key>`	Activate the StellarProtect (Legacy Mode) program using the specified license key. For example, type: `SLCmd.exe activate XX-XXXX-XXXXX-XXXXXXXXXX-XXXXX-XXXXX`

`set adminpassword`	`<new_password>`	Prompt the currently logged on administrator to specify a new password
		For example, type:
		`SLCmd.exe -p <admin_password> set adminpassword`
		Change the currently logged on administrator password to the newly specified password
		For example, type:
		`SLCmd.exe -p <admin_password> set adminpassword P@ssW0Rd`

Command	Parameter	Description
`set lock`		Display the current StellarProtect (Legacy Mode) Application Lockdown status For example, type: `SLCmd.exe -p <admin_password> set lock` **Note** The default status is "disable".
	`enable`	Turn on Application Lockdown For example, type: `SLCmd.exe -p <admin_password> set lock enable`
	`disable`	Turn off Application Lockdown For example, type: `SLCmd.exe -p <admin_password> set lock disable`

Command	Parameter	Description
`set blockedfilenotification`		Display the current notification setting For example, type: `SLCmd.exe -p <admin_password> set blockedfilenotification` **Note** The default status is "disable".
	`enable`	Display a notification on the managed endpoint when StellarProtect (Legacy Mode) blocks a file. For example, type: `SLCmd.exe -p <admin_password> set blockedfilenotification enable`
	`disable`	Do not display any notification when StellarProtect (Legacy Mode) blocks a file. For example, type: `SLCmd.exe -p <admin_password> set blockedfilenotification disable`

Command	Parameter	Description
`show blockedlog`		Display a list of applications blocked by StellarProtect (Legacy Mode) For example, type: `SLCmd.exe -p <admin_password> show blockedlog`
`show license`		Display the current StellarProtect (Legacy Mode) license information For example, type: `SLCmd.exe show license`
`show settings`		Display the current status of the vulnerability attack prevention features For example, type: `SLCmd.exe -p <admin_password> show settings`
`start service`		Start the StellarProtect (Legacy Mode) service For example, type: `SLCmd.exe start service`
`status`		Display the current status of Application Lockdown and the auto update function of the Approved List For example, type: `SLCmd.exe -p <admin_password> status`

Command	Parameter	Description
`stop service`		Stop the StellarProtect (Legacy Mode) service For example, type: `SLCmd.exe -p <admin_password> stop service`
`version`		Display the current versions of StellarProtect (Legacy Mode) components For example, type: `SLCmd.exe -p <admin_password> version`

Central Management Commands

Configure central management features using the Command Line Interface by typing your command in the following format:

```
SLCmd.exe -p <admin_password> <command> <parameter> <value>
```

To illustrate, if users want to test the agent-server connection, type:
`SLCmd.exe -p <admin_password> test mm`

The following table lists the available abbreviated forms of parameters.

Table 4-4. Abbreviations and Uses

Parameter	Abbreviation	Use
`managedmodeconfiguration`	`mmc`	Manage the configuration file
`servercertification`	`sc`	Manage server certificate files
`managedmode`	`mm`	Manage agent “Managed Mode”

The following table lists the commands, parameters, and values available.

TABLE 4-5. Central Management Commands

COMMAND	PARAMETER	DESCRIPTION
decrypt managedmodeconfiguration	<path_of_encrypted_file> <path_of_decrypted_output_file>	Decrypt the configuration file used by Managed Mode
encrypt managedmodeconfiguration	<path_of_file> <path_of_encrypted_output_file>	Encrypt the configuration file used by Managed Mode
export managedmodeconfiguration	<path_of_encrypted_output>	Export the encrypted configuration file used by Managed Mode
export servercertification	<path_of_certificate_file>	Export the encrypted StellarOne SSL communication certificate file
import managedmodeconfiguration	<path_of_encrypted_input>	Import the encrypted configuration file used by Managed Mode
import servercertification	<path_of_certificate_file>	Import the encrypted StellarOne SSL communication certificate file

Command	Parameter	Description
`set managedmode`	`enable [-cfg <path_of_encrypted_file>] [-sc <path_of_certificate_file>]`	Enable Managed Mode **Note** The default status is "disable". The following optional parameters are available: • `-cfg <path_of_encrypted_file>` Use -cfg value to specify the path of the configuration file • `-sc <path_of_certificate_file>`Use -sc value to specify the path of the ertificate file
`set managedmode`		Display the current Managed Mode status
`show managedmodeconfiguration`		Display the configuration used by Managed Mode
`test managedmode`		Connect a test Managed Mode session with StellarOne server

Optional Feature Commands

Configure optional security features using the Command Line Interface by typing your command in the following format:

```
SLCmd.exe -p <admin_password> <command> <parameter> <value>
```

The following table lists the available abbreviated forms of parameters.

TABLE 4-6. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
apihookingprevention	api	Manage API Hooking Prevention
customaction	ca	Manage actions taken when StellarProtect (Legacy Mode) blocks specific types of events
dlldriverlockdown	dd	Manage DLL/Driver Lockdown
dllinjectionprevention	dll	Manage DLL Injection Prevention
exceptionpath	ep	Manage exceptions to Application Lockdown
integritymonitoring	in	Manage Integrity Monitoring
memoryrandomization	mr	Manage Memory Randomization
script	scr	Manage Script Lockdown
storagedeviceblocking	sto	Allows or blocks storage devices (CD/DVD drives, floppy disks, and network drives) from accessing the managed endpoint.
usbmalwareprotection	usb	Manage USB Malware Protection
writeprotection	wp	Manage Write Protection

Parameter	Abbreviation	Use
writeprotection-includesapprovedlist	wpal	Manage Write Protection including the Approved List

The following table lists the commands, parameters, and values available.

Table 4-7. Optional Feature Commands

Command	Parameter	Description
set apihookingprevention		Display the current status of API Hooking Prevention For example, type: `SLCmd.exe -p <admin_password> set apihookingprevention`
	enable	Enable API Hooking Prevention For example, type: `SLCmd.exe -p <admin_password> set apihookingprevention enable` **Note** The default status is "disable".
	disable	Disable API Hooking Prevention For example, type: `SLCmd.exe -p <admin_password> set apihookingprevention disable`

Command	Parameter	Description
`set customaction`		Display the current setting for actions taken when StellarProtect (Legacy Mode) blocks specific types of events **Note** The default setting is "ask".
	`ignore`	Ignore blocked files or processes when Application Lockdown blocks any of the following events: • Process launch • DLL loading • Script file access For example, type: `SLCmd.exe -p <admin_password> set customaction ignore`
	`quarantine`	Quarantine blocked files or processes when Application Lockdown blocks any of the following events: • Process launch • DLL loading • Script file access For example, type: `SLCmd.exe -p <admin_password> set customaction quarantine`

Command	Parameter	Description
		Note StellarProtect (Legacy Mode) does not support a custom action of "quarantine" on Windows (Standard) XP Embedded SP1.
	`ask`	Ask what to do for blocked files or processes when Application Lockdown blocks any of the following events: • Process launch • DLL loading • Script file access For example, type: `SLCmd.exe -p <admin_password> set customaction ask`
`set dlldriverlockdown`		Display the current status of DLL/Driver Lockdown For example, type: `SLCmd.exe -p <admin_password> set dlldriverlockdown` **Note** The default status is "enable".
	`enable`	Enable DLL/Driver Lockdown

Command	Parameter	Description
		For example, type: `SLCmd.exe -p <admin_password> set dlldriverlockdown enable`
	`disable`	Disable DLL/Driver Lockdown For example, type: `SLCmd.exe -p <admin_password> set dlldriverlockdown disable`
`set dllinjectionprevention`		Display the current status of DLL Injection Prevention For example, type: `SLCmd.exe -p <admin_password> set dllinjectionprevention` **Note** The default status is "disable".
	`enable`	Enable DLL Injection Prevention For example, type: `SLCmd.exe -p <admin_password> set dllinjectionprevention enable`
	`disable`	Disable DLL Injection Prevention For example, type:

Command	Parameter	Description
		`SLCmd.exe -p <admin_password> set dllinjectionprevention disable`
`set exceptionpath`		Display current setting for using exceptions to Application Lockdown For example, type: `SLCmd.exe -p <admin_password> set exceptionpath` **Note** The default setting is "disable".
	`enable`	Enable exceptions to Application Lockdown For example, type: `SLCmd.exe -p <admin_password> set exceptionpath enable`
	`disable`	Disable exceptions to Application Lockdown For example, type: `SLCmd.exe -p <admin_password> set exceptionpath disable`
`set integritymonitoring`		Display the current status of Integrity Monitoring For example, type:

COMMAND	PARAMETER	DESCRIPTION
		`SLCmd.exe -p <admin_password> set integritymonitoring` **Note** The default setting is "disable".
	`enable`	Enable Integrity Monitoring For example, type: `SLCmd.exe -p <admin_password> set integritymonitoring enable`
	`disable`	Disable Integrity Monitoring For example, type: `SLCmd.exe -p <admin_password> set integritymonitoring disable`
`set memoryrandomization`		Display the current status of Memory Randomization For example, type: `SLCmd.exe -p <admin_password> set memoryrandomization` **Note** The default setting is "disable".
	`enable`	Enable Memory Randomization

Command	Parameter	Description
		For example, type: `SLCmd.exe -p <admin_password> set memoryrandomization enable`
	`disable`	Disable Memory Randomization For example, type: `SLCmd.exe -p <admin_password> set memoryrandomization disable`
`set script`		Display the current status of Script Lockdown For example, type: `SLCmd.exe -p <admin_password> set script` **Note** The default setting is "enable".
	`enable`	Enable Script Lockdown For example, type: `SLCmd.exe -p <admin_password> set script enable`
	`disable`	Disable Script Lockdown For example, type:

COMMAND	PARAMETER	DESCRIPTION
		`SLCmd.exe -p <admin_password> set script disable`
`set storagedeviceblocking`		Display the current status of Storage Device Blocking For example, type: `SLCmd.exe -p <admin_password> set storagedeviceblocking` **Note** The default setting is "disable".
	`enable`	Enable Storage Device Blocking For example, type: `SLCmd.exe -p <admin_password> set storagedeviceblocking enable`
	`disable`	Disable Storage Device Blocking For example, type: `SLCmd.exe -p <admin_password> set storagedeviceblocking disable`
`set usbmalwareprotection`		Display the current status of USB Malware Protection For example, type:

Command	Parameter	Description
		`SLCmd.exe -p <admin_password> set usbmalwareprotection` **Note** The default setting is "disable".
	`enable`	Enable USB Malware Protection For example, type: `SLCmd.exe -p <admin_password> set usbmalwareprotection enable`
	`disable`	Disable USB Malware Protection For example, type: `SLCmd.exe -p <admin_password> set usbmalwareprotection disable`
`set writeprotection`		Display the current status of Write Protection For example, type: `SLCmd.exe -p <admin_password> set writeprotection` **Note** The default setting is "disable".

COMMAND	PARAMETER	DESCRIPTION
	`enable`	Enable Write Protection For example, type: `SLCmd.exe -p <admin_password> set writeprotection enable`
	`disable`	Disable Write Protection For example, type: `SLCmd.exe -p <admin_password> set writeprotection disable`
`set writeprotection-includes-approvedlist`		Display the current status of Write Protection including the Approved List For example, type: `SLCmd.exe -p <admin_password> set writeprotection-includesapprovedlist` **Note** The default status is "disable". However, the status changes to "enabled" if Write Protection is enabled.
	`enable`	Enable protection of the Approved List (in addition to the Write Protection List) when Write Protection is enabled For example, type:

Command	Parameter	Description
		`SLCmd.exe -p <admin_password> set writeprotection-includesapprovedlist enable`
	`disable`	Disable protection of the Approved List (in addition to the Write Protection List) when Write Protection is enabled For example, type: `SLCmd.exe -p <admin_password> set writeprotection-includesapprovedlist disable`

User Account Commands

Configure the User Account using the Command Line Interface by typing your command in the following format:

```
SLCmd.exe -p <admin_password> <command> <parameter> <value>
```

The following table lists the available abbreviated forms of parameters.

Table 4-8. Abbreviations and Uses

Parameter	Abbreviation	Use
`user`	`us`	Manage the User account
`userpassword`	`up`	Manage the User password

The following table lists the commands, parameters, and values available.

TABLE 4-9. User Account Commands

COMMAND	PARAMETER	DESCRIPTION
`set user`		Display the User account status For example, type: `SLCmd.exe -p <admin_password> set user` **Note** The default status is "disable".
	`enable`	Enable the User account For example, type: `SLCmd.exe -p <admin_password> set user enable`
	`disable`	Disable the User account For example, type: `SLCmd.exe -p <admin_password> set user disable`
`set userpassword`		Prompt the currently logged on administrator to specify a new User account password For example, type: `SLCmd.exe -p <admin_password> set userpassword`

Command	Parameter	Description
	`ignore`	Change the User account password to the newly specified password For example, type: `SLCmd.exe -p <admin_password> set userpassword P@ssW0Rd`

Script Commands

Deploy scripts using the Command Line Interface by typing your command in the following format:

```
SLCmd.exe -p <admin_password> <command> <parameter> <value>
```

The following table lists the available abbreviated forms of parameters.

Table 4-10. Abbreviations and Uses

Parameter	Abbreviation	Use
`script`	`scr`	Manage script commands

The following table lists the commands, parameters, and values available.

TABLE 4-11. Script Commands

COMMAND	PARAMETER	DESCRIPTION
`add script`	`<extension>[interpreter 1][interpreter2]`	Add the specified script extension and the interpreter(s) required to execute the script For example, to add the script extension `JSP` with the interpreter file `jscript.js`, type: `SLCmd.exe -p <admin_password> add script jsp C:\Scripts \jscript.js`

Command	Parameter	Description
`remove script`	`<extension>[interpreter 1][interpreter2]`	Remove the specified script extension and the interpreter(s) required to execute the script For example, to remove the script extension `JSP` with the interpreter file `jscript.js`, type: `SLCmd.exe -p <admin_password> remove script jsp C:\Scripts \jscript.js` **Note** If you do not specify any interpreter, the command removes all interpreters related to the script extension. If you specify interpreters, the command only removes the interpreters specified from the script extension rule.
`show script`		Display all script rules For example, type: `SLCmd.exe -p <admin_password> show script`

Note

StellarProtect (Legacy Mode) uses the following default script rules:

- bat <cmd.exe>
- cmd <cmd.exe>
- com <ntvdm.exe>
- dll <ntvdm.exe>
- drv <ntvdm.exe>
- exe <ntvdm.exe>
- js <cscript.exe>, <wscript.exe>
- msi <msiexec.exe>
- pif <ntvdm.exe>
- ps1 <powershell.exe>
- sys <ntvdm.exe>
- vbe <cscript.exe>, <wscript.exe
- vbs <cscript.exe>, <wscript.exe

Approved List Commands

Configure the Approved List using the Command Line Interface by typing your command in the following format:

```
SLCmd.exe -p <admin_password> <command> <parameter> <value>
```

The following table lists the available abbreviated forms of parameters.

TABLE 4-12. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
approvedlist	al	Manage files in the Approved List

Parameter	Abbreviation	Use
`list`	`li`	Manage the Approved List import and export functions

The following table lists the commands, parameters, and values available.

Table 4-13. Approved List Commands

Command	Parameter	Description
`add approvedlist`	`[-r]<file_or_folder_path>`	Add the specified file to the Approved List For example, to add all Microsoft Office files to the Approved List, type: `SLCmd.exe -p <admin_password> add approvedlist -r "C:\Program Files \Microsoft Office"` **Note** Using the optional `-r` value includes the specified folder and related subfolders.
`remove approvedlist`	`<file_path>`	Remove the specified file from the Approved List For example, to remove `notepad.exe` from the Approved List, type: `SLCmd.exe -p <admin_password> remove approvedlist C:\Windows \notepad.exe`

Command	Parameter	Description
`show approvedlist`		Display the files in the Approved List For example, type: `SLCmd.exe -p <admin_password> show approvedlist`
`check approvedlist`	`-f`	Update the hash values in the Approved List and display detailed results For example, type: `SLCmd.exe -p <admin_password> check approvedlist -f`
	`-q`	Update the hash values in the Approved List and display summarized results For example, type: `SLCmd.exe -p <admin_password> check approvedlist -q`
	`-v`	Compare the hash values in the Approved List with the hash values calculated from the actual files and prompt the user after detecting mismatched values For example, type: `SLCmd.exe -p <admin_password> check approvedlist -v`

Command	Parameter	Description
`export list`	`<output_file>`	Export the Approved List to the file path and file name specified For example, type: `SLCmd.exe -p <admin_password> export list c:\approvedlist\ap.db` **Note** The output file type must be `DB` format.
`import list`	`[o] <input_file>`	Import an Approved List from the file path and file name specified For example, type: `SLCmd.exe -p <admin_password> import list c:\approvedlist\ap.db` **Note** The input file type must be `DB` format. Using the optional `-o` value overwrites the existing list.

Application Lockdown Commands

Perform actions related to Application Lockdown using the Command Line Interface by typing your command in the following format:

```
SLCmd.exe -p <admin_password> <command> <parameter> <value>
```

The following table lists the available abbreviated forms of parameters.

Note

StellarProtect (Legacy Mode) supports extended regular expressions (ERE). For more information, see https://pubs.opengroup.org/onlinepubs/7908799/xbd/re.html#tag_007_004.

TABLE 4-14. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
`quarantinedfile`	`qf`	Manage quarantined files
`exceptionpath`	`ep`	Manage exceptions to Application Lockdown

The following table lists the commands, parameters, and values available.

TABLE 4-15. Application Lockdown Commands

COMMAND	PARAMETER	DESCRIPTION
`show quarantinedfile`		Display a list of quarantined files
`restore quarantinedfile`	`<id> [-al] [-f]`	Restore the specified file from quarantine. Using the optional `-al` value also adds the restored file to the Approved List. Using the optional `-f` value forces the restore.
`remove quarantinedfile`	`<id>`	Delete the specified file
`show exceptionpath`		Display current exceptions to Application Lockdown For example, type: `SLCmd.exe -p <admin_password> show exceptionpath -f`

Command	Parameter	Description
`add exceptionpath`	`-e <file_path> -tfile`	Add an exception for the specified file For example, type: `SLCmd.exe -p <admin_password> add exceptionpath -e c:\sample.bat -t file`
	`-e <folder_path> -t folder`	Add an exception for the specified folder For example, type: `SLCmd.exe -p <admin_password> add exceptionpath -e c:\folder -t folder`
	`-e <folder_path> -t folderandsub`	Add an exception for the specified folder and related subfolders For example, type: `SLCmd.exe -p <admin_password> add exceptionpath -e c:\folder -t folderandsub`
	`-e <regular_expression> -t regexp`	Add an exception using the regular expression For example, type: • `SLCmd.exe -p <admin_password> add exceptionpath -e c:\\folder\\.* -t regexp` • `SLCmd.exe -p <admin_password> add exceptionpath -`

Command	Parameter	Description
		`e \\computer\ \folder\ \.*\ \file.exe -t regexp`
`remove exceptionpath`	`-e <file_path> -tfile`	Add an exception for the specified file For example, type: `SLCmd.exe -p <admin_password> remove exceptionpath -e c:\sample.bat -t file`
	`-e <folder_path> -t folder`	Remove an exception for the specified folder For example, type: `SLCmd.exe -p <admin_password> remove exceptionpath -e c:\folder -t folder` **Note** Specify the exact <folder_path> originally specified in the corresponding add command.
	`-e <folder_path> -t folderandsub`	Remove an exception for the specified folder and related subfolders For example, type: `SLCmd.exe -p <admin_password> remove exceptionpath -e c:\folder -t folderandsub`

Command	Parameter	Description
		Note Specify the exact <folder_path> originally specified in the corresponding add command.
	`-e <regular_expression> -t regexp`	Remove an exception using the regular expression For example, type: `SLCmd.exe -p <admin_password> remove exceptionpath -e c:\\test\\.* -t regexp` **Note** Specify the exact <regular_expression> originally specified in the corresponding add command.
`test exceptionpath`	`<regular_expression> <string> -t regexp`	Check if the regular expression matches the string For example, type: `LCmd.exe -p <admin_password> test exceptionpath C:\\test\\.* C:\\test \\sample.exe -t regexp`

Write Protection Commands

Configure Write Protection List and Write Protection Exception List using the Command Line Interface by typing your command in the following format:

```
SLCmd.exe -p <admin_password> <command> <parameter> <value>
```

The following table lists the available abbreviated forms of parameters.

TABLE 4-16. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
writeprotection	wp	Manage the Write Protection feature
writeprotection- file	wpfi	Manage files in the Write Protection List
writeprotection- folder	wpfo	Manage folders in the Write Protection List
writeprotection-regvalue	wprv	Manage registry values and associated registry keys in the Write Protection List
writeprotection- regkey	wprk	Manage registry keys in the Write Protection List
writeprotection-fileexception	wpfie	Manage files in the Write Protection Exception List
writeprotection-folderexception	wpfoe	Manage folders in the Write Protection Exception List
writeprotection-regvalueexception	wprve	Manage registry values and associated registry keys in the Write Protection Exception List
writeprotectionregkey-exception	wprke	Manage registry keys in the Write Protection Exception List

The following table lists the commands, parameters, and values available.

TABLE 4-17. Write Protection List "File" Commands

COMMAND	PARAMETER	VALUE	DESCRIPTION
show	writeprotection		Display the entire Write Protection List
	writeprotection-file		Display the files in the Write Protection List For example, type: `SLCmd.exe -p <admin_password> show writeprotection-file`
	writeprotection-file-exception		Display the files in the Write Protection Exception List For example, type: `SLCmd.exe -p <admin_password> show writeprotection-file-exception`
	writeprotection-folder		Display the folders in the Write Protection List For example, type: `SLCmd.exe -p <admin_password> show writeprotection-folder`
	writeprotection-folder- exception		Display the folders in the Write Protection Exception List For example, type: `SLCmd.exe -p <admin_password> show writeprotection-folder-exception`
add	writeprotection-file	<file_path>	Add the specified file to the Write Protection List For example, type:

Command	Parameter	Value	Description
			`SLCmd.exe -p <admin_password> add writeprotection-file archive.txt` **Note** The value pattern matches from the end of the path toward the beginning of the path. For example, specifying `userfile.txt` matches `c:\Windows\userfile.txt` and `c:\Temp\userfile.txt`.
	`writeprotection-file-exception`	`-t <file_path> -p <process_path>`	Add the specified file and a specific process path for that file to the Write Protection Exception List For example, to add write access by a process named `notepad.exe` to a file named `userfile.txt`, type: `SLCmd.exe -p <admin_password> add writeprotection-file-exception -t userfile.txt -p notepad.exe`

Command	Parameter	Value	Description
			 **Note** The `-p` and `-t` values pattern match from the end of the path toward the beginning of the path. For example, specifying `userfile.txt` matches `c:\Windows\userfile.txt` and `c:\Temp\userfile.txt`.
		`-t <file_path>`	Add the specified file to the Write Protection Exception List For example, to add write access by any process to a file named `userfile.txt`, type: `SLCmd.exe -p <admin_password> add writeprotection-file-exception -t userfile.txt`

Command	Parameter	Value	Description
			 **Note** The `-t` value pattern matches from the end of the path toward the beginning of the path. For example, specifying `userfile.txt` matches `c:\Windows\userfile.txt` and `c:\Temp\userfile.txt`.
		`-p <process_path>`	Add the specified process path to the Write Protection Exception List For example, to add write access by a process named `notepad.exe` to any files, type: `SLCmd.exe -p <admin_password> add writeprotection-fileexception -p notepad.exe`

Command	Parameter	Value	Description
			 **Note** The `-p` value pattern matches from the end of the process path toward the beginning of the path. For example, specifying `notepad.exe` matches `c:\Windows\notepad.exe` and `c:\Temp\notepad.exe`.
	`writeprotection-folder`	`[-r] <folder_path>`	Add the specified folder(s) to the Write Protection List For example, type: `SLCmd.exe -p <admin_password> add writeprotection-folder -r userfolder`

Command	Parameter	Value	Description
			Note Using the optional `-r` value includes the specified folder and related subfolders. The value pattern matches from the end of the path toward the beginning of the path. For example, specifying `userfile.txt` matches`c:\Windows\userfolder` and `c:\Temp\userfolder`.
	`writeprotection-folderexception`	`[-r] -t <folder_path> -p <process_path>`	Add the specified folder and processes run from the specified path to the Write Protection Exception List For example, to add write access by a process named `notepad.exe` to a folder and related subfolders at `c:\Windows\System32\Temp`, type: `SLCmd.exe -p <admin_password> add writeprotectionfolder-exception -r -t c:\Windows\System32\Temp -p notepad.exe`

Command	Parameter	Value	Description
			 **Note** Using the optional `-r` value includes the specified folder and related subfolders. The `-p` and `-t` values pattern match from the end of the path toward the beginning of the path. For example, specifying `userfile.txt` matches `c:\Windows\userfile.txt` and `c:\Temp\userfile.txt`.
		`[-r] -t <folder_path>`	Add the specified folder(s) to the Write Protection Exception List For example, to add write access by any process to a folder at `userfolder`, type: `SLCmd.exe -p <admin_password> add writeprotectionfolder-exception -r -t userfolder`

Command	Parameter	Value	Description
			 **Note** Using the optional `-r` value includes the specified folder and related subfolders. The `-t` value pattern matches from the last part of the folder path toward the beginning of the path. For example, specifying `userfolder` matches `c:\Windows\userfolder` and `c:\Temp\userfolder`.
		-p <process_path>	Add processes run from the specified paths to the Write Protection Exception List For example, to add write access by a process named `notepad.exe` to any folder, type: `SLCmd.exe -p <admin_password> add writeprotectionfolder-exception -p c:\Windows\notepad.exe`

Command	Parameter	Value	Description
			 **Note** The `-p` value pattern matches from the end of the process path toward the beginning of the path. For example, specifying `notepad.exe` matches `c:\Windows\notepad.exe` and `c:\Temp\notepad.exe`.
`remove`	`writeprotection-file`	`<file_path>`	Remove the specified file from the Write Protection List For example, type: `SLCmd.exe -p <admin_password> remove writeprotection-file archive.txt`  **Note** Specify the exact `<file_path>` originally specified in the corresponding add command.
	`writeprotection-file-exception`	`-t <file_path> -p <process_path>`	Remove the specified file and process path from the Write Protection Exception List For example, type: `SLCmd.exe -p <admin_password> remove`

COMMAND	PARAMETER	VALUE	DESCRIPTION
			`writeprotection-file-exception -t userfile.txt -p notepad.exe` **Note** Specify the exact <file_path> and <process_path> originally specified in the corresponding add command.
		`-t <file_path>`	Remove the specified file from the Write Protection Exception List For example, type: `SLCmd.exe -p <admin_password> remove writeprotection-file-exception -t userfile.txt`

Command	Parameter	Value	Description
			 **Note** The `-t` value pattern matches from the end of the path toward the beginning of the path. For example, specifying `userfile.txt` matches `c:\Windows\userfile.txt` and `c:\Temp\userfile.txt`.
		`-p <process_path>`	Remove the specified process path from the Write Protection Exception List For example, type: `SLCmd.exe -p <admin_password> remove writeprotection-file-exception -p notepad.exe`

Command	Parameter	Value	Description
			 **Note** The `-p` value pattern matches from the end of the process path toward the beginning of the path. For example, specifying `notepad.exe` matches `c:\Windows\notepad.exe` and `c:\Temp\notepad.exe`.
	`writeprotection-folder`	`[-r] <folder_path>`	Remove the specified folder(s) from the Write Protection List For example, type: `SLCmd.exe -p <admin_password> remove writeprotection-folder -r c:\Windows`  **Note** Using the optional `-r` value includes the specified folder and related subfolders. Specify the exact <folder_path> and `-r` value originally specified in the corresponding add command.

Command	Parameter	Value	Description
	writeprotection-folder-exception	`[-r] -t <folder_path> -p <process_path>`	Remove the specified folder and process path from the Write Protection Exception List For example, type: `SLCmd.exe -p <admin_password> remove writeprotection-folder-exception -r -t c:\Windows\System32\Temp -p c:\Windows\notepad.exe` **Note** Using the optional `-r` value includes the specified folder and related subfolders. Specify the exact <folder_path>, <process_path>, and `-r` value originally specified in the corresponding add command.
		`[-r] -t <folder_path>`	Remove the specified folder(s) from the Write Protection Exception List For example, type: `SLCmd.exe -p <admin_password> remove writeprotection-folder-exception -r -t userfolder`

Command	Parameter	Value	Description
			Note Using the optional `-r` value includes the specified folder and related subfolders. The `-t` value pattern matches from the last part of the folder path toward the beginning of the path. For example, specifying `userfolder` matches `c:\Windows\userfolder` and `c:\Temp\userfolder`.
		`-p <process_path>`	Remove the specified process path from the Write Protection Exception List For example, type: `SLCmd.exe -p <admin_password> remove writeprotection-folder-exception -p c:\Windows\System32`

Command	Parameter	Value	Description
			 **Note** The `-p` value pattern matches from the end of the process path toward the beginning of the path. For example, specifying `notepad.exe` matches `c:\Windows\notepad.exe` and `c:\Temp\notepad.exe`.

Table 4-18. Write Protection List "Registry" Commands

Command	Parameter	Value	Description
`show`	`writeprotection`		Display the entire Write Protection List
	`writeprotection-regvalue`		Display the registry values in the Write Protection List
	`writeprotection-regvalue-exception`		Display the registry values in the Write Protection Exception List
	`writeprotection-regkey`		Display the registry keys in the Write Protection List
	`writeprotection-regkey-exception`		Display the registry keys in the Write Protection Exception List

Command	Parameter	Value	Description
add	writeprotection-regvalue	<path_of_registry_key> <registry_value>	Add the specified registry value and its related registry key to the Write Protection List For example, to add the registry value of "testvalue" in the "HKEY \test" registry key to the Write Protection List, type: SLCmd.exe -p <admin_password> add writeprotection-regvalue HKEY \test testvalue
	writeprotection-regvalue-exception	-t <path_of_registry_key> <registry_value> -p <process_path>	Add the specified registry value and its related registry key and a specific process path for that value to the Write Protection Exception List

Command	Parameter	Value	Description
			 **Note** This command allows write access by the specified process to the specified registry values. The `-p` value pattern matches from the end of the path toward the beginning of the path.
		`-t <path_of_registry_key> <registry_value>`	Add the specified registry value and its related registry key to the Write Protection Exception List

Command	Parameter	Value	Description
			Note This command allows write access by any process to the specified registry value.
		`-p <process_path>`	Add the specified process to the Write Protection Exception List

Command	Parameter	Value	Description
			Note This command allows write access by the specified process to any registry values. The `-p` value pattern matches from the end of the process path toward the beginning of the path.
	`writeprotection-regkey`	`[-r] <path_of_registry_key>`	Add the specified registry key to the Write Protection List **Note** Using the optional `-r` value includes the specified registry key and related subkeys.

Command	Parameter	Value	Description
	`writeprotection-regkey-exception`	`[-r] <path_of_registry_key> -p <process_path>`	Add the specified registry key and processes run from the specified path to the Write Protection Exception List **Note** This command allows write access by the specified process to the specified registry keys. Using the optional `-r` value includes the specified registry key and related subkeys. The `-p` value pattern matches from the end of the process path toward the beginning of the path.

Command	Parameter	Value	Description
		`[-r] -t <path_of_registry_key>`	Add the specified registry key to the Write Protection Exception List **Note** This command allows write access by any process to the specified registry keys. Using the optional `-r` value includes the specified registry key and related subkeys.
		`-p <process_path>`	Add processes run from the specified paths to the Write Protection Exception List

Command	Parameter	Value	Description
			 **Note** This command allows write access by the specified process to any registry keys. The `-p` value pattern matches from the end of the process path toward the beginning of the path.
`remove`	`writeprotection-regvalue`	`<path_of_registry_key> <registry_value>`	Remove the specified registry value from the Write Protection List

Command	Parameter	Value	Description
			Note Specify the exact <path_of_registry_key> and <registry_value>originally specified in the corresponding add command.
	writeprotection-regvalue-exception	-t <path_of_registry_key> <registry_value> -p <process_path>	Remove the specified registry value and process path from the Write Protection Exception List

Command	Parameter	Value	Description
			 **Note** Specify the exact `<path_of_registry_key>`, `<registry_value>`, and `<process_path>` originally specified in the corresponding add command. The `-p` value pattern matches from the end of the path toward the beginning of the path.
		`-t <path_of_registry_key> <registry_value>`	Remove the specified registry value from the Write Protection Exception List
		`-p <process_path>`	Remove the specified process path from the Write Protection Exception List

Command	Parameter	Value	Description
			Note The `-p` value pattern matches from the end of the path toward the beginning of the path.
	`writeprotection-regkey`	`[-r] <path_of_registry_key>`	Remove the specified registry key from the Write Protection List

Command	Parameter	Value	Description
			Note Specify the exact `<path_of_registry_key>` and `-r` value originally specified in the corresponding add command. Using the optional `-r` value includes the specified registry key and related subkeys
	`writeprotection-regkey-exception`	`[-r] <path_of_registry_key> -p <process_path>`	Remove the specified registry key and process path from the Write Protection Exception List

Command	Parameter	Value	Description
			Note Specify the exact `<path_of_registry_key>`, `<process_path>`, and `-r` value originally specified in the corresponding add command. Using the optional `-r` value includes the specified registry key and related subkeys. The `-p` value pattern matches from the end of the path toward the beginning of the path.

Command	Parameter	Value	Description
		`[-r] -t <path_of_registry_key>`	Remove the specified registry key from the Write Protection Exception List **Note** Using the optional `-r` value includes the specified registry key and related subkeys.
		`-p <process_path>`	Remove the specified process path from the Write Protection Exception List **Note** The `-p` value pattern matches from the end of the path toward the beginning of the path.

Trusted Certificate Commands

Configure Trusted Certificates using the Command Line Interface by typing your command in the following format:

```
SLCmd.exe -p <admin_password> <command> <parameter> <value>
```

The following table lists the available abbreviated forms of parameters.

TABLE 4-19. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
`trustedcertification`	tc	Manage Trusted Certificates

The following table lists the commands, parameters, and values available.

TABLE 4-20. Trusted Certificate Commands

COMMAND	PARAMETER	DESCRIPTION
`set trustedcertification`		Display current setting for using Trusted Certifications **Note** The default setting is "enable".
	`enable`	Enable using Trusted Certifications
	`disable`	Disable using Trusted Certifications
`show trustedcertification`	`[-v]`	Display the certificate files in the Trusted Certifications List Using the optional `-v` value displays detailed information.
`add trustedcertification`	`-c <file_path> [-l<label>] [-u]`	Add the specified certificate file to the Trusted Certifications List Using the optional `-l` value specifies the unique label for this certificate file Using the optional `-u` value treats the file signed by this certificate file as a Trusted Updater
`remove trustedcertification`	`-l<label>`	Remove a certificate file from the Trusted Certifications List by specifying its label

Intelligent Runtime Learning Commands

Configure Intelligent Runtime Learning using the Command Line Interface by typing your command in the following format:

```
SLCmd.exe -p <admin_password> <command> <parameter> <value>
```

The following table lists the available abbreviated forms of parameters.

TABLE 4-21. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
`intelligentruntime learning`	irl	Agent will allow runtime execution files that are generated by applications in the Approved List

The following table lists the commands, parameters, and values available.

TABLE 4-22. Intelligent Runtime Learning Commands

COMMAND	PARAMETER	DESCRIPTION
`set intelligentruntime learning`		Display current settings for using Intelligent Runtime Learning
	`enable`	Enable using Intelligent Runtime Learning
	`disable`	Disable using Intelligent Runtime Learning

Trusted Hash List Commands

Configure trusted hash values using the Command Line Interface by typing your command in the following format:

```
SLCmd.exe -p <admin_password> <command> <parameter> <value>
```

The following table lists the available abbreviated forms of parameters.

TABLE 4-23. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
`trustedhash`	th	Manage trusted hash values (files) added by the StellarProtect (Legacy Mode) administrator

The following table lists the commands, parameters, and values available.

TABLE 4-24. Intelligent Runtime Learning Commands

COMMAND	PARAMETER	DESCRIPTION
`set trustedhash`		Display current setting for using Trusted Hash List **Note** The default setting is "disable".
	`enable`	Enable using Trusted Hash List
	`disable`	Disable using Trusted Hash List
`show trustedhash`		Display the hash values in the Trusted Hash List For example, type: `SLCmd.exe -p <admin_password> show trustedhash`
`add trustedhash`	`-v <hash> [-l<label>] [-u][-al] [-t <file_path>][-n <note>]`	Add the specified hash value to the Trusted Hash List For example, to add a trusted file with a hash value xxx to the Trusted Hash List, type: `SLCmd.exe -p <admin_password> add trustedhash -v xxx` Using the optional `-l` value specifies the unique label for this hash value.

COMMAND	PARAMETER	DESCRIPTION
		Using the optional `-u` value treats the file of the specified hash value as a Trusted Updater. **Note** The `-u` value requires the Predefined Trusted Updater List enabled. Using the optional `-al` value adds the file of the specified hash value to Approved List Using the optional `-t` value specifies a file path to check for the hash value **Note** The `-t` value pattern matches from the end of the path toward the beginning of the path. For example, specifying `userfile.txt` matches `c:\Windows\userfile.txt`and `c:\Temp\userfile.txt`. Using the optional `-n` value adds a note for the file hash
`remove trustedhash`	`-l <label>`	Remove a file from the Trusted Hash List by specifying its label
	`-a`	Remove all the hash values in the Trusted Hash List

Trusted Updater Commands

To execute installers or files not specified in agent Approved Lists, configure Trusted Updater by typing your command in the following format:

```
SLCmd.exe -p <admin_password> <command> <parameter> <value>
```

The following table lists the available abbreviated forms of parameters.

TABLE 4-25. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
`trustedupdater`	tu	Manage the Predefined Trusted Updater tool process

The following table lists the commands, parameters, and values available.

TABLE 4-26. Trusted Updater Commands

COMMAND	PARAMETER	DESCRIPTION
`start trustedupdater`	`[-r] <path_of_installer>`	Start Trusted Updater to add installer files (`EXE` and `MSI` file types) to the specified folder of the Approved List For example, to include all installation packages in the `C:\Installers` folder and all sub-folders, type: `SLCmd.exe -p <admin_password> start trustedupdater -r C:\Installers` **Note** Using the optional `-r` value includes the specified folder and related subfolders.

COMMAND	PARAMETER	DESCRIPTION
`stop trustedupdater`	`[-f]`	Disable Trusted Updater to stop adding new or updated files to the Approved List For example, to stop the Trusted Updater and commit all identified installers (identified before receiving the stop command) to the Approved List after receiving a prompt, type: `SLCmd.exe -p <admin_password> stop trustedupdater -f` **Note** Using the optional `-f` value specifies that the Trusted Updater does not prompt the administrator before committing a file to the Approved List.

Real-Time Scan Commands

Enable or disable the Real-Time Scan function using the Command Line Interface by typing your command in the following format:

```
SLCmd.exe -p <admin_password> <command> <parameter> <value>
```

Note

The Real-Time Scan command should not work if the license edition does not support scanning function.

The following table lists the commands, parameters, and values available.

TABLE 4-27. Real-Time Scan Commands

COMMAND	PARAMETER	DESCRIPTION
`set rts`		Display the current status of Real-Time Scan **Note** The default setting is "disable".
	`enable`	Enable Real-Time Scan For example, type: `SLCmd.exe -p <admin_password> set rts enable`
	`disable`	Disable Real-Time Scan For example, type: `SLCmd.exe -p <admin_password> set rts disable`

Trusted USB Device Commands

Configure the trusted USB device list using the Command Line Interface by typing your command in the following format:

```
SLCmd.exe -p <admin_password> <command> <parameter> <value>
```

The following table lists the available abbreviated forms of parameters.

TABLE 4-28. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
`trustedusbdevice`	tud	Manage the trusted USB device list

The following table lists the commands, parameters, and values available.

TABLE 4-29. Trusted USB Device Commands

COMMAND	PARAMETER	DESCRIPTION
`show usbinfo`	`<drive_letter>`	Display the identifiers (VID/PID/SN) of a USB storage device For example, if the USB is in Drive D, type: `SLCmd.exe -p <admin_password> show usbinfo d`
`show trustedusbdevice`	`[-f]`	Display all trusted USB storage devices For example, type: `SLCmd.exe -p <admin_password> show trustedusbdevice`
`add trustedusbdevice`	`[-vid <VID>] [-pid <PID>] [-sn <SN>]`	Add a trusted USB storage device with the specified identifiers. You must specify at least one device identifier For example, type: `SLCmd.exe -p <admin_password> add trustedusbdevice -sn 123456`
`remove trustedusbdevice`	`[-vid <VID>] [-pid <PID>] [-sn <SN>]`	Remove a trusted USB storage device with the specified identifiers. You must specify at least one device identifier For example, type: `SLCmd.exe -p <admin_password> remove trustedusbdevice -sn 123456`

Predefined Trusted Updater Commands

Configure Predefined Trusted Updater using the Command Line Interface by typing your command in the following format:

```
SLCmd.exe -p <admin_password> <command> <parameter> <value>
```

The following table lists the available abbreviated forms of parameters.

TABLE 4-30. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
`predefinedtrustedupdater`	ptu	Manage files in the Predefined Trusted Updater Lists

The following table lists the commands, parameters, and values available.

TABLE 4-31. Predefined Trusted Updater Commands

COMMAND	PARAMETER	DESCRIPTION
`add predefinedtrustedupdater`	`-e <folder_or_file_exception>`	Add the specified file or folder to the Predefined Trusted Updater Exception List For example, to add `notepad.exe` to the Predefined Trusted Updater Exception List, type: `SLCmd.exe -p <admin_password> add predefinedtrustedupdater -e C:\Windows\notepad.exe` **Important** The "`add`" command for adding files to the Predefined Trusted Updater List follows a different format than the other commands specified in this list. For details on adding files to the Predefined Trusted Updater List (not the Predefined Trusted Updater Exception List), see *Predefined Trusted Updater "Add" Command* in the following section.

Command	Parameter	Description
decrypt predefinedtrustedupdater	<path_of_encrypted_file> <path_of_decrypted_output_file>	Decrypt a file to the specified location For example, to decrypt C:\Notepad.xen to C:\Editors\notepad.xml, type: SLCmd.exe -p <admin_password> decrypt predefinedtrustedupdater C:\Notepad.xen C:\Editors\notepad.xml
encrypt predefinedtrustedupdater	<path_of_file> <path_of_encrypted_output_file>	Encrypt a file to the specified location For example, to encrypt C:\notepad.xml to C:\Editors\Notepad.xen, type: SLCmd.exe -p <admin_password> encrypt predefinedtrustedupdater C:\Editors\notepad.xml C:\Notepad.xen
export predefinedtrustedupdater	<path_of_encrypted_output>	Export the Predefined Trusted Updater List to the specified encrypted file For example, type: SLCmd.exe -p <admin_password> export predefinedtrustedupdater C:\Lists\ptu_list.xen
import predefinedtrustedupdater	<path_of_encrypted_input>	Import a Predefined Trusted Updater List from the specified encrypted file For example, type: SLCmd.exe -p <admin_password> import predefinedtrustedupdater C:\Lists\ptu_list.xen

Command	Parameter	Description
`remove predefinedtrustedupdater`	`-l <label_name>`	Remove the specified labeled rule from the Predefined Trusted Updater List For example, to remove the “Notepad” rule, type: `SLCmd.exe -p <admin_password> remove predefinedtrustedupdater -l Notepad`
	`-e <folder_or_file_exception>`	Remove the specified exception from the Predefined Trusted Updater Exception List For example, to remove the `notepad.exe` exception, type: `SLCmd.exe -p <admin_password> remove predefinedtrustedupdater -e C:\Windows\notepad.exe`
`set predefinedtrustedupdater`		Display the status of the Predefined Trusted Updater List **Note** The default setting is "disable".
	`enable`	Enable the Predefined Trusted Updater List
	`disable`	Disable the Predefined Trusted Updater List
`show predefinedtrustedupdater`		Display the files in the Predefined Trusted Updater List For example, type: `SLCmd.exe -p <admin_password> show predefinedtrustedupdater`

Command	Parameter	Description
	`-e`	Display the files in the Predefined Trusted Updater Exception List For example, type: `SLCmd.exe -p <admin_password> show predefinedtrustedupdater -e`

Important

The "`add`" command for adding files to the Predefined Trusted Updater List follows a different format than the general commands specified in the Predefined Trusted Updater Commands table. For details on adding files to the Predefined Trusted Updater List, refer to the *Predefined Trusted Updater "Add" Command* in the following section.

Predefined Trusted Updater "Add" Command

Add processes, files, or folders to the Predefined Trusted Updater List using the Command Line Interface by typing your command in the following format:

```
SLCmd.exe -p <admin_password> add predefinedtrustedupdater -u
<folder_or_file> -t <type_of_object> [<optional_values>]
```

The following table lists the command, parameter, and base value.

TABLE 4-32. Predefined Trusted Updater "Add" Command

COMMAND	PARAMETER	VALUE	DESCRIPTION
`add`	`predefinedtrustedupdater`	<folder_or_file>	Add a specified file or folder to the Predefined Trusted Updater List For example, to add `notepad.exe` to the Predefined Trusted Updater List, type: `SLCmd.exe -p <admin_password> add predefinedtrustedupdater C:\Windows\notepad.exe`

Append the following additional values at the end of the command:

TABLE 4-33. Predefined Trusted Updater "Add" Additional Values

VALUE	REQUIRED/ OPTIONAL	DESCRIPTION	EXAMPLE
`-u <folder_or_file >`	Required	Add the specified file or folder to the Predefined Trusted Updater List	N/A **Note** This parameter requires the use of the `-t <type_of_object>` value.
`-t <type_of_object>`	Required	Specify the type of object to add to the Predefined Trusted Updater List located in `-u <folder_or_file>`	`SLCmd.exe -p <admin_password> add predefinedtrusted updater -u C:\Windows`

Value	Required/ Optional	Description	Example
		Available objects types are as follows: • process: Indicates only EXE file types • file: Indicates only MSI and BAT file types • folder: Indicates all EXE, MSI, and BAT files in the specified folder • folderandsub: Indicates all EXE, MSI, and BAT files in the specified folder and related subfolders	\notepad.exe -t process
-p <parent_process>	Optional	Add the full file path to the specified parent process used to invoke the file(s) specified in -u <folder_or_file>	SLCmd.exe -p <admin_password> add predefinedtrustedupdater -u C:\Windows \notepad.exe -t process -p C:\batch files \note.bat
-l <label_name>	Optional	Specify a label name for the file(s) specified in -u <folder_or_file> **Note** When left blank, StellarProtect (Legacy Mode) assigns an arbitrary label name.	SLCmd.exe -p <admin_password> add predefinedtrusted updater -u C:\Windows \notepad.exe -t process -l EDITOR
-al enable	Optional	Compare the hash values in the Approved List with the hash	SLCmd.exe -p <admin_password>

Value	Required/ Optional	Description	Example
		values calculated from the actual files **Note** Enabled by default even when `-al` is not specified.	`add predefinedtrusted updater -u C:\Windows \notepad.exe -t process -al enable`
`-al disable`	Optional	Do not compare the hash values in the Approved List with the hash values calculated from the actual files	`SLCmd.exe -p <admin_password> add predefinedtrusted updater -u C:\Windows \notepad.exe -t process -al disable`

Windows Update Support

Configure Windows Update Support using the Command Line Interface by typing your command in the following format:

```
SLCmd.exe -p <admin_password> <command> <parameter> <value>
```

The following table lists the available abbreviated forms of parameters.

Table 4-34. Abbreviations and Uses

Parameter	Abbreviation	Use
`windowsupdatesupport`	wus	Allow Windows Update to run on the agent with the Application Lockdown on

The following table lists the commands, parameters, and values available.

TABLE 4-35. Windows Update Support Commands

COMMAND	PARAMETER	DESCRIPTION
`set windowsupdatesupport`		Display current setting for Windows Update Support **Note** The default setting is "disable".
	`enable`	Enable Windows Update Support
	`disable`	Disable Windows Update Support

Blocked File Notification Commands

Enable or disable notifications for file blocking using the Command Line Interface by typing your command in the following format:

```
SLCmd.exe -p <admin_password> <command> <parameter> <value>
```

The following table lists the available abbreviated forms of parameters.

TABLE 4-36. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
`blockedfilenotification`	bfn	Display notifications on the managed endpoint when StellarProtect (Legacy Mode) blocks and prevents an application from running or making changes to the endpoint

The following table lists the commands, parameters, and values available.

TABLE 4-37. Windows Update Support Commands

COMMAND	PARAMETER	DESCRIPTION
`set blockedfilenotification`		Display the current setting **Note** The default setting is "disable".
	`enable`	Enable pop-up notifications
	`disable`	Disable pop-up notifications

Configuration File Commands

Perform actions on the configuration file using the Command Line Interface by typing your command in the following format:

```
SLCmd.exe -p <admin_password> <command> <parameter> <value>
```

The following table lists the available abbreviated forms of parameters.

TABLE 4-38. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
`configuration`	con	Manage the configuration file

The following table lists the commands, parameters, and values available.

TABLE 4-39. Configuration File Commands

COMMAND	PARAMETER	DESCRIPTION
`decrypt configuration`	`<path_of_encrypted_file>` `<path_of_decrypted_output_file>`	Decrypts a configuration file to the specified location For example, to decrypt `C:\config.xen` to `C:\config.xml`, type: `SLCmd.exe -p <admin_password> decrypt configuration C:\config.xen C:\config.xml`

Command	Parameter	Description
`encrypt configuration`	`<path_of_file> <path_of_encrypted_output_file>`	Encrypts a configuration file to the specified location For example, to encrypt `C:\config.xml` to `C:\config.xen`, type: `SLCmd.exe -p <admin_password> encrypt configuration C:\config.xml C:\config.xen`
`export configuration`	`<path_of_encrypted_output>`	Export the configuration file to the specified location For example, type: `SLCmd.exe -p <admin_password> export configuration C:\config.xen`
`import configuration`	`<path_of_encrypted_input>`	Import a configuration file from the specified location For example, type: `SLCmd.exe -p <admin_password> import configuration C:\config.xen`

Fileless Attack Prevention Commands

Configure Fileless Attack Prevention features using the Command Line Interface by typing your command in the following format:

```
SLCmd.exe -p <admin_password> <command> <parameter> <value>
```

The following table lists the available abbreviated forms of parameters.

Table 4-40. Abbreviations and Uses

Parameter	Abbreviation	Use
`filelessattackprevention`	`flp`	Manage Fileless Attack Prevention

Parameter	Abbreviation	Use
filelessattackpreventio n-process	flpp	Manage Fileless Attack Prevention processes
filelessattackpreventio n-exception	flpe	Manage Fileless Attack Prevention exceptions

The following table lists the commands, parameters, and values available.

Table 4-41. Configuration File Commands

Command	Parameter	Description
set filelessattackp revention		Display the current Fileless Attack Prevention status For example, type: `SLCmd.exe -p <admin_password> set filelessattackprevention`
	<enable	Enable Fileless Attack Prevention For example, type: `SLCmd.exe -p <admin_password> set filelessattackprevention enable`
	disable	Disable Fileless Attack Prevention For example, type: `SLCmd.exe -p <admin_password> set filelessattackprevention disable`
show filelessattackp revention-process		Display the list of monitored processes For example, type: `SLCmd.exe -p <admin_password> show filelessattackprevention-process`
show filelessattackp		Display the Fileless Attack Prevention Exception List

Command	Parameter	Description
revention-exception		For example, type: `SLCmd.exe -p <admin_password>show filelessattackprevention-exception`
add filelessattackprevention-process	<monitored_process> <Parentprocess1> <Parentprocess2> <Parentprocess3> <Parentprocess4> -a <arguments> -regex -l <label>	Add a Fileless Attack Prevention exception For example, given the following exception: • Monitored Process: cscript.exe • Parentprocess1: a.exe • Parentprocess2: • Parentprocess3: c.exe • Parentprocess4: • Arguments: -abc –def • Use regular expression for arguments: No To add the exception, type: `SLCmd.exe -p <admin_password> addflpe cscript.exe a.exe "" c.exe "" -a "-abc - def"`
remove filelessattackprevention-exception	-l <label>	Remove a Fileless Attack Prevention exception For example, type: `SLCmd.exe -p <admin_password> remove filelessattackprevention-exception -l <label>`

Note

- If a monitored process is launched before StellarProtect (Legacy Mode) is started,StellarProtect (Legacy Mode) is unable to detect and block the monitored process.
- In systems running Windows Vista x86 (no service pack installed), the Fileless Attack Prevention feature can run the process chain check without issues, but is unable to perform the command line argument check. If a process passes the process chain check on these systems, the command line argument check is skipped completely.

Maintenance Mode Commands

Perform actions related to Maintenance Mode using the Command Line Interface by typing your command in the following format:

```
SLCmd.exe -p <admin_password> <command> <parameter> <value>
```

The following table lists the available abbreviated forms of parameters.

TABLE 4-42. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
`approvedlist`	`al`	Manage Approved List in Maintenance Mode
`maintenancemode`	`mtm`	Manage Maintenance Mode
`maintenancemodeschedule`	`mtms`	Manage Maintenance Mode schedule

The following table lists the commands, parameters, and values available.

TABLE 4-43. Maintenance Mode Commands

COMMAND	PARAMETER	DESCRIPTION
`start maintenancemode`		Start Maintenance Mode For example, type:

Command	Parameter	Description
		`SLCmd.exe -p <admin_password> start maintenancemode`
	`-duration`	Set an action to take place after Maintenance Mode as well as a duration for Maintenance Mode in hours (1 -999) For example, type: `SLCmd.exe -p <admin_password> start maintenancemode -scan al -duration 3`
	`-scan quarantine`	Start Maintenance Mode and enable file scanning after the maintenance period StellarProtect (Legacy Mode) will scan files that are created/executed/ modified during the maintenance period and quarantines detected files, then add files that are not detected as malicious to the Approved List For example, type: `SLCmd.exe -p <admin_password> start maintenancemode -scan quarantine`
	`-scan al`	Start Maintenance Mode and enable file scanning after the maintenance period. StellarProtect (Legacy Mode) scans files that are created/ executed/modified files during the period and adds these files (including files that aredetected as malicious) to the Approved List For example, type: `SLCmd.exe -p <admin_password> start maintenancemode -scan al`
`stop maintenancemode`		Stop Maintenance Mode For example, type:

Command	Parameter	Description
		`SLCmd.exe -p <admin_password> stop maintenancemode` **Note** You cannot stop Maintenance Mode when an agent is preparing to leave Maintenance Mode.
	`-discard`	Stop Maintenance Mode and do not add files in the file queue to the Approved List For example, type: `SLCmd.exe -p <admin_password> stop maintenancemode discard` **Note** You cannot stop Maintenance Mode when an agent is preparing to leave Maintenance Mode.
`set maintenancemode schedule`	`-start YYYY-MMDDTHH:MM:SS -end YYYY-MMDDTHH:MM:SS`	Set the schedule for Maintenance Mode For example, type: `SLCmd.exe -p <admin_password> set maintenancemodeschedule -start 2019-04- 07T01:00:00 -end 2019-04-07T05:00:00`

COMMAND	PARAMETER	DESCRIPTION
		Note • You cannot set the Maintenance Mode schedule when an agent is already in Maintenance Mode or is preparing to leave Maintenance Mode. • If you configure the Maintenance Mode schedule to start earlier than the current time, the system starts the maintenance period immediately after you save the settings.
	`-start YYYY-MMDDTHH:MM:SS -end YYYY-MMDDTHH:MM:SS -scan quarantine`	Use this command to configure the following: • Set the schedule for Maintenance Mode • Enable file scanning after the maintenance period: StellarProtect (Legacy Mode) will scan files that are created/executed/modified during the maintenance period, quarantine detected threats, and add files that are not detected as malicious to the Approved List For example, type: `SLCmd.exe -p <admin_password> set maintenancemodeschedule -start 2019-04- 07T01:00:00 -end 2019-04-07T05:00:00 -scan quarantine`

Command	Parameter	Description
		Note • You cannot set the Maintenance Mode schedule when an agent is already in Maintenance Mode or is preparing to leave Maintenance Mode. • If you configure the Maintenance Mode schedule to start earlier than the current time, the system starts the maintenance period immediately after you save the settings.
	`-start YYYY-MMDDTHH:MM:SS -end YYYY-MMDDTHH:MM:SS -scan al`	Use this command to configure the following: • Set the schedule for Maintenance Mode • Enable file scanning after the maintenance period: StellarProtect (Legacy Mode) will scan files that are created/executed/modified during the maintenance period and add these files (including files that are detected as malicious) to the Approved List For example, type: `SLCmd.exe -p <admin_password> set maintenancemodeschedule -start 2019-04-07T01:00:00 -end 2019-04-07T05:00:00 -scan al`

Command	Parameter	Description
		Note • You cannot set the Maintenance Mode schedule when an agent is already in Maintenance Mode or is preparing to leave Maintenance Mode. • If you configure the Maintenance Mode schedule to start earlier than the current time, the system starts the maintenance period immediately after you save the settings.
`remove maintenancemode schedule`		Clear the Maintenance Mode schedule settings For example, type: `SLCmd.exe -p <admin_password> remove maintenancemodeschedule` **Note** You cannot delete schedule settings when an agent is already in Maintenance Mode or is preparing to leave Maintenance Mode.
`show maintenancemode`		Display the Maintenance Mode status For example, type:

Command	Parameter	Description
		`SLCmd.exe -p <admin_password> show maintenancemode`
`show maintenancemode schedule`		Display the Maintenance Mode schedule settings For example, type: `SLCmd.exe -p <admin_password> show maintenancemodeschedule`

Important

Before using Maintenance Mode, apply the required updates on the following supported platforms:

- 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.

Note

- To reduce risk of infection, run only applications from trusted sources on endpoints during the maintenance period.
- Agents start one scheduled maintenance period at a time. If you configure a new maintenance period, the system overwrites existing maintenance schedule that has not started yet.
- When the agent is about to leave Maintenance Mode, restarting the agent endpoint prevents StellarProtect (Legacy Mode) from adding files in the queue to the Approved List.
- During the maintenance period, you cannot perform agent patch updates on endpoints.
- When Maintenance Mode is enabled, StellarProtect (Legacy Mode) does not support Windows updates that require restarting an endpoint during the maintenance period.
- To run an installer that deploys files to a network folder during the maintenance period, StellarProtect (Legacy Mode) must have access permission to the network folder.
- Maintenance Mode does not support the Windows Visual Studio debugger.

Manual Scan Commands

Perform actions related to manual scans on endpoints using the Command Line Interface by typing your command in the following format:

```
SLCmd.exe -p <admin_password> <command> <parameter> <value>
```

Note

- The Manual Scan commands require special licensing. Ensure that you choose the correct license edition before using Manual Scan commands. For more information on how to obtain the required license edition, contact your sales representative.
- For agent component updates, make sure that StellarProtect (Legacy Mode) agents can connect to an update source without using a proxy server.
- After a component update is complete, you cannot roll back the component to a previous version

The following table lists the commands, parameters, and values available.

TABLE 4-44. Manual Scan Commands

COMMAND	PARAMETER	DESCRIPTION
`start scan`	`[-action <action>]`	Start a manual scan on an endpoint Use the `-action` option to specify an action to perform when an anomaly is detected Available actions are as follows: • 0: No action • 1: Clean, or delete if the clean action is unsuccessfu • 2: Clean, or quarantine if the clean action is unsuccessful This is the default action. • 3: Clean, or ignore if the clean action is unsuccessful For example, type: `SLCmd.exe -p <admin_password> start scan - action 1`

Command	Parameter	Description
		Note • For each manual scan, StellarProtect (Legacy Mode) saves the scan results in a log file (with a file name of `ScanResult_YYYYMMDDHHMMSS.log`) in `C:\Program Files\TXOne\StellarProtect (Legacy Mode)\Scan\log`. • With administrator privileges, you can restore quarantined files using the following command: `WKSupportTool.exe RestorePrescan <QuarantinedFilePath> <FilePathToRestore>` where `<QuarantinedFilePath>` is the file path of the quarantined file and `<FilePathToRestore>` is the folder location to restore the file. For information about quarantined files, see the scan logs.

Command	Parameter	Description
`start update`		Update StellarProtect (Legacy Mode) agent components (pattern file and scan engine)
`set update`	`-source <source>`	Set the update source for component updates
`show update`	`-source <source>`	Display the current update source

Chapter 5

Working with the Agent Configuration File

This chapter describes how to configure TXOne StellarProtect (Legacy Mode) using theconfiguration file.

Topics in this chapter include:

Working with the Agent Configuration File

The configuration file allows administrators to create and deploy a single configuration across multiple machines.

Refer to *Exporting or Importing a Config File on page 5-3* for more information.

Changing Advanced Settings

Some settings can only be changed though the configuration file using the command line interface (CLI). See *Using SLCmd at the Command Line Interface (CLI) on page 4-16* for more information.

Procedure

1. Export the configuration file.
2. Decrypt the configuration file.
3. Edit the configuration file with Windows Notepad or another text editor.

Important

StellarProtect (Legacy Mode) only supports configuration files in the UTF-8 file format.

Tip

To update multiple agents with shared settings, you may choose to only import the modified settings.

4. Encrypt the edited configuration file.
5. Import the edited configuration file.

Exporting or Importing a Config File

Note

TXOne StellarProtect (Legacy Mode) encrypts the configuration file before export. Users must decrypt the configuration file before modifying the contents.

Procedure

1. Open the TXOne StellarProtect (Legacy Mode) console using the desktop icon (if available) or the **Start** menu by clicking **All Programs** > **TXOne StellarProtect (Legacy Mode)**.
2. Provide the password and click **Log On**.
3. Click the **Settings** on the **Side Navigation Menu** to access the **Export/Import Configuration** section.
   - To export the configuration file as a database (`.xen`) file:
     a. Click **Export**, and choose where 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**.

     StellarProtect (Legacy Mode) overwrites the existing configuration settings with the settings in the database file.

Configuration File Syntax

The configuration file uses the XML format to specify parameters used by StellarProtect (Legacy Mode).

Important

StellarProtect (Legacy Mode) only supports configuration files in the UTF-8 file format.

Refer to the following example of the configuration file.

```
<?xml version="1.0" encoding="UTF-8"?>
<Configurations version="1.00.000" xmlns:xsi="http://www.w3.org/2001/XMLSc hema-instance"
xsi:noNamespaceSchemaLocation="WKConfig.xsd">
    <Configuration>
        <AccountGroup>
            <Account Id="{24335D7C-1204-43d1-9CBB-332D688C85B6}" Enable=
  "no">
                <Password/>
            </Account>
        </AccountGroup>
        <UI>
            <SystemTaskTrayIcon Enable="yes">
                <BlockNotification Enable="no" AlwaysOnTop="yes" ShowDetai
ls="yes" Authenticate="yes">
                    <Title/>
                    <Message/>
                </BlockNotification>
            </SystemTaskTrayIcon>
        </UI>
        <Feature>
            <ApplicationLockDown LockDownMode="2">
                <TrustList RecentHistoryUnapprovedFilesLimit="50">
                    <ExclusionList/>
                </TrustList>
                <ScriptLockdown Enable="yes">
                    <Extension Id="bat">
                        <Interpreter>cmd.exe</Interpreter>
                    </Extension>
                    <Extension Id="cmd">
                        <Interpreter>cmd.exe</Interpreter>
                    </Extension>
                    <Extension Id="com">
                        <Interpreter>ntvdm.exe</Interpreter>
                    </Extension>
                    <Extension Id="dll">
                        <Interpreter>ntvdm.exe</Interpreter>
```

```
</Extension>
<Extension Id="drv">
        <Interpreter>ntvdm.exe</Interpreter>
            </Extension>
            <Extension Id="exe">
                <Interpreter>ntvdm.exe</Interpreter>
            </Extension>
            <Extension Id="js">
                <Interpreter>cscript.exe</Interpreter>
                <Interpreter>wscript.exe</Interpreter>
            </Extension>
            <Extension Id="msi">
                <Interpreter>msiexec.exe</Interpreter>
            </Extension>
            <Extension Id="pif">
                <Interpreter>ntvdm.exe</Interpreter>
            </Extension>
            <Extension Id="ps1">
              <Interpreter>powershell.exe</Interpreter>
            </Extension>
            <Extension Id="sys">
                <Interpreter>ntvdm.exe</Interpreter>
            </Extension>
            <Extension Id="vbe">
                <Interpreter>cscript.exe</Interpreter>
                <Interpreter>wscript.exe</Interpreter>
            </Extension>
            <Extension Id="vbs">
                <Interpreter>cscript.exe</Interpreter>
                <Interpreter>wscript.exe</Interpreter>
            </Extension>
        </ScriptLockdown>
        <TrustedUpdater>
            <PredefinedTrustedUpdater Enable="no">
                <RuleSet/>
            </PredefinedTrustedUpdater>
            <WindowsUpdateSupport Enable="no"/>
        </TrustedUpdater>
        <DllDriverLockDown Enable="yes"/>
        <ExceptionPath Enable="no">
            <ExceptionPathList/>
        </ExceptionPath>
```

```
                    <TrustedCertification Enable="yes"/>
                    <TrustedHash Enable="no"/>
                    <WriteProtection Enable="no" ActionMode= "1"
                    ProtectApprov
            <CustomAction ActionMode="0"/>
            <FilelessAttackPrevention Enable="no">
                <ExceptionList/>
            </FilelessAttackPrevention>
            <IntelligentRuntimeLearning Enable="no"/>
    </ApplicationLockDown>
    <UsbMalwareProtection Enable="no" ActionMode="1"/>
    <DllInjectionPrevention Enable="no" ActionMode="1"/>
    <ApiHookingPrevention Enable="no" ActionMode="1"/>
    <IntegrityMonitoring Enable="no"/>
    <StorageDeviceBlocking Enable="no" ActionMode="1" AllowNonMassStorageUSBDevice="no">
            <DeviceException>
                <DeviceGroup name="UserDefined"/>
            </DeviceException>
      </StorageDeviceBlocking>
      <Log>
            <EventLog Enable="yes">
                <Level>
                    <WarningLog Enable="yes"/>
                    <InformationLog Enable="no"/>
                </Level>
                <BlockedAccessLog Enable="yes"/>
                <ApprovedAccessLog Enable="yes">
                    <TrustedUpdaterLog Enable="yes"/>
                    <DllDriverLog Enable="no"/>
                    <ExceptionPathLog Enable="yes"/>
                    <TrustedCertLog Enable="yes"/>
                    <TrustedHashLog Enable="yes"/>
                    <WriteProtectionLog Enable="yes"/>
                </ApprovedAccessLog>
                <SystemEventLog Enable="yes">
                    <ExceptionPathLog Enable="yes"/>
                    <WriteProtectionLog Enable="yes"/>
                </SystemEventLog>
                <ListLog Enable="yes"/>
                <UsbMalwareProtectionLog Enable="yes"/>
                <ExecutionPreventionLog Enable="yes"/>
```

```
                    <NetworkVirusProtectionLog Enable="yes"/>
                    <IntegrityMonitoringLog>
                        <FileCreatedLog Enable="yes"/>
                        <FileModifiedLog Enable="yes"/>
                        <FileDeletedLog Enable="yes"/>
                        <FileRenamedLog Enable="yes"/>
                            <RegValueModifiedLog Enable="yes"/>
                            <RegValueDeletedLog Enable="yes"/>
                            <RegKeyCreatedLog Enable="yes"/>
                            <RegKeyDeletedLog Enable="yes"/>
                            <RegKeyRenamedLog Enable="yes"/>
                        </IntegrityMonitoringLog>
                        <DeviceControlLog Enable="yes"/>
                    </EventLog>
                    <DebugLog Enable="yes"/>
                </Log>
            </Feature>
        <ManagedMode Enable="no">
            <Agent>
                <Port/>
                <FixedIp/>
            </Agent>
            <Server>
                <HostName/>
                <FastPort/>
            </Server>
            <Message InitialRetryInterval="120" MaxRetryInterv
al="7680">
            </Message>
ex="0"      <MessageRandomization TotalGroupNum="1" OwnGroupInd

            <Proxy Mode="0">
                <HostName/>
                <Port/>
                <UserName/>
                <Password/>
            </Proxy>
            <GroupPolicy>
                <SyncInterval>20</SyncInterval>
            </GroupPolicy>
        </ManagedMode>
    </Configuration>
```

```
                <Permission>
                    <AccountRefId="{24335D7C-1204-43d1-9CBB-
                    332D688C85B6}">
                        <UIControlId="DetailSetting" State="no"/>
                        <UIControlId="LockUnlock" State="yes"/>
                        <UIControlId="LaunchUpdater" State="yes"/>
                        <UIControl Id="RecentHistoryUnapprovedFiles"
                        State="yes"/>
                        <UIControlId="ImportExportList" State="yes"/>
            <UIControl Id="ListManagement" State="yes"/>
            <UIControl Id="SupportToolUninstall" State="no"/>
        </AccountRef>
        </Permission>
    </Configurations>
```

Configuration File Parameters

The configuration file contains sections that specify parameters used by StellarProtect (Legacy Mode).

TABLE 5-1. Configuration File Sections and Descriptions

SECTION	DESCRIPTION	ADDITIONAL INFORMATION
`Configuration`	Container for the Configuration section	
`AccountGroup`	Parameters to configure the User account	*Account Group Section on page 5-9*
`UI`	Parameters to configure the display of the system tray icon	*UI Section on page 5-10*
`Feature`	Container for the Feature section	
`ApplicationLockDown`	Parameters to configure StellarProtect (Legacy Mode) features and functions	*Feature Section on page 5-12*
`UsbMalwareProtection`		
`DllInjectionPrevention`		
`ApiHookingPrevention`		
`MemoryRandomization`		

Section	Description	Additional Information
NetworkVirusProtection		
IntegrityMonitoring		
StorageDeviceBlocking	A parameter to control storage device access to managed endpoints	
Log	Parameters to configure individual log types	*Log Section on page 5-27*
ManagedMode	Parameters to configure Centralized Management functions	*Managed Mode Section on page 5-32*
Permission	Container for the Permission section	
AccountRef	Parameters to configure the StellarProtect (Legacy Mode) console controls available to the User account	*AccountRef Section on page 5-36*

Account Group Section

The following table lists the parameters to configure the User account. Refer to *Password and Account Types on page 3-49* for more information about the User account.

Table 5-2. Configuration File - `AccountGroup` **Section Parameters**

Parameter	Settings	Value	Description
Configuration	Container for the Configuration section		
AccountGroup	Container for the AccountGroup section		
Account	ID	<GUID>	User account GUID
	Enable	yes	Enable the User account

Parameter	Settings	Value	Description
		no	Disable the User account
	Password	<admin_password>	Password for the User account to access the StellarProtect (Legacy Mode) console **Note** The StellarProtect (Legacy Mode) Administrator and User passwords cannot be the same.

UI Section

The following table lists the parameters to configure the display of the system tray icon.

Table 5-3. Configuration File - UI Section Parameters

Parameter	Settings	Value	Description
Configuration	Container for the Configuration section		
UI	Container for the UI section		
SystemTaskTrayIcon	Enable	yes	Display the system tray icon and Windows notifications

Parameter	Settings	Value	Description
		no	Hide the system tray icon and Windows notifications
BlockNotification	Enable	yes	Display a notification on the managed endpoint when a file not specified in the agent Approved List is blocked
		no	Do not display any notifications on the managed endpoint when files not specified in the agent Approved List are blocked
	Authenticate	yes	Prompt for the administrator password when the user attempts to close the notification
		no	Password is not required to close the notification
	ShowDetails	yes	Show file path of the blocked file and the event time
		no	Do not show event details
	AlwaysOnTop	yes	Keep the notification on top of any other screen
		no	Allow other screens to cover the notification

Parameter	Settings	Value	Description
	Title	<Title>	Specify the title for the notification
	Message	<Message>	Specify the message for the notification

Feature Section

The following table lists the parameters to configure StellarProtect (Legacy Mode) features and functions. See *About Feature Settings on page 3-59* for more information about the features and functions.

Table 5-4. Configuration File - `Feature` Section Parameters

Parameter	Settings	Value	Description
Configuration	Container for the Configuration section		
Feature	Container for the Feature section		
Application Lockdown	LockDownMode	1	Turn on Application Lockdown
		2	Turn off Application Lockdown
IntelligentRuntimeLearning		Enable	Enable using Intelligent Runtime Learning
		Disable	Disable using Intelligent Runtime Learning
TrustList	RecentHistoryUnapprovedFilesLimit	0 - 65535	Maximum number of entries in the Blocked Files log
ExclusionList	Folder	<folder_path>	Exclusion folder path
	Extension	<file_extension>	Exclusion file extension

Parameter	Settings	Value	Description
ScriptLockDown	Enable	yes	Enable Script Lockdown
	Disable	no	Disable Script Lockdown
Extension	ID	<file_extension>	File extension for Script Lockdown to block For example, specify a value of MSI to block .msi files
Interpreter		<file_name>	Interpreter for the specified file extension For example, specify msiexec.exe as the interpreter for .msi files
TrustedUpdater PredefinedTrustedUpdater	Enable	yes	Enable Trusted Updater
		no	Disable Trusted Updater
RuleSet: Container for RuleSet conditions			
Condition	ID	<unique_ruleset_name>	Unique name for the set of rules
Approved ListCheck	Enable	yes	Enable hash checks for programs executed using the Trusted Updater
		no	Disable hash checks for programs executed using the Trusted Updater

Parameter	Settings	Value	Description
ParentProcess	Enable	process_path>	Path of the parent process to add to the Trusted Updater List
Exception	Path	process_path>	Path to exclude from the Trusted Updater List
Rule	Label	unique_rule_name>	Unique name for this rule
Updater	Type	process	Use the specified EXE file
		file	Use the specified MSI or BAT file
		folder	Use the EXE, MSI, or BAT file in the specified folder
		folderandsub	Use the EXE, MSI or BAT files in the specified folder and its subfolders
	path	<updater_path>	Trusted Update path
	ConditionRef	<condition_ID>	Condition ID to provide a more detailed rule for the Trusted Updater
WindowsUpdateSupport	Enable	yes	Allow Windows Update to run on the managed endpoint when it is locked down

Parameter	Settings	Value	Description
		no	Block Windows Update on the managed endpoint when it is locked down
DLLDriverLockdown	Enable	yes	Enable DLL/Driver Lockdown
		no	Disable DLL/Driver Lockdown
ExceptionPath	Enable	yes	Enable exception paths
		no	Disable exception paths
ExceptionPathList: Container for the Exception List			
ExceptionPath	Path	<exception_path>	Exception path
	Type	file	Use only the specified file
		folder	Use the files in the specified folder
		folderandsub	Use the files in the specified folder and its subfolders
		regexp	Use an exception using the regular expression
TrustedCertification	Enable	yes	Enable using Trusted Certifications
		no	Disable using Trusted Certifications

Parameter	Settings	Value	Description
PredefinedTrusteddC ertification	Type	updater	File signed by this certificate is treated as a Trusted Update
		lockdo wn	File signed by this certificate is not treated as a Trusted Update
	Hash	SHA-1 _hash_ value>	SHA1-hash value of this certificate
	Label	<label>	Description of this certificate
	Subject	<subject>	Subject of this certificate
	Issuer	<issuer>	Issuer of this certificate
TrustedHash	Enable	yes	Enable using the Trusted Hash List
		noe	Disable using the Trusted Hash List
PredefinedTrusteddHash	Type	updater	File matched by this hash value is treated as a Trusted Update
		lockdown	File matched by this hash value is not treated as a Trusted Update
	Hash	<SHA-1 _hash_value>	SHA-1 hash value of this file
	Label	<label>	Description of this file

Parameter	Settings	Value	Description
	AddToApprovedList	yes	Add the file matched by this hash value to the Approved List when it is accessed for the first time
		no	Do not add the file matched by this hash value to the Approved List
	Path	<file_path>	File path
	Note	<note>	Add a note for the file matched by this hash value
WriteProtection	Enable	yes	Enable Write Protection
		no	Disable Write Protection
	ActionMode	0	Allow actions such as edit, rename, and delete
		1	Block actions such as edit, rename, and delete
	ProtectApprovedList	yes	Enable protection of the Approved List (in addition to the Write Protection List) when Write Protection is enabled

Parameter	Settings	Value	Description
		no	Disable protection of the Approved List (in addition to the Write Protection List) when Write Protection is enabled
List: Container for the Write Protection List			
File	Path	<file_path>	File path
Folder	Path	<folder_path>	Folder path
	IncludeSubfolder	yes	Use the files in the specified folder and its subfolders
		no	Use the files in the specified folder

Parameter	Settings	Value	Description
RegistryKey	Key	<reg_key>	Registry key <reg_key> can be abbreviated or expanded as shown below: • HKEY_LOCAL_MACHINE\test HKLM\test • HKEY_CURRENT_CONFIG\test HKCC\test • HKEY_CLASSES_ROOT\test HKCR\test • HKEY_CURRENT_USER\test HKCU\test • HKEY_USERS\test HKU\test
	IncludeSubkey	yes	Include any subkeys
		no	Do not include any subkeys

Parameter	Settings	Value	Description
RegistryValue	Key	<reg_key>	Registry key <reg_key> can be abbreviated or expanded as shown below: • HKEY_LOCAL_MACHINE\test HKLM\test • HKEY_CURRENT_CONFIG\test HKCC\test • HKEY_CLASSES_ROOT\test HKCR\test • HKEY_CURRENT_USER\test HKCU\test • HKEY_USERS\test HKU\test
	Name	reg_value_name>	Registry value name
ExceptionList: Container for the Write Protection Exception List			
Process	Path	<process_path>	Path of the process
File	Path	<file_path>	File path
Folder	Path	<folder_path>	Folder path
	IncludeSubfolder	yes	Use the files in the specified folder and its subfolders

Parameter	Settings	Value	Description
		no	Use the files in the specified folder
RegistryKey	Key	<reg_key>	Registry key <reg_key> can be abbreviated or expanded as shown below: • HKEY_LOCAL_MACHINE\test HKLM\test • HKEY_CURRENT_CONFIG\test HKCC\test • HKEY_CLASSES_ROOT\test HKCR\test • HKEY_CURRENT_USER\test HKCU\test • HKEY_USERS\test HKU\test
	IncludeSubkey	yes	Include any subkeys
		no	Do not include any subkeys

Parameter	Settings	Value	Description
RegistryValue	Key	<reg_key>	Registry key <reg_key> can be abbreviated or expanded as shown below: • HKEY_LOCAL_MACH INE \testHKLM \test • HKEY_CURRENT_CO NFIG \testHKCC \test • HKEY_CLASSES_RO OT \testHKCR \test • HKEY_CURRENT_US ER \testHKCU \test • HKEY_USERS \testHKU\test
	Name	<reg_value_name>	Registry value name
CustomAction	ActionMode	0	Ignore blocked files or processes when Application Lockdown blocks any of the following events: • Process launch • DLL loading • Script file access

Parameter	Settings	Value	Description
		1	Quarantine blocked files or processes when Application Lockdown blocks any of the following events: • Process launch • DLL loading • Script file access
		2	Ask what to do for blocked files or processes when Application Lockdown blocks any of the following events: • Process launch • DLL loading • Script file access
UsbMalwareProtection	Enable	yes	Enable USB Malware Protection
		no	Disable USB Malware Protection
	ActionMode	0	Allow action by detected malware
		1	Block action by detected malware
DllInjectionPrevention	Enable	yes	Enable DLL Injection Prevention
		no	Disable DLL Injection Prevention

Parameter	Settings	Value	Description
	ActionMode	0	Allows DLL injections
		1	Blocks DLL injections
ApiHookingPrevention	Enable	yes	Enable API Hooking Prevention
		no	Disable API Hooking Prevention
	ActionMode	0	Allow API hooking
		1	Block API hooking
MemoryRandomization	Enable	yes	Enable Memory Randomization
		no	Disable Memory Randomization
IntegrityMonitoring	Enable	yes	Enable Integrity Monitoring
		no	Disable Integrity Monitoring
StorageDeviceBlocking	Enable	yes	Blocks access of storage devices (CD/DVD drives, floppy disks, and USB devices) to managed endpoints
	Disable	no	Allows access of storage devices (CD/DVD drives, floppy disks, and USB devices) to managed endpoints
	ActionMode	0	Allow actions such as edit, rename, and delete

Parameter	Settings	Value	Description
		1	Block actions such as edit, rename, and delete
	AllowNonMassStorageUSBDevice	yes	Allow some drivers (e.g., Touch screen/ Infrared sensor/ Android mobile phone) from being loaded when those hardware devices are plugged in and storage device blocking is enabled.
		no	Block some drivers (e.g., Touch screen/ Infrared sensor/ Android mobile phone) from being loaded when those hardware devices are plugged in and storage device blocking is enabled.
DeviceException: Container for the Storage Device Blocking device exception list			
DeviceGroup: Container for the Storage Device Blocking device list			
	name: Unique name of the device list		
Device	vid		Device vendor ID
	pid		Device product ID
	sn		Device serial number
Log: Container for configuring logs Refer to *Log Section on page 5-27* for more details.			

Parameter	Settings	Value	Description
FilelessAttackPrevention	Enable	yes	Enable Fileless Attack Prevention
		no	Disable Fileless Attack Prevention
ExceptionList: Container for the Fileless Attack Prevention Exception List			
Exception	Target	<monitored process>	Specify powershell.exe, wscript.exe, CScript.exe, or mshta.exe
	Label	<label>	Unique name of this exception
Arguments		<arguments>	Arguments to be approved
	Regex	yes	Specify yes if argument includes a regular exception
		no	Specify no if argument does not include a regular exception
Parent1		<parent process>	Parent process of the monitored process
Parent2		<grandparent process>	Grandparent process of the monitored process
Parent3		<great grandparent process>	Great grandparent process of the monitored process

Parameter	Settings	Value	Description
Parent4		<great great grandparent process>	Great great grandparent process of the monitored process

Log Section

The following table lists the parameters to configure individual log types. Refer to *Agent Event Log Descriptions for StellarProtect (Legacy Mode) on page 6-24* for more information about log descriptions.

Table 5-5. Configuration File - Log Section Parameters

Parameter	Settings	Value	Description
Configuration	Container for the Configuration section		
Feature	Container for the Feature section		
Log	Container for configuring logs		
EventLog	Enable	yes	Log the StellarProtect (Legacy Mode) events specified in the following elements
		no	Do not log the StellarProtect (Legacy Mode) events specified in the following elements
Level: Container for configuring log levels			
WarningLog	Enable	yes	Log “Warning” level events related to StellarProtect (Legacy Mode)

Parameter	Settings	Value	Description
		no	Do not log “Warning” level events related to StellarProtect (Legacy Mode)
InformationLog	Enable	yes	Log “Information” level events related to StellarProtect (Legacy Mode)
		no	Do not log “Information” level events related to StellarProtect (Legacy Mode)
BlockedAccessLog	Enable	yes	Log files blocked by StellarProtect (Legacy Mode)
		no	Do not log files blocked by StellarProtect (Legacy Mode)
ApprovedAccessLog	Enable	yes	Log files approved by StellarProtect (Legacy Mode)
		no	Do not log files approved by StellarProtect (Legacy Mode)
TrustedUpdaterLog	Enable	yes	Log Trusted Updater approved access
		no	Do not log Trusted Updater approved access
DLLDriver Log	Enable	yes	Log DLL/Driver approved access

Parameter	Settings	Value	Description
		no	Do not log DLL/Driver approved access
Exception PathLog	Enable	yes	Log Application Lockdown exception path approved access
		no	Do not log Application Lockdown exception path approved access
TrustedCe rtLog	Enable	yes	Log Trusted Certifications approved access
		no	Do not log Trusted Certifications approved access
WriteProt ectionLog	Enable	yes	Log Write Protection approved access
		no	Do not log Write Protection approved access
SystemEventLog	Enable	yes	Log events related to the system
		no	Do not log events related to the system
Exception PathLog	Enable	yes	Log exceptions to Application Lockdown
		noe	Do not log exceptions to Application Lockdown
WriteProt ectionLog	Enable	yes	Log Write Protection events

Parameter	Settings	Value	Description
		no	Do not log Write Protection events
ListLog	Enable	yes	Log events related to the Approved list
		no	Do notlog events related to the Approved list
UsbMalwareProtectionLog	Enable	yes	Log events that trigger USB Malware Protection
		no	Do not log events that trigger USB Malware Protection
ExecutionPreventionLog	Enable	yes	Log events that trigger Execution Prevention
		no	Do not log events that trigger Execution Prevention
IntegrityMonitoringLog: Container for configuring Integrity Monitoring logs			
FileCreatedLog	Enable	yes	Log file and folder created events
		no	Do not log file and folder created events
FileModifiedLog	Enable	yes	Log file modified events
		no	Do not log file modified events
FileDeletedLog	Enable	yes	Log file and folder deleted events

Parameter	Settings	Value	Description
		no	Do not log file and folder deleted events
FileRenamedLog	Enable	yes	Log file and folder renamed events
		no	Do not log file and folder renamed events
RegValueModifiedLog	Enable	yes	Log registry value modified events
		no	Do not log registry value modified events
RegValueDeletedLog	Enable	yes	Log registry value deleted events
		no	Do not log registry value deleted events
RegKeyCreatedLog	Enable	yes	Log registry key created events
		no	Do not log registry key created events
RegKeyDeletedLog	Enable	yes	Log registry key deleted events
		no	Do not log registry key deleted events
RegKeyRenamedLog	Enable	yes	Log registry key renamed events
		no	Do not log registry key renamed events
DeviceControlLog	Enable	yes	Log storage device control events

Parameter	Settings	Value	Description
		no	Do not log storage device control events
DebugLog	Enable	yes	Log debugging information
		no	Do not log debugging information

Managed Mode Section

The following table lists the parameters to configure Centralized Management functions.

Table 5-6. Configuration File - ManagedMode **Section Parameters**

Parameter	Settings	Value	Description
Configuration GroupPolicy	Container for the Configuration section Container for configuring group policy to StellarOne		
SyncInterval		0 ~ 2147483647 **Note** Unite: Minutes	Agent information will be updated periodically according to this sync period
Agent: Container for configuring StellarProtect (Legacy Mode) agents			
Port		<server_messages_port>	Specify the secure port for server communications (formerly the agent listening port)
		no	Do not log “Warning” level events related to StellarProtect (Legacy Mode)

Parameter	Settings	Value	Description
FixedIp		• A.B.C.D/E • A,B,C,D: 0~255 • E: 1~32	Specify the agent IP address (in Classless inter-domain routing (CIDR) format) to communicate with the StellarOne server
server: Container for configuring StellarOne			
HostName		<hostname>	Specify the host name of the StellarOne
FastPort		<logs_port>	Specify secure port for collecting logs and status (formerly Fast Lane)
Message : Container for configuring automated messages to StellarOne			
InitialRetryInterval		0~2147483647 **Note** Unit: Seconds	Starting interval, in seconds, between attempts to resend an event to StellarOne This interval doubles in size for each unsuccessful attempt, until it exceeds the MaxRetryInterval value
MaxRetryInterval		0~2147483647 **Note** Unit: Seconds	Maximum interval between attempts to resend events to StellarOne

Parameter	Settings	Value	Description
`RegularStatusUpdate`		• `0` • `1`	0: Agent information will not be updated periodically during this sync period 1: Agent information will be updated periodically during this sync period

Parameter	Settings	Value	Description
MessageRandomization **Note** StellarProtect (Legacy Mode) agents respond as soon as possible to direct requests from StellarProtect (Legacy Mode) Central Console. For details, refer to Applying Message TimeGroups in the StellarProtect (Legacy Mode) Administrator's Guide	TotalGroupNum	Positive Integer (>= 1)	Specify the total number of message time groups
	OwnGroupIndex	Zero or Positive Integer, <TotalGroupNum>	Specify the message time group ID number of this StellarProtect (Legacy Mode) agent
	TimePeriod	Zero or Positive Integer	Specify the duration of time in whole seconds that this message time group ID number will send automated messages to StellarOne when this group's message sending cycle is active **Note** Message time groups do not become active if their duration is set to zero (0).
Proxy	Mode	0	Do not use a proxy (direct access)
		1	Use a proxy (manual setting)

Parameter	Settings	Value	Description
		2	Synchronize proxy settings with Internet Explorer
HostName		<proxy_hostname>	Specify the proxy host name
Port		<proxy_port>	Specify the proxy port number
UserName		<proxy_user_name>	Specify the proxy user name
Password		<proxy_password>	Specify the proxy password

AccountRef Section

The following table lists the parameters to configure the StellarProtect (Legacy Mode) console controls available to the User account.

Refer to *Password and Account Types on page 3-49* for more information about the StellarProtect (Legacy Mode) acount types.

Table 5-7. Configuration File - AccountRef Section Parameters

Parameter	Settings	Value	Description
Configuration	Container for the Configuration section		
Permission	Container for the Permission section		
AccountRef	Container for the AccountRef section		
UIControl	ID	DetailSetting	Access the features and functions on the StellarProtect (Legacy Mode) console Settings page

Parameter	Settings	Value	Description
			Note The Password page is not available to the User account.
		LockUnlock	Access the Application Lockdown setting on the **Overview** screen
		LaunchUpdater	Access the **Automatically add files created or modified by the selected application installer** option when a User clicks **Add Item** on the **Approved List** screen
		RecentHistoryUnapprovedFiles	Access the Block logs if a User clicks **Last application blocked** link on the **Overview** screen
		ImportExportList	Access the **Import List** and **Export List** buttons
		ListManagement	Access the following items on the **Approved List** screen: • The **Delete Item** button

Parameter	Settings	Value	Description
			• The **Update Hash** button • The **Add Item** > **Add Files/ Folders** menu
	State	yes	Enable the permission specified by ID
		no	Disable the permission specified by ID

Chapter 6

Agent Event Logs

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

Overview of Agent Event Logs

The StellarProtect/StellarProtect (Legacy Mode) agent logs events within three classifications.

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

StellarProtect Events

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

- *Accessing StellarProtect Event Logs on page 6-2*
- *Agent Event Log Descriptions for StellarProtect on page 6-2*

Accessing StellarProtect Event Logs

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

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

Agent Event Log Descriptions for StellarProtect

This table details the Windows event log descriptions for StellarProtect.

Event ID	Level	Category	Event	Details
256	Information	System	Service has started.	

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
257	Information	System	Policy has been applied successfully. (Version: %version%)	
258	Information	System	Patch has been applied. File Name: %file_name%	
259	Information	System	Patching in progress	After the earlier-applied patch is completed, the system will automatically try to apply this patch: %deferred_file_name%.
513	Information	intelli_av	Application vault update was successful	
514	Information	intelli_av	Real Time Scan has been enabled.	
515	Information	intelli_av	A scheduled scan has started.	

Event ID	Level	Category	Event	Details
516	Information	intelli_av	A scheduled scan has ended.	Folders scanned: %1 Symbolic links: %2 Regular files: %3 Files scanned: %4 Files passed: %5 Threats detected: %6
517	Information	intelli_av	A manually launched scan has started.	
518	Information	intelli_av	A manually launched scan has ended.	Folders scanned: %1 Symbolic links: %2 Regular files: %3 Files scanned: %4 Files passed: %5 Threats detected: %6
519	Information	intelli_av	A scheduled scan has been enabled.	Next scan will be on %NextScan %.
520	Information	intelli_av	A scheduled scan has been disabled.	

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
521	Information	intelli_av	A scan manually launched by local user has started.	
522	Information	intelli_av	A scan manually launched by local user has ended.	Folders scanned: %1 Symbolic links: %2 Regular files: %3 Files scanned: %4 Files passed: %5 Threats detected: %6
768	Information	anomaly_detect	Operations Behavior Anomaly Detection (Script Behavior) has been enabled.	Mode: %Mode% Level: %Level% Learning time: %LearningTime % day(s)

Event ID	Level	Category	Event	Details
769	Information	anomaly_detect	Script behavior has been added to the Situational Awareness baseline.	Access User: %USERNAME% ID: %ID% Target Process: %PATH% %ARGUMENT% Parent Process 1: %PATH% %ARGUMENT% Parent Process 2: %PATH% %ARGUMENT% Parent Process 3: %PATH% %ARGUMENT% Parent Process 4: %PATH% %ARGUMENT%
770	Information	anomaly_detect	A script behavior has been excluded from the Situational Awareness baseline.	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	Details
771	Information	anomaly_detect	Operations Behavior Anomaly Detection (User Login) has been enabled.	Mode: %Mode% Level: %Level% Learning time: %LearningTime % day(s)
772	Information	anomaly_detect	Operations Behavior Anomaly Detection (Application Behavior) has been enabled.	Mode: %Mode% Level: %Level% Learning time: %LearningTime % day(s)
773	Information	anomaly_detect	A user login account has been added to the Situational Awareness baseline.	Domain: %Domain% Account: %Account% Login Type: %LoginType% Source IP: %IP%
774	Information	anomaly_detect	A user login account has been excluded from the Situational Awareness baseline.	Domain: %Domain% Account: %Account% Login Type: %LoginType% Source IP: %IP%
775	Information	anomaly_detect	An application has been added to the Situational Awareness baseline.	Application Path: %Path%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
776	Information	anomaly_detect	An application has been excluded from the Situational Awareness baseline.	Application Path: %Path%
784	Information	anomaly_detect	DLL Injection Prevention has been enabled.	
1280	Information	device_control	Device Control has been enabled.	
1281	Information	device_control	Trusted USB device has been added.	Vendor ID: %HEX% Product ID: %HEX% Serial Number: %STRING% Type: permanent or one time
1282	Information	device_control	Trusted USB device has been removed.	Vendor ID: %HEX% Product ID: %HEX% Serial Number: %STRING%

Event ID	Level	Category	Event	Details
1792	Information	lockdown	File access has been allowed: %PATH%	Access Image Path: %PATH% Access User: %USERNAME% Mode: %MODE% List: %LIST%
1793	Information	lockdown	A new file has been added to Approved List in Maintenance Mode.	Path: %PATH% Hash: %SHA256_HEXSTR%
1794	Information	lockdown	The hash of an existing file in Approved List has been updated in Maintenance Mode.	Path: %PATH% Hash: %SHA256_HEXSTR%
1795	Information	lockdown	Approved List initialization has started.	
1796	Information	lockdown	Approved List initialization has completed	Count: %COUNT%
1797	Information	lockdown	Application Lockdown has been enabled	Mode: %MODE%
1798	Information	lockdown	DLL/Driver Lockdown has been enabled.	
1799	Information	lockdown	Script Lockdown has been enabled.	

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
1800	Information	lockdown	Intelligent Runtime Learning has been enabled.	
2048	Information	update	Component update has started.	
2049	Information	update	Component update has ended.	
2050	Information	update	Scheduled component update has been enabled. Next update will be on %NEXT_UPDATE_LOCAL_TIME_STR% (agent's local system time).	
2051	Information	update	Scheduled component update has been disabled.	
3840	Information	misc	User account has been enabled.	
3841	Information	misc	User account has been disabled.	
3842	Information	misc	User password has been changed.	

Event ID	Level	Category	Event	Details
4352	Warning	system	Service has stopped.	
4353	Warning	system	Unable to apply policy (Version: %version%)	
4354	Warning	system	Unable to update file.	Source Path: %src_path% Destination Path: %dst_path% Error Code: %err_code%
4355	Warning	system	Unable to apply patch.	File Name: %file_name% Error Code: %err_code%

Event ID	Level	Category	Event	Details
4609	Warning	intelli_av	Incoming Files Scanned, Action Taken by Antivirus: %PATH%	Incoming files were scanned by antivirus. Action was 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	DETAILS
4610	Warning	intelli_av	Incoming Files Scanned, Action Taken by Next-Generation Antivirus: %PATH%	Incoming files were scanned by next-generation antivirus. Action was 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	Details
4611	Warning	intelli_av	Local Files Scanned, Action Taken by Antivirus: %PATH%	Local files were scanned by antivirus. Action was 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	Details
4612	Warning	intelli_av	Local Files Scanned, Action Taken by Next-Generation Antivirus: %PATH%	Local files were scanned by next-generation antivirus. Action was taken according to settings. File Path: %PATH% File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING% Action Result: %INTEGER% Quarantine Path: %PATH%
4613	Warning	intelli_av	Suspicious Program Execution Blocked	Suspicious program execution was blocked. File Path: %PATH% File Hash: %STRING%

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

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
4617	Warning	intelli_av	Application Execution Blocked By Next-Generation Antivirus	Application execution was blocked by next-generation antivirus. Process Image Path: %PATH% File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING%
4864	Warning	anomaly_detect	Operations Behavior Anomaly Detection (Script Behavior) has been disabled.	

Event ID	Level	Category	Event	Details
4865	Warning	anomaly_detect	Script Behavior has been allowed by Operations Behavior Anomaly Detection: %PATH%	Access User: %USERNAME% Parent Process 1: %PATH% %ARGUMENT% Parent Process 2: %PATH% %ARGUMENT% Parent Process 3: %PATH% %ARGUMENT% Parent Process 4: %PATH% %ARGUMENT% Mode: %Mode% Level: %LEVEL%
4866	Warning	anomaly_detect	Script Behavior has been blocked by Operations Behavior Anomaly Detection: %PATH%	Access User: %USERNAME% Parent Process 1: %PATH% %ARGUMENT% Parent Process 2: %PATH% %ARGUMENT% Parent Process 3: %PATH% %ARGUMENT% Parent Process 4: %PATH% %ARGUMENT% Mode: %Mode% Level: %LEVEL%

Event ID	Level	Category	Event	Details
4867	warning	anomaly_detect	Operations Behavior Anomaly Detection (User Login) has been disabled.	
4868	warning	anomaly_detect	Operations Behavior Anomaly Detection (Application Behavior) has been disabled.	
4869	warning	anomaly_detect	A user login failure has been detected by Operations Behavior Anomaly Detection.	Domain: %Domain% Account: %Account% Login Type: %LoginType% Source IP: %IP%
4870	warning	anomaly_detect	An abnormal user Login has been detected by Operations Behavior Anomaly Detection.	Domain: %Domain% Account: %Account% Login Type: %LoginType% Source IP: %IP%

Event ID	Level	Category	Event	Details
4871	warning	anomaly_detect	Suspicious application behavior has been detected by Operations Behavior Anomaly Detection.	Program Path: %Path% Program Hash: %SHA256% Program Size: %Size% Certificate: %CertificateSigner% Vendor: %VendorName% Product: %Product%
4872	warning	anomaly_detect	An unrecognized application has been detected by Operations Behavior Anomaly Detection.	PID: %PID% Program Path: %Path% Program Hash: %SHA256% Program Size: %Size% Certificate: %CertificateSigner% Vendor: %VendorName% Product: %Product%

Event ID	Level	Category	Event	Details
4873	warning	anomaly_detect	Malicious application behavior has been detected by Operations Behavior Anomaly Detection	Program Path: %Path% Program Hash: %SHA256% Program Size: %Size% Certificate: %CertificateSigner% Vendor: %VendorName% Product: %Product%
4880	Warning	anomaly_detect	DLL Injection Prevention has been disabled.	
5120	Warning	change_control	Change to an ICS file was blocked by OT Application Safeguard.	Blocked Process: %PATH% Target File: %PATH%
5121	Warning	change_control	Manipulation to existing ICS process was blocked by OT Application Safeguard.	Blocked Process: %PATH% Target Process: %PATH%
5376	Warning	device_control	Device Control has been disabled.	

Event ID	Level	Category	Event	Details
5377	Warning	device_control	USB access has been blocked: %PATH%	Access Image Path: %PATH% Access User: %USERNAME% Vendor ID: %HEX% Product ID: %HEX% Serial Number: %STRING%
5888	Warning	lockdown	File access has been allowed: %PATH%	Access Image Path: %PATH% Access User: %USERNAME% Mode: %MODE% Reason: %ALLOWED_REASON% File hash allowed: %SHA256_HEXSTR% %THROTTLING_INFO_MSG%

Event ID	Level	Category	Event	Details
5889	Warning	lockdown	File access has been blocked: C:\object_file_path	Access Image Path: %PATH% Access User: %USERNAME% Mode: %MODE% Reason: %BLOCKED_REASON% File hash blocked: %SHA256_HEXSTR% %THROTTLING_INFO_MSG%
5890	Warning	lockdown	Unable to add to or update Approved List: %PATH%	
5891	Warning	lockdown	Application Lockdown has been disabled	
5892	Warning	lockdown	DLL/Driver Lockdown has been disabled.	
5893	Warning	lockdown	Script Lockdown has been disabled.	
5894	Warning	lockdown	Intelligent Runtime Learning has been disabled.	
5895	Warning	lockdown	Approved List initialization has been canceled.	

Event ID	Level	Category	Event	Details
8706	Critical	intelli_av	Real-Time Scan has been disabled.	
9216	Critical	change_control	The Maintenance Mode has now started.	
9217	Critical	change_control	The Maintenance Mode has now ended.	

StellarProtect (Legacy Mode) Events

This section describes events as they will be recorded within the TXOne StellarProtect (Legacy Mode) Agent. Topics include:

- *Agent Event Log Descriptions for StellarProtect (Legacy Mode) on page 6-24*
- *Agent Error Code Descriptions for StellarProtect (Legacy Mode) on page 6-70*

Agent Event Log Descriptions for StellarProtect (Legacy Mode)

This table details the Windows event log descriptions for StellarProtect (Legacy Mode).

Event ID	Level	Category	Event	Details
1000	Information	System	Service started	
1001	Warning	System	Service stopped	
1002	Information	System	Application Lockdown Turned On	
1003	Warning	System	Application Lockdown Turned Off	

Event ID	Level	Category	Event	Details
1004	Information	System	Disabled	
1005	Information	System	Administrator password changed	
1006	Information	System	User password changed	
1007	Information	System	User account enabled	
1008	Information	System	User account disabled	
1009	Information	System	Product activated	
1010	Information	System	Product deactivated	
1011	Warning	System	License Expired. Grace period enabled.	
1012	Warning	System	License Expired. Grace period ended.	
1013	Information	System	Product configuration import started: %path%	
1014	Information	System	Product configuration import completed: %path%	
1015	Information	System	Product configuration exported to: %path%	

Event ID	Level	Category	Event	Details
1016	Information	System	USB Malware Protection set to Allow	
1017	Information	System	USB Malware Protection set to Block	
1018	Information	System	USB Malware Protection enabled	
1019	Warning	System	USB Malware Protection disabled	
1025	Information	System	Memory Randomization enabled	
1026	Warning	System	Memory Randomization disabled	
1027	Information	System	API Hooking Prevention set to Allow	
1028	Information	System	API Hooking Prevention set to Block	
1029	Information	System	API Hooking Prevention enabled	
1030	Warning	System	API Hooking Prevention disabled	
1031	Information	System	DLL Injection Prevention set to Allow	

Event ID	Level	Category	Event	Details
1032	Information	System	DLL Injection Prevention set to Block	
1033	Information	System	DLL Injection Prevention enabled	
1034	Warning	System	DLL Injection Prevention disabled	
1035	Information	System	Pre-defined Trusted Update enabled	
1036	Information	System	Pre-defined Trusted Update disabled	
1037	Information	System	DLL/Driver Lockdown enabled	
1038	Warning	System	DLL/Driver Lockdown disabled	
1039	Information	System	Script Lockdown enabled	
1040	Warning	System	Script Lockdown disabled	
1041	Information	System	Script added	File extension: %extension% Interpreter: %interpreter%
1042	Information	System	Script removed	File extension: %extension%

Event ID	Level	Category	Event	Details
				Interpreter: %interpreter%
1044	Information	System	Exception path enabled	
1045	Information	System	Exception path disabled	
1047	Information	System	Trusted certificate enabled	
1048	Information	System	Trusted certificate disabled	
1049	Information	System	Write Protection enabled	
1050	Warning	System	Write Protection disabled	
1051	Information	System	Write Protection set to Allow	
1052	Information	System	Write Protection set to Block	
1055	Information	System	Added file to Write Protection List Path: %path%	
1056	Information	System	Removed file from Write Protection List Path: %path%	
1057	Information	System	Added file to Write Protection Exception List Path: %path%	

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
			Process: %process%	
1058	Information	System	Removed file from Write Protection Exception List Path: %path% Process: %process%	
1059	Information	System	Added folder to Write Protection List Path: %path% Scope: %scope%	
1060	Information	System	Removed folder from Write Protection List Path: %path% Scope: %scope%	
1061	Information	System	Added folder to Write Protection Exception List Path: %path% Scope: %scope% Process: %process%	
1062	Information	System	Removed folder from Write Protection Exception List Path: %path%	

Event ID	Level	Category	Event	Details
			Scope: %scope% Process: %process%	
1063	Information	System	Added registry value to Write Protection List Registry Key: %regkey% Registry Value Name: %regvalue%	
1064	Information	System	Removed registry value from Write Protection List Registry Key: %regkey% Registry Value Name: %regvalue%	
1065	Information	System	Added registry value to Write Protection Exception List Registry Key: %regkey% Registry Value Name: %regvalue% Process: %process%	
1066	Information	System	Removed registry value from Write Protection Exception List	

Event ID	Level	Category	Event	Details
			Registry Key: %regkey% Registry Value Name: %regvalue% Process: %process%	
1067	Information	System	Added registry key to Write Protection List Path: %regkey% Scope: %scope%	
1068	Information	System	Removed registry key from Write Protection List Path: %regkey% Scope: %scope%	
1069	Information	System	Added registry key to Write Protection Exception List Path: %regkey% Scope: %scope% Process: %process%	
1070	Information	System	Removed registry key from Write Protection Exception List Path: %regkey% Scope: %scope%	

Event ID	Level	Category	Event	Details
			Process: %process%	
1071	Information	System	Custom Action set to Ignore	
1072	Information	System	Custom Action set to Quarantine	
1073	Information	System	Custom Action set to Ask StellarOne	
1074	Information	System	Quarantined file is restored.	Original Location: %path% Source: %source %
1075	Information	System	Quarantined file is deleted.	Original Location: %path% Source: %source %
1076	Information	System	Integrity Monitoring enabled	
1077	Information	System	Integrity Monitoring disabled	
1078	Information	System	Root cause analysis report unsuccessful	Access Image Path: %path%
1079	Information	System	Server certification imported: %path %	
1080	Information	System	Server certification	

Event ID	Level	Category	Event	Details
			exported: %path %	
1081	Information	System	Managed mode configuration imported: %path %	
1082	Information	System	Managed mode configuration exported: %path %	
1083	Information	System	Managed mode enabled	
1084	Information	System	Managed mode disabled	
1085	Information	System	Protection applied to Write Protection List and Approved List while Write Protection is enabled	
1086	Warning	System	Protection applied to Write Protection List while Write Protection is enabled.	
1088	Information	System	Windows Update Support enabled	
1089	Information	System	Windows Update Support disabled	
1094	Information	System	Applied a patch to agent by StellarOne	

Event ID	Level	Category	Event	Details
			File applied: %file_name%	
1096	Information	System	Trusted hash enabled	
1097	Information	System	Trusted hash disabled	
1099	Information	System	Storage device access set to Allow	
1100	Information	System	Storage device access set to Block	
1101	Information	System	Storage device control enabled	
1102	Warning	System	Storage device control disabled	
1103	Information	System	Event Log settings changed	Windows Event Log: %ON|off% Level: Warning Log: %ON|off% Information Log: %ON|off% System Log: %ON|off% Exception Path Log: %ON|off% Write Protection Log: %ON|off% List Log: %ON|off%

Event ID	Level	Category	Event	Details
				Approved Access Log: DllDriver Log: %ON|off% Trusted Updater Log: %ON|off% Exception Path Log: %ON|off% Trusted Certification Log: %ON|off% Trusted Hash Log: %ON|off% Write Protection Log: %ON|off% Blocked Access Log: %ON|off% USB Malware Protection Log: %ON|off% Execution Prevention Log: %ON|off% Integrity Monitoring Log File Created Log: %ON|off% File Modified Log: %ON|off% File Deleted Log: %ON|off% File Renamed Log: %ON|off%

Event ID	Level	Category	Event	Details
				RegValue Modified Log: %ON|off% RegValue Deleted Log: %ON|off% RegKey Created Log: %ON|off% RegKey Deleted Log: %ON|off% RegKey Renamed Log: %ON|off% Device Control Log: %ON|off% Debug Log: %ON|off%
1104	Warning	System	Memory Randomization is not available in this version of Windows.	
1105	Information	System	Blocked File Notification enabled	
1106	Information	System	Blocked File Notification disabled	
1107	Information	System	Administrator password changed remotely	
1111	Information	System	Fileless Attack Prevention enabled	

Event ID	Level	Category	Event	Details
1112	Warning	System	Fileless Attack Prevention disabled	
1500	Information	List	Trusted Update started.	
1501	Information	List	Trusted Update stopped.	
1502	Information	List	Approved List import started: %path%	
1503	Information	List	Approved List import complete: %path%	
1504	Information	List	Approved List exported to: %path%	
1505	Information	List	Added to Approved List: %path%	
1506	Information	List	Added to Trusted Updater List: %path%	
1507	Information	List	Removed from Approved List: %path%	
1508	Information	List	Removed from Trusted Updater List: %path%	
1509	Information	List	Approved List updated: %path%	

Event ID	Level	Category	Event	Details
1510	Information	List	Trusted Updater List updated: %path%	
1511	Warning	List	Unable to add to or update Approved List: %path%	
1512	Warning	List	Unable to add to or update Trusted Updater List: %path%	
1513	Information	System	Added to Exception Path List	Type: %exceptionpathtype% Path: %exceptionpath%
1514	Information	System	Removed from Exception Path List	Type: %exceptionpathtype% Path: %exceptionpath%
1515	Information	System	Added to Trusted Certification List	Label: %label% Hash: %hashvalue% Type: %type% Subject: %subject% Issuer: %issuer%

Event ID	Level	Category	Event	Details
1516	Information	System	Removed from Trusted Certification List	Label: %label% Hash: %hashvalue% Type: %type% Subject: %subject% Issuer: %issuer%
1517	Information	System	Added to Trusted Hash List.%n	Label : %label% Hash : %hashvalue% Type : %type% Add to Approved List: %yes|no% Path : %path% Note: %note%
1518	Information	System	Removed from Trusted Hash List.%n	Label : %label% Hash : %hashvalue% Type : %type% Add to Approved List: %yes|no% Path : %path% Note: %note%
1519	Information	List	Removed from Approved List remotely: %path%	
1520	Warning	List	Unable to create Approved List because an	

Event ID	Level	Category	Event	Details
			unexpected error occurred during enumeration of the files in %1 %n Error Code: %2 %n	
1521	Information	System	Added Fileless Attack Prevention exception	Label : %label% Target Process: %process_name % Arguments: %arguments% %regex_flag% Parent Process 1 Image Path: %path% Parent Process 2 Image Path: %path% Parent Process 3 Image Path: %path% Parent Process 4 Image Path: %path%
1522	Information	System	Removed Fileless Attack Prevention exception	Label : %label% Target Process: %process_name % Arguments: %arguments% %regex_flag%

Event ID	Level	Category	Event	Details
				Parent Process 1 Image Path: %path% Parent Process 2 Image Path: %path% Parent Process 3 Image Path: %path% Parent Process 4 Image Path: %path%
1523	Information	System	Maintenance Mode started	
1524	Information	System	Leaving Maintenance Mode	
1525	Information	System	Maintenance Mode stopped	
1526	Information	List	Added to Approved List in Maintenance Mode Path: %1 Hash: %2	
1527	Information	List	Approved List updated in Maintenance Mode Path: %1 Hash: %2	

Event ID	Level	Category	Event	Details
2000	Information	Access Approved	File access allowed: %path%	Access Image Path: %path% Access User: %username% Mode: %mode% List: %list%
2001	Warning	Access Approved	File access allowed: %path%	Access Image Path: %path% Access User: %username% Mode: %mode% File Hash allowed: %hash%
2002	Warning	Access Approved	File access allowed: %path% Unable to get the file path while checking the Approved List	Access Image Path: %path% Access User: %username% Mode: %mode%
2003	Warning	Access Approved	File access allowed: %path% Unable to calculate hash while checking the Approved List	Access Image Path: %path% Access User: %username% Mode: %mode%
2004	Warning	Access Approved	File access allowed: %path% Unable to get notifications to monitor process	

Event ID	Level	Category	Event	Details
2005	Warning	Access Approved	File access allowed: %path% Unable to add process to non exception list	
2006	Information	Access Approved	File access allowed: %path%	Access Image Path: %path% Access User: %username% Mode: %mode%
2007	Warning	Access Approved	File access allowed: %path% An error occurred while checking the Exception Path List	Access Image Path: %path% Access User: %username% Mode: %mode%
2008	Warning	Access Approved	File access allowed: %path% An error occurred while checking the Trusted Certification List	Access Image Path: %path% Access User: %username% Mode: %mode%
2011	Information	Access Approved	Registry access allowed Registry Key: %regkey% Registry Value Name: %regvalue %	Access Image Path: %path% Access User: %username% Mode: %mode%
2012	Information	Access Approved	Registry access allowed	Access Image Path: %path% Access User: %username%

Event ID	Level	Category	Event	Details
			Registry Key: %regkey%	Mode: %mode%
2013	Information	Access Approved	Change of File/ Folder allowed by Exception List: %path%	Access Image Path: %path% Access User: %username% Mode: %mode%
2015	Information	Access Approved	Change of Registry Value allowed by Exception List Registry Key: %regkey% Registry Value Name: %regvalue %	Access Image Path: %path% Access User: %username% Mode: %mode%
2016	Information	Access Approved	Change of Registry Key allowed by Exception List Registry Key: %regkey%	Access Image Path: %path% Access User: %username% Mode: %mode%
2017	Warning	Access Approved	Change of File/ Folder allowed: %path%	Access Image Path: %path% Access User: %username% Mode: %mode%
2019	Warning	Access Approved	Change of Registry Value allowed Registry Key: %regkey%	Access Image Path: %path% Access User: %username% Mode: %mode%

Event ID	Level	Category	Event	Details
			Registry Value Name: %regvalue %	
2020	Warning	Access Approved	Change of Registry Key allowed Registry Key: %regkey%	Access Image Path: %path% Access User: %username% Mode: %mode%
2021	Warning	Access Approved	File access allowed: %path% An error occurred while checking the Trusted Hash List	Access Image Path: %path% Access User: %username% Mode: %mode%
2022	Warning	Access Approved	Process allowed by Fileless Attack Prevention: %path% %argument%	Access User: %username% Parent Process 1 Image Path: %path% Parent Process 2 Image Path: %path% Parent Process 3 Image Path: %path% Parent Process 4 Image Path: %path% Mode: Unlocked Reason: %reason %

Event ID	Level	Category	Event	Details
2503	Warning	Access Blocked	Change of File/ Folder blocked: %path%	Access Image Path: %path% Access User: %username% Mode: %mode%
2505	Warning	Access Blocked	Change of Registry Value blocked. Registry Key: %regkey% Registry Value Name: %regvalue %	Access Image Path: %path% Access User: %username% Mode: %mode%
2506	Warning	Access Blocked	Change of Registry Key blocked. Registry Key: %regkey%	Access Image Path: %path% Access User: %username% Mode: %mode%
2507	Information	Access Blocked	Action completed successfully: %path%	Action: %action% Source: %source %
2508	Warning	Access Blocked	Unable to take specified action: %path%	Action: %action% Source: %source %
2509	Warning	Access Blocked	File access blocked: %path%	Access Image Path: %path% Access User: %username% Mode: %mode% Reason: Not in Approved List

Event ID	Level	Category	Event	Details
				File Hash blocked: %hash%
2510	Warning	Access Blocked	File access blocked: %path%	Access Image Path: %path% Access User: %username% Mode: %mode% Reason: Hash does not match expected value File Hash blocked: %hash%
2511	Information	Access Blocked	Change of File/ Folder blocked: %path%	Access Image Path: %path% Access User: %username% Mode: %mode%
2512	Warning	Access Blocked	Change of Registry Value blocked. Registry Key: %regkey% Registry Value Name: %regvalue%	Access Image Path: %path% Access User: %username%

Event ID	Level	Category	Event	Details
				Note Enabling the Service Creation Prevention feature triggers Event ID 2512.
2513	Warning	Access Blocked	Process blocked by Fileless Attack Prevention: %path% %argument%	Access User: %username% Parent Process 1 Image Path: %path% Parent Process 2 Image Path: %path% Parent Process 3 Image Path: %path% Parent Process 4 Image Path: %path% Mode: locked Reason: %reason%
2514	Warning	Access Blocked	File access blocked: %BLOCKED_FILE_PATH%	Access Image Path: %PARENT_PROCESS_PATH% Access User: %USER_NAME%

Event ID	Level	Category	Event	Details
				Reason: Blocked file is in a folder that has the case sensitive attribute enabled.
3000	Warning	USB Malware Protection	Device access allowed: %path%	Access Image Path: %path% Access User: %username% Device Type: %type%
3001	Warning	USB Malware Protection	Device access blocked: %path%	Access Image Path: %path% Access User: %username% Device Type: %type%
4000	Warning	Process Protection Event	API Hooking/DLL Injection allowed: %path%	Threat Image Path: %path% Threat User: %username%
4001	Warning	Process Protection Event	API Hooking/DLL Injection blocked: %path%	Threat Image Path: %path% Threat User: %username%
4002	Warning	Process Protection Event	API Hooking allowed: %path%	Threat Image Path: %path% Threat User: %username%
4003	Warning	Process Protection Event	API Hooking blocked: %path%	Threat Image Path: %path%

Event ID	Level	Category	Event	Details
				Threat User: %username%
4004	Warning	Process Protection Event	DLL Injection allowed: %path%	Threat Image Path: %path% Threat User: %username%
4005	Warning	Process Protection Event	DLL Injection blocked: %path%	Threat Image Path: %path% Threat User: %username%
4500	Information	Changes in System	File/Folder created: %path%	Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4501	Information	Changes in System	File modified: %path%	Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4502	Information	Changes in System	File/Folder deleted: %path%	Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4503	Information	Changes in System	File/Folder renamed: %path %	Access Image Path: %path% Access Process Id: %pid%

Event ID	Level	Category	Event	Details
			New Path: %path %	Access User: %username%
4504	Information	Changes in System	Registry Value modified. Registry Key: %regkey% Registry Value Name: %regvalue % Registry Value Type: %regvaluetype%	Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4505	Information	Changes in System	Registry Value deleted. Registry Key: %regkey% Registry Value Name: %regvalue %	Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4506	Information	Changes in System	Registry Key created. Registry Key: %regkey%	Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4507	Information	Changes in System	Registry Key deleted. Registry Key: %regkey%	Access Image Path: %path% Access Process Id: %pid% Access User: %username%

Event ID	Level	Category	Event	Details
4508	Information	Changes in System	Registry Key renamed. Registry Key: %regkey% New Registry Key: %regkey%	Access Image Path: %path% Access Process Id: %pid% Access User: %username%
5000	Warning	Device Control	Storage device access allowed: %PATH%	Access Image path: %PATH% Access User: %USERNAME% Device Type: %TYPE% %DEVICEINFO%
5001	Warning	Device Control	Storage device access blocked: %PATH%	Access Image path: %PATH% Access User: %USERNAME% Device Type: %TYPE% %DEVICEINFO%
6000	Information	System	%Result%	Update Source: %SERVER% [Original Version] Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection

Event ID	Level	Category	Event	Details
				Pattern: %VERSION% Damage Cleanup Template: %VERSION% Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION% [Updated Version] Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION% Damage Cleanup Template: %VERSION% Damage Cleanup Engine

Event ID	Level	Category	Event	Details
				Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%
6001	Warning	System	Update failed: %ERROR_MSG% (%ERROR_CODE%)	Update Source: %SERVER% [Original Version] Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION% Damage Cleanup Template: %VERSION% Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION%

Event ID	Level	Category	Event	Details
				Damage Cleanup Engine: %VERSION% Scanner: %VERSION% [Updated Version] Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION% Damage Cleanup Template: %VERSION% Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%

Event ID	Level	Category	Event	Details
6002	Information	System	Malware scan started: %SCAN_TYPE%	Files to scan: %SCAN_FOLDER_TYPE% Scanned folders: %PATHS% Excluded paths: %PATHS% Excluded files: %PATHS% Excluded extensions: %PATHS% [Components] Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION% Damage Cleanup Template: %VERSION% Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION%

Event ID	Level	Category	Event	Details
				Damage Cleanup Engine: %VERSION% Scanner: %VERSION%
6003	Information	System	Malware scan completed: %SCAN_TYPE%. Number of infected files: %NUM%	Files to scan: %SCAN_FOLDER_TYPE% Scanned folders: %PATHS% Excluded paths: %PATHS% Excluded files: %PATHS% Excluded extensions: %PATHS% Start date/time: %DATE_TIME% End date/time: %DATE_TIME% Number of scanned files: %NUM% Number of infected files: %NUM% Number of cleaned files: %NUM% Number of files cleaned after reboot: %NUM% [Components]

Event ID	Level	Category	Event	Details
				Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION% Damage Cleanup Template: %VERSION% Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%
6004	Warning	System	Malware scan unsuccessful: %SCAN_TYPE% %ERROR%	Files to scan: %SCAN_FOLDER_TYPE% Scanned folders: %PATHS% Excluded paths: %PATHS%

Event ID	Level	Category	Event	Details
				Excluded files: %PATHS% Excluded extensions: %PATHS% Start date/time: %DATE_TIME% End date/time: %DATE_TIME% Number of scanned files: %NUM% Number of infected files: %NUM% Number of cleaned files: %NUM% Number of files cleaned after reboot: %NUM% [Components] Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION%

Event ID	Level	Category	Event	Details
				Damage Cleanup Template: %VERSION% Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%
6005	Information	System	Malware detected: %ACTION% File path: %PATH%	Reboot required: %NEED_REBOOT% [Scan Result] Threat type: %TYPE% Threat name: %NAME% [Components] Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection

Event ID	Level	Category	Event	Details
				Pattern: %VERSION% Damage Cleanup Template: %VERSION% Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%
6006	Warning	System	Malware detected. Unable to perform scan actions: %PATH%	First action: %1ST_ACTION% Second action: %2ND_ACTION% Threat type: %TYPE% Threat name: %NAME% [Components] Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION%

Event ID	Level	Category	Event	Details
				Program Inspection Pattern: %VERSION% Damage Cleanup Template: %VERSION% Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%
6007	Warning	Maintenance Mode	Malware detected in Maintenance Mode (file quarantine successful): %PATH%	Component versions: %VERSION% Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION%

Event ID	Level	Category	Event	Details
				Damage Cleanup Template: %VERSION% Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%
6008	Warning	Maintenance Mode	Malware detected in Maintenance Mode (file quarantine unsuccessful): %PATH%	Component versions: Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION% Damage Cleanup Template: %VERSION% Damage Cleanup Engine Configuration: %VERSION%

Event ID	Level	Category	Event	Details
				Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%
6009	Warning	Maintenance Mode	Malware detected in Maintenance Mode: %PATH%	Component versions: Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION% Damage Cleanup Template: %VERSION% Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION%

Event ID	Level	Category	Event	Details
				Scanner: %VERSION%
7000	Information	System	Group policy applied	Old Group Name: %GROUP NAME% Old Policy Version: %VERSION% New Group Name: %GROUP NAME% New Policy Version: %VERSION%
7001	Warning	System	Unable to synchronize group policy	Old Group Name: %GROUP NAME% Old Policy Version: %VERSION% New Group Name: %GROUP NAME% New Policy Version: %VERSION% Reason: %Reason %
8000	Information	System	Real Time Scan is enabled.	
8001	Warning	System	Real Time Scan is disabled.	
8010	Warning	System	Incoming files were scanned by antivirus. Action	File Path: %PATH %

Event ID	Level	Category	Event	Details
			was taken according to settings.	File Hash: %HASH% Threat Type: %TYPE% Threat Name: %NAME% Action Result: %INTEGER% Quarantine Path: %PATH%
8011	Warning	System	Application execution was blocked by antivirus.	Process Image Path: %PATH% File Hash: %HASH% Threat Type: %TYPE% Threat Name: %NAME%
8500	Information	System	Scheduled component update has been enabled. Next update will be on %TIME% (agent's local system time).	
8501	Information	System	Scheduled component update has been disabled.	
8601	Information	anomaly_detect	Operations Behavior Anomaly Detection (User	Mode: %Mode% Level: %Level%

Event ID	Level	Category	Event	Details
			Login) has been enabled.	Learning time: %LearningTime% day(s)
8602	Information	anomaly_detect	Operations Behavior Anomaly Detection (User Login) has been disabled.	
8603	Information	anomaly_detect	Operations Behavior Anomaly Detection (Application Behavior) has been enabled.	Mode: %Mode% Level: %Level% Learning time: %LearningTime% day(s)
8604	Information	anomaly_detect	Operations Behavior Anomaly Detection (Application Behavior) has been disabled.	
8610	warning	anomaly_detect	An abnormal user login has been detected by Operations Behavior Anomaly Detection.	Domain: %Domain% Account: %Account% Login Type: %LoginType% Source IP: %IP%
8611	warning	anomaly_detect	A user login failure has been detected by Operations Behavior	Domain: %Domain% Account: %Account%

Event ID	Level	Category	Event	Details
			Anomaly Detection.	Login Type: %LoginType% Source IP: %IP%
8612	warning	anomaly_detect	An unrecognized application has been detected by Operations Behavior Anomaly Detection.	PID: %PID% Program Path: %Path% Program Hash: %SHA256% Program Size: %Size% Certificate: %CertificateSigner% Vendor: %VendorName% Product: %Product%
8613	warning	anomaly_detect	Malicious application behavior has been detected by Operations Behavior Anomaly Detection	Program Path: %Path% Program Hash: %SHA256% Program Size: %Size% Certificate: %CertificateSigner% Vendor: %VendorName% Product: %Product%
8614	warning	anomaly_detect	Suspicious application	Program Path: %Path%

Event ID	Level	Category	Event	Details
			behavior has been detected by Operations Behavior Anomaly Detection.	Program Hash: %SHA256% Program Size: %Size% Certificate: %CertificateSigner% Vendor: %VendorName% Product: %Product%
8620	Information	anomaly_detect	A user login account has been added to the Situational Awareness baseline.	Domain: %Domain% Account: %Account% Login Type: %LoginType% Source IP: %IP%
8621	Information	anomaly_detect	A user login account has been excluded from the Situational Awareness baseline.	Domain: %Domain% Account: %Account% Login Type: %LoginType% Source IP: %IP%
8622	Information	anomaly_detect	An application has been added to the Situational Awareness baseline.	Application Path: %Path%
8623	Information	anomaly_detect	An application has been	Application Path: %Path%

Event ID	Level	Category	Event	Details
			excluded from the Situational Awareness baseline.	

Agent Error Code Descriptions for StellarProtect (Legacy Mode)

This list describes the various error codes used in StellarProtect (Legacy Mode) agent.

Code	Description
0x00040200	Operation successful.
0x80040201	Operation unsuccessful.
0x80040202	Operation unsuccessful.
0x00040202	Operation partially successful.
0x00040203	Requested function not installed.
0x80040203	Requested function not supported.
0x80040204	Invalid argument.
0x80040205	Invalid status.
0x80040206	Out of memory.
0x80040207	Busy. Request ignored.
0x00040208	Retry. (Usually the result of a task taking too long)
0x80040208	System Reserved. (Not used)
0x80040209	The file path is too long.
0x0004020a	System Reserved. (Not used)
0x8004020b	System Reserved. (Not used)

Code	Description
0x0004020c	System Reserved. (Not used)
0x0004020d	System Reserved. (Not used)
0x8004020d	System Reserved. (Not used)
0x0004020e	Reboot required.
0x8004020e	Reboot required for unexpected reason.
0x0004020f	Allowed to perform task.
0x8004020f	Permission denied.
0x00040210	System Reserved. (Not used)
0x80040210	Invalid or unexpected service mode.
0x00040211	System Reserved. (Not used)
0x80040211	Requested task not permitted in current status. Check license.
0x00040212	System Reserved. (Not used)
0x00040213	System Reserved. (Not used)
0x80040213	Passwords do not match.
0x00040214	System Reserved. (Not used)
0x80040214	System Reserved. (Not used)
0x00040215	Not found.
0x80040215	"Expected, but not found."
0x80040216	Authentication is locked.
0x80040217	Invalid password length.
0x80040218	Invalid characters in password.
0x00040219	Duplicate password. Administrator and Restricted User passwords cannot match.

Code	Description
0x80040220	System Reserved. (Not used)
0x80040221	System Reserved. (Not used)
0x80040222	System Reserved. (Not used)
0x80040223	File not found (as expected, and not an error).
0x80040224	System Reserved. (Not used)
0x80040225	System Reserved. (Not used)
0x80040240	Library not found.
0x80040241	Invalid library status or unexpected error in library function.
0x80040260	System Reserved. (Not used)
0x80040261	System Reserved. (Not used)
0x80040262	System Reserved. (Not used)
0x80040263	System Reserved. (Not used)
0x80040264	System Reserved. (Not used)
0x00040265	System Reserved. (Not used)
0x80040265	System Reserved. (Not used)
0x80040270	System Reserved. (Not used)
0x80040271	System Reserved. (Not used)
0x80040272	System Reserved. (Not used)
0x80040273	System Reserved. (Not used)
0x80040274	System Reserved. (Not used)
0x80040275	System Reserved. (Not used)
0x80040280	Invalid Activation Code.

Code	Description
0x80040281	Incorrect Activation Code format.

Chapter 7

Troubleshooting Resources

This chapter provides available troubleshooting resources for the Agent.

Topics in this chapter include

Frequently Asked Questions (FAQ)

What if the endpoint becomes infected by a threat?

Do one of the following to remove the threat on the endpoint:

- Start a manual scan on the endpoint.
  - To initiate the manual scan on the console GUI, see *StellarProtect Operations on page 3-21* or *StellarProtect (Legacy Mode) Operations on page 3-52*.
  - To initiate the manual scan via the console CLI,, see *Manual Scan Commands* section in *OPCmd Program Commands on page 4-4* for StellarProtect or *SLCmd Program Commands on page 4-19* for StellarProtect (Legacy Mode).
- Access the StellarOne web management console and send a scan command to start malware scanning on the endpoint.

Where can I get more help with TXOne StellarProtect/StellarProtect (Legacy Mode)?

To get the most up-to-date information and support, see *Technical Support on page 8-1*.

Troubleshooting StellarProtect (Legacy Mode)

The TXOne StellarProtect (Legacy Mode) Diagnostic Toolkit offers administrators the ability to perform a number of diagnostic functions, including:

- Create, collect, and delete debugging logs
- Enable or disable Self Protection

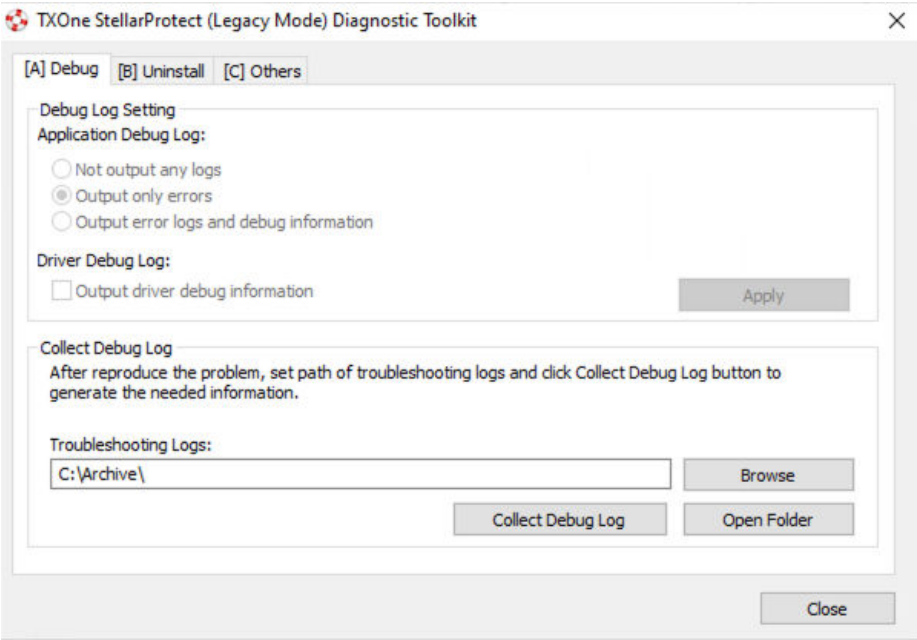

FIGURE 7-1. The TXOne StellarProtect (Legacy Mode) Diagnostic Toolkit Debug Tab A [Debug]

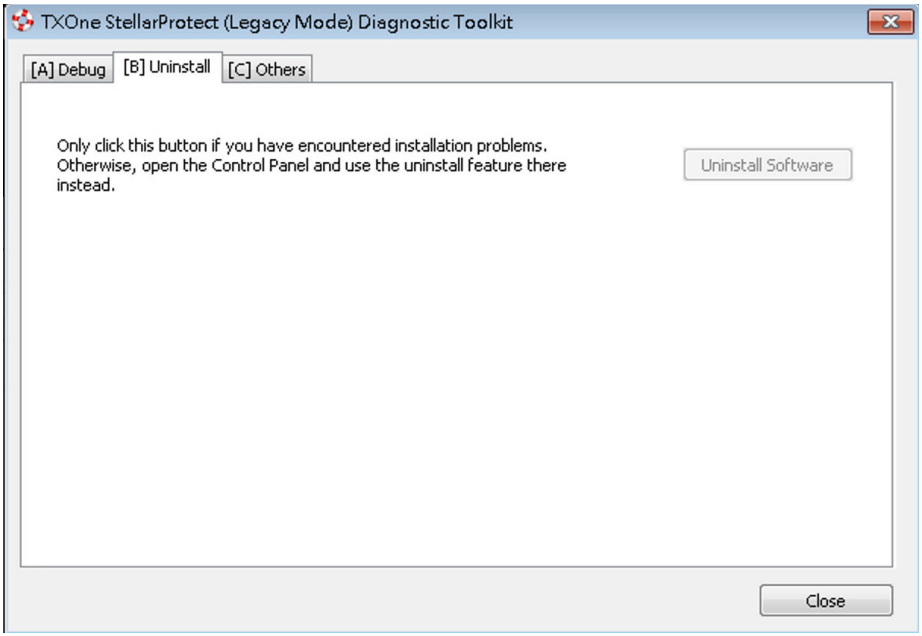

FIGURE 7-2. The TXOne StellarProtect (Legacy Mode) Diagnostic Toolkit Debug Tab B [Uninstall]

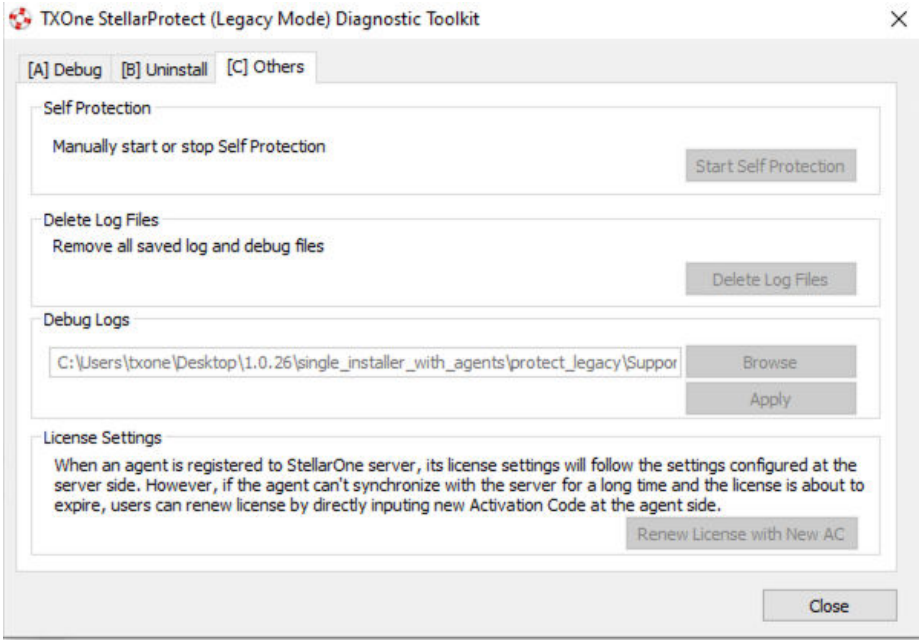

FIGURE 7-3. The TXOne StellarProtect (Legacy Mode) Diagnostic Toolkit Debug Tab C [Others]

Using the Diagnostic Toolkit

If TXOne StellarProtect (Legacy Mode) experiences problems, generate a complete set of application and driver diagnostic logs for analysis, or send them to to TXOne Networks Technical Support. Both the TXOne Networks Administrator and User accounts can collect the logs.

Procedure

1. Open the Diagnostic Toolkit and enable full logging:
   a. Open the TXOne StellarProtect (Legacy Mode) installation folder and run `WKSupportTool.exe`.

Note

The default installation location is `c:\Program Files\TXOne \StellarProtect (Legacy Mode)\`.

b. Provide the TXOne Networks administrator or User password and click **OK**.

c. On the **[A] Debug** tab, select **Output error logs and debug information** and **Output driver debug information**, and click **Apply**.

2. Reproduce the problem.

3. Collect the diagnostic logs:

a. Reopen the Diagnostic Toolkit.

b. On the **[A] Debug** tab, click **Browse** to choose the location where TXOne StellarProtect (Legacy Mode) saves the logs.

Note

The default location for saved logs is: `c:\Program Files\TXOne \StellarProtect (Legacy Mode)\Log\Archive\`.

c. Click **OK** when finished.

d. Click **Collect Debug Log**.

e. Once the Debug Logs have been collected, click **Open Folder** to access the zipped log files for review, or to send them to TXOne Networks Technical Support.

Chapter 8

Technical Support

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

Learn about the following topics:

Troubleshooting Resources

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

Using the Support Portal

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

Procedure

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

   Tip

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

   https://success.trendmicro.com/smb-new-request

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

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro and TXOne combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to https://www.trendmicro.com/vinfo/us/threat-encyclopedia/#malware and https://www.encyclopedia.txone.com/ to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports

Contacting Trend Micro and TXOne

In the United States, Trend Micro and TXOne representatives are available by below contact information:

TABLE 8-1. Trend Micro Contact Information

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

TABLE 8-2. TXOne Contact Information

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

- Worldwide support offices:

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

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

- Trend Micro product documentation:

  https://docs.trendmicro.com

Speeding Up the Support Call

To improve problem resolution, have the following information available:

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

Sending Suspicious Content to Trend Micro

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

Email Reputation Services

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

https://ers.trendmicro.com/

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

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

File Reputation Services

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

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

Record the case number for tracking purposes.

Web Reputation Services

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

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

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

Other Resources

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

Download Center

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

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

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

Appendix A

StellarProtect (Legacy Mode) Limitations by Operating Systems

StellarProtect (Legacy Mode) installed on the following operating systems has the limitations as described below.

Operating Systems	Limitations

Windows 10	• 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.
	• To improve performance, disable the following Windows 10 components:
	  • Windows Defender Antivirus. This may be disabled via group policy.
	  • Windows 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.

Windows 10 Fall Creators Update	OndDrive integration is not supported. Ensure that OneDrive integration is disabled before installing StellarProtect (Legacy Mode).

Operating Systems	Limitations

Windows 10 April 2018 Update (Redstone 4) and later versions	• OndDrive integration is not supported. Ensure that OneDrive integration is disabled before installing StellarProtect (Legacy Mode).
	• See 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 StellarProtect (Legacy Mode) from performing certain actions (e.g., prescan, custom actions) on that folder. Folders that do not have the attribute enabled are not affected.
	  • StellarProtect (Legacy Mode) blocks all processes started from folders where the *case sensitive* attribute is enabled. Additionally, StellarProtect (Legacy Mode) is unable to provide any information for the blocked processes, except for file path.
	  • The StellarProtect (Legacy Mode) 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 XP Embedded SP1	The custom action of “quarantine” for Application Lockdown or Real-Time Scan is not supported
• Windows 2000 SP4 (without update rollup) • Windows XP SP1 • Windows XP Embedded • Windows 2000 Server SP4	The following functions are not supported: • DLL/Driver Lockdown • Script Lockdown • Integrity Monitoring • USB Malware Protection • Storage Device Blocking • Maintenance Mode • Predefined Trusted Updater

Index

T

U

TXONE NETWORKS INCORPORATED

222 West Las Colinas Boulevard, Suite 1650
Irving, TX 75039 U.S.A
Email: support@txone.com
www.txone.com

Item Code: APEM39735/230619