txOne networks | Keep the Operation Running

1.4 TXOne StellarProtect (Legacy Mode)

Administrator's Guide

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

Windows

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

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

Document Part No.: APEM219660/221221

Release Date: January 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, StellarProtect, and StellarProtect (Legacy Mode) 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: Working with the Agent Configuration File

Chapter 5: Frequently Asked Questions (FAQ)

Chapter 6: Troubleshooting StellarProtect (Legacy Mode)

Chapter 7: Technical Support

Chapter 8: Log Descriptions for StellarProtect (Legacy Mode)

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 (Legacy Mode) and guides administrators through installation and deployment.

Topics in this chapter include:

About the Documentation

TXOne Networks StellarProtect (Legacy Mode) 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 (Legacy Mode).
Administrator's Guide	A PDF document that discusses StellarProtect (Legacy Mode) 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 (Legacy Mode) documentation is intended for administrators responsible for StellarProtect (Legacy Mode) 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
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 (Legacy Mode) documentation:

Terminology	Description
server	The StellarOne console server program
agents	The host running the StellarProtect (Legacy Mode) program
managed agents managed endpoints	The hosts running the StellarProtect (Legacy Mode) program that are known to the StellarOne server program
target endpoints	The hosts where the StellarProtect (Legacy Mode) managed agents will be installed
Administrator (or StellarProtect (Legacy Mode) administrator)	The person managing the StellarProtect (Legacy Mode) agent
StellarProtect (Legacy Mode) console	The user interface for configuring and managing StellarProtect (Legacy Mode) settings
StellarOne (management) console	The user interface for configuring and managing the StellarProtect (Legacy Mode) agents managed by StellarOne
CLI	Command Line Interface
license activation	Includes the type of StellarProtect (Legacy Mode) 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 (Legacy Mode) 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 (Legacy Mode)`

Chapter 1

Introduction

This section introduces TXOne StellarProtect (Legacy Mode), delivers a simple, no-maintenancesolution to lockdown and protect fixed-function computers, helping protect businesses against security threats and increase productivity.

Topics in this chapter include:

About TXOne Stellar

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

- StellarOne™ , the centralized management console designed to streamline administration of both StellarProtect for modernized systems and StellarProtect (Legacy Mode) for legacy systems.
- StellarProtect ™, the unified agent with industrial-grade next-generation antivirus and application lockdown endpoint security deployment for modernized OT/ICS endpoints.
- StellarProtect (Legacy Model) ™, for trust-list based application lockdown of legacy and fixed-use OT/ICS endpoints with anti-malware or on-demand AV scan.

Together, TXOne Stellar allows protection for modernized and legacy systems running side-by-side to be coordinated and maintained from the same management console, helping protect businesses against security threats and increase productivity.

Key Features and Benefits

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

The StellarProtect (Legacy Mode) provides following features and benefits.

TABLE 1-1. Features and Benefits

FEATURE	BENEFIT
Application Lockdown	By preventing programs, DLL files, drivers, and scripts not specifically on the Approved List of applications from running (also known as application trust listing), StellarProtect (Legacy Mode) provides both improved productivity and system integrity by blocking malicious software and preventing unintended use. StellarProtect (Legacy Mode) Write Protection blocks modification and deletion of files, folders, and registry entries.
Exploit Prevention	Known targeted threats like Downad and Stuxnet, as well as new and unknown threats, are a significant risk to ICS and kiosk computers. Systems without the latest operating system updates are especially vulnerable to targeted attacks. For advanced threat prevention, StellarProtect (Legacy Mode) includes intrusion prevention, execution prevention, application lockdown, and devicecontrolto stop threats from spreading to the endpoint or executing.
Approved List Management	When software needs to be installed or updated, you can use one of thefollowing methods to make changes to the endpoint and automatically add new or modified files to the Approved List, all without having to unlock TXOne StellarProtect (Legacy Mode): • Maintenance Mode • Trusted Updater • Predefined Trusted Updater List • Command Line Interface (CLI) • Trusted hash • Trusted certificate
Small Footprint	Compared to other endpoint security solutions that rely on large pattern files that require constant updates, application lockdown uses less memory and disk space, without the need to download updates.

Feature	Benefit
Role Based Administration	TXOne StellarProtect (Legacy Mode) provides a separate administrator and Restricted User account, providing full control during installation and setup, as well as simplified monitoring and maintenance after deployment.
Graphical and Command Line Interfaces	Anyone who needs to check the software can use the console, while systemadministrators can take advantage of the command line interface (CLI) to access all of the features and functions available.
Self Protection	Self Protection provides ways for TXOne StellarProtect (Legacy Mode) to defend its processes and resources, required to function properly, from being disabledby programs or actual users. Self Protection blocks all attempts to terminate the following services: • Trend Micro Unauthorized Change Prevention Service (`TMBMSRV.exe`) • Trend Micro Personal Firewall (`TmPfw.exe`) • TXOne StellarProtect (Legacy Mode) Service (`WkSrv.exe`)

What's New

TXOne StellarProtect (Legacy Mode) 1.4 provides following new features and enhancements.

Table 1-2. What's New in TXOne StellarProtect (Legacy Mode) 1.4

Feature	Benefit
Anti-Malware Scanning (Real-Time Scan)	With this new feature, the StellarProtect (Legacy Mode) can persistently scan new and changed files, along with system memory, to provide security assessment for maximum protection against malware.
Self-management status	The self-management status displayed on the agent's console GUI enables users to know whether the agent is following StellarOne's policy settings.

Feature	Benefit
Single installer package	A single installer package for the Agent – StellarProtect and StellarProtect (Legacy Mode) is available now. After being invoked, the single installer can identify the version of Windows installed on the endpoint and launch the suitable installer for the endpoint to install.
Supporting license key/file	Supports license key and license file for product activation

System Requirements

This section introduces the system requirements for StellarProtect (Legacy Mode), including hardware and OS requirements.

Software and Hardware Requirements

TXOne StellarProtect and 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 and StellarProtect (Legacy Mode)

HARDWARE	DESCRIPTION

Available free disk space	StellarProtect: 400MB
	
	StellarProtect (Legacy Mode): 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

By default, 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 (Legacy Mode)'s use.

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

Important

- 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 endpointsolutions except Windows Defender Antivirus
- Ensure that the following root certification authority (CA) certificates are installed with intermediate CAs, which are found in `WKSrv.exe`. These root CAs should be installed on the 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
  - DigiCert Trusted Root G4

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

Note

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

Tip

For the x64 platform, removing x86 folders in the installation package can reduce the size of the installer and vice versa.

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) Anniversary Update, Creators Update, Fall Creators Update, April 2018 Update, November 2018 Update, May 2019 Update, November 2019 Update, May 2020 Update, October 2020 Update, May 2021 Update, November 2021 Update, 2022 Update
- Windows 11 (NoSP) [Pro/Enterprise] (64bit) 2022 Update

Note

- Unlock the endpoint before updating your Windows 10 operating system to the Anniversary Update, Creators Update, Fall Creators Update, April 2018 Update, October 2018 Update, or later versions.
- OndDrive integration in Windows 10 Fall Creators Update, Spring Creators Update, or later versions is not supported. Ensure that OneDrive integration is disabled before installing StellarProtect (Legacy Mode).
- 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.
- In Windows 10 April 2018 Update (Redstone 4) and later, StellarProtect (Legacy Mode) has the following limitations when working with folders where the case sensitive attribute has been enabled:
  - Enable 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 fromfolders 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/SP2) (32bit)

Note

StellarProtect (Legacy Mode) does not support a custom action of "quarantine" on Windows XP Embedded SP1.

- Windows Embedded Standard 2009 (NoSP) (32bit)
- Windows Embedded POSReady 2009 (32bit)
- Windows Vista for Embedded Systems (NoSP/SP1/SP2) (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)
- Widows Embedded POSReady (32bit)

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)
- Windows Server 2003 for Embedded Systems (SP1/SP2) (32bit)
- Windows Server 2003 R2 for Embedded Systems (NoSP/SP2) (32bit)
- Windows Server 2008 for Embedded Systems (SP1/SP2) (32/64bit)
- Windows Server 2008 R2 for Embedded Systems (NoSP/SP1) (64bit)
- Windows Server 2012 for Embedded Systems (NoSP) (64bit)
- Windows Server 2012 R2 for Embedded Systems (NoSP) (64bit)

Note

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

To support these features, install Filter Manager:

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

Preparing the Agent for Upgrade to a Later Version

This version of StellarProtect (Legacy Mode) supports upgrade from the following version:

- StellarEnforce 1.0

- StellarEnforce 1.1
- StellarEnforce 1.2
- StellarEnforce 1.2 Patch 1
- StellarProtect (Legacy Mode) 1.3

Note

The StellarEnforce was renamed StellarProtect (Legacy Mode) upon the release of version 1.3.

The latest updates can be downloaded from the StellarProtect (Legacy Mode) Software Download Center.

Note

Before upgrading, close the wksupporttool UI and/or StellarProtect (Legacy Mode) agent console.

WARNING!

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

TABLE 1-4. Fresh Installation of the StellarProtect (Legacy Mode) Agent

INSTALLATION METHOD	INSTALLED AGENT VERSION	REQUIRED ACTION	SETTINGS RETAINED
Local installation using Windows installer	StellarEnforce 1.0 / 1.1 / 1.2 / 1.2 Patch 1 / StellarProtect (Legacy Mode) 1.3	It's necessary to manually add the install file (`SL_Install.exe`) into the trusted HASH list and enable PTU function before using it.	No settings retained

Installation Method	Installed Agent Version	Required Action	Settings Retained
Local installation using command line interface installer	StellarEnforce 1.0 / 1.1 / 1.2 / 1.2 Patch 1 / StellarProtect (Legacy Mode) 1.3	It's necessary to manually add the install file (`SL_Install.exe`) into the trusted HASH list before using it.	No settings retained

Table 1-5. Post-Installation Agent Upgrade(Legacy OS - Supports SHA1)

Installation Method	Installed Agent Version	Required Action	Settings Retained
For example, deploy patching by running `stellar_patch.exe`. To do a silent install instead, open the command prompt as an administrator and enter the following command:`>stellar_patch.exe -s -a -s/g`	StellarEnforce 1.0 / 1.1 / 1.2 / 1.2 Patch 1 / StellarProtect (Legacy Mode) 1.3	No preparation needed	Compatible settings retained
Remote Installation	StellarEnforce 1.1 / 1.2 / 1.2 Patch 1 / StellarProtect (Legacy Mode) 1.3 **Note** StellarEnforce 1.0 supports only local installation.	No preparation needed	Compatible settings retained

TABLE 1-6. Post-Installation Agent Upgrade (Modern OS – Supports SHA2)

INSTALLATION METHOD	INSTALLED AGENT VERSION	REQUIRED ACTION	SETTINGS RETAINED
For example, deploy patching by running `stellar_patch.exe`. To do a silent install instead, open the command prompt as an administrator and enter the following command:`>stellar_patch.exe -s -a -s/g`	StellarEnforce 1.2 Patch 1 / StellarProtect (Legacy Mode) 1.3	No preparation needed	Compatible settings retained

Installation Method	Installed Agent Version	Required Action	Settings Retained
	Note For agents with versions below 1.2 Patch 1, local upgrade for standalone StellarProtect (Legacy Mode) agents is not supported. Please implement either workaround listed below: • Remotely upgrade StellarProtect (Legacy Mode) agents from StellarOne web console • Add the patch file hash as trusted hash, enable PTU function and then perform local upgrade.		

Installation Method	Installed Agent Version	Required Action	Settings Retained
Remote Installation	StellarEnforce 1.0 / 1.1 / 1.2 / 1.2 Patch 1 / StellarProtect (Legacy Mode) 1.3	No preparation needed	Compatible settings retained

Agent Use Overview

TXOne StellarProtect (Legacy Mode) is a trust list-based solution that locks down computers, preventing all applications not on the Approved List from running. StellarProtect (Legacy Mode) can be configured and maintained using the graphical user interface (GUI) agent console or the command line interface (CLI).

System updates can be applied without turning off ApplicationLockdown at the endpoint through Maintenance Mode, trust hash, trust certification, predefined trusted updater list or by using the Trusted Updater.

Consider this typical use case scenario:

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

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

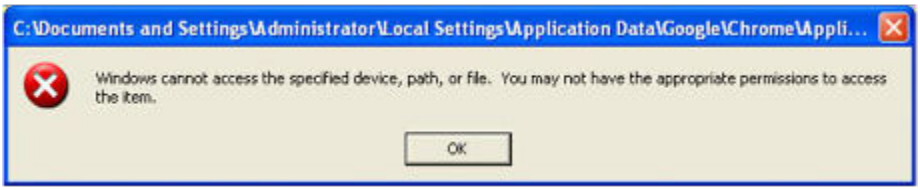

FIGURE 1-1. StellarProtect (Legacy Mode) Blocking Message

Chapter 2

Using the StellarProtect (Legacy Mode) Agent Console

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

Topics in this chapter include:

Setting Up the Approved List

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

Procedure

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

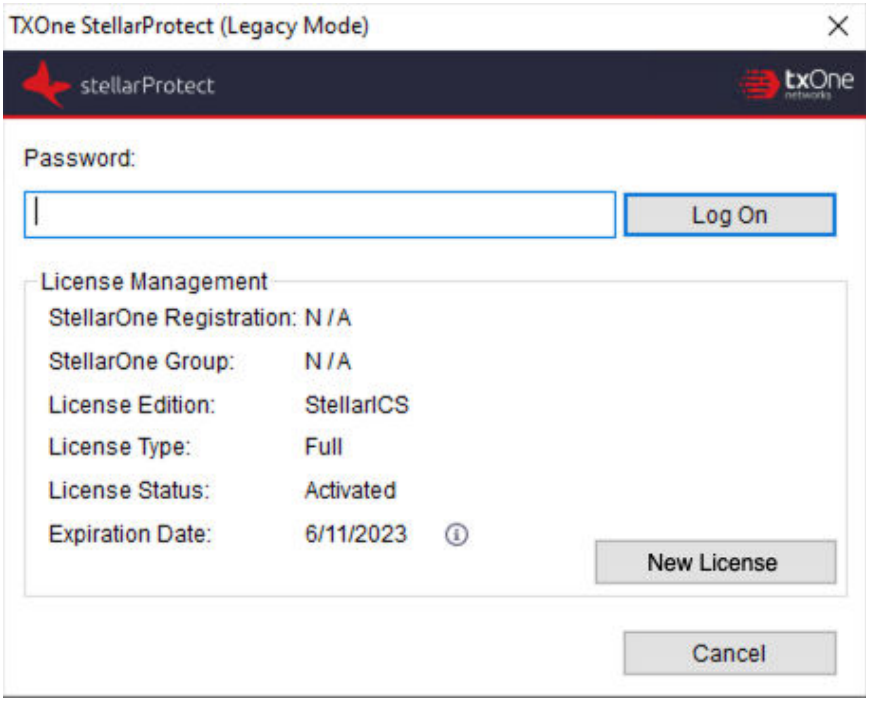

FIGURE 2-1. StellarProtect (Legacy Mode) Log On Screen

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

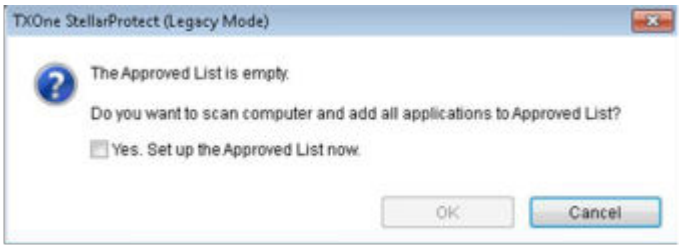

FIGURE 2-2. The Approved List is Empty

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.

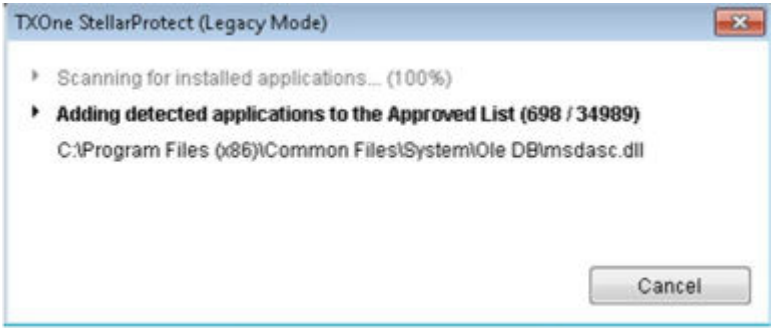

FIGURE 2-3. Scanning for Creating Approved List

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

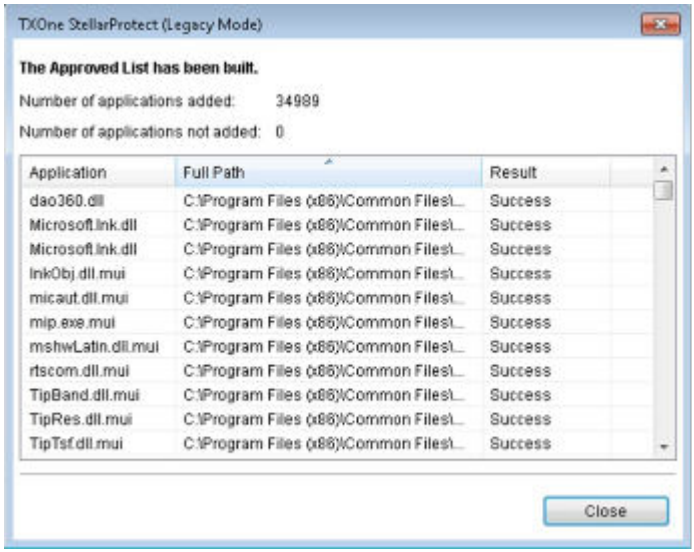

FIGURE 2-4. Approved List Created

Note

- When TXOne StellarProtect (Legacy Mode) Application Lockdown is on, 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**.

About the StellarProtect (Legacy Mode) Agent Console

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

Overview

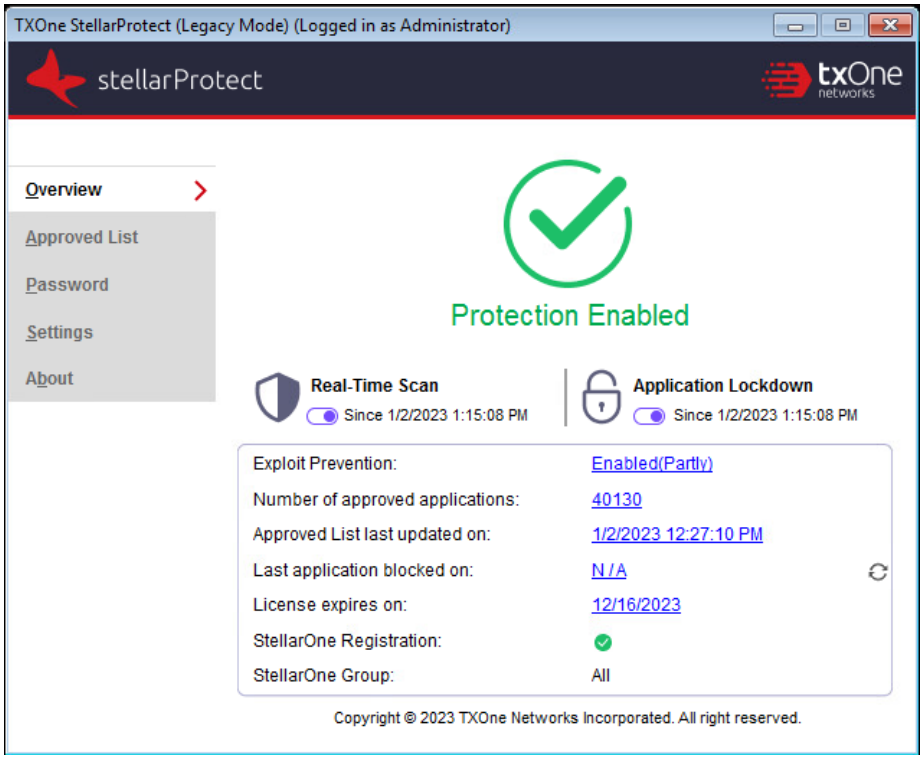

FIGURE 2-5. Overview of theStellarProtect (Legacy Mode) Agent Console - Protection Enabled

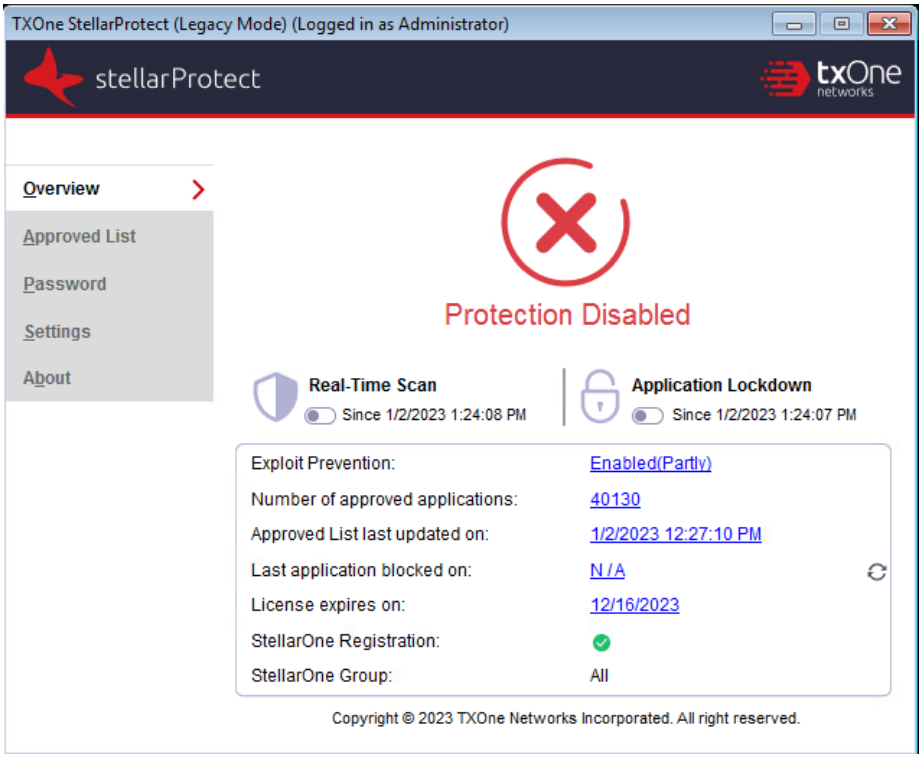

FIGURE 2-6. Overview of theStellarProtect (Legacy Mode) Agent Console - Protection Disabled

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

TABLE 2-1. 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 let users manage the list

ITEM	FUNCTION	DESCRIPTION
	Password	Enables administrators to change the StellarProtect (Legacy Mode) Administrator or Restricted User passwords **Note** Only users logged in as the administrator can change the passwords.
	Settings	Enables or disables vulnerability protection settings and exports or imports the system configuration
	About	Displays the product 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 the endpoint is 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. **Note** StellarProtect (Legacy Mode) installed on Windows 2000 SP4 (without update rollup) or Windows XP SP1 supports real-time scan only when files are executed; it does not support real-time scan when files are newly added or changed.

Item	Function	Description
		Tip The date and time that the Real-Time Scan was last turned on or off are shown next to the toggle switch.
	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 is 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
Approved List status	Number of approved applications:	Click the corresponding number to open the **Approved List** and view details.
	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.

Approved List

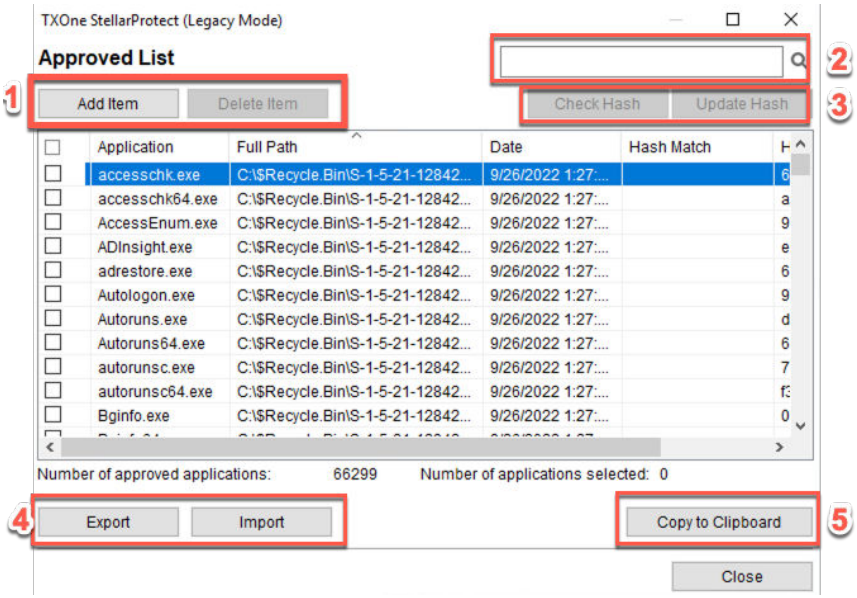

FIGURE 2-7. The Approved List Window

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

TABLE 2-2. 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

#	ITEM	DESCRIPTION
3	**Check Hash / Update Hash**	Checks or updates the hash values for applications in the Approved List For more details, refer to: • *About Hashes on page 2-19* • *Checking or Updating Hashes on page 2-20*
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

Password

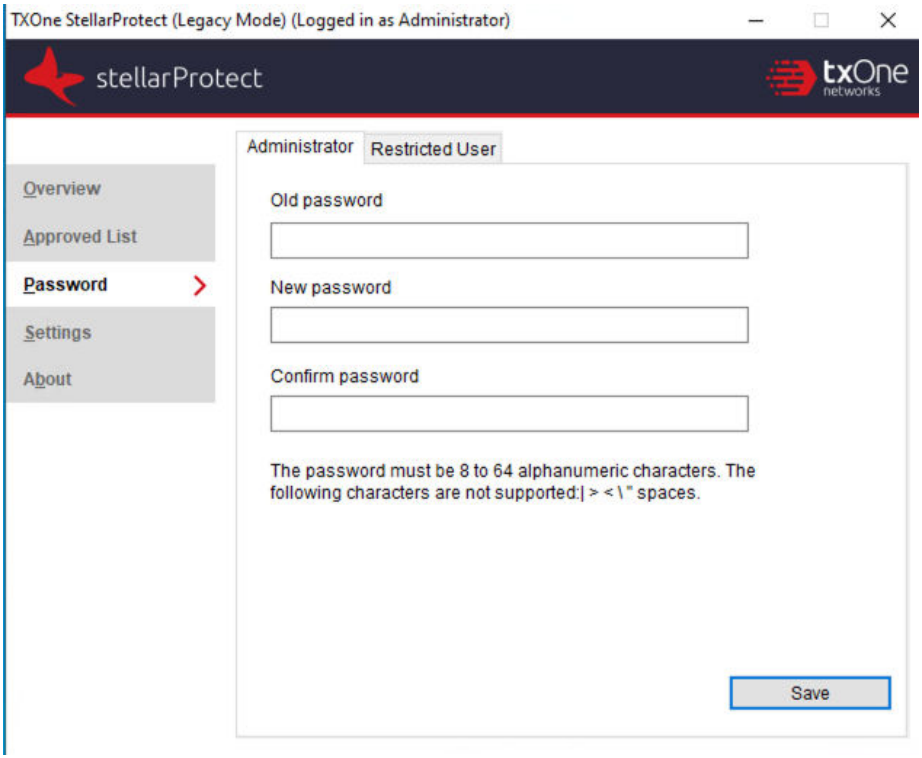

FIGURE 2-8. Password Setting

The following table describes the account types available on the **Password** window.

StellarProtect (Legacy Mode) provides role-based administration, allowing administrators to grant users access to certain features on the main console. Through the configuration file, StellarProtect (Legacy Mode) administrators can specify the features available to **Restricted User** accounts.

TABLE 2-3. StellarProtect (Legacy Mode) Account Types

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

To enable **Restricted User** accounts, refer to *Configuring Passwords on page 2-26*. To sign in with a specific account, specify the password for that account.

About Feature Settings

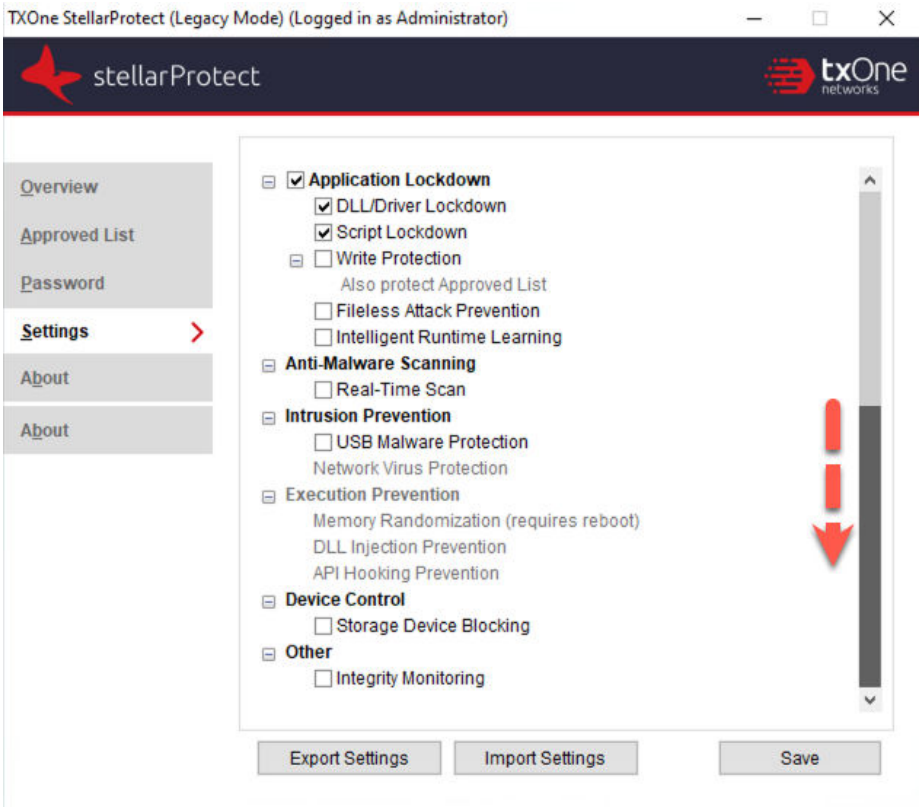

FIGURE 2-9. StellarProtect (Legacy Mode) Settings Screen

StellarProtect (Legacy Mode) offers the following protection features.

TABLE 2-4. 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 2-5. Anti-Malware Scanning

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 Malware 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. **Note** StellarProtect (Legacy Mode) installed on Windows 2000 SP4 (without update rollup) or Windows XP SP1 supports real-time scan only when files are executed; it does not support real-time scan when files are newly added or changed.

TABLE 2-6. Intrusion Prevention

SETTING	DESCRIPTION
USB Malware Protection	USB Malware Protection prevents automated threats on USB or remote drives from infecting the endpoint. Just viewing the contents of the drive may be enough to pass along an infection. Enable this feature to prevent files on USB devices from automatically infecting the endpoint.
Network Virus Protection	Network Virus Protection scans incoming and outgoing network traffic, blocking threats from infected computers or other devices on the network. Enable this feature to prevent threats on the network from infecting the endpoint.

TABLE 2-7. 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.
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 2-8. 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** > **ControlPanel** > **Administrative Tools** and access Event Viewer.

To enable or disable the feature settings, refer to *Enabling or Disabling Feature Settings on page 2-28* for more details.

About

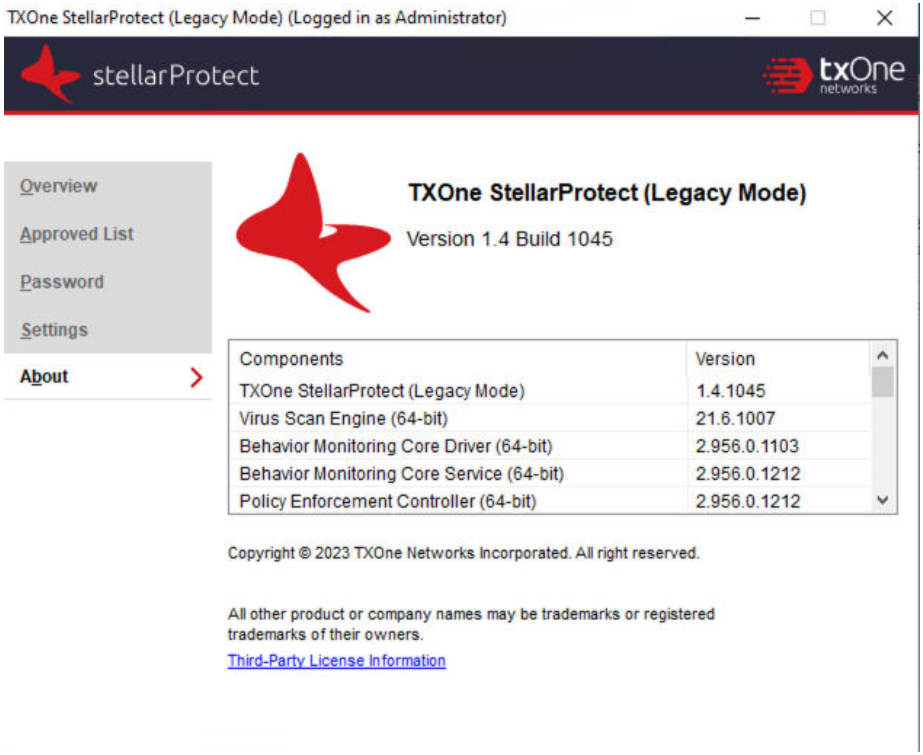

FIGURE 2-10. The About Page

This page displays StellarProtect (Legacy Mode) product information, version and build number, as well as third-party license information.

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**.

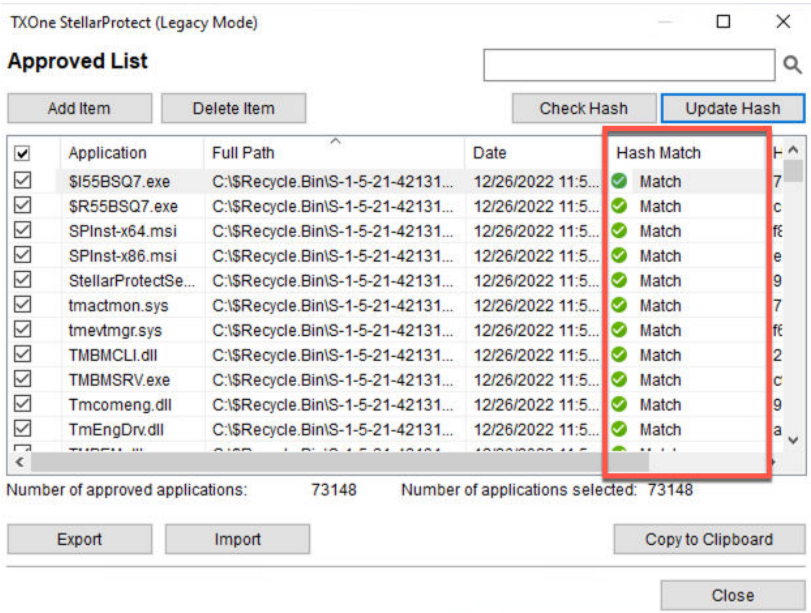

FIGURE 2-11. Hash Values Matched

Important

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

Configuring the Approved List

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

TABLE 2-9. 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.
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**.

Account Types

TXOne Networks StellarProtect (Legacy Mode) provides role-based administration, allowing administrators to grant users access to certain features on the main console. Through the configuration file, StellarProtect (Legacy Mode) administrators can specify the features available to Restricted User accounts.

TABLE 2-10. StellarProtect (Legacy Mode) Accounts

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

To enable Restricted User accounts, refer to *Configuring Passwords on page 2-26*. To sign in with a specific account, specify the password for that account.

Configuring Passwords

While the StellarProtect (Legacy Mode) **Administrator** and **Restricted User** passwords can be changed from the console, only the administrator can

change passwords. To log on to the console as the administrator account, provide the administrator password when launching the console.

Important

The StellarProtect (Legacy Mode) administrator and Restricted 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 Restricted User password:
     a. Click the tab to switch to the **Restricted User** page
     b. Select the **Enable Restricted User** check box.
     c. Specify and confirm the password, and click **Save**.
   - To change an existing Restricted User password:
     a. Specify and confirm the new password, and click **Save**.

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.
- User must check **Install Network Virus Protection** during the initial installation; otherwise, the Network Virus Protection feature cannot be selected. If user wants to enable the Network Virus Protection, he must uninstall the TXOne StellarProtect (Legacy Mode), then reinstall it and make sure the **Install Network Virus Protection** is checked during the installation. Please refer to the Installation Guide for more details.

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 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**.

Chapter 3

Using the Agent Command Line Interface (CLI)

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

Topics in this chapter 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

Function	SLCmd Program at the Command Line Interface (CLI)	Console
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
Start/Stop Trusted Updater	Yes	Yes
Trusted Hash List	Yes	No
Start/Stop the service	Yes	No
Uninstall	No	No

Function	SLCmd Program at the Command Line Interface (CLI)	Console
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 4-2* for information about modifying the system configuration.

SLCmd Program Commands

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 3-1. 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

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

TABLE 3-2. 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`

Command	Parameter	Description

`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 3-3. 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 3-4. 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 3-5. 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
networkvirusprotection	net	Manage Network Virus Protection
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 3-6. 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 For example, type:

COMMAND	PARAMETER	DESCRIPTION
		`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: `SLCmd.exe -p <admin_password> set`

Command	Parameter	Description
		`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: `SLCmd.exe -p <admin_password> set integritymonitoring`

Command	Parameter	Description
		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 For example, type: `SLCmd.exe -p <admin_password> set`

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

Command	Parameter	Description
		`networkvirusprotection 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: `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`

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

Command	Parameter	Description
		`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".
	`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`

Command	Parameter	Description
`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: `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-`

Command	Parameter	Description
		`includesapprovedlist disable`

Restricted User Account Commands

Configure the Restricted 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 3-7. Abbreviations and Uses

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

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

TABLE 3-8. Restricted User Account Commands

COMMAND	PARAMETER	DESCRIPTION
`set user`		Display the Restricted User account status For example, type: `SLCmd.exe -p <admin_password> set user` **Note** The default status is "disable".
	`enable`	Enable the Restricted User account For example, type: `SLCmd.exe -p <admin_password> set user enable`
	`disable`	Disable the Restricted User account For example, type: `SLCmd.exe -p <admin_password> set user disable`

Command	Parameter	Description
`set userpassword`		Prompt the currently logged on administrator to specify a new Restricted User account password For example, type: `SLCmd.exe -p <admin_password> set userpassword`
	`ignore`	Change the Restricted 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 3-9. Abbreviations and Uses

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

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

TABLE 3-10. 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 3-11. 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 3-12. 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 3-13. 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 3-14. 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`
`add exceptionpath`	`-e <file_path> -tfile`	Add an exception for the specified file

COMMAND	PARAMETER	DESCRIPTION
		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 -e \\computer\`

Command	Parameter	Description
		`\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 3-15. 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 3-16. Write Protection List "File" Commands

COMMAND	PARAMETER	VALUE	DESCRIPTION
show	writeprotection		Display the entire Write Protection List

Command	Parameter	Value	Description
	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: `SLCmd.exe -p <admin_password> add`

Command	Parameter	Value	Description
			`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` **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`.

Command	Parameter	Value	Description
		`-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` **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 writeprotection-file-exception -t`

Command	Parameter	Value	Description
			`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` **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:

Command	Parameter	Value	Description
			`SLCmd.exe -p <admin_password> remove writeprotection-file-exception -p notepad.exe` **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 3-17. 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
`add`	`writeprotection-regvalue`	`<path_of_registry_key> <registry_value>`	Add the specified registry value and its related registry key to

Command	Parameter	Value	Description
			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 **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.

Command	Parameter	Value	Description
		`-t <path_of_registry_key> <registry_value>`	Add the specified registry value and its related registry key to the Write Protection Exception List **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 **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

Command	Parameter	Value	Description
			Note Using the optional `-r` value includes the specified registry key and related subkeys.
	`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

Command	Parameter	Value	Description
			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.
		`[-r] -t <path_of_registry_key>`	Add the specified 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 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 **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.

COMMAND	PARAMETER	VALUE	DESCRIPTION
remove	writeprotection-regvalue	<path_of_registry_key> <registry_value>	Remove the specified registry value from the Write Protection List **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 **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.
		`[-r] -t <path_of_registry_key>`	Remove the specified registry key from the Write Protection Exception List

Command	Parameter	Value	Description
			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 3-18. Abbreviations and Uses

Parameter	Abbreviation	Use
`trustedcertification`	tc	Manage Trusted Certificates

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

TABLE 3-19. 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 3-20. 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 3-21. 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 3-22. 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 3-23. 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. 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.

Command	Parameter	Description
		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 3-24. 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 3-25. 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.
`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 3-26. 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 3-27. 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 3-28. 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`

Command	Parameter	Description
`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 3-29. 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 3-30. 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`

COMMAND	PARAMETER	DESCRIPTION
		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.
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:

COMMAND	PARAMETER	DESCRIPTION
		`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`
`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".

Command	Parameter	Description
	`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`
	`-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 3-31. 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 3-32. 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>` Available objects types are as follows:	`SLCmd.exe -p <admin_password> add predefinedtrusted updater -u C:\Windows\notepad.exe -t process`

Value	Required/ Optional	Description	Example
		• 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	
-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 predefinedtrustedupdater -u C:\Windows\notepad.exe -t process -l EDITOR
-al enable	Optional	Compare the hash values in the Approved List with the hash values calculated from the actual files	SLCmd.exe -p <admin_password> add predefinedtrustedupdater -u

Value	Required/ Optional	Description	Example
		Note Enabled by default even when `-al` is not specified.	`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 3-33. 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 3-34. 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 3-35. 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 3-36. 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 3-37. Abbreviations and Uses

PARAMETER	ABBREVIATION	USE
`configuration`	con	Manage the configuration file

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

TABLE 3-38. 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 3-39. 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 3-40. 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`
add filelessattackp	<monitored_process>	Add a Fileless Attack Prevention exception

Command	Parameter	Description
revention-process	<Parentprocess1> <Parentprocess2> <Parentprocess3> <Parentprocess4> -a <arguments> -regex -l <label>	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 3-41. 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 3-42. Maintenance Mode Commands

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

COMMAND	PARAMETER	DESCRIPTION
		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: `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:

COMMAND	PARAMETER	DESCRIPTION
		`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` **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

Command	Parameter	Description
		• 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` **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:

Command	Parameter	Description
		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` **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`

Command	Parameter	Description
		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: `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 3-43. 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.
`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 4

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 4-3* 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 3-2* 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 4-1. Configuration File Sections and Descriptions

SECTION	DESCRIPTION	ADDITIONAL INFORMATION
`Configuration`	Container for the Configuration section	
`AccountGroup`	Parameters to configure the Restricted User account	*Account Group Section on page 4-9*
`UI`	Parameters to configure the display of the system tray icon	*UI Section on page 4-10*
`Feature`	Container for the Feature section	

Section	Description	Additional Information
ApplicationLockDown	Parameters to configure StellarProtect (Legacy Mode) features and functions	*Feature Section on page 4-13*
UsbMalwareProtection		
DllInjectionPrevention		
ApiHookingPrevention		
MemoryRandomization		
NetworkVirusProtection		
IntegrityMonitoring		
StorageDeviceBlocking	A parameter to control storage device access to managed endpoints	
Log	Parameters to configure individual log types	*Log Section on page 4-29*
ManagedMode	Parameters to configure Centralized Management functions	*Managed Mode Section on page 4-35*
Permission	Container for the Permission section	
AccountRef	Parameters to configure the StellarProtect (Legacy Mode) console controls available to the Restricted User account	*AccountRef Section on page 4-38*

Account Group Section

The following table lists the parameters to configure the Restricted User account. Refer to *Account Types on page 2-26* for more information about the Restricted User account.

TABLE 4-2. Configuration File - `AccountGroup` Section Parameters

PARAMETER	SETTINGS	VALUE	DESCRIPTION
`Configuration` `AccountGroup`	Container for the Configuration section Container for the AccountGroup section		
`Account`	`ID`	`<GUID>`	Restricted User account GUID
	`Enable`	`yes`	Enable the Restricted User account
		`no`	Disable the Restricted User account
	`Password`	`<admin_password>`	Password for the Restricted User account to access the StellarProtect (Legacy Mode) console **Note** The StellarProtect (Legacy Mode) administrator and Restricted User passwords cannot be the same.

UI Section

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

TABLE 4-3. 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
		`no`	Hide the system tray icon and Windows notifications

Parameter	Settings	Value	Description
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
	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. Refer to *About Feature Settings* section in *About the StellarProtect (Legacy Mode) Agent Console on page 2-4* for more information about the features and functions.

TABLE 4-4. Configuration File - `Feature` Section Parameters

PARAMETER	SETTINGS	VALUE	DESCRIPTION
`Configuration` `Feature`	Container for the Configuration section 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
`ScriptLockDown`	`Enable`	`yes`	Enable Script Lockdown
	`Disable`	`no`	Disable Script Lockdown

Parameter	Settings	Value	Description
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
ParentProcess	Enable	process_path>	Path of the parent process to add to the Trusted Updater List

Parameter	Settings	Value	Description
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
		no	Block Windows Update on the managed endpoint when it is locked down

Parameter	Settings	Value	Description
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

Parameter	Settings	Value	Description
PredefinedTrustedHash	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
	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

Parameter	Settings	Value	Description
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
		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

Parameter	Settings	Value	Description
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
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

Parameter	Settings	Value	Description
CustomAction	ActionMode	0	Ignore blocked files or processes when Application Lockdown blocks any of the following events: • Process launch • DLL loading • Script file access
		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

Parameter	Settings	Value	Description
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
	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

Parameter	Settings	Value	Description
NetworkVirusProtection	Enable	yes	Enable Network Virus Protection
		no	Disable Network Virus Protection
	ActionMode	0	Allow action by detected network viruses
		1	Block action by detected network viruses
IntegrityMonitoring	Enable	yes	Enable Integrity Monitoring
		no	Disable Integrity Monitoring

Parameter	Settings	Value	Description
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
		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.

Parameter	Settings	Value	Description
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 4-29* for more details.			
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

PARAMETER	SETTINGS	VALUE	DESCRIPTION
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
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 8-2* for more information about log descriptions.

TABLE 4-5. 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		

Parameter	Settings	Value	Description
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)
		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)

Parameter	Settings	Value	Description
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
		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

Parameter	Settings	Value	Description
WriteProtectionLog	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
ExceptionPathLog	Enable	yes	Log exceptions to Application Lockdown
		noe	Do not log exceptions to Application Lockdown
WriteProtectionLog	Enable	yes	Log Write Protection events
		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

Parameter	Settings	Value	Description
ExecutionPreventionLog	Enable	yes	Log events that trigger Execution Prevention
		no	Do not log events that trigger Execution Prevention
NetworkVirusProtectionLog	Enable	yes	Log events that trigger Network Virus Protection
		no	Do not log events that trigger Network Virus Protection
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
		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

Parameter	Settings	Value	Description
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
		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 4-6. 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)
`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

Parameter	Settings	Value	Description
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
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)
		2	Synchronize proxy settings with Internet Explorer
HostName		<proxy_hostname>	Specify the proxy host name

Parameter	Settings	Value	Description
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 Restricted User account.

Refer to *Account Types on page 2-26* for more information about the StellarProtect (Legacy Mode) acount types.

Table 4-7. 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 **Note** The Password page is not available to the Restricted User account.

Parameter	Settings	Value	Description
		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 Restricted User clicks **Add Item** on the **Approved List** screen
		RecentHistoryUnapprovedFiles	Access the Block logs if a Restricted 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 • The **Update Hash** button • The **Add Item** > **Add Files/ Folders** menu

Parameter	Settings	Value	Description
	State	yes	Enable the permission specified by ID
		no	Disable the permission specified by ID

Chapter 5

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.

  For more information, see *Manual Scan Commands* section in *SLCmd Program Commands on page 3-4*.

- Access the TXOne StellarProtect (Legacy Mode) Central Console console and send a scan command to start malware scanning on the endpoint.

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

To get the most up-to-date information and support, refer to *Technical Support on page 7-1*.

Chapter 6

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

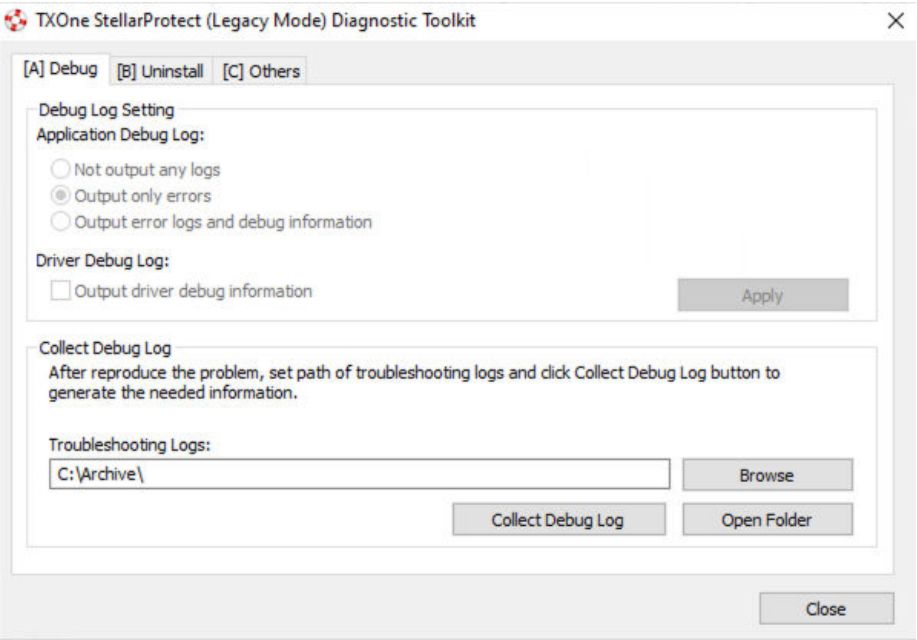

FIGURE 6-1. The TXOne StellarProtect (Legacy Mode) Diagnostic Toolkit Debug Tab A [Debug]

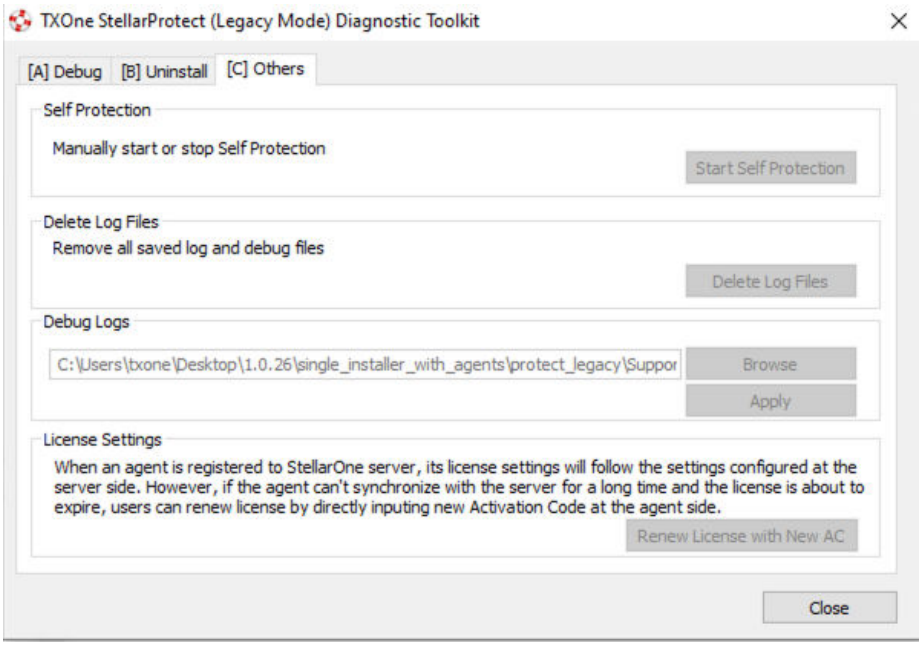

FIGURE 6-2. The TXOne StellarProtect (Legacy Mode) Diagnostic Toolkit Debug Tab B [Uninstall]

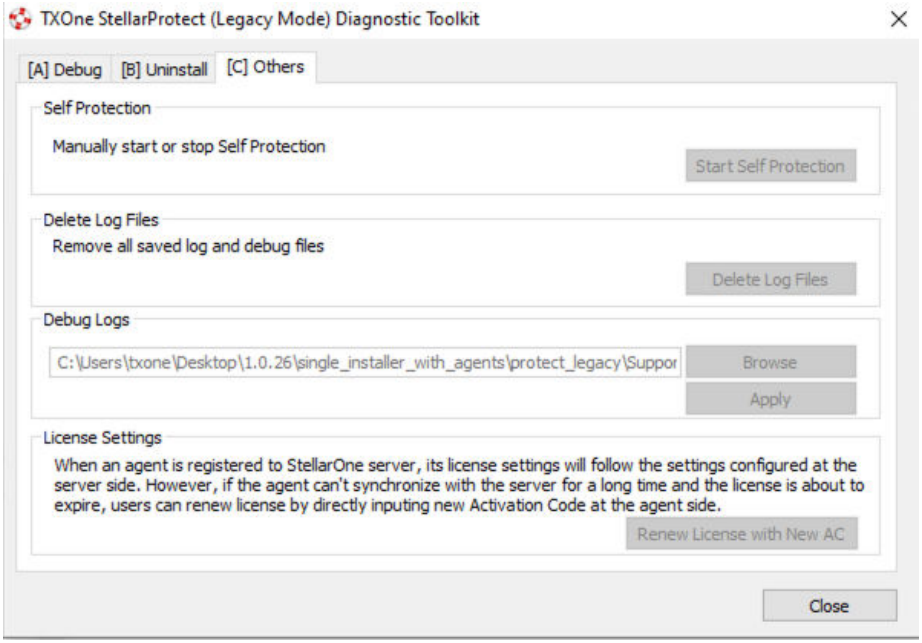

FIGURE 6-3. The TXOne StellarProtect (Legacy Mode) Diagnostic Toolkit Debug Tab C [Others]

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 Restricted 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 Restricted 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 \SStellarProtect (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 7

Technical Support

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

Learn about the following topics:

Troubleshooting Resources

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 7-1. 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 7-2. 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.

Chapter 8

Log Descriptions for StellarProtect (Legacy Mode)

The following tables provides log descriptions for StellarProtect (Legacy Mode).

Topics in this section include:

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 Description
1000	Information	System	Service started.
1002	Information	System	Application Lockdown Turned On.
1004	Information	System	Disabled.
1005	Information	System	Administrator password changed.
1006	Information	System	Restricted User password changed.
1007	Information	System	Restricted User account enabled.
1008	Information	System	Restricted User account disabled.
1009	Information	System	Product activated.
1010	Information	System	Product deactivated.
1013	Information	System	Product configuration import complete: %path%
1015	Information	System	Product configuration exported to: %path%
1016	Information	System	USB Malware Protection set to Allow.
1017	Information	System	USB Malware Protection set to Block.

Event ID	Level	Category	Event Description
1018	Information	System	USB Malware Protection enabled.
1020	Information	System	Network Virus Protection set to Allow.
1021	Information	System	Network Virus Protection set to Block.
1022	Information	System	Network Virus Protection enabled.
1025	Information	System	Memory Randomization enabled.
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.
1031	Information	System	DLL Injection Prevention set to Allow.
1032	Information	System	DLL Injection Prevention set to Block.
1033	Information	System	DLL Injection Prevention enabled.
1035	Information	System	Pre-defined Trusted Update enabled.
1036	Information	System	Pre-defined Trusted Update disabled.
1037	Information	System	DLL/Driver Lockdown enabled.
1039	Information	System	Script Lockdown enabled.
1041	Information	System	Script added. [Details]

Event ID	Level	Category	Event Description
			File extension: %extension% Interpreter: %interpreter%
1042	Information	System	Script removed. [Details] File extension: %extension% Interpreter: %interpreter%
1044	Information	System	Exception path enabled.
1045	Information	System	Exception path disabled.
1047	Information	System	Trusted certification enabled.
1048	Information	System	Trusted certification disabled.
1049	Information	System	Write Protection enabled.
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% Process: %process%
1058	Information	System	Removed file from Write Protection Exception List. Path: %path% Process: %process%

Event ID	Level	Category	Event Description
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% 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%

Event ID	Level	Category	Event Description
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. 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%

Event ID	Level	Category	Event Description
			Scope: %scope% 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 Intelligent Manager
1074	Information	System	Quarantined file is restored. [Details] Original Location: %path% Source: %source%
1075	Information	System	Quarantined file is deleted. [Details] 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. [Details] Access Image Path: %path%
1079	Information	System	Server certification imported: %path%
1080	Information	System	Server certification exported to: %path%
1081	Information	System	Managed mode configuration imported: %path%
1082	Information	System	Managed mode configuration exported to: %path%

Event ID	Level	Category	Event Description
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
1088	Information	System	Windows Update Support enabled.
1089	Information	System	Windows Update Support disabled.
1094	Information	System	TXOne StellarProtect (Legacy Mode) updated. File applied: %file_name%
1096	Information	System	Trusted Hash List enabled.
1097	Information	System	Trusted Hash List 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
1103	Information	System	Event Log settings changed. [Details] Windows Event Log: %ON|off% Level: Warning Log: %ON|off% Information Log: %ON|off% System Log: %ON|off% Exception Path Log: %ON|off%

Event ID	Level	Category	Event Description
			Write Protection Log: %ON|off% List Log: %ON|off% 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% Network Virus Protection 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% RegValue Modified Log: %ON|off% RegValue Deleted Log: %ON|off% RegKey Created Log: %ON|off% RegKey Deleted Log: %ON|off%

Event ID	Level	Category	Event Description
			RegKey Renamed Log: %ON|off% Device Control Log: %ON|off% Debug Log: %ON|off%
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.
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%

Event ID	Level	Category	Event Description
1509	Information	List	Approved List updated: %path %
1510	Information	List	Trusted Updater List updated: %path%
1513	Information	System	Added to Exception Path List. [Details] Type: %exceptionpathtype% Path: %exceptionpath%
1514	Information	System	Removed from Exception Path List. [Details] Type: %exceptionpathtype% Path: %exceptionpath%
1515	Information	System	Added to Trusted Certification List. [Details] Label: %label% Hash: %hashvalue% Type: %type% Subject: %subject% Issuer: %issuer%
1516	Information	System	Removed from Trusted Certification List. [Details] Label: %label% Hash: %hashvalue% Type: %type% Subject: %subject% Issuer: %issuer%
1517	Information	System	Added to the Trusted Hash List.%n [Details]

Event ID	Level	Category	Event Description
			Label : %label% Hash : %hashvalue% Type : %type% Add to Approved List: %yes|no % Path : %path% Note: %note%
1518	Information	System	Removed from the Trusted Hash List.%n [Details] 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%
1521	Information	System	Added Fileless Attack Prevention exception. [Details] Label : %label% Target Process: %process_name% Arguments: %arguments% %regex_flag% Parent Process 1 Image Path: %path%

Event ID	Level	Category	Event Description
			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. [Details] 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%
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

Event ID	Level	Category	Event Description
1527	Information	List	Approved List updated in Maintenance Mode. Path: %1 Hash: %2
2000	Information	Access Approved	File access allowed: %path% [Details] Access Image Path: %path% Access User: %username% Mode: %mode% List: %list%
2006	Information	Access Approved	File access allowed: %path% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2011	Information	Access Approved	Registry access allowed. Registry Key: %regkey% Registry Value Name: %regvalue% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2012	Information	Access Approved	Registry access allowed. Registry Key: %regkey% [Details]

Event ID	Level	Category	Event Description
			Access Image Path: %path% Access User: %username% Mode: %mode%
2013	Information	Access Approved	Change of File/Folder allowed by Exception List: %path% [Details] Access Image 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% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2016	Information	Access Approved	Change of Registry Key allowed by Exception List. Registry Key: %regkey% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2507	Information	Access Blocked	Action completed successfully: %path% [Details]

Event ID	Level	Category	Event Description
			Action: %action% Source: %source%
2511	Information	Access Blocked	Change of File/Folder blocked: %path% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
4500	Information	Changes in System	File/Folder created: %path% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4501	Information	Changes in System	File modified: %path% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4502	Information	Changes in System	File/Folder deleted: %path% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4503	Information	Changes in System	File/Folder renamed: %path% New Path: %path% [Details]

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

Event ID	Level	Category	Event Description
4507	Information	Changes in System	Registry Key deleted. Registry Key: %regkey% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4508	Information	Changes in System	Registry Key renamed. Registry Key: %regkey% New Registry Key: %regkey% [Details] Access Image Path: %path% Access Process Id: %pid% Access User: %username%
6000	Information	System	%Result% [Details] 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%

Event ID	Level	Category	Event Description
			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 Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%
6002	Information	System	Malware scan started: %SCAN_TYPE% [Details] Files to scan: %SCAN_FOLDER_TYPE% Scanned folders: %PATHS% Excluded paths: %PATHS% Excluded files: %PATHS% Excluded extensions: %PATHS% [Components]

Event ID	Level	Category	Event Description
			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%
6003	Information	System	Malware scan completed: %SCAN_TYPE%. Number of infected files: %NUM% [Details] 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%

Event ID	Level	Category	Event Description
			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% 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% [Details] Reboot required: %NEED_REBOOT% [Scan Result] Threat type: %TYPE% Threat name: %NAME%

Event ID	Level	Category	Event Description
			[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% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%
7000	Information	System	Group policy applied [Details] Old Group Name: %GROUP NAME% Old Policy Version: %VERSION% New Group Name: %GROUP NAME% New Policy Version: %VERSION %
8000	Information	System	Real Time Scan is enabled
8500	Information	System	Scheduled component update has been enabled. Next update will be on %TIME% (agent's local system time).

Event ID	Level	Category	Event Description
8501	Information	System	Scheduled component update has been disabled.
1001	Warning	System	Service stopped
1003	Warning	System	Application Lockdown Turned Off.
1011	Warning	System	License Expired. Grace period enabled.
1012	Warning	System	License Expired. Grace period ended.
1019	Warning	System	USB Malware Protection disabled.
1023	Warning	System	Network Virus Protection disabled.
1026	Warning	System	Memory Randomization disabled.
1030	Warning	System	API Hooking Prevention disabled.
1034	Warning	System	DLL Injection Prevention disabled.
1038	Warning	System	DLL/Driver Lockdown disabled.
1040	Warning	System	Script Lockdown disabled.
1050	Warning	System	Write Protection disabled.
1086	Warning	System	Protection applied to Write Protection List while Write Protection is enabled.
1102	Warning	System	Storage device control disabled
1104	Warning	System	Memory Randomization is not available in this version of Windows.

Event ID	Level	Category	Event Description
1112	Warning	System	Fileless Attack Prevention disabled.
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%
1520	Warning	List	Unable to create Approved List because an unexpected error occurred during enumeration of the files in %1 %n Error Code: %2 %n
2001	Warning	Access Approved	File access allowed: %path% [Details] 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. [Details] 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. [Details]

Event ID	Level	Category	Event Description
			Access Image Path: %path% Access User: %username% Mode: %mode%
2004	Warning	Access Approved	File access allowed: %path% Unable to get notifications to monitor process.
2005	Warning	Access Approved	File access allowed: %path% Unable to add process to non exception list.
2007	Warning	Access Approved	File access allowed: %path% An error occurred while checking the Exception Path List. [Details] 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. [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2017	Warning	Access Approved	Change of File/Folder allowed: %path% [Details]

Event ID	Level	Category	Event Description
			Access Image Path: %path% Access User: %username% Mode: %mode%
2019	Warning	Access Approved	Change of Registry Value allowed. Registry Key: %regkey% Registry Value Name: %regvalue% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2020	Warning	Access Approved	Change of Registry Key allowed. Registry Key: %regkey% [Details] 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. [Details] Access Image Path: %path% Access User: %username% Mode: %mode%

Event ID	Level	Category	Event Description
2022	Warning	Access Approved	Process allowed by Fileless Attack Prevention: %path% %argument% [Details] 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%
2503	Warning	Access Blocked	Change of File/Folder blocked: %path% [Details] 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% [Details] Access Image Path: %path% Access User: %username%

Event ID	Level	Category	Event Description
			Mode: %mode%
2506	Warning	Access Blocked	Change of Registry Key blocked. Registry Key: %regkey% [Details] Access Image Path: %path% Access User: %username% Mode: %mode%
2508	Warning	Access Blocked	Unable to take specified action: %path% [Details] Action: %action% Source: %source%
2509	Warning	Access Blocked	File access blocked: %path% [Details] Access Image Path: %path% Access User: %username% Mode: %mode% Reason: Not in Approved List File Hash blocked: %hash%
2510	Warning	Access Blocked	File access blocked: %path% [Details] Access Image Path: %path% Access User: %username% Mode: %mode% Reason: Hash does not match expected value

Event ID	Level	Category	Event Description
			File Hash blocked: %hash%
2512	Warning	Access Blocked	Change of Registry Value blocked. Registry Key: %regkey% Registry Value Name: %regvalue% [Details] Access Image Path: %path% Access User: %username% **Note** Enabling the Service Creation Prevention feature triggers Event ID 2512.
2513	Warning	Access Blocked	Process blocked by Fileless Attack Prevention: %path% %argument% [Details] 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%

Event ID	Level	Category	Event Description
2514	Warning	Access Blocked	File access blocked: %BLOCKED_FILE_PATH% [Details] Access Image Path: %PARENT_PROCESS_PATH% Access User: %USER_NAME% Reason: Blocked file is in a folder that has the case sensitive attribute enabled.
3000	Warning	USB Malware Protection	Device access allowed: %path% [Details] Access Image Path: %path% Access User: %username% Device Type: %type%
3001	Warning	USB Malware Protection	Device access blocked: %path% [Details] Access Image Path: %path% Access User: %username% Device Type: %type%
3500	Warning	Network Virus Protection	Network virus allowed: %name % [Details] Protocol: TCP Source IP Address: %ip_address% Source Port: %port% Destination IP Address: %ip_address% Destination Port: 80

Event ID	Level	Category	Event Description
3501	Warning	Network Virus Protection	Network virus blocked: %name % [Details] Protocol: TCP Source IP Address: %ip_address% Source Port: %port% Destination IP Address: %ip_address% Destination Port: 80
4000	Warning	Process Protection Event	API Hooking/DLL Injection allowed: %path% [Details] Threat Image Path: %path% Threat User: %username%
4001	Warning	Process Protection Event	API Hooking/DLL Injection blocked: %path% [Details] Threat Image Path: %path% Threat User: %username%
4002	Warning	Process Protection Event	API Hooking allowed: %path% [Details] Threat Image Path: %path% Threat User: %username%
4003	Warning	Process Protection Event	API Hooking blocked: %path% [Details] Threat Image Path: %path% Threat User: %username%

Event ID	Level	Category	Event Description
4004	Warning	Process Protection Event	DLL Injection allowed: %path% [Details] Threat Image Path: %path% Threat User: %username%
4005	Warning	Process Protection Event	DLL Injection blocked: %path% [Details] Threat Image Path: %path% Threat User: %username%
5000	Warning	Device Control	Storage device access allowed: %PATH% [Details] Access Image path: %PATH% Access User: %USERNAME% Device Type: %TYPE% %DEVICEINFO%
5001	Warning	Device Control	Storage device access blocked: %PATH% [Details] Access Image path: %PATH% Access User: %USERNAME% Device Type: %TYPE% %DEVICEINFO%
6001	Warning	System	Update failed: %ERROR_MSG% (%ERROR_CODE%) [Details] Update Source: %SERVER% [Original Version]

Event ID	Level	Category	Event Description
			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% [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 Description
6004	Warning	System	Malware scan unsuccessful: %SCAN_TYPE% %ERROR% [Details] 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] 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 DESCRIPTION
			Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%
6006	Warning	System	Malware detected. Unable to perform scan actions: %PATH% [Details] 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% 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

Event ID	Level	Category	Event Description
			quarantine successful): %PATH % [Details] 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% Scanner: %VERSION%
6008	Warning	Maintenance Mode	Malware detected in Maintenance Mode (file quarantine unsuccessful): %PATH% [Details] Component versions: Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection Pattern: %VERSION%

Event ID	Level	Category	Event Description
			Damage Cleanup Template: %VERSION% Damage Cleanup Engine Configuration: %VERSION% Virus Scan Engine: %VERSION% Damage Cleanup Engine: %VERSION% Scanner: %VERSION%
6009	Warning	Maintenance Mode	Malware detected in Maintenance Mode: %PATH% [Details] 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% Scanner: %VERSION%
7001	Warning	System	Unable to synchronize group policy [Details]

Event ID	Level	Category	Event Description
			Old Group Name: %GROUP NAME% Old Policy Version: %VERSION% New Group Name: %GROUP NAME% New Policy Version: %VERSION % Reason: %Reason%
8001	Warning	System	Real Time Scan is disabled.
8010	Warning	System	Incoming files were scanned by antivirus. Action was taken according to settings. • File Path: %PATH% • 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%

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)
0x0004020c	System Reserved. (Not used)
0x0004020d	System Reserved. (Not used)
0x8004020d	System Reserved. (Not used)

Code	Description
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.
0x80040220	System Reserved. (Not used)
0x80040221	System Reserved. (Not used)
0x80040222	System Reserved. (Not used)

Code	Description
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.
0x80040281	Incorrect Activation Code format.

Index

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: APEM219660/221221