



Keep the Operation Running

# TXOne StellarProtect

# 3.0 Service Pack 1

## Administrator's Guide

Unified agent providing asset lifetime all-terrain protection

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>

TXOne Networks, StellarOne, and StellarProtect are trademarks or registered trademarks of TXOne Networks Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2023. TXOne Networks Incorporated. All rights reserved.

Document Part No.: APEM39832/230913

Release Date: September 2023

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

## Privacy and Personal Data Collection Disclosure

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

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

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

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

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



# Table of Contents

## **Preface**

|                               |   |
|-------------------------------|---|
| Preface .....                 | 1 |
| About the Documentation ..... | 2 |
| Audience .....                | 2 |
| Document Conventions .....    | 2 |
| Terminology .....             | 3 |

## **Chapter 1: Introduction**

|  |      |
|--|------|
| About TXOne Stellar .....                | 1-2  |
| Key Features and Benefits .....          | 1-3  |
| What's New .....                         | 1-6  |
| System Requirements .....                | 1-7  |
| Software and Hardware Requirements ..... | 1-7  |
| Operating Systems .....                  | 1-10 |

## **Chapter 2: Setting Up the Approved List**

|                                    |     |
|------------------------------------|-----|
| Setting Up the Approved List ..... | 2-2 |
|------------------------------------|-----|

## **Chapter 3: Using the Agent Console**

|  |      |
|--|------|
| Using the StellarProtect Agent Console ..... | 3-2  |
| Overview .....                               | 3-2  |
| OT Applications .....                        | 3-9  |
| OT Certificates .....                        | 3-10 |
| Approved List .....                          | 3-11 |
| About Hashes .....                           | 3-14 |
| Checking or Updating Hashes .....            | 3-14 |
| Configuring the Approved List .....          | 3-16 |
| Adding or Removing Files .....               | 3-17 |
| Exporting or Importing the File Hashes ..... | 3-18 |

|  |      |
|--|------|
| Password and Account Types .....                           | 3-19 |
| Account Settings .....                                     | 3-20 |
| Operations .....   | 3-21 |
| Scan Now .....   | 3-23 |
| Sync Now .....   | 3-24 |
| Check Connection .....                                     | 3-24 |
| Setting Maintenance Mode .....                             | 3-25 |
| About Feature Settings .....                               | 3-27 |
| Enabling or Disabling Feature Settings .....               | 3-32 |
| About StellarProtect .....                                 | 3-33 |
| Using the StellarProtect (Legacy Mode) Agent Console ..... | 3-34 |
| Overview .....   | 3-34 |
| Approved List .....  | 3-40 |
| About Hashes .....   | 3-42 |
| Checking or Updating Hashes .....                          | 3-42 |
| Configuring the Approved List .....                        | 3-44 |
| Adding or Removing Files .....                             | 3-45 |
| Updating or Installing Using the Trusted Updater ....      | 3-46 |
| Exporting or Importing the Approved List .....             | 3-48 |
| Password and Account Types .....                           | 3-49 |
| Account Settings .....                                     | 3-51 |
| Operations .....   | 3-52 |
| Scan Now .....   | 3-54 |
| Sync Now .....   | 3-55 |
| Check Connection .....                                     | 3-55 |
| Setting Maintenance Mode .....                             | 3-56 |
| About Feature Settings .....                               | 3-59 |
| Enabling or Disabling Feature Settings .....               | 3-63 |
| About StellarProtect (Legacy Mode) .....                   | 3-64 |

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

|   |     |
|---|-----|
| Using StellarProtect Command Line Interface (CLI) ..... | 4-2 |
| Using OPCmd at the Command Line Interface (CLI) .....   | 4-2 |
| Overview of StellarProtect CLI .....                    | 4-2 |
| OPCmd Program Commands .....                            | 4-4 |

|   |      |
|---|------|
| Using StellarProtect (Legacy Mode) Command Line Interface (CLI) ..... | 4-16 |
| Using SLCmd at the Command Line Interface (CLI) .....                 | 4-16 |
| SLCmd Program and Console Function Comparison .....                   | 4-16 |
| Overview of StellarProtect (Legacy Mode) CLI .....                    | 4-18 |
| SLCmd Program Commands .....  | 4-19 |

## **Chapter 5: Working with the Agent Configuration File**

|   |      |
|---|------|
| Working with the Agent Configuration File ..... | 5-2  |
| Changing Advanced Settings .....                | 5-2  |
| Exporting or Importing a Config File .....      | 5-3  |
| Configuration File Syntax .....                 | 5-3  |
| Configuration File Parameters .....             | 5-8  |
| Account Group Section .....                     | 5-9  |
| UI Section .....                                | 5-10 |
| Feature Section .....                           | 5-12 |
| Log Section .....                               | 5-27 |
| Managed Mode Section .....                      | 5-32 |
| AccountRef Section .....                        | 5-36 |

## **Chapter 6: Agent Event Logs**

|  |      |
|--|------|
| Overview of Agent Event Logs .....                                   | 6-2  |
| StellarProtect Events .....  | 6-2  |
| Accessing StellarProtect Event Logs .....                            | 6-2  |
| Agent Event Log Descriptions for StellarProtect .....                | 6-2  |
| StellarProtect (Legacy Mode) Events .....                            | 6-24 |
| Agent Event Log Descriptions for StellarProtect (Legacy Mode) .....  | 6-24 |
| Agent Error Code Descriptions for StellarProtect (Legacy Mode) ..... | 6-72 |

## **Chapter 7: Troubleshooting Resources**

|  |     |
|--|-----|
| Frequently Asked Questions (FAQ) ..... | 7-2 |
|--|-----|

|  |     |
|--|-----|
| Troubleshooting StellarProtect .....   | 7-2 |
| Using the StellarProtect Diagnostic Toolkit for<br>Troubleshooting .....               | 7-4 |
| Troubleshooting StellarProtect (Legacy Mode) .....                                     | 7-5 |
| Using the StellarProtect (Legacy Mode) Diagnostic Toolkit<br>for Troubleshooting ..... | 7-8 |

## **Chapter 8: Technical Support**

|   |     |
|---|-----|
| Troubleshooting Resources .....                 | 8-2 |
| Using the Support Portal .....                  | 8-2 |
| Threat Encyclopedia .....                       | 8-2 |
| Contacting Trend Micro and TXOne .....          | 8-3 |
| Speeding Up the Support Call .....              | 8-4 |
| Sending Suspicious Content to Trend Micro ..... | 8-4 |
| Email Reputation Services .....                 | 8-4 |
| File Reputation Services .....                  | 8-5 |
| Web Reputation Services .....                   | 8-5 |
| Other Resources .....                           | 8-5 |
| Download Center .....                           | 8-5 |

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

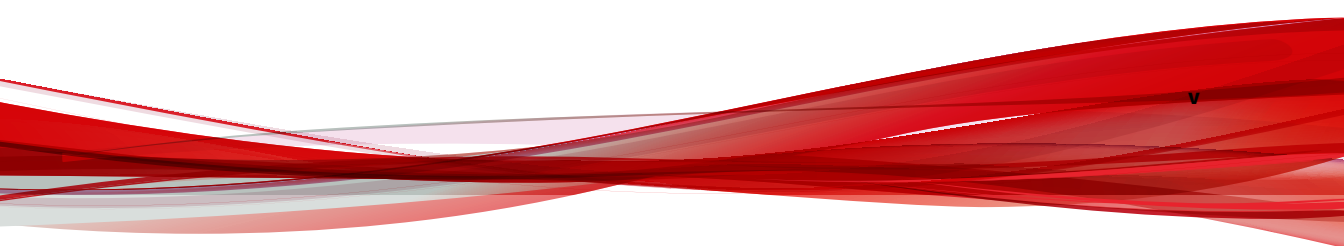
### **Index**

|             |      |
|-------------|------|
| Index ..... | IN-1 |
|-------------|------|



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](mailto:docs@txone-networks.com).





# Preface

## Preface

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

Topics in this chapter include:

- *About the Documentation on page 2*
- *Audience on page 2*
- *Document Conventions on page 2*
- *Terminology on page 3*

## About the Documentation

TXOne Networks StellarProtect documentation includes the following:

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

## Audience





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

## Document Conventions

The documentation uses the following conventions.

**TABLE 1. Document Conventions**

| CONVENTION | DESCRIPTION   |
|------------|---|
| UPPER CASE | Acronyms, abbreviations, and names of certain commands and keys on the keyboard |

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

## Terminology

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

| TERMINOLOGY | DESCRIPTION                                 |
|-------------|---|
| server      | The StellarOne console server program       |
| agents      | The host running the StellarProtect program |

| <b>TERMINOLOGY</b>                              | <b>DESCRIPTION</b>  |
|---|---|
| managed agents<br>managed endpoints             | The hosts running the StellarProtect program that are known to the StellarOne server program  |
| target endpoints                                | The hosts where the StellarProtect™ managed agents will be installed  |
| Administrator (or StellarProtect administrator) | The person managing the StellarProtect agents   |
| StellarProtect console                          | The user interface for configuring and managing StellarProtect settings   |
| StellarOne (management) console                 | The user interface for configuring and managing the StellarProtect agents managed by StellarOne   |
| CLI   | Command Line Interface  |
| license activation                              | Includes the type of StellarProtect agent installation and the allowed period of usage that you can use the application   |
| agent installation folder                       | The folder on the host that contains the StellarProtect agent files. If you accept the default settings during installation, you will find the installation folder at one of the following locations:<br><br>C:\Program Files\TXOne\StellarProtect<br><br>C:\Program Files\TXOne\StellarProtect (Legacy Mode) |

# Chapter 1

## Introduction

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

Topics in this chapter include:

- *About TXOne Stellar on page 1-2*
- *Key Features and Benefits on page 1-3*
- *What's New on page 1-6*
- *System Requirements on page 1-7*

## About TXOne Stellar

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

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

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

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

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



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

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

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


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

## Key Features and Benefits

The StellarProtect provides following features and benefits.

**TABLE 1-1. Features and Benefits**

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

| FEATURE                   | BENEFIT  |
|---------------------------|--|
| Approved List Management  | <p>When software needs to be installed or updated, you can use one of the following methods to make changes to the endpoint that automatically adds new or modified files to the Approved List, all without having to unlock TXOne StellarProtect or StellarProtect (Legacy Mode):</p> <ul style="list-style-type: none"> <li>• Maintenance Mode</li> <li>• Trusted Updater (Legacy Mode only)</li> <li>• Predefined Trusted Updater List (Legacy Mode only)</li> <li>• Command Line Interface (CLI)</li> <li>• Trusted hash</li> <li>• Trusted certificate</li> </ul> |
| DLL Injection Prevention  | <p>This feature detects and blocks API call behaviors used by malicious software. Blocking these threats helps prevent malicious processes from running.</p>   |
| Device Control            | <p>This feature prevents insider threats by only allowing usage of USB ports on a case-by-case administrator reviewed basis.</p> <hr/> <p> <b>Note</b><br/>For StellarProtect (Legacy Mode), Device Control is included as one of the features of <i>Exploit Prevention</i> settings.</p> <hr/>   |
| Maintenance Mode          | <p>To perform file updates on endpoints, users can configure Maintenance Mode settings to define a period when StellarProtect or StellarProtect (Legacy Mode) allows all file executions and adds all files that are created, executed, or modified to the Approved List.</p>  |
| Role Based Administration | <p>TXOne StellarProtect and StellarProtect (Legacy Mode) both provide a separate Administrator and User account, providing full control during installation and setup, as well as simplified monitoring and maintenance after deployment.</p>  |
| Self Protection           | <p>With self protection features, StellarProtect/StellarProtect (Legacy Mode) are capable of defending its processes and resources, required to function properly, from being disabled by programs or actual users.</p>  |

| FEATURE   | BENEFIT   |
|---|---|
| Graphical and Command Line Interfaces   | Anyone who needs to check the software can use the console, while system administrators can take advantage of the command line interface (CLI) to access all of the features and functions available.   |
| Features designed specifically for modernized assets: <ul style="list-style-type: none"> <li>• OT Application Safeguard</li> <li>• Operations Behavior Anomaly Detection</li> </ul>                 | <p>For modernized assets, StellarProtect offers features such as <b>OT Application Safeguard</b> and <b>Operations Behavior Anomaly Detection</b> that detect behavioral anomalies and quickly determine operational credibility using an expansive library of OT/ICS applications and certificates.</p> <p><b>OT Application Safeguard</b> intelligently locates and secures the operational integrity of the critical OT/ICS applications by preventing the un-authorized changes. TXOne Networks continuously builds up the only OT/ICS context-focused database that can identify thousands of applications and certificates to ensure undisturbed operations.</p> <p>Meanwhile, <b>Operations Behavior Anomaly Detection</b> detects abnormal operations and exercises least privilege-based control to prevent malware-free attacks by means of its auto-learn runtime behavior to adapt to the dynamic needs of autonomous operations.</p> |
| Features designed specifically for legacy assets: <ul style="list-style-type: none"> <li>• Write Protection</li> <li>• Fileless Attack Prevention</li> <li>• Exploit Prevention settings</li> </ul> | <p>For fixed-use and legacy systems, StellarProtect (Legacy Mode) provides more options available from Application Lockdown settings. <b>Write Protection</b> blocks modification and deletion of files, folders, and registry entries; <b>Fileless Attack Prevention</b> detects and blocks unapproved process chains and arguments that may lead to a fileless attack event.</p> <p>For advanced threat prevention, StellarProtect (Legacy Mode) <i>Exploit Prevention</i> settings includes Intrusion Prevention, Execution Prevention, and Device Control to stop threats from spreading to the endpoint or executing.</p>  |

## What's New

TXOne StellarProtect 3.0 Service Pack 1 provides following new features and enhancements.

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

| FEATURE  | BENEFIT  |
|--|--|
| Script Behavior functionality for StellarProtect (Legacy Mode)                   | The Script Behavior functionality complements the Operations Behavior Anomaly Detection feature for StellarProtect (Legacy Mode), providing a solid protection against script-based or fileless attacks. |
| Application Behavior functionality enhancements for StellarProtect (Legacy Mode) | The enhancements of the Application Behavior functionality for StellarProtect (Legacy Mode) implement effective application security.  |
| Last components update timestamp available on the GUI                            | The last components update timestamp for StellarProtect (Legacy Mode) agents can be viewed on the Overview page.   |
| Spyware detection enhancement  | Improves the spyware scan functionality.   |


## System Requirements

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

### Software and Hardware Requirements

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

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

| HARDWARE                  | DESCRIPTION  |
|---------------------------|--|
| Available free disk space | 400MB<br><br><hr/>  <b>Note</b> <ul style="list-style-type: none"> <li>• Recommended free disk space for StellarProtect Single Installer required during the installation process: 1.5GB</li> <li>• Minimum memory usage required when Application Lockdown and Real-Time Scan are both enabled:               <ul style="list-style-type: none"> <li>• StellarProtect: 350MB</li> <li>• StellarProtect (Legacy Mode): 300MB</li> </ul> </li> <li>• Minimum memory usage required when Application Lockdown is enabled and Real-Time Scan is disabled:               <ul style="list-style-type: none"> <li>• StellarProtect: 120MB</li> <li>• StellarProtect (Legacy Mode): 100MB</li> </ul> </li> </ul> |
| Monitor and resolution    | VGA (640 x 480), 16 colors   |

**TABLE 1-4. Required Software for StellarProtect**

| SOFTWARE       | DESCRIPTION                      |
|----------------|----------------------------------|
| .NET framework | Version 3.5 SP1 or 4.0 available |

**Note**

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

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

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

---



### Important

- StellarProtect/StellarProtect (Legacy Mode) cannot be installed on a system that already runs one of the following:
  - Trend Micro OfficeScan
  - Trend Micro Titanium
  - Other Trend Micro endpoint solutions
  - Other antivirus products
- Ensure that the following root certification authority (CA) certificates are installed with intermediate CAs, which are found in StellarSetup.exe. These root CAs should be installed on the StellarProtect/StellarProtect (Legacy Mode) agent environment to communicate with StellarOne.
  - Intermediate Symantec Class 3 SHA256 Code Signing CA
  - Root VeriSign Class 3 Public Primary Certification Authority - G5
  - DigiCert Assured ID Root CA (Legacy Mode only)
  - DigiCert Trusted Root G4 (Legacy Mode only)

To check root CAs, refer to the [Microsoft support site](#).

---



### Note

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

---

## Operating Systems

### Windows Client:

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

**Note**

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

---



**Windows Server:**

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

**Note**

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



# Chapter 2

## Setting Up the Approved List

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

- [Setting Up the Approved List on page 2-2](#)

## Setting Up the Approved List

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

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



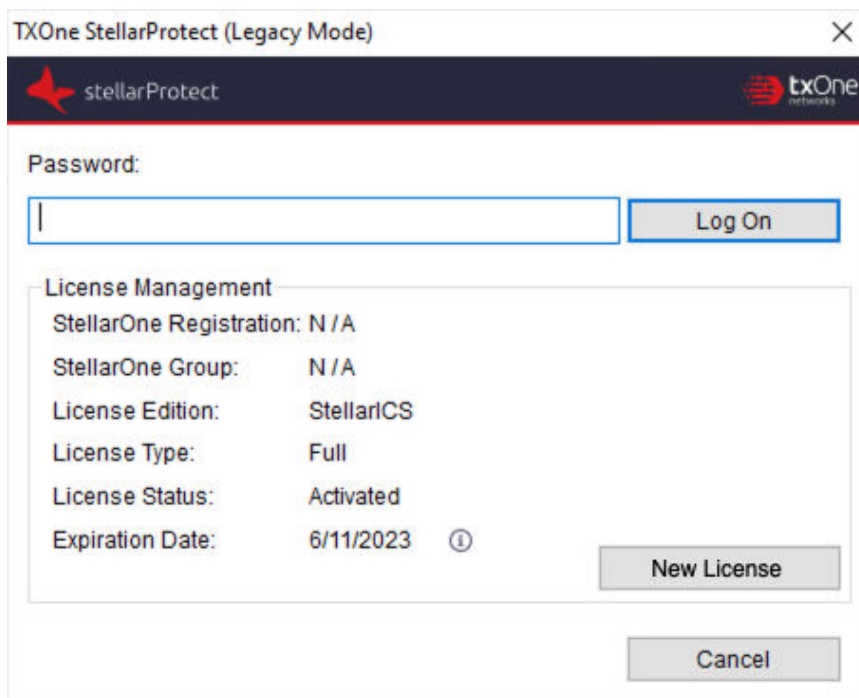
### Note

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

---

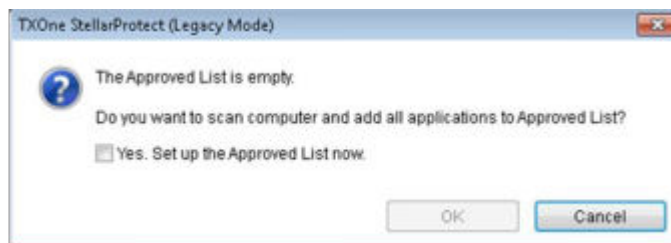
### Procedure

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



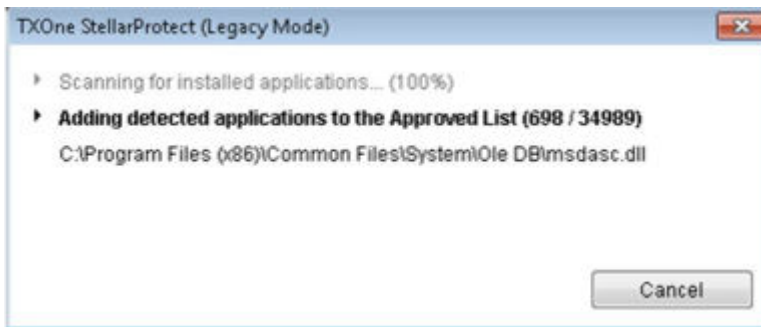
**FIGURE 2-1. StellarProtect (Legacy Mode) Log On Screen**

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



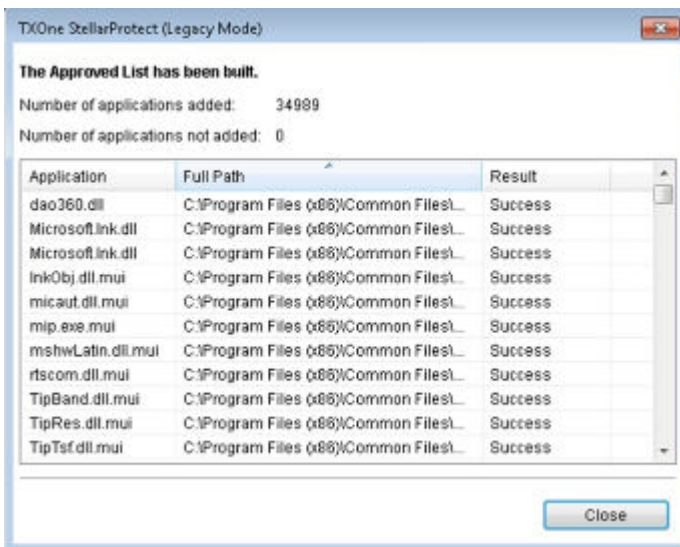
**FIGURE 2-2. The Approved List is Empty**

- 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**

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



**FIGURE 2-4. Approved List Created**



**Note**

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

**6. Click Close.**

---





# Chapter 3

## Using the Agent Console

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

Topics in this chapter include:

- *Using the StellarProtect Agent Console on page 3-2*
- *Using the StellarProtect (Legacy Mode) Agent Console on page 3-34*

## Using the StellarProtect Agent Console

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

Topics include:

- [Overview on page 3-2](#)
- [OT Applications on page 3-9](#)
- [OT Certificates on page 3-10](#)
- [Approved List on page 3-11](#)
- [Password and Account Types on page 3-19](#)
- [Operations on page 3-21](#)
- [About Feature Settings on page 3-27](#)
- [About StellarProtect on page 3-33](#)

### Overview

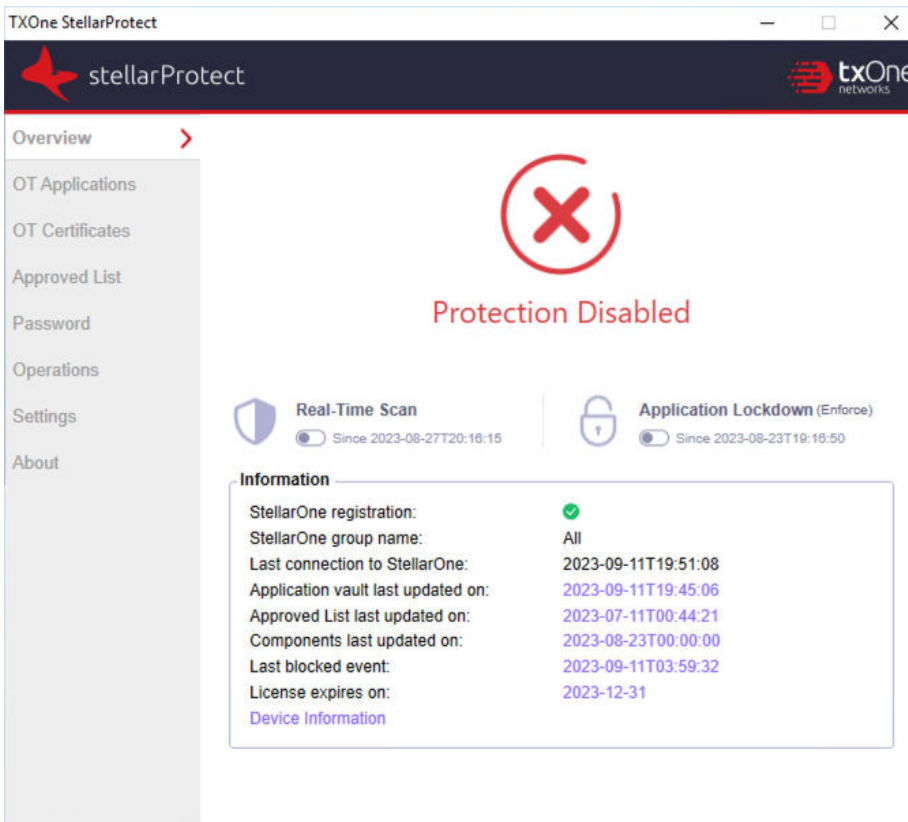
The agent console provides easy access to commonly used features in TXOne StellarProtect.

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

The screenshot shows the StellarProtect console interface. The top navigation bar includes the 'stellarProtect' logo and the 'txOne networks' logo. A left sidebar contains navigation options: Overview (selected), OT Applications, OT Certificates, Approved List, Password, Operations, Settings, and About. The main content area features a large green checkmark icon and the text 'Protection Enabled'. Below this, there are two status indicators: 'Real-Time Scan' (enabled since 2023-08-27T20:16:15) and 'Application Lockdown (Enforce)' (disabled since 2023-08-23T19:16:50). An 'Information' section provides a list of system details:

| Information                        |                     |
|------------------------------------|---------------------|
| StellarOne registration:           | ✓                   |
| StellarOne group name:             | All                 |
| Last connection to StellarOne:     | 2023-09-11T19:51:08 |
| Application vault last updated on: | 2023-09-11T19:45:06 |
| Approved List last updated on:     | 2023-07-11T00:44:21 |
| Components last updated on:        | 2023-08-23T00:00:00 |
| Last blocked event:                | 2023-09-11T03:59:32 |
| License expires on:                | 2023-12-31          |
| <a href="#">Device Information</a> |                     |

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









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




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

**TABLE 3-1. Overview Item Descriptions**

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

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

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

| ITEM                                     | FUNCTION  | DESCRIPTION   |
|--|---|---|
| <b>StellarOne registration</b>           |  | Indicates the StellarProtect agent is successfully registered to a designated StellarOne web console.   |
|  |  | Indicates the registration to a StellarOne web console has failed.  |
|  | N/A   | Indicates the agent was installed in standalone mode and has not registered to any StellarOne web console.  |
| <b>StellarOne group name</b>             |   | <p>Displays the name of the group the agent belongs to. When you mouse over the displayed name, information about the group name, group ID, and policy version will appear.</p> <hr/> <p> <b>Note</b></p> <ul style="list-style-type: none"> <li>• If the agent does not belong to any group, the group name displayed should be <b>All</b>.</li> <li>• For standalone agents, the group name displayed should be <b>N/A</b>.</li> </ul> |
| <b>Last connection to StellarOne</b>     |   | Indicates the last time the agent was connected with StellarOne console.  |
| <b>Application vault last updated on</b> |   | Displays the last time the application vault was updated. By clicking the link, you will be directed to the <b>OT Applications</b> tab page for viewing the details and number of the OT applications installed on the endpoint.  |
| <b>Approved List last updated on</b>     |   | Displays the last time the approved list was updated. By clicking the link, you will be directed to the <b>Approved List</b> tab page for viewing the details and number of the applications added into the approved list on this endpoint.   |

| ITEM                              | FUNCTION | DESCRIPTION   |
|-----------------------------------|----------|---|
| <b>Components last updated on</b> |          | Displays the last time the components were updated. By clicking the link, you will be directed to the <b>About</b> tab page for viewing the details of the components updated on this endpoint. |
| <b>Last blocked event</b>         |          | Clicking the link shows the most recent blocked events.   |
| <b>License expires on</b>         |          | Displays the date and time the software expires. Clicking the link shows more license information such as license edition, type, and status.  |
| <b>Device Information</b>         |          | Clicking the link shows device information about the endpoint, such as Vendor, Model, Location, and Remark.   |

**Note**

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

| LICENSE EDITION     | MAIN PROTECTION FEATURES   |
|---------------------|--|
| <b>StellarICS</b>   | <ul style="list-style-type: none"> <li>• Real-Time Scan</li> <li>• Application Lockdown</li> </ul> |
| <b>StellarKiosk</b> | Real-Time Scan   |
| <b>StellarOEM</b>   | Application Lockdown   |



## OT Applications

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

| Software                 | Vendor               | Version     | Install Path  |
|--------------------------|----------------------|-------------|---------------|
| Fisher® Specification... | Fisher Controls...   | 2.20.00     | C:\Program... |
| Winflows                 | GE                   | 1.1.37      |               |
| CitectSCADA 7.20         | Schneider Electric   | 7.20.0000   | C:\Program... |
| FANUC LADDER-III         | FANUC                | 1.00.000    | C:\Program... |
| Common Licensing         | GE Digital           | 00019.00... | C:\Program... |
| SMARTDAC+ Data...        | Yokogawa Electric... | 3.7.3       | C:\Program... |

Number of applications in Application vault: 6

**FIGURE 3-3. StellarProtect OT Applications**

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

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

## OT Certificates

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

| Issue To                      | Issued By                | Hash            |
|-------------------------------|--------------------------|-----------------|
| Beckhoff Automation GmbH &... | DigiCert SHA2 High...    | 8020A7770578... |
| General Electric Company      | Symantec Class 3...      | 5006C8F010D...  |
| SIEMENS AG                    | Symantec Class 3...      | 2FDDE9CC186...  |
| Schneider Electric            | VeriSign Class 3 Code... | 48A5F6877981... |
| Schneider Electric            | VeriSign Class 3 Code... | E776B9C503D...  |

Number of certifications: 5

**FIGURE 3-4. StellarProtect OT Certificates**

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

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

## Approved List

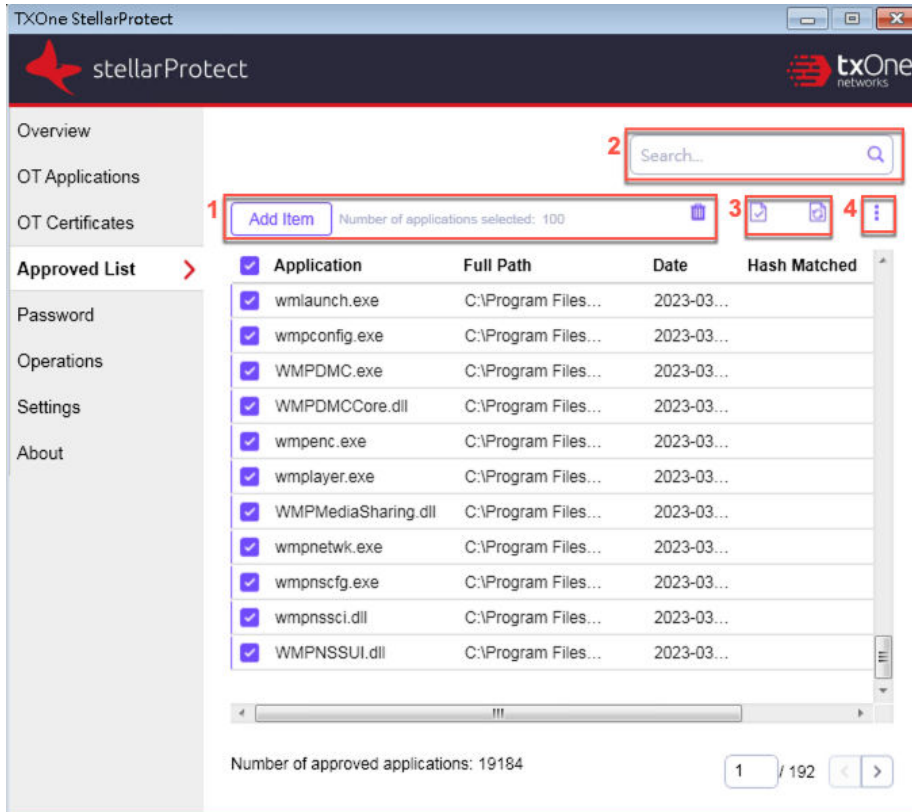
If you enabled **Creating Approved List** during the installation, applications found would be added to and shown on the **Approved List** page. The following table describes the features available on the **Approved List**.



### Note

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

---

**FIGURE 3-5. StellarProtect Approved List**




**TABLE 3-2. Approved List Item Descriptions**

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

## About Hashes

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

The following table describes the hash check status icons.

| ICON  | DESCRIPTION  |
|---|--|
|  | The calculated hash value matches the stored value.        |
|  | The calculated hash value does not match the stored value. |
|  | There was an error calculating the hash value.             |

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

### Checking or Updating Hashes

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

---

#### Procedure

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

- a. Select the target file(s). To check all files, select the check box at the top of the Approved List.
  - b. Click the **Check Hash** icon that appears at the upper right hand.
- To update the file hash values:
    - a. Select the target file(s). To check all files, select the check box at the top of the Approved List.
    - b. Click the **Update Hash** icon that appears at the upper right hand.

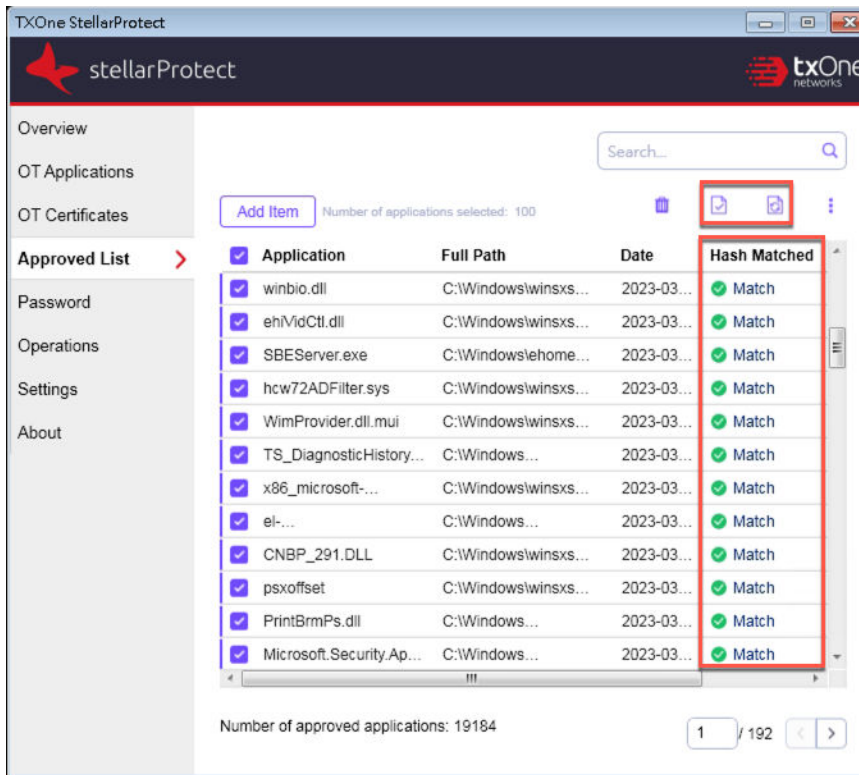
The Hash Matched column shows the hash checking or updating result.



**Important**

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

---



**FIGURE 3-6. Hash Values Matched**

## Configuring the Approved List

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

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



**Note**

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

---

## Adding or Removing Files

---

### Procedure

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

**Note**

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

---

- d. The selected applications will be listed and displayed for double-check. Confirm the items to be added, and click **Add**.
  - e. After adding the desired items to the Approved List, click **Finish**.
- To remove an item:
    - a. Search the Approved List for the application to remove.
    - b. Select the checkbox next to the file name to be removed, and click the **Delete** icon.
    - c. When asked to remove the item, click **Yes**.
    - d. Click **OK** to close the confirmation window.
- 

### Exporting or Importing the File Hashes

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

---



#### **WARNING!**

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

---

### Procedure

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

- a. Search and select the applications, or check the check box next to the **Application** header to select all files.
  - b. Click **More actions** icon at the upper right hand, and then choose **Export All Hash**.
  - c. Provide a filename and specify where to save the file.
  - d. Click **Save**.
  - e. A success message appears. Click **OK**.
- To import file hashes from an Approved List:
    - a. Click **More actions** icon at the upper right hand, and then choose **Import All Hash**.
    - b. A notification window appears. Read the message carefully and determine if you want to overwrite the existing hash values with the imported hash values generated from the same applications. Click **Continue**.

**Note**

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

---

- c. Locate the file (a .csv file) to import.
  - d. Select the file, and click **Open**.
  - e. A success message appears. Click **OK**.
- 

## Password and Account Types

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

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

- GUI: See [Account Settings on page 3-20](#)
- CLI: See [OPCmd Program Commands on page 4-4](#)

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

**TABLE 3-3. StellarProtect Account Types**

| ACCOUNT       | DETAILS   |
|---------------|---|
| Administrator | <ul style="list-style-type: none"> <li>• Default account</li> <li>• Full access to StellarProtect functions</li> <li>• Can use both the console GUI and command line interface (CLI)</li> </ul> |
| User          | <ul style="list-style-type: none"> <li>• Secondary maintenance account</li> <li>• Limited access to StellarProtect functions</li> <li>• Can only use the console GUI</li> </ul>                 |

## Account Settings

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



### Important

The StellarProtect Administrator and User passwords cannot be the same.

## Procedure

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

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

**WARNING!**

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

---

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

## Operations

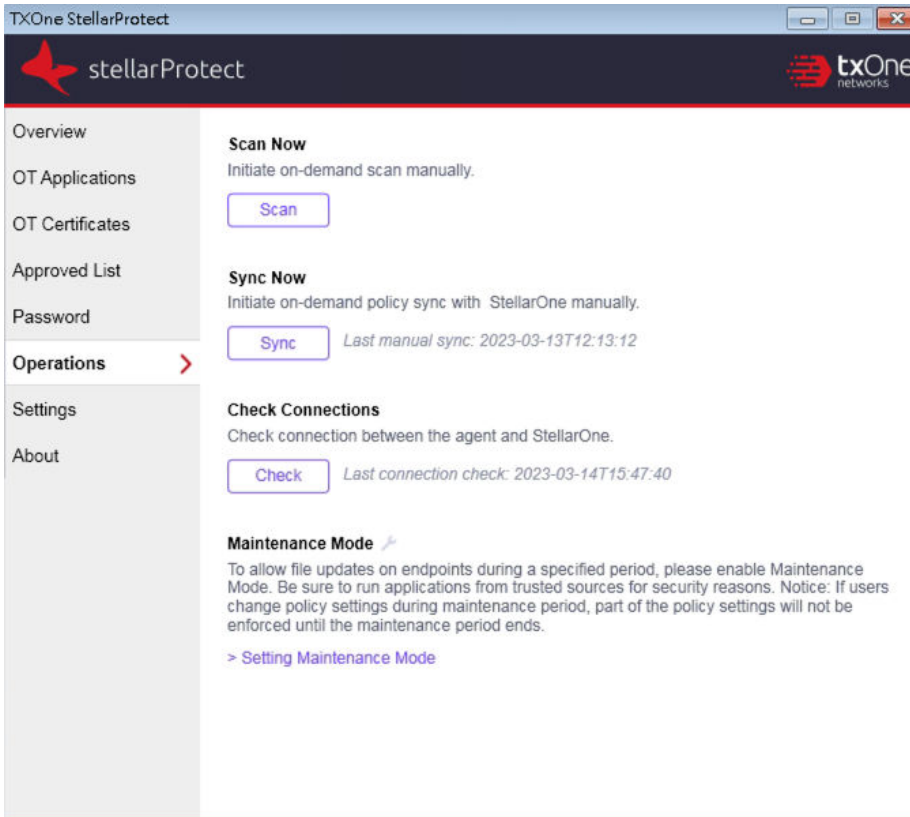
The **Operations** page provides options to perform tasks such as on-demand scan, policy sync, connection check, and maintenance mode setting.

---

**Note**

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

---



**FIGURE 3-7. StellarProtect Operations Page**

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

| ITEM     | DESCRIPTION  |
|----------|--|
| Scan Now | Click the <b>Scan</b> button to initiate on-demand scanning. See <a href="#">Scan Now on page 3-23</a> for more details.               |
| Sync Now | Click the <b>Sync</b> button to synchronize policy with StellarOne server. See <a href="#">Sync Now on page 3-24</a> for more details. |

| ITEM             | DESCRIPTION   |
|------------------|---|
| Check Connection | Click the <b>Check</b> button to check if the agent is properly connected with the StellarOne server. See <a href="#">Check Connection on page 3-24</a> for more details.                             |
| Maintenance Mode | Read the description of the Maintenance Mode carefully and click <b>Setting Maintenance Mode</b> to enable or disable it. See <a href="#">Setting Maintenance Mode on page 3-25</a> for more details. |

## Scan Now

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

### Procedure

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



#### Note

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

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

## Sync Now

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

---

### Procedure

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

## Check Connection

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

---

### Procedure

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



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

## Setting Maintenance Mode

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

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



### Note

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



---

## Procedure

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

**Note**

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

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

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

**Important**

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

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

**Note**

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

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

**Important**

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

## About Feature Settings

StellarProtect offers the following protection features.

stellaProtect bxOne networks

Overview Self-management OFF: The Agent is now following StellarOne's policy settings.

OT Applications

OT Certificates

Approved List

Password

Operations

**Settings** >

About

**Application Lockdown**

- Detect: When an application not in the Approved List launches, it is allowed and the user will receive a notification.
- Enforce: When an application not in the Approved List launches, it is blocked and the user will receive a notification.
- Disable: Application lockdown is disabled.

**Multi-method Threat Prevention**

Real-Time Scan

**Operations Behavior Anomaly Detection** (script behaviors only)

- Learn: Collect behavioral patterns from the monitored agent-device to establish the baseline fingerprint.
- Detect: Identify and send alerts for any unexpected changes and security threats by analyzing current behaviors against the fingerprint at the agent-device and central management levels.
- Enforce: Take preventative action on detected fingerprint deviations to defend operation stability and security.
- Disable

Strict mode Approved Script Behaviors (0)

Enabling Strict mode reduces the level of fingerprint deviation allowed. In more dynamic processes where devices and access behaviors are more subject to change, this may generate more events.

**OT Application Safeguard**

Protect OT applications and files / folders from unauthorized changes.

**FIGURE 3-8. StellarProtect Settings Screen**

## Application Lockdown

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

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

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

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

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

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

## Multi-Method Threat Prevention

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

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

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

## Operations Behavior Anomaly Detection

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

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

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

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

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



### Important

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

---

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

- **Strict mode:** This special mode appears when you select the **Detect** mode. Enabling the **Strict mode** reduces the level of the fingerprint deviation allowed; in other words, it performs stricter comparison between the established baseline and currently-running operational behaviors. In more dynamic operating environments where devices and access behaviors are more subject to change, this may generate more events.
- **Enforce:** In this mode, StellarProtect takes preventative action on detected fingerprint deviations to defend operation stability and security.
  - **Strict mode:** This special mode appears when you select the **Enforce** mode. Enabling the **Strict mode** reduces the level of the fingerprint deviation allowed; in other words, it performs stricter comparison between the established baseline and currently-running operational behaviors. In more dynamic operating environments where devices and access behaviors are more subject to change, this may generate more events and require more preventative actions to be taken.
- **Disable:** The Operations Behavior Anomaly Detection can also be disabled if needed, but it is recommended to have this function enabled to maintain security against behavior anomalies.

### OT Application Safeguard

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

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

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

## DLL Injection Prevention

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



### Note

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

---

## Device Control

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

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

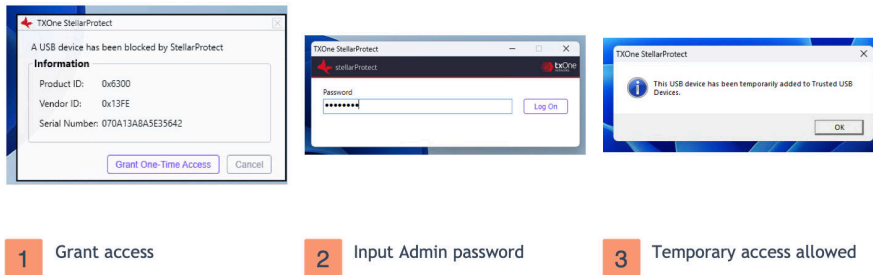
Device Control can also grant a one-time permission to an unapproved USB storage access after administrator authentication. When an unauthorized USB storage device is inserted into the endpoint the first time, the user will be prompted to enter the administrator password. This is set up as a single authorization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

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

The Device Control use case is as follows:

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

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



**FIGURE 3-9. Use Case of Device Control**

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

## Enabling or Disabling Feature Settings

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



### Note

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

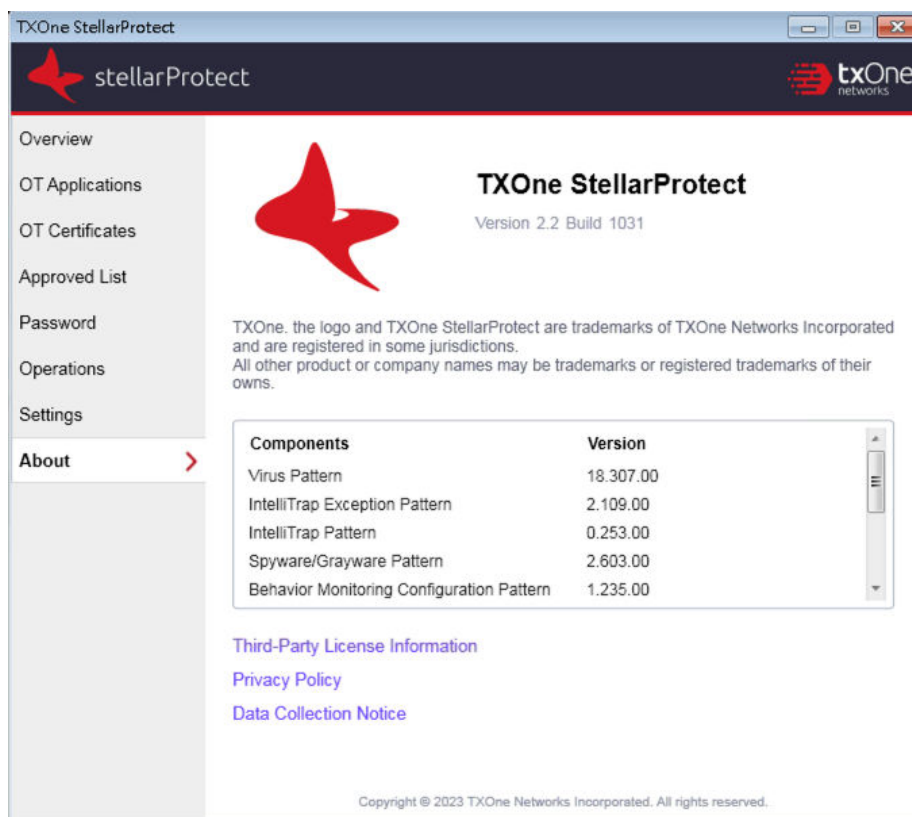
## Procedure

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



4. Check or uncheck to enable or disable the desired features.
5. Click **Save**.

## About StellarProtect



**FIGURE 3-10. About StellarProtect**

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

## Using the StellarProtect (Legacy Mode) Agent Console

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

Topics include:

- [Overview on page 3-34](#)
- [Approved List on page 3-40](#)
- [Password and Account Types on page 3-49](#)
- [Operations on page 3-52](#)
- [About Feature Settings on page 3-59](#)
- [About StellarProtect \(Legacy Mode\) on page 3-64](#)

### Overview

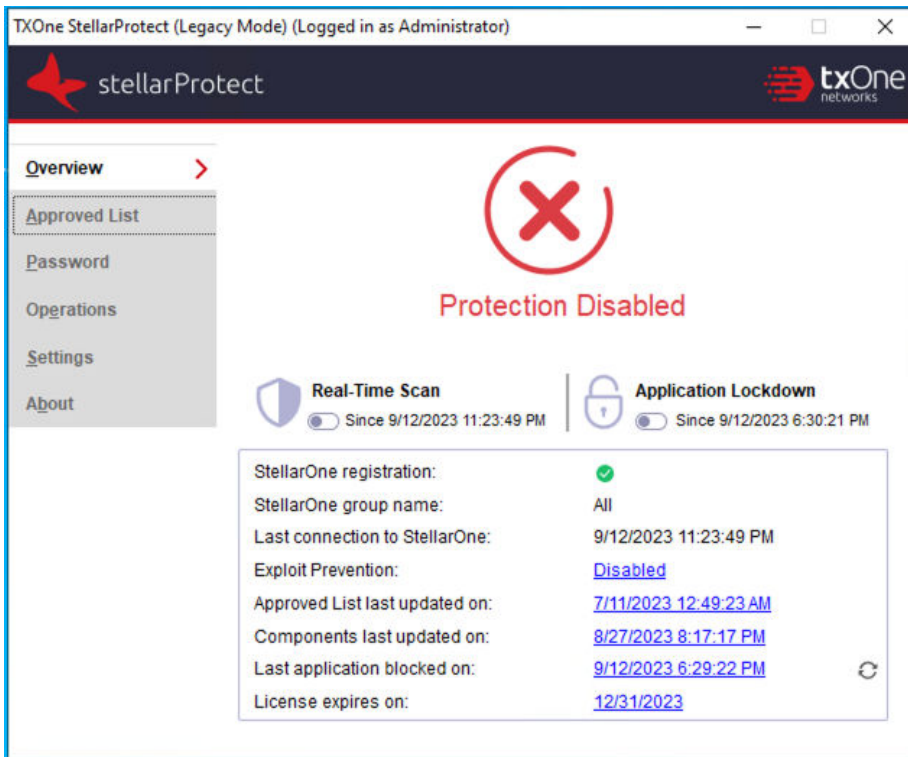
The agent console provides easy access to commonly used features in TXOne StellarProtect (Legacy Mode).

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

The screenshot displays the TXOne StellarProtect (Legacy Mode) console interface. The window title is "TXOne StellarProtect (Legacy Mode) (Logged in as Administrator)". The interface features a dark header with the "stellarProtect" logo on the left and the "txOne networks" logo on the right. A left-hand navigation menu includes "Overview" (selected), "Approved List", "Password", "Operations", "Settings", and "About". The main content area shows a large green checkmark icon with the text "Protection Enabled" below it. Two toggle switches are visible: "Real-Time Scan" (turned on) and "Application Lockdown" (turned off), both with a timestamp of "Since 9/12/2023 9:51:56 AM". Below these is a summary box containing the following information:

|                                |                                       |
|--------------------------------|---------------------------------------|
| StellarOne registration:       | ✓                                     |
| StellarOne group name:         | All                                   |
| Last connection to StellarOne: | 9/12/2023 11:44:19 AM                 |
| Exploit Prevention:            | <a href="#">Disabled</a>              |
| Approved List last updated on: | <a href="#">9/12/2023 11:39:49 AM</a> |
| Components last updated on:    | <a href="#">9/12/2023 11:44:59 AM</a> |
| Last application blocked on:   | <a href="#">N/A</a>                   |
| License expires on:            | <a href="#">12/19/2023</a>            |

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





**FIGURE 3-12. Overview of StellarProtect (Legacy Mode) Console - Protection Disabled**

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

**TABLE 3-4. Overview Item Descriptions**

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

| ITEM                      | FUNCTION                | DESCRIPTION  |
|---------------------------|-------------------------|--|
|                           | <b>Password</b>         | <p>Enables administrators to change the StellarProtect (Legacy Mode) Administrator or User passwords.</p> <hr/> <p> <b>Note</b><br/>Only users logged in as the administrator can change the passwords.</p> <hr/>   |
|                           | <b>Operations</b>       | Provides options to perform tasks such as on-demand scan, policy sync, connection check, and maintenance mode setting.   |
|                           | <b>Settings</b>         | Enables or disables vulnerability protection settings and exports or imports the system configuration.   |
|                           | <b>About</b>            | Displays the product information and component version numbers   |
| <b>Status Information</b> | <b>Protection Check</b> | <ul style="list-style-type: none"> <li>• The green check indicates the Real-time Scan and/or Application Lockdown are/is enabled</li> <li>• The red cross indicates main protection features have been turned off and the endpoint may be vulnerable to security threats</li> </ul>  |
|                           | <b>Real-Time Scan</b>   | <p>Enables users to toggle on the <b>Real-Time Scan</b> function, which provides persistent and ongoing file scan for the endpoints when a file is received, opened, downloaded, copied, or modified.</p> <hr/> <p> <b>Tip</b><br/>The date and time that the Real-Time Scan was last turned on or off are shown next to the toggle switch.</p> <hr/> |

| ITEM                           | FUNCTION                    | DESCRIPTION  |
|--------------------------------|-----------------------------|--|
|                                | <b>Application Lockdown</b> | <p>Enables users to toggle on the <b>Application Lockdown</b> function, which locks down the system, blocking applications not on the Approved List from running.</p> <hr/> <p> <b>Note</b><br/>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.</p> <hr/> <p> <b>Tip</b><br/>The date and time that the Application Lockdown was last turned on or off are shown next to the toggle switch.</p> <hr/> |
| <b>StellarOne registration</b> |                             | 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.  |
| <b>StellarOne group name</b>   |                             | 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.  |

| ITEM                                 | FUNCTION                             | DESCRIPTION  |
|--------------------------------------|--------------------------------------|--|
| <b>Last connection to StellarOne</b> |                                      | Indicates the last time the agent was connected with StellarOne console  |
| <b>Exploit Prevention</b>            |                                      | <ul style="list-style-type: none"> <li>• <b>Enabled:</b> All Exploit Prevention features are enabled. Click the status to open the settings screen.</li> <li>• <b>Enabled (Partly):</b> Some Exploit Prevention features are enabled. Click the status to open the settings screen.</li> <li>• <b>Disabled:</b> No Exploit Prevention features are enabled. Click the status to open the settings screen.</li> </ul> |
| <b>Approved List status</b>          | <b>Approved List last updated on</b> | Click the corresponding last updated date to open the <b>Approved List</b> and view details.   |
| <b>Components last updated on</b>    |                                      | Displays the last time the components were updated. By clicking the link, you will be directed to the <b>About</b> tab page for viewing the details of the components updated on this endpoint.  |
| <b>Approved List status</b>          | <b>Last application blocked on</b>   | Click the corresponding last application blocked date to open the <b>Blocked Application Event Log</b> and view details.   |
| <b>License expires on</b>            |                                      | 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.   |

**Note**

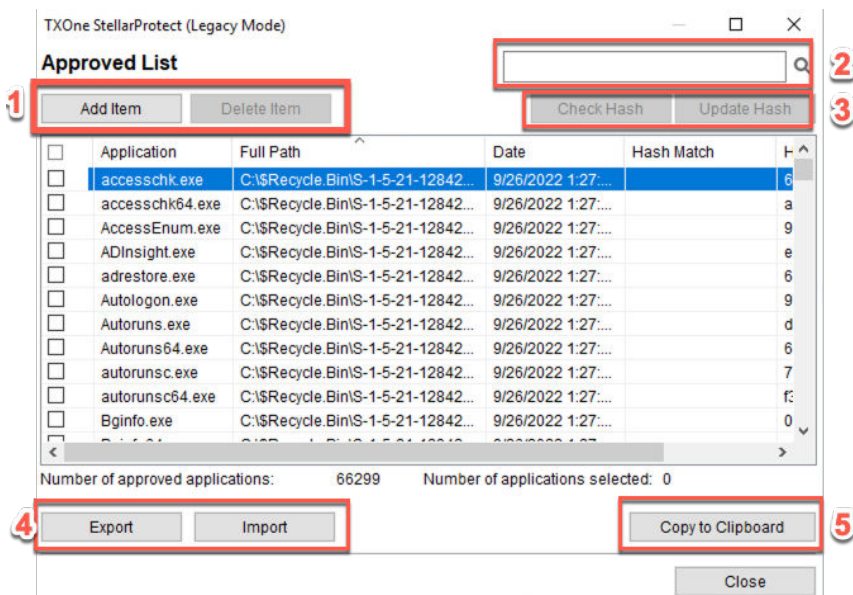
The Overview displays different protection features depending on different license editions:

| LICENSE EDITION     | MAIN PROTECTION FEATURES  |
|---------------------|---|
| <b>StellarICS</b>   | <ul style="list-style-type: none"><li>• Real-Time Scan</li><li>• Application Lockdown</li></ul> |
| <b>StellarKiosk</b> | <ul style="list-style-type: none"><li>• Real-Time Scan</li><li>• Application Lockdown</li></ul> |
| <b>StellarOEM</b>   | Application Lockdown  |

## Approved List

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





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

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

**TABLE 3-5. Approved List Item Descriptions**




| # | ITEM                            | DESCRIPTION   |
|---|---------------------------------|---|
| 1 | <b>Add Item / Delete Item</b>   | Adds or removes selected items to or from the Approved List   |
| 2 | <b>Search Bar</b>               | Searches the Application and File Path columns  |
| 3 | <b>Check Hash / Update Hash</b> | Checks or updates the hash values for applications in the Approved List<br><br>For more details, see: <ul style="list-style-type: none"> <li>• <a href="#">About Hashes on page 3-42</a></li> <li>• <a href="#">Checking or Updating Hashes on page 3-42</a></li> </ul> |

| # | ITEM                     | DESCRIPTION   |
|---|--------------------------|---|
| 4 | <b>Export / Import</b>   | Exports or imports the Approved List using a SQL database (.db) file  |
| 5 | <b>Copy to Clipboard</b> | Copies the Approved List to the clipboard with comma separated values (CSV) format for easy review or reporting |

## About Hashes

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

The following table describes the hash check status icons.

| ICON  | DESCRIPTION  |
|---|--|
|  | The calculated hash value matches the stored value.        |
|  | The calculated hash value does not match the stored value. |
|  | There was an error calculating the hash value.             |

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

## Checking or Updating Hashes

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

---

## Procedure

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

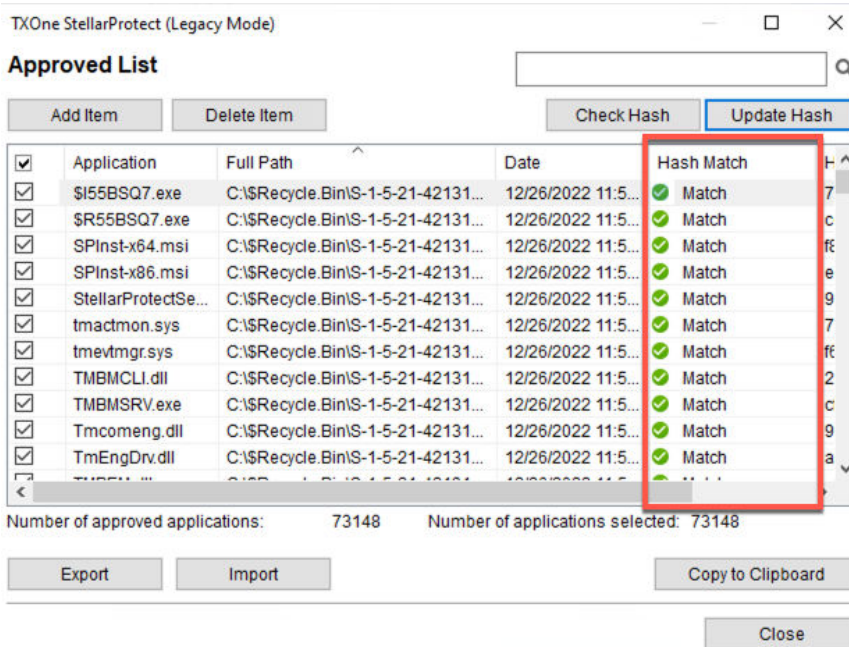
The Hash Match column shows the hash checking or updating result.



### Important

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

---



**FIGURE 3-14.** Hash Values Matched

## Configuring the Approved List

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

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

| OPTION                                  | WHEN TO USE  |
|---|--|
| <b>Manually browse and select files</b> | <p>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.</p> <p>For example, if Windows Media Player (<code>wmp\layer.exe</code>) is not in the Approved List after initial setup, users can add it to the list using the console.</p> |

| OPTION  | WHEN TO USE  |
|---|--|
| <p><b>Automatically add files created or modified by the selected application installer</b><br/>(using the Trusted Updater)</p> | <p>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.</p> <p>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.</p> |

**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, and click **OK**.
- If you choose **All applications in a specified path**, specify the file or folder path in the text field displayed, and click **OK**.



**Note**

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

---

- d. Click **OK**.
  - e. The selected applications will be listed and displayed for double-check. Confirm the items to be added, and click **Approve**.
  - f. After adding the desired items to the Approved List, click **Close**.
- To remove an item:
    - a. Search the Approved List for the application to remove.
    - b. Select the check box next to the file name to be removed, and click **Delete Item**.
    - c. When asked to remove the item, click **OK**.
    - d. Click **OK** again to close the confirmation window.

---

### Updating or Installing Using the Trusted Updater

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

---

## Procedure

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

**Note**

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

---

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

## Exporting or Importing the Approved List

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



### **WARNING!**

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

---

## Procedure

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

The exported file includes the following information:

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



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

## Password and Account Types

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

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

- GUI: See [Account Settings on page 3-51](#)

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

TXOne StellarProtect (Legacy Mode) (Logged in as Administrator)

stellarProtect txOne networks

Administrator User

Old password

New password

Confirm password

The password must be 8 to 64 alphanumeric characters. The following characters are not supported: | > < \ " spaces.

Save

**FIGURE 3-15. Password Screen**

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

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

| ACCOUNT       | DETAILS   |
|---------------|---|
| Administrator | <ul style="list-style-type: none"> <li>• Default account</li> <li>• Full access to StellarProtect (Legacy Mode) functions</li> <li>• Can use both the console GUI and command line interface (CLI)</li> </ul> |
| User          | <ul style="list-style-type: none"> <li>• Secondary maintenance account</li> <li>• Limited access to StellarProtect (Legacy Mode) functions</li> <li>• Can only use the console GUI</li> </ul>                 |

## Account Settings

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



### Important

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

## Procedure

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

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



**WARNING!**

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

---

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

## Operations

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

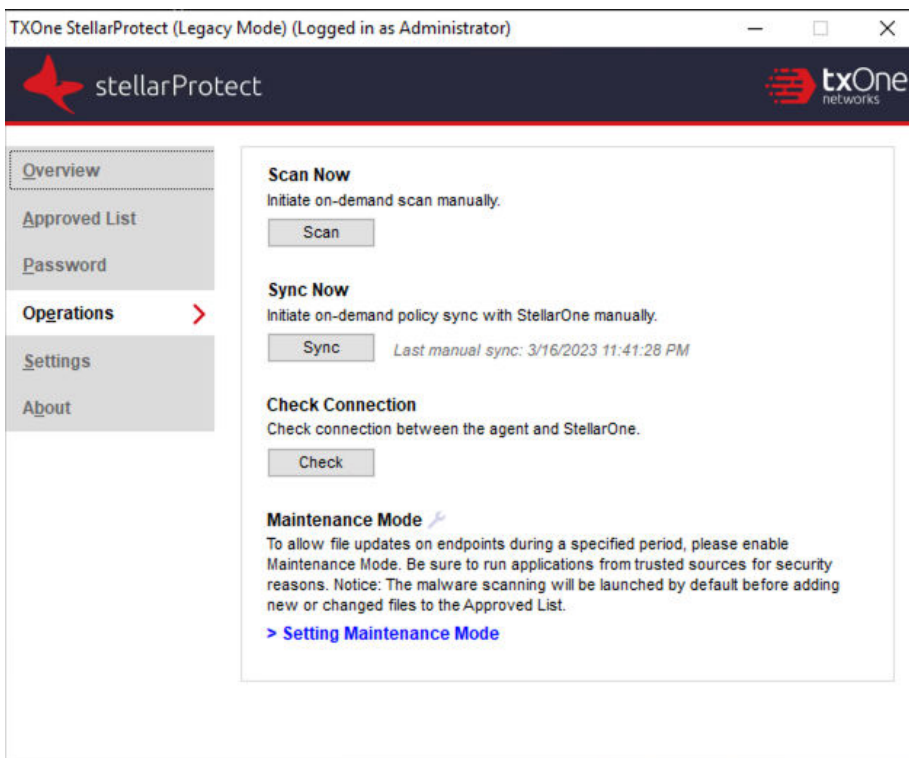
---



**Note**

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

---



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

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

| ITEM             | DESCRIPTION   |
|------------------|---|
| Scan Now         | Click the <b>Scan</b> button to initiate on-demand scanning. See <a href="#">Scan Now on page 3-54</a> for more details.  |
| Sync Now         | Click the <b>Sync</b> button to synchronize policy with StellarOne server. See <a href="#">Sync Now on page 3-55</a> for more details.                                    |
| Check Connection | Click the <b>Check</b> button to check if the agent is properly connected with the StellarOne server. See <a href="#">Check Connection on page 3-55</a> for more details. |

| ITEM             | DESCRIPTION   |
|------------------|---|
| Maintenance Mode | Read the description of the Maintenance Mode carefully and click <b>Setting Maintenance Mode</b> to enable or disable it. See <a href="#">Setting Maintenance Mode on page 3-56</a> for more details. |

## Scan Now

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

---

### Procedure

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



#### Note

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

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

## Sync Now

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

---

### Procedure

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

## Check Connection

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

---

### Procedure

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

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

## Setting Maintenance Mode

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

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

---



### Important

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

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



### Note

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



---



## Procedure

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



### Note

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

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

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



### Important

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

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

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



**Note**

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

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



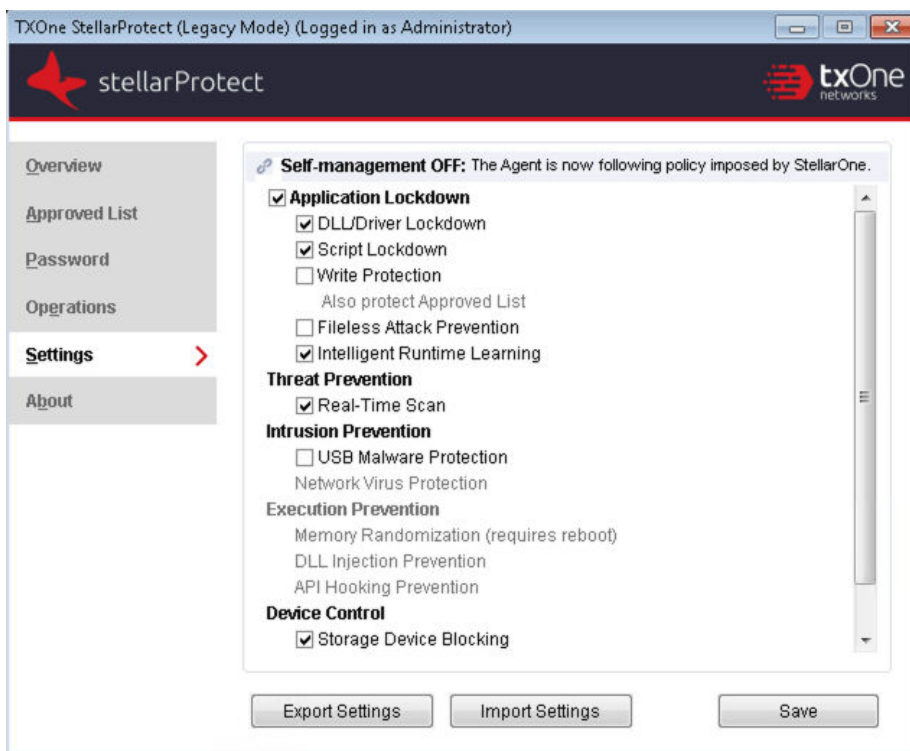
**Important**

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

---


## About Feature Settings

StellarProtect (Legacy Mode) offers the following protection features.



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


**TABLE 3-8. Application Lockdown**

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

**TABLE 3-9. Threat Prevention**


| SETTING        | DESCRIPTION  |
|----------------|--|
| Real-Time Scan | <p>Real-time Scan provides persistent and ongoing file scan for the endpoints. Each time a file is received, opened, downloaded, copied, or modified, Real-Time Scan always scans the file for security assessment. If a security risk or possible virus/malware has been detected during the scanning, a notification message appears indicating the name of the infected file and the specific security risk.</p> <p>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.</p> |

**TABLE 3-10. Execution Prevention**

| SETTING              | DESCRIPTION  |
|----------------------|--|
| Memory Randomization | <p>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.</p> <p>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.</p> <hr/> <p> <b>Note</b><br/>The endpoint must be restarted to enable or disable Memory Randomization.</p> |

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

**TABLE 3-11. Device Control & Other**

| SETTING                 | DESCRIPTION   |
|-------------------------|---|
| Storage Device Blocking | Blocks storage devices, including USB drives, CD/DVD drives, and floppy disks from accessing the managed endpoint.  |
| Integrity Monitoring    | <p>Integrity Monitoring logs events related to changes for files, folders, and the registry on the managed endpoint.</p> <hr/> <p> <b>Note</b><br/>To view Integrity Monitoring logs on the managed endpoint, go to <b>Start &gt; Control Panel &gt; Administrative Tools</b> and access Event Viewer.</p> |

See [Enabling or Disabling Feature Settings on page 3-63](#) for how to enable or disable the feature settings.

---

## Enabling or Disabling Feature Settings

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

**Note**

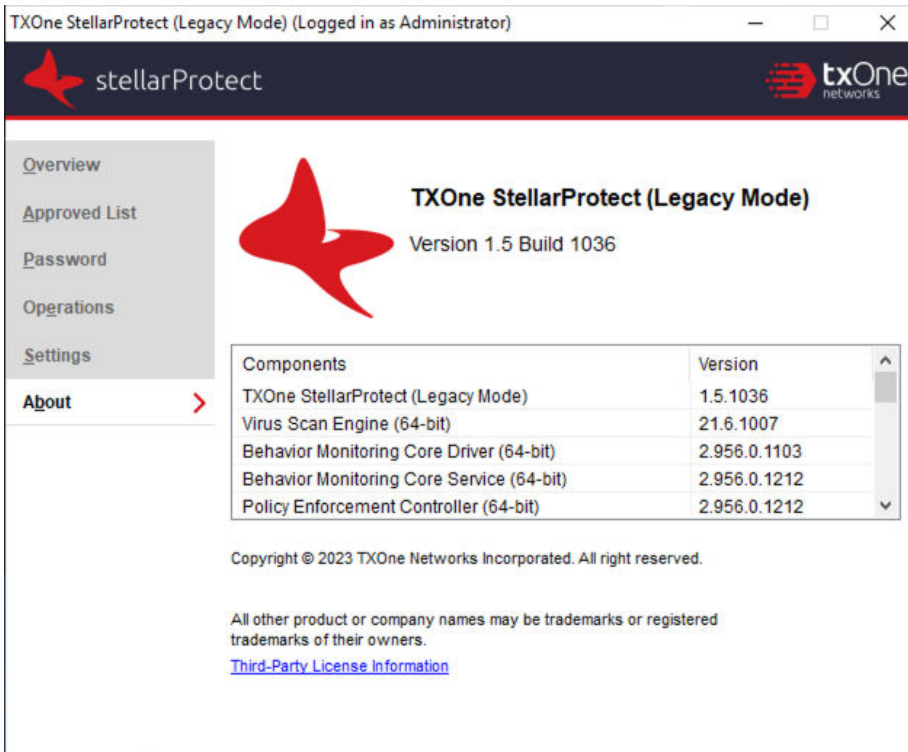
By default, TXOne StellarProtect (Legacy Mode) enables the DLL/Driver Lockdown and Script Lockdown features under the Application Lockdown.

---

### Procedure

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

## About StellarProtect (Legacy Mode)



| Components                                | Version      |
|---|--------------|
| TXOne StellarProtect (Legacy Mode)        | 1.5.1036     |
| Virus Scan Engine (64-bit)                | 21.6.1007    |
| Behavior Monitoring Core Driver (64-bit)  | 2.956.0.1103 |
| Behavior Monitoring Core Service (64-bit) | 2.956.0.1212 |
| Policy Enforcement Controller (64-bit)    | 2.956.0.1212 |

Copyright © 2023 TXOne Networks Incorporated. All right reserved.

All other product or company names may be trademarks or registered trademarks of their owners.

[Third-Party License Information](#)

**FIGURE 3-18. About StellarProtect (Legacy Mode)**

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



# Chapter 4

## Using the Agent Command Line Interface (CLI)

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

Topics in this chapter include:

- *Using StellarProtect Command Line Interface (CLI) on page 4-2*
- *Using StellarProtect (Legacy Mode) Command Line Interface (CLI) on page 4-16*

## Using StellarProtect Command Line Interface (CLI)

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

Topics include:

- [Using OPCmd at the Command Line Interface \(CLI\) on page 4-2](#)
- [Overview of StellarProtect CLI on page 4-2](#)
- [OPCmd Program Commands on page 4-4](#)

## Using OPCmd at the Command Line Interface (CLI)

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

---

### Procedure

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

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

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

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

## Overview of StellarProtect CLI

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

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

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

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

### Options

Separate long option and argument with an equal sign:

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

Argument follows the option character immediately:

```
-o<argument>
```

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

```
-o <argument>
```



#### Important

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

---

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

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

### Global Options

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

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

Argument: No

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

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



#### Note

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

Argument: Optional. Password in plain text.

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


Description: Show CLI program version.



Argument: No

## OPCmd Program Commands


**TABLE 4-1. List of All Commands**

| COMMAND                                 | DESCRIPTION   | OPTIONS |
|---|---|---------|
| <code>opcnd.exe about components</code> | You can browse versions of components from the GUI program, or you can get the list in YAML format with this command. | None    |

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


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


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

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



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

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

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

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

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

| COMMAND  | DESCRIPTION  | OPTIONS   |
|--|--|---|
| <code>opcmod.exe -p quarantine restore [QUARANTINENAME]</code> | Restores the specified quarantined file                      | None  |
| <code>opcmod.exe -p udso list</code>                           | Lists user-defined suspicious objects                        | <ul style="list-style-type: none"><li>-a, --all: Lists all types of suspicious objects.</li><li>-p, --file-path: Lists file path to the suspicious objects</li><li>-h, --file-sha1: Lists file SHA1 of the suspicious objects.</li><li>-H, --file-sha2: Lists file SHA2 of the suspicious objects</li></ul> |
| <code>opcmod.exe -p udso scan</code>                           | Scans existing processes for user-defined suspicious objects | You'll be asked for confirmation before terminating these suspicious processes.   |

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

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

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

Topics include:

- [Using SLCmd at the Command Line Interface \(CLI\) on page 4-16](#)
- [SLCmd Program and Console Function Comparison on page 4-16](#)
- [SLCmd Program Commands on page 4-19](#)

### 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.



| <b>FUNCTION</b>  | <b>SLCMD PROGRAM AT THE<br/>COMMAND LINE INTERFACE<br/>(CLI)</b> | <b>CONSOLE</b> |
|--|--|----------------|
| Account management                                       | Yes  | Yes            |
| Agent event aggregation                                  | No   | No             |
| Approved List management                                 | Yes  | Yes            |
| Decrypt/Encrypt<br>configuration file                    | Yes  | No             |
| Display the blocked log                                  | Yes  | Yes            |
| Export/Import Approved List                              | Yes  | Yes            |
| Export/Import configuration                              | Yes  | Yes            |
| Policy sync  | No   | Yes            |
| 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<br>Lockdown                      | Yes  | Yes            |
| Enable/disable pop-up<br>notifications for blocked files | Yes  | No             |

| FUNCTION                   | SLCMD PROGRAM AT THE COMMAND LINE INTERFACE (CLI) | CONSOLE |
|----------------------------|---|---------|
| Start/Stop Trusted Updater | Yes   | Yes     |
| Trusted Hash List          | Yes   | No      |
| Start/Stop the service     | Yes   | No      |
| Uninstall                  | No  | No      |
| Storage Device Control     | Yes   | Yes     |
| Fileless Attack Prevention | Yes   | Yes     |
| Add Trusted USB Device     | Yes   | No      |
| Configure Maintenance Mode | Yes   | Yes     |
| On-demand Scan             | Yes   | Yes     |
| Check connection           | Yes   | Yes     |
| Real-Time Scan             | Yes   | Yes     |

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

## Overview of StellarProtect (Legacy Mode) CLI

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

**Note**

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

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

**General Commands**

Perform general actions using the Command Line Interface.

The following table lists the available abbreviated forms of parameters.

**TABLE 4-2. Abbreviations and Uses**


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


**SLCmd Program Commands**

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

**TABLE 4-3. General Commands**

| COMMAND           | PARAMETER      | DESCRIPTION   |
|-------------------|----------------|---|
| help              |                | <p>Display a list of StellarProtect (Legacy Mode) commands</p> <p>For example, type:</p> <pre>SLCmd.exe help</pre>  |
| activate          | <license_key>  | <p>Activate the StellarProtect (Legacy Mode) program using the specified license key.</p> <p>For example, type:</p> <pre>SLCmd.exe activate XX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX</pre>   |
| set adminpassword | <new_password> | <p>Prompt the currently logged on administrator to specify a new password</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set adminpassword</pre> <p>Change the currently logged on administrator password to the newly specified password</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set adminpassword P@ssW0Rd</pre> |

| COMMAND  | PARAMETER | DESCRIPTION   |
|----------|-----------|---|
| set lock |           | <p>Display the current StellarProtect (Legacy Mode) Application Lockdown status</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set lock</pre> <hr/> <p> <b>Note</b><br/>The default status is "disable".</p> |
|          | enable    | <p>Turn on Application Lockdown</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set lock enable</pre>  |
|          | disable   | <p>Turn off Application Lockdown</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set lock disable</pre>  |

| COMMAND                        | PARAMETER | DESCRIPTION  |
|--------------------------------|-----------|--|
| set<br>blockedfilenotification |           | <p>Display the current notification setting</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set blockedfilenotification</pre> <hr/> <p> <b>Note</b><br/>The default status is "disable".</p> |
|                                | enable    | <p>Display a notification on the managed endpoint when StellarProtect (Legacy Mode) blocks a file.</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set blockedfilenotification enable</pre>   |
|                                | disable   | <p>Do not display any notification when StellarProtect (Legacy Mode) blocks a file.</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set blockedfilenotification disable</pre>   |

| COMMAND         | PARAMETER | DESCRIPTION   |
|-----------------|-----------|---|
| show blockedlog |           | <p>Display a list of applications blocked by StellarProtect (Legacy Mode)</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; show blockedlog</pre>                      |
| show license    |           | <p>Display the current StellarProtect (Legacy Mode) license information</p> <p>For example, type:</p> <pre>SLCmd.exe show license</pre>   |
| show settings   |           | <p>Display the current status of the vulnerability attack prevention features</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; show settings</pre>                    |
| start service   |           | <p>Start the StellarProtect (Legacy Mode) service</p> <p>For example, type:</p> <pre>SLCmd.exe start service</pre>  |
| status          |           | <p>Display the current status of Application Lockdown and the auto update function of the Approved List</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; status</pre> |

| COMMAND      | PARAMETER | DESCRIPTION   |
|--------------|-----------|---|
| stop service |           | <p>Stop the StellarProtect (Legacy Mode) service</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; stop service</pre>                      |
| version      |           | <p>Display the current versions of StellarProtect (Legacy Mode) components</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; version</pre> |

### Central Management Commands

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

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

To illustrate, if users want to test the agent-server connection, type:

```
SLCmd.exe -p <admin_password> test mm
```

The following table lists the available abbreviated forms of parameters.

**TABLE 4-4. Abbreviations and Uses**


| PARAMETER                | ABBREVIATION | USE                             |
|--------------------------|--------------|---------------------------------|
| managedmodeconfiguration | mmc          | Manage the configuration file   |
| servercertification      | sc           | Manage server certificate files |
| managedmode              | mm           | Manage agent "Managed Mode"     |

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



**TABLE 4-5. Central Management Commands**

| COMMAND                             | PARAMETER   | DESCRIPTION  |
|-------------------------------------|---|--|
| decrypt<br>managedmodeconfiguration | <path_of_encrypted_file<br>><br><br><path_of_decrypted_output_file> | Decrypt the configuration file used by Managed Mode                |
| encrypt<br>managedmodeconfiguration | <path_of_file><br><br><path_of_encrypted_output_file>               | Encrypt the configuration file used by Managed Mode                |
| export<br>managedmodeconfiguration  | <path_of_encrypted_output>  | Export the encrypted configuration file used by Managed Mode       |
| export<br>servercertification       | <path_of_certificate_file>  | Export the encrypted StellarOne SSL communication certificate file |
| import<br>managedmodeconfiguration  | <path_of_encrypted_input>   | Import the encrypted configuration file used by Managed Mode       |
| import<br>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>] | <p>Enable Managed Mode</p> <hr/>  <b>Note</b><br>The default status is "disable".<br><br>The following optional parameters are available: <ul style="list-style-type: none"> <li>• -cfg &lt;path_of_encrypted_file&gt;<br/>Use -cfg value to specify the path of the configuration file</li> <li>• -sc &lt;path_of_certificate_file&gt;<br/>Use -sc value to specify the path of the certificate file</li> </ul> |
| set managedmode               |   | Display the current Managed Mode status   |
| show managedmodeconfiguration |   | Display the configuration used by Managed Mode  |
| test managedmode              |   | Connect a test Managed Mode session with StellarOne server  |

## Optional Feature Commands

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

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

The following table lists the available abbreviated forms of parameters.


**TABLE 4-6. Abbreviations and Uses**


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



| PARAMETER                                | ABBREVIATION | USE  |
|--|--------------|--|
| writeprotection-<br>includesapprovedlist | wpal         | Manage Write Protection<br>including the Approved List |


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


**TABLE 4-7. Optional Feature Commands**

| COMMAND                     | PARAMETER | DESCRIPTION   |
|-----------------------------|-----------|---|
| set<br>apihookingprevention |           | Display the current status of<br>API Hooking Prevention<br><br>For example, type:<br><br><code>SLCmd.exe -p<br/>&lt;admin_password&gt; set<br/>apihookingprevention</code>  |
|                             | enable    | Enable API Hooking<br>Prevention<br><br>For example, type:<br><br><code>SLCmd.exe -p<br/>&lt;admin_password&gt; set<br/>apihookingprevention<br/>enable</code><br><br> <b>Note</b><br>The default status is<br>"disable". |
|                             | disable   | Disable API Hooking<br>Prevention<br><br>For example, type:<br><br><code>SLCmd.exe -p<br/>&lt;admin_password&gt; set<br/>apihookingprevention<br/>disable</code>  |


| COMMAND          | PARAMETER  | DESCRIPTION   |
|------------------|------------|---|
| set customaction |            | <p>Display the current setting for actions taken when StellarProtect (Legacy Mode) blocks specific types of events</p> <hr/> <p> <b>Note</b><br/>The default setting is "ask".</p>   |
|                  | ignore     | <p>Ignore blocked files or processes when Application Lockdown blocks any of the following events:</p> <ul style="list-style-type: none"> <li>• Process launch</li> <li>• DLL loading</li> <li>• Script file access</li> </ul> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set customaction ignore</pre>         |
|                  | quarantine | <p>Quarantine blocked files or processes when Application Lockdown blocks any of the following events:</p> <ul style="list-style-type: none"> <li>• Process launch</li> <li>• DLL loading</li> <li>• Script file access</li> </ul> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set customaction quarantine</pre> |


| COMMAND               | PARAMETER | DESCRIPTION   |
|-----------------------|-----------|---|
|                       |           |  <b>Note</b><br>StellarProtect (Legacy Mode) does not support a custom action of "quarantine" on Windows (Standard) XP Embedded SP1.   |
| set dlldriverlockdown | ask       | Ask what to do for blocked files or processes when Application Lockdown blocks any of the following events: <ul style="list-style-type: none"> <li>• Process launch</li> <li>• DLL loading</li> <li>• Script file access</li> </ul> For example, type:<br><pre>SLCmd.exe -p &lt;admin_password&gt; set customaction ask</pre> |
|                       | enable    | Display the current status of DLL/Driver Lockdown<br>For example, type:<br><pre>SLCmd.exe -p &lt;admin_password&gt; set dlldriverlockdown</pre> <hr/>  <b>Note</b><br>The default status is "enable".                                      |


| COMMAND                       | PARAMETER | DESCRIPTION  |
|-------------------------------|-----------|--|
|                               |           | For example, type:<br><pre>SLCmd.exe -p &lt;admin_password&gt; set dlldriverlockdown enable</pre>  |
|                               | disable   | Disable DLL/Driver Lockdown<br><br>For example, type:<br><pre>SLCmd.exe -p &lt;admin_password&gt; set dlldriverlockdown disable</pre>  |
| set<br>dllinjectionprevention |           | Display the current status of<br>DLL Injection Prevention<br><br>For example, type:<br><pre>SLCmd.exe -p &lt;admin_password&gt; set dllinjectionprevention</pre> <hr/>  <b>Note</b><br>The default status is "disable". <hr/> |
|                               | enable    | Enable DLL Injection<br>Prevention<br><br>For example, type:<br><pre>SLCmd.exe -p &lt;admin_password&gt; set dllinjectionprevention enable</pre>   |
|                               | disable   | Disable DLL Injection<br>Prevention<br><br>For example, type:  |



| COMMAND                 | PARAMETER | DESCRIPTION   |
|-------------------------|-----------|---|
|                         |           | <pre>SLCmd.exe -p &lt;admin_password&gt; set dllinjectionprevention disable</pre>   |
| set exceptionpath       |           | <p>Display current setting for using exceptions to Application Lockdown</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set exceptionpath</pre> <hr/> <p> <b>Note</b><br/>The default setting is "disable".</p> |
|                         | enable    | <p>Enable exceptions to Application Lockdown</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set exceptionpath enable</pre>  |
|                         | disable   | <p>Disable exceptions to Application Lockdown</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set exceptionpath disable</pre>  |
| set integritymonitoring |           | <p>Display the current status of Integrity Monitoring</p> <p>For example, type:</p>   |




| COMMAND                 | PARAMETER | DESCRIPTION   |
|-------------------------|-----------|---|
|                         |           | <pre>SLCmd.exe -p &lt;admin_password&gt; set integritymonitoring</pre> <hr/>  <b>Note</b><br>The default setting is "disable".   |
|                         | enable    | Enable Integrity Monitoring<br>For example, type:<br><pre>SLCmd.exe -p &lt;admin_password&gt; set integritymonitoring enable</pre>  |
|                         | disable   | Disable Integrity Monitoring<br>For example, type:<br><pre>SLCmd.exe -p &lt;admin_password&gt; set integritymonitoring disable</pre>  |
| set memoryrandomization |           | Display the current status of Memory Randomization<br>For example, type:<br><pre>SLCmd.exe -p &lt;admin_password&gt; set memoryrandomization</pre> <hr/>  <b>Note</b><br>The default setting is "disable". |
|                         | enable    | Enable Memory Randomization   |

| COMMAND    | PARAMETER | DESCRIPTION  |
|------------|-----------|--|
|            |           | For example, type:<br><pre>SLCmd.exe -p &lt;admin_password&gt; set memoryrandomization enable</pre>  |
|            | disable   | Disable Memory Randomization<br>For example, type:<br><pre>SLCmd.exe -p &lt;admin_password&gt; set memoryrandomization disable</pre>   |
| set script |           | Display the current status of Script Lockdown<br>For example, type:<br><pre>SLCmd.exe -p &lt;admin_password&gt; set script</pre> <hr/>  <b>Note</b><br>The default setting is "enable". <hr/> |
|            | enable    | Enable Script Lockdown<br>For example, type:<br><pre>SLCmd.exe -p &lt;admin_password&gt; set script enable</pre>   |
|            | disable   | Disable Script Lockdown<br>For example, type:  |

| COMMAND                              | PARAMETER | DESCRIPTION  |
|--------------------------------------|-----------|--|
|                                      |           | <pre>SLCmd.exe -p &lt;admin_password&gt; set script disable</pre>  |
| <pre>set storagedeviceblocking</pre> |           | <p>Display the current status of Storage Device Blocking</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set storagedeviceblocking</pre> <hr/> <p> <b>Note</b><br/>The default setting is "disable".</p> |
|                                      | enable    | <p>Enable Storage Device Blocking</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set storagedeviceblocking enable</pre>  |
|                                      | disable   | <p>Disable Storage Device Blocking</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set storagedeviceblocking disable</pre>  |
| <pre>set usbmalwareprotection</pre>  |           | <p>Display the current status of USB Malware Protection</p> <p>For example, type:</p>  |

| COMMAND             | PARAMETER | DESCRIPTION   |
|---------------------|-----------|---|
|                     |           | <pre>SLCmd.exe -p &lt;admin_password&gt; set usbmalwareprotection</pre> <hr/>  <b>Note</b><br>The default setting is "disable".  |
|                     | enable    | Enable USB Malware Protection<br><br>For example, type:<br><br><pre>SLCmd.exe -p &lt;admin_password&gt; set usbmalwareprotection enable</pre>   |
|                     | disable   | Disable USB Malware Protection<br><br>For example, type:<br><br><pre>SLCmd.exe -p &lt;admin_password&gt; set usbmalwareprotection disable</pre>   |
| set writeprotection |           | Display the current status of Write Protection<br><br>For example, type:<br><br><pre>SLCmd.exe -p &lt;admin_password&gt; set writeprotection</pre> <hr/>  <b>Note</b><br>The default setting is "disable". |

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

| COMMAND | PARAMETER | DESCRIPTION  |
|---------|-----------|--|
|         |           | SLCmd.exe -p<br><admin_password> set<br>writeprotection-<br>includesapprovedlist<br>enable   |
|         | disable   | Disable protection of the Approved List (in addition to the Write Protection List) when Write Protection is enabled<br><br>For example, type:<br><br>SLCmd.exe -p<br><admin_password> set<br>writeprotection-<br>includesapprovedlist<br>disable |

### User Account Commands

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

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


The following table lists the available abbreviated forms of parameters.

**TABLE 4-8. Abbreviations and Uses**

| PARAMETER    | ABBREVIATION | USE                      |
|--------------|--------------|--------------------------|
| user         | us           | Manage the User account  |
| userpassword | up           | Manage the User password |

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

**TABLE 4-9. User Account Commands**

| COMMAND          | PARAMETER | DESCRIPTION  |
|------------------|-----------|--|
| set user         |           | <p>Display the User account status</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set user</pre> <hr/> <p> <b>Note</b><br/>The default status is "disable".</p> <hr/> |
|                  | enable    | <p>Enable the User account</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set user enable</pre>  |
|                  | disable   | <p>Disable the User account</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set user disable</pre>  |
| set userpassword |           | <p>Prompt the currently logged on administrator to specify a new User account password</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set userpassword</pre>   |

| COMMAND | PARAMETER | DESCRIPTION   |
|---------|-----------|---|
|         | ignore    | Change the User account password to the newly specified password<br><br>For example, type:<br><br>SLCmd.exe -p<br><admin_password> set<br>userpassword P@ssW0Rd |

### Script Commands

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

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

The following table lists the available abbreviated forms of parameters.

**TABLE 4-10. Abbreviations and Uses**


| PARAMETER | ABBREVIATION | USE                    |
|-----------|--------------|------------------------|
| script    | scr          | Manage script commands |

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



**TABLE 4-11. Script Commands**

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

| COMMAND       | PARAMETER                                | DESCRIPTION  |
|---------------|--|--|
| remove script | <extension>[interpreter 1][interpreter2] | <p>Remove the specified script extension and the interpreter(s) required to execute the script</p> <p>For example, to remove the script extension JSP with the interpreter file <code>jscript.js</code>, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; remove script jsp C:\Scripts \jscript.js</pre> <hr/> <p> <b>Note</b></p> <p>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.</p> |
| show script   |  | <p>Display all script rules</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; show script</pre>   |

**Note**

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

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

**Approved List Commands**

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

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

The following table lists the available abbreviated forms of parameters.


**TABLE 4-12. Abbreviations and Uses**

| PARAMETER    | ABBREVIATION | USE                               |
|--------------|--------------|-----------------------------------|
| approvedlist | al           | Manage files in the Approved List |



| PARAMETER | ABBREVIATION | USE  |
|-----------|--------------|--|
| list      | li           | Manage the Approved List import and export functions |

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

**TABLE 4-13. Approved List Commands**

| COMMAND             | PARAMETER                 | DESCRIPTION   |
|---------------------|---------------------------|---|
| add approvedlist    | [-r]<file_or_folder_path> | <p>Add the specified file to the Approved List</p> <p>For example, to add all Microsoft Office files to the Approved List, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; add approvedlist -r "C:\Program Files \Microsoft Office"</pre> <hr/> <p> <b>Note</b><br/>Using the optional -r value includes the specified folder and related subfolders.</p> |
| remove approvedlist | <file_path>               | <p>Remove the specified file from the Approved List</p> <p>For example, to remove notepad.exe from the Approved List, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; remove approvedlist C:\Windows \notepad.exe</pre>  |

| COMMAND            | PARAMETER | DESCRIPTION  |
|--------------------|-----------|--|
| show approvedlist  |           | Display the files in the Approved List<br><br>For example, type:<br><br><pre>SLCmd.exe -p &lt;admin_password&gt; show approvedlist</pre>   |
| check approvedlist | -f        | Update the hash values in the Approved List and display detailed results<br><br>For example, type:<br><br><pre>SLCmd.exe -p &lt;admin_password&gt; check approvedlist -f</pre>   |
|                    | -q        | Update the hash values in the Approved List and display summarized results<br><br>For example, type:<br><br><pre>SLCmd.exe -p &lt;admin_password&gt; check approvedlist -q</pre>   |
|                    | -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<br><br>For example, type:<br><br><pre>SLCmd.exe -p &lt;admin_password&gt; check approvedlist -v</pre> |

| COMMAND     | PARAMETER        | DESCRIPTION  |
|-------------|------------------|--|
| export list | <output_file>    | <p>Export the Approved List to the file path and file name specified</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; export list c:\approvedlist \ap.db</pre> <hr/> <p> <b>Note</b><br/>The output file type must be DB format.</p>  |
| import list | [o] <input_file> | <p>Import an Approved List from the file path and file name specified</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; import list c:\approvedlist \ap.db</pre> <hr/> <p> <b>Note</b><br/>The input file type must be DB format.<br/>Using the optional -o value overwrites the existing list.</p> |

### 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](https://pubs.opengroup.org/onlinepubs/7908799/xbd/re.html#tag_007_004).

**TABLE 4-14. Abbreviations and Uses**

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


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



**TABLE 4-15. Application Lockdown Commands**

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

| COMMAND           | PARAMETER                            | DESCRIPTION   |
|-------------------|--------------------------------------|---|
| add exceptionpath | -e <file_path> -tfile                | Add an exception for the specified file<br><br>For example, type:<br><br>SLCmd.exe -p<br><admin_password> add<br>exceptionpath -e<br>c:\sample.bat -t file  |
|                   | -e <folder_path> -t<br>folder        | Add an exception for the specified folder<br><br>For example, type:<br><br>SLCmd.exe -p<br><admin_password> add<br>exceptionpath -e<br>c:\folder -t folder  |
|                   | -e <folder_path> -t<br>folderandsub  | Add an exception for the specified folder and related subfolders<br><br>For example, type:<br><br>SLCmd.exe -p<br><admin_password> add<br>exceptionpath -e<br>c:\folder -t<br>folderandsub  |
|                   | -e <regular_expression><br>-t regexp | Add an exception using the regular expression<br><br>For example, type: <ul style="list-style-type: none"> <li>SLCmd.exe -p<br/>&lt;admin_password&gt;<br/>add exceptionpath -<br/>e c:\\folder\\.* -t<br/>regexp</li> <li>SLCmd.exe -p<br/>&lt;admin_password&gt;<br/>add exceptionpath -</li> </ul> |



| COMMAND              | PARAMETER                        | DESCRIPTION   |
|----------------------|----------------------------------|---|
|                      |                                  | <pre>e \\computer\ \folder\ \.*\ \file.exe -t regexp</pre>  |
| remove exceptionpath | -e <file_path> -tfile            | <p>Add an exception for the specified file</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; remove exceptionpath -e c:\sample.bat -t file</pre>   |
|                      | -e <folder_path> -t folder       | <p>Remove an exception for the specified folder</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; remove exceptionpath -e c:\folder -t folder</pre> <hr/> <p> <b>Note</b></p> <p>Specify the exact &lt;folder_path&gt; originally specified in the corresponding add command.</p> <hr/> |
|                      | -e <folder_path> -t folderandsub | <p>Remove an exception for the specified folder and related subfolders</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; remove exceptionpath -e c:\folder -t folderandsub</pre>   |

| COMMAND            | PARAMETER                                  | DESCRIPTION  |
|--------------------|--|--|
|                    |  |  <b>Note</b><br>Specify the exact <folder_path> originally specified in the corresponding add command.  |
|                    | -e <regular_expression><br>-t regexp       | Remove an exception using the regular expression<br>For example, type:<br><pre>SLCmd.exe -p &lt;admin_password&gt; remove exceptionpath -e c:\ \test\.* -t regexp</pre> <hr/>  <b>Note</b><br>Specify the exact <regular_expression> originally specified in the corresponding add command. |
| test exceptionpath | <regular_expression><br><string> -t regexp | Check if the regular expression matches the string<br>For example, type:<br><pre>LCmd.exe -p &lt;admin_password&gt; test exceptionpath C:\\test\ .* C:\\test \ \sample.exe -t regexp</pre>   |

### Write Protection Commands

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

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

The following table lists the available abbreviated forms of parameters.


**TABLE 4-16. Abbreviations and Uses**

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


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


**TABLE 4-17. Write Protection List “File” Commands**

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


| COMMAND | PARAMETER                      | VALUE   | DESCRIPTION  |
|---------|--------------------------------|---|--|
|         |                                |   | <pre>SLCmd.exe -p &lt;admin_password&gt; add writeprotection-file archive.txt</pre> <hr/> <p> <b>Note</b></p> <p>The value pattern matches from the end of the path toward the beginning of the path. For example, specifying <code>userfile.txt</code> matches <code>c:\Windows\userfile.txt</code> and <code>c:\Temp\userfile.txt</code>.</p> |
|         | writeprotection-file-exception | <pre>-t &lt;file_path&gt; - p &lt;process_path &gt;</pre> | <p>Add the specified file and a specific process path for that file to the Write Protection Exception List</p> <p>For example, to add write access by a process named <code>notepad.exe</code> to a file named <code>userfile.txt</code>, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; add writeprotection-file- exception -t userfile.txt -p notepad.exe</pre>  |


| COMMAND | PARAMETER | VALUE  | DESCRIPTION   |
|---------|-----------|--|---|
|         |           |  | <div data-bbox="803 261 861 310"></div> <p><b>Note</b></p> <p>The <code>-p</code> and <code>-t</code> values pattern match from the end of the path toward the beginning of the path. For example, specifying <code>userfile.txt</code> matches <code>c:\Windows\userfile.txt</code> and <code>c:\Temp\userfile.txt</code>.</p> |
|         |           | <p><code>-t</code><br/> <code>&lt;file_path&gt;</code></p> | <p>Add the specified file to the Write Protection Exception List</p> <p>For example, to add write access by any process to a file named <code>userfile.txt</code>, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; add writeprotection-file- exception -t userfile.txt</pre>   |


| COMMAND | PARAMETER | VALUE   | DESCRIPTION  |
|---------|-----------|---|--|
|         |           |   |  <b>Note</b><br>The <code>-t</code> value pattern matches from the end of the path toward the beginning of the path. For example, specifying <code>userfile.txt</code> matches <code>c:\Windows\userfile.txt</code> and <code>c:\Temp\userfile.txt</code> . |
|         |           | <code>-p</code><br><code>&lt;process_path</code><br><code>&gt;</code> | Add the specified process path to the Write Protection Exception List<br><br>For example, to add write access by a process named <code>notepad.exe</code> to any files, type:<br><br><pre>SLCmd.exe -p &lt;admin_password&gt; add writeprotection- fileexception -p notepad.exe</pre>  |



| COMMAND | PARAMETER              | VALUE                 | DESCRIPTION   |
|---------|------------------------|-----------------------|---|
|         |                        |                       |  <b>Note</b><br>The <code>-p</code> value pattern matches from the end of the process path toward the beginning of the path. For example, specifying <code>notepad.exe</code> matches <code>c:\Windows\notepad.exe</code> and <code>c:\Temp\notepad.exe</code> . |
|         | writeprotection-folder | [-r]<br><folder_path> | Add the specified folder(s) to the Write Protection List<br><br>For example, type:<br><br><pre>SLCmd.exe -p &lt;admin_password&gt; add writeprotection-folder -r userfolder</pre>   |





| COMMAND | PARAMETER   | VALUE   | DESCRIPTION  |
|---------|---|---|--|
|         |   |   |  <b>Note</b><br>Using the optional <code>-r</code> value includes the specified folder and related subfolders.<br><br>The value pattern matches from the end of the path toward the beginning of the path. For example, specifying <code>userfile.txt</code> matches <code>c:\Windows\userfolder</code> and <code>c:\Temp\userfolder</code> . |
|         | <code>writепrotection-<br/>folderexception</code> | <pre>[-r] -t &lt;folder_path&gt; -p &lt;process_path&gt; &gt;</pre> | Add the specified folder and processes run from the specified path to the Write Protection Exception List<br><br>For example, to add write access by a process named <code>notepad.exe</code> to a folder and related subfolders at <code>c:\Windows\System32\Temp</code> , type:<br><br><pre>SLCmd.exe -p &lt;admin_password&gt; add writепrotectionfolder- exception -r -t c:\Windows \System32\Temp -p notepad.exe</pre>    |



| COMMAND | PARAMETER | VALUE                                  | DESCRIPTION  |
|---------|-----------|--|--|
|         |           |  |  <p><b>Note</b></p> <p>Using the optional <code>-r</code> value includes the specified folder and related subfolders. The <code>-p</code> and <code>-t</code> values pattern match from the end of the path toward the beginning of the path. For example, specifying <code>userfile.txt</code> matches <code>c:\Windows\userfile.txt</code> and <code>c:\Temp\userfile.txt</code>.</p> |
|         |           | <pre>[-r] -t &lt;folder_path&gt;</pre> | <p>Add the specified folder(s) to the Write Protection Exception List</p> <p>For example, to add write access by any process to a folder at <code>userfolder</code>, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; add writeprotectionfolder- exception -r -t userfolder</pre>  |


| COMMAND | PARAMETER | VALUE   | DESCRIPTION   |
|---------|-----------|---|---|
|         |           |   |  <p><b>Note</b></p> <p>Using the optional <code>-r</code> value includes the specified folder and related subfolders. The <code>-t</code> value pattern matches from the last part of the folder path toward the beginning of the path. For example, specifying <code>user</code> folder matches <code>c:\Windows\userfolder</code> and <code>c:\Temp\userfolder</code>.</p> |
|         |           | <p><code>-p</code><br/> <code>&lt;process_path&gt;</code></p> | <p>Add processes run from the specified paths to the Write Protection Exception List</p> <p>For example, to add write access by a process named <code>notepad.exe</code> to any folder, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; add writeprotectionfolder- exception -p c:\Windows \notepad.exe</pre>  |

| COMMAND | PARAMETER                      | VALUE  | DESCRIPTION   |
|---------|--------------------------------|--|---|
|         |                                |  |  <b>Note</b><br>The <code>-p</code> value pattern matches from the end of the process path toward the beginning of the path. For example, specifying <code>notepad.exe</code> matches <code>c:\Windows\notepad.exe</code> and <code>c:\Temp\notepad.exe</code> .                             |
| remove  | writeprotection-file           | <file_path>                                    | Remove the specified file from the Write Protection List<br><br>For example, type:<br><br><pre>SLCmd.exe -p &lt;admin_password&gt; remove writeprotection-file archive.txt</pre> <hr/>  <b>Note</b><br>Specify the exact <file_path> originally specified in the corresponding add command. |
|         | writeprotection-file-exception | -t<br><file_path> -<br>p<br><process_path<br>> | Remove the specified file and process path from the Write Protection Exception List<br><br>For example, type:<br><br><pre>SLCmd.exe -p &lt;admin_password&gt; remove</pre>  |


| COMMAND | PARAMETER | VALUE                           | DESCRIPTION   |
|---------|-----------|---------------------------------|---|
|         |           |                                 | <pre>writeprotection-file-exception -t userfile.txt -p notepad.exe</pre> <hr/>  <b>Note</b><br>Specify the exact <file_path> and <process_path> originally specified in the corresponding add command. |
|         |           | <pre>-t &lt;file_path&gt;</pre> | Remove the specified file from the Write Protection Exception List<br><br>For example, type:<br><br><pre>SLCmd.exe -p &lt;admin_password&gt; remove writeprotection-file-exception -t userfile.txt</pre>  |


| COMMAND | PARAMETER | VALUE | DESCRIPTION  |
|---------|-----------|-------|--|
|         |           |       | <p data-bbox="807 261 861 310"> <b>Note</b></p> <p data-bbox="878 297 1089 651">The <code>-t</code> value pattern matches from the end of the path toward the beginning of the path. For example, specifying <code>userfile.txt</code> matches <code>c:\Windows\userfile.txt</code> and <code>c:\Temp\userfile.txt</code>.</p> <hr/> <p data-bbox="606 691 771 764">-p<br/>&lt;process_path<br/>&gt;</p> <p data-bbox="801 691 1089 764">Remove the specified process path from the Write Protection Exception List</p> <p data-bbox="801 789 975 813">For example, type:</p> <pre data-bbox="801 833 1083 964">SLCmd.exe -p &lt;admin_password&gt; remove writeprotection-file- exception -p notepad.exe</pre> |

| COMMAND | PARAMETER              | VALUE                 | DESCRIPTION   |
|---------|------------------------|-----------------------|---|
|         |                        |                       |  <p><b>Note</b></p> <p>The <code>-p</code> value pattern matches from the end of the process path toward the beginning of the path. For example, specifying <code>notepad.exe</code> matches <code>c:\Windows\notepad.exe</code> and <code>c:\Temp\notepad.exe</code>.</p>   |
|         | writeprotection-folder | [-r]<br><folder_path> | <p>Remove the specified folder(s) from the Write Protection List</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; remove writeprotection-folder -r c:\Windows</pre> <hr/>  <p><b>Note</b></p> <p>Using the optional <code>-r</code> value includes the specified folder and related subfolders. Specify the exact <code>&lt;folder_path&gt;</code> and <code>-r</code> value originally specified in the corresponding add command.</p> |

| COMMAND | PARAMETER                        | VALUE   | DESCRIPTION  |
|---------|----------------------------------|---|--|
|         | writeprotection-folder-exception | <pre>[-r] -t &lt;folder_path&gt; -p &lt;process_path&gt; &gt;</pre> | <p>Remove the specified folder and process path from the Write Protection Exception List</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; remove writeprotection-folder-exception -r -t c:\Windows \System32\Temp -p c:\Windows\notepad.exe</pre> <hr/> <p> <b>Note</b></p> <p>Using the optional <code>-r</code> value includes the specified folder and related subfolders. Specify the exact <code>&lt;folder_path&gt;</code>, <code>&lt;process_path&gt;</code>, and <code>-r</code> value originally specified in the corresponding add command.</p> <hr/> <p>Remove the specified folder(s) from the Write Protection Exception List</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; remove writeprotection-folder-exception -r -t user folder</pre> |




| COMMAND | PARAMETER | VALUE   | DESCRIPTION   |
|---------|-----------|---|---|
|         |           |   |  <b>Note</b><br>Using the optional <code>-r</code> value includes the specified folder and related subfolders. The <code>-t</code> value pattern matches from the last part of the folder path toward the beginning of the path. For example, specifying <code>user folder</code> matches <code>c:\Windows\userfolder</code> and <code>c:\Temp\userfolder</code> . |
|         |           | <code>-p</code><br><code>&lt;process_path</code><br><code>&gt;</code> | Remove the specified process path from the Write Protection Exception List<br><br>For example, type:<br><br><pre>SLCmd.exe -p &lt;admin_password&gt; remove writeprotection-folder- exception -p c:\Windows \System32</pre>   |


| COMMAND | PARAMETER | VALUE | DESCRIPTION   |
|---------|-----------|-------|---|
|         |           |       |  <b>Note</b><br>The <code>-p</code> value pattern matches from the end of the process path toward the beginning of the path. For example, specifying <code>notepad.exe</code> matches <code>c:\Windows\notepad.exe</code> and <code>c:\Temp\notepad.exe</code> . |



**TABLE 4-18. Write Protection List “Registry” Commands**


| COMMAND | PARAMETER                          | VALUE | DESCRIPTION  |
|---------|------------------------------------|-------|--|
| show    | writeprotection                    |       | Display the entire Write Protection List                           |
|         | writeprotection-regvalue           |       | Display the registry values in the Write Protection List           |
|         | writeprotection-regvalue-exception |       | Display the registry values in the Write Protection Exception List |
|         | writeprotection-regkey             |       | Display the registry keys in the Write Protection List             |
|         | writeprotection-regkey-exception   |       | Display the registry keys in the Write Protection Exception List   |


| COMMAND | PARAMETER                          | VALUE  | DESCRIPTION  |
|---------|------------------------------------|--|--|
| add     | writeprotection-regvalue           | <path_of_registry_key><br><registry_value>                               | <p>Add the specified registry value and its related registry key to the Write Protection List</p> <p>For example, to add the registry value of “testvalue” in the “HKEY \test” registry key to the Write Protection List, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; add writeprotection-regvalue HKEY \test testvalue</pre> |
|         | writeprotection-regvalue-exception | -t<br><path_of_registry_key><br><registry_value><br>-p<br><process_path> | <p>Add the specified registry value and its related registry key and a specific process path for that value to the Write Protection Exception List</p>   |

| COMMAND | PARAMETER | VALUE   | DESCRIPTION  |
|---------|-----------|---|--|
|         |           |   | <p data-bbox="891 261 946 310"> <b>Note</b></p> <p data-bbox="962 297 1089 854">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.</p> <hr/> <p data-bbox="881 889 1089 1016">Add the specified registry value and its related registry key to the Write Protection Exception List</p> |
|         |           | <p data-bbox="655 889 854 995">-t<br/>&lt;path_of_registry_key&gt;<br/>&lt;registry_value&gt;</p> |  |


| COMMAND | PARAMETER | VALUE                | DESCRIPTION  |
|---------|-----------|----------------------|--|
|         |           |                      |  <b>Note</b><br>This command allows write access by any process to the specified registry value. |
|         |           | -p<br><process_path> | Add the specified process to the Write Protection Exception List   |


| COMMAND | PARAMETER              | VALUE                       | DESCRIPTION  |
|---------|------------------------|-----------------------------|--|
|         |                        |                             |  <p><b>Note</b><br/>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.</p> |
|         | writeprotection-regkey | [-r] <path_of_registry_key> | <p>Add the specified registry key to the Write Protection List</p> <hr/>  <p><b>Note</b><br/>Using the optional -r value includes the specified registry key and related subkeys.</p>                   |


| COMMAND | PARAMETER                        | VALUE   | DESCRIPTION  |
|---------|----------------------------------|---|--|
|         | writeprotection-regkey-exception | [-r]<br><path_of_registry_key> -p<br><process_path> | <p>Add the specified registry key and processes run from the specified path to the Write Protection Exception List</p> <hr/> <p> <b>Note</b></p> <p>This command allows write access by the specified process to the specified registry keys.</p> <p>Using the optional <code>-r</code> value includes the specified registry key and related subkeys.</p> <p>The <code>-p</code> value pattern matches from the end of the process path toward the beginning of the path.</p> |


| COMMAND | PARAMETER | VALUE   | DESCRIPTION   |
|---------|-----------|---|---|
|         |           | <pre>[-r] -t &lt;path_of_registry_key&gt;</pre> | <p>Add the specified registry key to the Write Protection Exception List</p> <hr/> <p> <b>Note</b></p> <p>This command allows write access by any process to the specified registry keys.</p> <p>Using the optional <code>-r</code> value includes the specified registry key and related subkeys.</p> |
|         |           | <pre>-p &lt;process_path&gt;</pre>              | <p>Add processes run from the specified paths to the Write Protection Exception List</p>  |





| COMMAND | PARAMETER                | VALUE                                      | DESCRIPTION  |
|---------|--------------------------|--|--|
|         |                          |  |  <p><b>Note</b></p> <p>This command allows write access by the specified process to any registry keys.</p> <p>The <code>-p</code> value pattern matches from the end of the process path toward the beginning of the path.</p> |
| remove  | writeprotection-regvalue | <path_of_registry_key><br><registry_value> | Remove the specified registry value from the Write Protection List   |



| COMMAND | PARAMETER                          | VALUE  | DESCRIPTION   |
|---------|------------------------------------|--|---|
|         |                                    |  |  <b>Note</b><br>Specify the exact <path_of_registry_key> and <registry_value> originally specified in the corresponding add command. |
|         | writeprotection-regvalue-exception | -t<br><path_of_registry_key><br><registry_value><br>-p<br><process_path> | Remove the specified registry value and process path from the Write Protection Exception List   |

| COMMAND | PARAMETER | VALUE  | DESCRIPTION   |
|---------|-----------|--|---|
|         |           |  |  <p><b>Note</b></p> <p>Specify the exact &lt;path_of_registry_key&gt;, &lt;registry_value&gt;, and &lt;process_path&gt; originally specified in the corresponding add command.</p> <p>The -p value pattern matches from the end of the path toward the beginning of the path.</p> |
|         |           | -t<br><path_of_registry_key><br><registry_value> | Remove the specified registry value from the Write Protection Exception List  |
|         |           | -p<br><process_path>                             | Remove the specified process path from the Write Protection Exception List  |

| COMMAND | PARAMETER              | VALUE                          | DESCRIPTION   |
|---------|------------------------|--------------------------------|---|
|         |                        |                                |  <b>Note</b><br>The <code>-p</code> value pattern matches from the end of the path toward the beginning of the path. |
|         | writeprotection-regkey | [-r]<br><path_of_registry_key> | Remove the specified registry key from the Write Protection List  |

| COMMAND | PARAMETER                        | VALUE   | DESCRIPTION  |
|---------|----------------------------------|---|--|
|         |                                  |   |  <p><b>Note</b></p> <p>Specify the exact &lt;path_of_registry_key&gt; and -r value originally specified in the corresponding add command.</p> <p>Using the optional -r value includes the specified registry key and related subkeys</p> |
|         | 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  |
|---------|-----------|-------|--|
|         |           |       | <p> <b>Note</b></p> <p>Specify the exact &lt;path_of_registry_key&gt;, &lt;process_path&gt;, and -r value originally specified in the corresponding add command.</p> <p>Using the optional -r value includes the specified registry key and related subkeys.</p> <p>The -p value pattern matches from the end of the path toward the beginning of the path.</p> |

| COMMAND | PARAMETER | VALUE   | DESCRIPTION  |
|---------|-----------|---|--|
|         |           | <code>[-r] -t<br/>&lt;path_of_registry_key&gt;</code> | <p>Remove the specified registry key from the Write Protection Exception List</p> <hr/> <p> <b>Note</b><br/>Using the optional <code>-r</code> value includes the specified registry key and related subkeys.</p>    |
|         |           | <code>-p<br/>&lt;process_path&gt;</code>              | <p>Remove the specified process path from the Write Protection Exception List</p> <hr/> <p> <b>Note</b><br/>The <code>-p</code> value pattern matches from the end of the path toward the beginning of the path.</p> |

### Trusted Certificate Commands

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

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


The following table lists the available abbreviated forms of parameters.

**TABLE 4-19. Abbreviations and Uses**

| PARAMETER            | ABBREVIATION | USE                         |
|----------------------|--------------|-----------------------------|
| trustedcertification | tc           | Manage Trusted Certificates |

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

**TABLE 4-20. Trusted Certificate Commands**

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



## Intelligent Runtime Learning Commands

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

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

The following table lists the available abbreviated forms of parameters.

**TABLE 4-21. Abbreviations and Uses**

| PARAMETER                      | ABBREVIATION | USE  |
|--------------------------------|--------------|--|
| intelligentruntime<br>learning | irl          | Agent will allow runtime execution files that are generated by applications in the Approved List |

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

**TABLE 4-22. Intelligent Runtime Learning Commands**

| COMMAND                               | PARAMETER | DESCRIPTION   |
|---------------------------------------|-----------|---|
| set<br>intelligentruntime<br>learning |           | Display current settings for using Intelligent Runtime Learning |
|                                       | enable    | Enable using Intelligent Runtime Learning                       |
|                                       | disable   | Disable using Intelligent Runtime Learning                      |

## Trusted Hash List Commands

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

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


The following table lists the available abbreviated forms of parameters.



**TABLE 4-23. Abbreviations and Uses**

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

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

**TABLE 4-24. Intelligent Runtime Learning Commands**

| COMMAND          | PARAMETER   | DESCRIPTION   |
|------------------|---|---|
| set trustedhash  |   | Display current setting for using Trusted Hash List<br><br> <b>Note</b><br>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<br><br>For example, type:<br><pre>SLCmd.exe -p &lt;admin_password&gt;<br/>show trustedhash</pre>   |
| add trustedhash  | -v <hash> [-l<label>] [-u] [-al] [-t <file_path>] [-n <note>] | Add the specified hash value to the Trusted Hash List<br><br>For example, to add a trusted file with a hash value xxx to the Trusted Hash List, type:<br><pre>SLCmd.exe -p &lt;admin_password&gt;<br/>add trustedhash -v xxx</pre><br>Using the optional -l value specifies the unique label for this hash value. |

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

## Trusted Updater Commands

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

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


The following table lists the available abbreviated forms of parameters.


**TABLE 4-25. Abbreviations and Uses**

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

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

**TABLE 4-26. Trusted Updater Commands**

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

| COMMAND                | PARAMETER | DESCRIPTION   |
|------------------------|-----------|---|
| stop<br>trustedupdater | [-f]      | <p>Disable Trusted Updater to stop adding new or updated files to the Approved List</p> <p>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:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; stop trustedupdater -f</pre> <hr/> <p> <b>Note</b><br/>Using the optional -f value specifies that the Trusted Updater does not prompt the administrator before committing a file to the Approved List.</p> |

### Real-Time Scan Commands

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

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




#### Note

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

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

**TABLE 4-27. Real-Time Scan Commands**

| COMMAND | PARAMETER | DESCRIPTION  |
|---------|-----------|--|
| set rts |           | Display the current status of Real-Time Scan<br><br><hr/>  <b>Note</b><br>The default setting is "disable". |
|         | enable    | Enable Real-Time Scan<br><br>For example, type:<br><pre>SLCmd.exe -p &lt;admin_password&gt; set rts enable</pre>   |
|         | disable   | Disable Real-Time Scan<br><br>For example, type:<br><pre>SLCmd.exe -p &lt;admin_password&gt; set rts disable</pre>   |

### Trusted USB Device Commands

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

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

The following table lists the available abbreviated forms of parameters.

**TABLE 4-28. Abbreviations and Uses**

| PARAMETER        | ABBREVIATION | USE                                |
|------------------|--------------|------------------------------------|
| trustedusbdevice | tud          | Manage the trusted USB device list |

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

**TABLE 4-29. Trusted USB Device Commands**

| COMMAND                 | PARAMETER                            | DESCRIPTION  |
|-------------------------|--------------------------------------|--|
| show usbinfo            | <drive_letter>                       | Display the identifiers (VID/PID/SN) of a USB storage device<br><br>For example, if the USB is in Drive D, type:<br><br><code>SLCmd.exe -p &lt;admin_password&gt;<br/>show usbinfo d</code>  |
| show trustedusbdevice   | [-f]                                 | Display all trusted USB storage devices<br><br>For example, type:<br><br><code>SLCmd.exe -p &lt;admin_password&gt;<br/>show trustedusbdevice</code>  |
| 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<br><br>For example, type:<br><br><code>SLCmd.exe -p &lt;admin_password&gt;<br/>add trustedusbdevice -sn<br/>123456</code>       |
| 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<br><br>For example, type:<br><br><code>SLCmd.exe -p &lt;admin_password&gt;<br/>remove trustedusbdevice -sn<br/>123456</code> |

**Predefined Trusted Updater Commands**

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

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


The following table lists the available abbreviated forms of parameters.

**TABLE 4-30. Abbreviations and Uses**

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


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

**TABLE 4-31. Predefined Trusted Updater Commands**

| COMMAND                         | PARAMETER                        | DESCRIPTION   |
|---------------------------------|----------------------------------|---|
| add<br>predefinedtrustedupdater | -e<br><folder_or_file_exception> | <p>Add the specified file or folder to the Predefined Trusted Updater Exception List</p> <p>For example, to add notepad.exe to the Predefined Trusted Updater Exception List, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; add predefinedtrustedupdater -e C:\Windows\notepad.exe</pre> <hr/> <p> <b>Important</b></p> <p>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 <i>Predefined Trusted Updater "Add" Command</i> in the following section.</p> |



| COMMAND                                 | PARAMETER   | DESCRIPTION   |
|---|---|---|
| decrypt<br>predefinedtrust<br>edupdater | <path_of_encrypted_file<br>><br><path_of_decrypted_outp<br>ut_file> | Decrypt a file to the specified location<br><br>For example, to decrypt<br>C:\Notepad.xen to C:\Editors<br>\notepad.xml, type:<br><br>SLCmd.exe -p <admin_password><br>decrypt<br>predefinedtrustedupdater<br>C:\Notepad.xen C:\Editors<br>\notepad.xml |
| encrypt<br>predefinedtrust<br>edupdater | <path_of_file><br><path_of_encrypted_outp<br>ut_file>               | Encrypt a file to the specified location<br><br>For example, to encrypt<br>C:\notepad.xml to C:\Editors<br>\Notepad.xen, type:<br><br>SLCmd.exe -p <admin_password><br>encrypt<br>predefinedtrustedupdater<br>C:\Editors\notepad.xml<br>C:\Notepad.xen  |
| export<br>predefinedtrust<br>edupdater  | <path_of_encrypted_outp<br>ut>                                      | Export the Predefined Trusted Updater<br>List to the specified encrypted file<br><br>For example, type:<br><br>SLCmd.exe -p <admin_password><br>export<br>predefinedtrustedupdater<br>C:\Lists\ptu_list.xen   |
| import<br>predefinedtrust<br>edupdater  | <path_of_encrypted_inpu<br>t>                                       | Import a Predefined Trusted Updater<br>List from the specified encrypted file<br><br>For example, type:<br><br>SLCmd.exe -p <admin_password><br>import<br>predefinedtrustedupdater<br>C:\Lists\ptu_list.xen   |

| COMMAND                                | PARAMETER                            | DESCRIPTION  |
|--|--------------------------------------|--|
| remove<br>predefinedtrust<br>edupdater | -l <label_name>                      | <p>Remove the specified labeled rule from the Predefined Trusted Updater List</p> <p>For example, to remove the "Notepad" rule, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; remove predefinedtrustedupdater -l Notepad</pre>                              |
|  | -e<br><folder_or_file_excepti<br>on> | <p>Remove the specified exception from the Predefined Trusted Updater Exception List</p> <p>For example, to remove the notepad.exe exception, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; remove predefinedtrustedupdater -e C:\Windows\notepad.exe</pre> |
| set<br>predefinedtrust<br>edupdater    |                                      | <p>Display the status of the Predefined Trusted Updater List</p> <hr/> <p> <b>Note</b><br/>The default setting is "disable".</p> <hr/>  |
|  | enable                               | Enable the Predefined Trusted Updater List   |
|  | disable                              | Disable the Predefined Trusted Updater List  |
| show<br>predefinedtrust<br>edupdater   |                                      | <p>Display the files in the Predefined Trusted Updater List</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; show predefinedtrustedupdater</pre>   |

| COMMAND | PARAMETER | DESCRIPTION   |
|---------|-----------|---|
|         | -e        | <p>Display the files in the Predefined Trusted Updater Exception List</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; show predefinedtrustedupdater -e</pre> |



### Important

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

### Predefined Trusted Updater "Add" Command

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

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


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


**TABLE 4-32. Predefined Trusted Updater “Add” Command**


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

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

**TABLE 4-33. Predefined Trusted Updater “Add” Additional Values**

| VALUE                   | REQUIRED/OPTIONAL | DESCRIPTION   | EXAMPLE   |
|-------------------------|-------------------|---|---|
| -u<br><folder_or_file > | Required          | Add the specified file or folder to the Predefined Trusted Updater List                                 | <p>N/A</p> <hr/> <p> <b>Note</b><br/>This parameter requires the use of the -t &lt;type_of_object&gt; value.</p> |
| -t<br><type_of_object>  | Required          | Specify the type of object to add to the Predefined Trusted Updater List located in -u <folder_or_file> | <pre>SLCmd.exe -p &lt;admin_password&gt; add predefinedtrustedupdater -u C:\Windows</pre>   |

| VALUE                                | REQUIRED/<br>OPTIONAL | DESCRIPTION   | EXAMPLE  |
|--------------------------------------|-----------------------|---|--|
|                                      |                       | <p>Available objects types are as follows:</p> <ul style="list-style-type: none"> <li>• process: Indicates only EXE file types</li> <li>• file: Indicates only MSI and BAT file types</li> <li>• folder: Indicates all EXE, MSI, and BAT files in the specified folder</li> <li>• folderandsub: Indicates all EXE, MSI, and BAT files in the specified folder and related subfolders</li> </ul> | <pre>\notepad.exe -t process</pre>   |
| <p>-p<br/>&lt;parent_process&gt;</p> | Optional              | <p>Add the full file path to the specified parent process used to invoke the file(s) specified in -u &lt;folder_or_file&gt;</p>   | <pre>SLCmd.exe -p &lt;admin_password&gt; add predefinedtrust edupdater -u C:\Windows \notepad.exe -t process -p C:\batch files \note.bat</pre> |
| <p>-l<br/>&lt;label_name&gt;</p>     | Optional              | <p>Specify a label name for the file(s) specified in -u &lt;folder_or_file&gt;</p> <hr/> <p> <b>Note</b><br/>When left blank, StellarProtect (Legacy Mode) assigns an arbitrary label name.</p>  | <pre>SLCmd.exe -p &lt;admin_password&gt; add predefinedtrusted updater -u C:\Windows \notepad.exe -t process -l EDITOR</pre>                   |
| <p>-al enable</p>                    | Optional              | <p>Compare the hash values in the Approved List with the hash</p>   | <pre>SLCmd.exe -p &lt;admin_password&gt;</pre>   |

| VALUE                       | REQUIRED/OPTIONAL | DESCRIPTION   | EXAMPLE  |
|-----------------------------|-------------------|---|--|
|                             |                   | values calculated from the actual files<br><hr/>  <b>Note</b><br>Enabled by default even when <code>-al</code> is not specified. | <pre>add predefinedtrusted updater -u C:\Windows \notepad.exe -t process -al enable</pre>                                      |
| <code>-al</code><br>disable | Optional          | Do not compare the hash values in the Approved List with the hash values calculated from the actual files   | <pre>SLCmd.exe -p &lt;admin_password&gt; add predefinedtrusted updater -u C:\Windows \notepad.exe -t process -al disable</pre> |

### Windows Update Support

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

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


The following table lists the available abbreviated forms of parameters.

**TABLE 4-34. Abbreviations and Uses**

| PARAMETER            | ABBREVIATION | USE   |
|----------------------|--------------|---|
| windowsupdatesupport | wus          | Allow Windows Update to run on the agent with the Application Lockdown on |

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

**TABLE 4-35. Windows Update Support Commands**

| COMMAND                         | PARAMETER | DESCRIPTION  |
|---------------------------------|-----------|--|
| set<br>windowsupdatesu<br>pport |           | Display current setting for Windows Update Support<br><br> <b>Note</b><br>The default setting is "disable". |
|                                 | enable    | Enable Windows Update Support  |
|                                 | disable   | Disable Windows Update Support   |

**Blocked File Notification Commands**

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

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


The following table lists the available abbreviated forms of parameters.

**TABLE 4-36. Abbreviations and Uses**

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

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

**TABLE 4-37. Windows Update Support Commands**

| COMMAND                        | PARAMETER | DESCRIPTION   |
|--------------------------------|-----------|---|
| set<br>blockedfilenotification |           | Display the current setting<br><br> <b>Note</b><br>The default setting is "disable". |
|                                | enable    | Enable pop-up notifications   |
|                                | disable   | Disable pop-up notifications  |

### Configuration File Commands

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

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

The following table lists the available abbreviated forms of parameters.

**TABLE 4-38. Abbreviations and Uses**

| PARAMETER     | ABBREVIATION | USE                           |
|---------------|--------------|-------------------------------|
| configuration | con          | Manage the configuration file |

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

**TABLE 4-39. Configuration File Commands**

| COMMAND                  | PARAMETER  | DESCRIPTION  |
|--------------------------|--|--|
| decrypt<br>configuration | <path_of_encrypted_file ><br><path_of_decrypted_output_file> | Decrypts a configuration file to the specified location<br><br>For example, to decrypt C:\config.xen to C:\config.xml, type:<br><pre>SLCmd.exe -p &lt;admin_password&gt;<br/>decrypt configuration<br/>C:\config.xen C:\config.xml</pre> |



| COMMAND                  | PARAMETER   | DESCRIPTION  |
|--------------------------|---|--|
| encrypt<br>configuration | <path_of_file><br><path_of_encrypted_output_file> | Encrypts a configuration file to the specified location<br><br>For example, to encrypt C:\config.xml to C:\config.xen, type:<br><br><code>SLCmd.exe -p &lt;admin_password&gt; encrypt configuration C:\config.xml C:\config.xen</code> |
| export<br>configuration  | <path_of_encrypted_output>                        | Export the configuration file to the specified location<br><br>For example, type:<br><br><code>SLCmd.exe -p &lt;admin_password&gt; export configuration C:\config.xen</code>   |
| import<br>configuration  | <path_of_encrypted_input>                         | Import a configuration file from the specified location<br><br>For example, type:<br><br><code>SLCmd.exe -p &lt;admin_password&gt; import configuration C:\config.xen</code>   |

### Fileless Attack Prevention Commands

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

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

The following table lists the available abbreviated forms of parameters.

**TABLE 4-40. Abbreviations and Uses**

| PARAMETER                | ABBREVIATION | USE                               |
|--------------------------|--------------|-----------------------------------|
| filelessattackprevention | flp          | Manage Fileless Attack Prevention |

| PARAMETER                          | ABBREVIATION | USE  |
|------------------------------------|--------------|--|
| filelessattackprevention-process   | flpp         | Manage Fileless Attack Prevention processes  |
| filelessattackprevention-exception | flpe         | Manage Fileless Attack Prevention exceptions |

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

**TABLE 4-41. Configuration File Commands**

| COMMAND                                    | PARAMETER | DESCRIPTION  |
|--|-----------|--|
| set<br>filelessattackprevention            |           | Display the current Fileless Attack Prevention status<br><br>For example, type:<br><br><code>SLCmd.exe -p &lt;admin_password&gt;<br/>set filelessattackprevention</code> |
|  | <enable   | Enable Fileless Attack Prevention<br><br>For example, type:<br><br><code>SLCmd.exe -p &lt;admin_password&gt;<br/>set filelessattackprevention<br/>enable</code>          |
|  | disable   | Disable Fileless Attack Prevention<br><br>For example, type:<br><br><code>SLCmd.exe -p &lt;admin_password&gt;<br/>set filelessattackprevention<br/>disable</code>        |
| show<br>filelessattackprevention-process   |           | Display the list of monitored processes<br><br>For example, type:<br><br><code>SLCmd.exe -p &lt;admin_password&gt;<br/>show filelessattackprevention-process</code>      |
| show<br>filelessattackprevention-exception |           | Display the Fileless Attack Prevention Exception List  |

| COMMAND                                   | PARAMETER   | DESCRIPTION  |
|---|---|--|
| revention-exception                       |   | For example, type:<br><pre>SLCmd.exe -p &lt;admin_password&gt;show filelessattackprevention-exception</pre>  |
| add filelessattackprevention-process      | <pre>&lt;monitored_process&gt; &lt;Parentprocess1&gt; &lt;Parentprocess2&gt; &lt;Parentprocess3&gt; &lt;Parentprocess4&gt; -a &lt;arguments&gt; -regex -l &lt;label&gt;</pre> | Add a Fileless Attack Prevention exception<br><br>For example, given the following exception: <ul style="list-style-type: none"> <li>• Monitored Process: cscript.exe</li> <li>• Parentprocess1: a.exe</li> <li>• Parentprocess2:</li> <li>• Parentprocess3: c.exe</li> <li>• Parentprocess4:</li> <li>• Arguments: -abc -def</li> <li>• Use regular expression for arguments: No</li> </ul> To add the exception, type:<br><pre>SLCmd.exe -p &lt;admin_password&gt; addflpe cscript.exe a.exe "" c.exe "" -a "-abc - def"</pre> |
| remove filelessattackprevention-exception | <pre>-l &lt;label&gt;</pre>   | Remove a Fileless Attack Prevention exception<br><br>For example, type:<br><pre>SLCmd.exe -p &lt;admin_password&gt; remove filelessattackprevention-exception -l &lt;label&gt;</pre>   |

**Note**

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

**Maintenance Mode Commands**

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

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

The following table lists the available abbreviated forms of parameters.

**TABLE 4-42. Abbreviations and Uses**



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


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


**TABLE 4-43. Maintenance Mode Commands**

| COMMAND                  | PARAMETER | DESCRIPTION                                      |
|--------------------------|-----------|--|
| start<br>maintenancemode |           | Start Maintenance Mode<br><br>For example, type: |



| COMMAND                 | PARAMETER        | DESCRIPTION   |
|-------------------------|------------------|---|
|                         |                  | <pre>SLCmd.exe -p &lt;admin_password&gt; start maintenancemode</pre>  |
|                         | -duration        | <p>Set an action to take place after Maintenance Mode as well as a duration for Maintenance Mode in hours (1 -999)</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; start maintenancemode -scan al -duration 3</pre>  |
|                         | -scan quarantine | <p>Start Maintenance Mode and enable file scanning after the maintenance period</p> <p>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</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; start maintenancemode -scan quarantine</pre> |
|                         | -scan al         | <p>Start Maintenance Mode and enable file scanning after the maintenance period</p> <p>StellarProtect (Legacy Mode) scans files that are created/ executed/modified files during the period and adds these files (including files that are detected as malicious) to the Approved List</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; start maintenancemode -scan al</pre>                              |
| stop<br>maintenancemode |                  | Stop Maintenance Mode   |

| COMMAND                            | PARAMETER  | DESCRIPTION  |
|------------------------------------|--|--|
|                                    |  | <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; stop maintenancemode</pre> <hr/> <p> <b>Note</b><br/>You cannot stop Maintenance Mode when an agent is preparing to leave Maintenance Mode.</p>  |
|                                    | -discard   | <p>Stop Maintenance Mode and do not add files in the file queue to the Approved List</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; stop maintenancemode discard</pre> <hr/> <p> <b>Note</b><br/>You cannot stop Maintenance Mode when an agent is preparing to leave Maintenance Mode.</p> |
| set<br>maintenancemode<br>schedule | -start YYYY-MMDDTHH:MM:SS -end<br>YYYY-MMDDTHH:MM:SS | <p>Set the schedule for Maintenance Mode</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set maintenancemodeschedule - start 2019-04- 07T01:00:00 - end 2019-04-07T05:00:00</pre>   |

| COMMAND | PARAMETER   | DESCRIPTION   |
|---------|---|---|
|         |   |  <p><b>Note</b></p> <ul style="list-style-type: none"> <li>You cannot set the Maintenance Mode schedule when an agent is already in Maintenance Mode or is preparing to leave Maintenance Mode.</li> <li>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.</li> </ul>   |
|         | <pre>-start YYYY- MMDDTHH:MM:SS -end YYYY-MMDDTHH:MM:SS - scan quarantine</pre> | <p>Use this command to configure the following:</p> <ul style="list-style-type: none"> <li>Set the schedule for Maintenance Mode</li> <li>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</li> </ul> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set maintenancemodeschedule - start 2019-04- 07T01:00:00 - end 2019-04-07T05:00:00 -scan quarantine</pre> |

| COMMAND | PARAMETER   | DESCRIPTION   |
|---------|---|---|
|         |   |  <p><b>Note</b></p> <ul style="list-style-type: none"> <li>You cannot set the Maintenance Mode schedule when an agent is already in Maintenance Mode or is preparing to leave Maintenance Mode.</li> <li>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.</li> </ul>   |
|         | <pre>-start YYYY- MMDDTHH:MM:SS -end YYYY-MMDDTHH:MM:SS - scan al</pre> | <p>Use this command to configure the following:</p> <ul style="list-style-type: none"> <li>Set the schedule for Maintenance Mode</li> <li>Enable file scanning after the maintenance period: StellarProtect (Legacy Mode) will scan files that are created/ executed/modified during the maintenance period and add these files (including files that are detected as malicious) to the Approved List</li> </ul> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; set maintenancemodeschedule - start 2019-04-07T01:00:00 -end 2019-04-07T05:00:00 -scan al</pre> |



| COMMAND                               | PARAMETER | DESCRIPTION  |
|---------------------------------------|-----------|--|
|                                       |           |  <b>Note</b> <ul style="list-style-type: none"> <li>You cannot set the Maintenance Mode schedule when an agent is already in Maintenance Mode or is preparing to leave Maintenance Mode.</li> <li>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.</li> </ul> |
| remove<br>maintenancemode<br>schedule |           | <p>Clear the Maintenance Mode schedule settings</p> <p>For example, type:</p> <pre>SLCmd.exe -p &lt;admin_password&gt; remove maintenancemodeschedule</pre> <hr/>  <b>Note</b> <p>You cannot delete schedule settings when an agent is already in Maintenance Mode or is preparing to leave Maintenance Mode.</p>   |
| show<br>maintenancemode               |           | <p>Display the Maintenance Mode status</p> <p>For example, type:</p>   |

| COMMAND  | PARAMETER | DESCRIPTION  |
|--|-----------|--|
|  |           | <code>SLCmd.exe -p &lt;admin_password&gt;<br/>show maintenancemode</code>  |
| <code>show<br/>maintenancemode<br/>schedule</code> |           | Display the Maintenance Mode<br>schedule settings<br><br>For example, type:<br><br><code>SLCmd.exe -p &lt;admin_password&gt;<br/>show maintenancemodeschedule</code> |

**Important**

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

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

**Note**

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

**Manual Scan Commands**

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

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

**Note**


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

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

**TABLE 4-44. Manual Scan Commands**

| COMMAND    | PARAMETER          | DESCRIPTION  |
|------------|--------------------|--|
| start scan | [-action <action>] | <p>Start a manual scan on an endpoint</p> <p>Use the <code>-action</code> option to specify an action to perform when an anomaly is detected</p> <p>Available actions are as follows:</p> <ul style="list-style-type: none"> <li>• 0: No action</li> <li>• 1: Clean, or delete if the clean action is unsuccessful</li> <li>• 2: Clean, or quarantine if the clean action is unsuccessful</li> </ul> <p>This is the default action.</p> <ul style="list-style-type: none"> <li>• 3: Clean, or ignore if the clean action is unsuccessful</li> <li>• 4: Use ActiveAction</li> </ul> <p>For example, type:</p> |

| COMMAND | PARAMETER | DESCRIPTION  |
|---------|-----------|--|
|         |           | SLCmd.exe -p <admin_password><br>start scan - action 1 |

| COMMAND | PARAMETER | DESCRIPTION   |
|---------|-----------|---|
|         |           | <p> <b>Note</b></p> <ul style="list-style-type: none"><li>• For each manual scan, StellarProtect (Legacy Mode) saves the scan results in a log file (with a file name of ScanResult_YYYYMMDDHMMSS.log) in C:\Program Files\TXOne\StellarProtect (Legacy Mode) \Scan \log.</li><li>• With administrator privileges, you can restore quarantined files using the following command:<br/><pre>WKSupportTool.exe<br/>RestorePrescan<br/>&lt;QuarantinedFilePath&gt;<br/>&gt;<br/>&lt;FilePathToRestore&gt;</pre>where<br/>&lt;QuarantinedFilePath&gt; is the file path of the quarantined file and<br/>&lt;FilePathToRestore&gt; is the folder location to restore the file. For information about quarantined files, see the scan logs.</li></ul> |

| <b>COMMAND</b> | <b>PARAMETER</b> | <b>DESCRIPTION</b>  |
|----------------|------------------|---|
| start update   |                  | Update StellarProtect (Legacy Mode) agent components (pattern file and scan engine) |
| set update     | -source <source> | Set the update source for component updates   |
| show update    | -source <source> | Display the current update source   |





# Chapter 5

## Working with the Agent Configuration File

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

Topics in this chapter include:

- *[Working with the Agent Configuration File on page 5-2](#)*

## Working with the Agent Configuration File

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

Refer to [Exporting or Importing a Config File on page 5-3](#) for more information.

## Changing Advanced Settings

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

---

### Procedure

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

**Important**

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

---

**Tip**

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

---

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

---

## Exporting or Importing a Config File

**Note**

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

---

**Procedure**

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

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

---

## Configuration File Syntax

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

**Important**

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

Refer to the following example of the configuration file.

```
<?xml version="1.0" encoding="UTF-8"?>
<Configurations version="1.00.000" xmlns:xsi="http://www.w3.org/2001/XMLSchema-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" ShowDetail
Is="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>
        </ScriptLockdown>
      </ApplicationLockDown>
    </Feature>
  </Configuration>
</Configurations>
```

```
</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>
    <DeviceGroupName="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"/>
  </EventLog>
</Log>
```

```

    <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>
  <MessageRandomization TotalGroupNum="1" OwnGroupInd
ex="0">
    <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"/>
    <UIControlId="RecentHistoryUnapprovedFiles"
State="yes"/>
    <UIControlId="ImportExportList" State="yes"/>
  <UIControlId="ListManagement" State="yes"/>
  <UIControlId="SupportToolUninstall" State="no"/>
</AccountRef>
</Permission>
</Configurations>

```

## Configuration File Parameters

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

**TABLE 5-1. Configuration File Sections and Descriptions**

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




| SECTION                | DESCRIPTION   | ADDITIONAL INFORMATION                            |
|------------------------|---|---|
| NetworkVirusProtection |   |   |
| IntegrityMonitoring    |   |   |
| StorageDeviceBlocking  | A parameter to control storage device access to managed endpoints                                       |   |
| Log                    | Parameters to configure individual log types  | <a href="#">Log Section on page 5-27</a>          |
| ManagedMode            | Parameters to configure Centralized Management functions  | <a href="#">Managed Mode Section on page 5-32</a> |
| Permission             | Container for the Permission section  |   |
| AccountRef             | Parameters to configure the StellarProtect (Legacy Mode) console controls available to the User account | <a href="#">AccountRef Section on page 5-36</a>   |

## Account Group Section

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

**TABLE 5-2. Configuration File - AccountGroup Section Parameters**

| PARAMETER     | SETTINGS                                | VALUE  | DESCRIPTION             |
|---------------|---|--------|-------------------------|
| Configuration | Container for the Configuration section |        |                         |
| AccountGroup  | Container for the AccountGroup section  |        |                         |
| Account       | ID                                      | <GUID> | User account GUID       |
|               | Enable                                  | yes    | Enable the User account |

| PARAMETER | SETTINGS | VALUE            | DESCRIPTION  |
|-----------|----------|------------------|--|
|           |          | no               | Disable the User account   |
|           | Password | <admin_password> | Password for the User account to access the StellarProtect (Legacy Mode) console<br><br><hr/>  <b>Note</b><br>The StellarProtect (Legacy Mode) Administrator and User passwords cannot be the same. |

## UI Section

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

**TABLE 5-3. Configuration File - UI Section Parameters**

| PARAMETER          | SETTINGS                                | VALUE | DESCRIPTION  |
|--------------------|---|-------|--|
| Configuration      | Container for the Configuration section |       |  |
| UI                 | Container for the UI section            |       |  |
| SystemTaskTrayIcon | Enable                                  | yes   | Display the system tray icon and Windows notifications |

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

| PARAMETER | SETTINGS | VALUE     | DESCRIPTION                              |
|-----------|----------|-----------|--|
|           | Title    | <Title>   | Specify the title for the notification   |
|           | Message  | <Message> | Specify the message for the notification |

## Feature Section

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

**TABLE 5-4. Configuration File - Feature Section Parameters**

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

| PARAMETER  | SETTINGS | VALUE                  | DESCRIPTION   |
|--|----------|------------------------|---|
| ScriptLockDown                                   | Enable   | yes                    | Enable Script Lockdown  |
|  | Disable  | no                     | Disable Script Lockdown   |
| Extension  | ID       | <file_extension>       | File extension for Script Lockdown to block<br><br>For example, specify a value of MSI to block .msi files              |
| Interpreter                                      |          | <file_name>            | Interpreter for the specified file extension<br><br>For example, specify msisexec.exe as the interpreter for .msi files |
| TrustedUpdater<br>PredefinedTrustedUpdater       | Enable   | yes                    | Enable Trusted Updater  |
|  |          | no                     | Disable Trusted Updater   |
| <b>RuleSet: Container for RuleSet conditions</b> |          |                        |   |
| Condition  | ID       | <unique_rule_set_name> | Unique name for the set of rules  |
| Approved ListCheck                               | Enable   | yes                    | Enable hash checks for programs executed using the Trusted Updater  |
|  |          | no                     | Disable hash checks for programs executed using the Trusted Updater   |

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

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

| PARAMETER                           | SETTINGS | VALUE                | DESCRIPTION  |
|-------------------------------------|----------|----------------------|--|
| PredefinedTruste<br>dC 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                                |
| PredefinedTruste<br>dHash           | Type     | updater              | File matched by this hash value is treated as a Trusted Update     |
|                                     |          | lockdown             | File matched by this hash value is not treated as a Trusted Update |
|                                     | Hash     | <SHA-1 _hash_ value> | SHA-1 hash value of this file                                      |
|                                     | Label    | <label>              | Description of this file   |



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

| PARAMETER                                     | SETTINGS         | VALUE         | DESCRIPTION   |
|---|------------------|---------------|---|
|   |                  | no            | Disable protection of the Approved List (in addition to the Write Protection List) when Write Protection is enabled |
| List: Container for the Write Protection List |                  |               |   |
| File  | Path             | <file_path>   | File path   |
| Folder  | Path             | <folder_path> | Folder path   |
|   | IncludeSubfolder | yes           | Use the files in the specified folder and its subfolders  |
|   |                  | no            | Use the files in the specified folder   |

| PARAMETER   | SETTINGS      | VALUE     | DESCRIPTION   |
|-------------|---------------|-----------|---|
| RegistryKey | Key           | <reg_key> | <p>Registry key</p> <p>&lt;reg_key&gt; can be abbreviated or expanded as shown below:</p> <ul style="list-style-type: none"> <li>• HKEY_LOCAL_MACHINE\test<br/>HKLM\test</li> <li>• HKEY_CURRENT_CONFIG\test<br/>HKCC\test</li> <li>• HKEY_CLASSES_ROOT\test<br/>HKCR\test</li> <li>• HKEY_CURRENT_USER\test<br/>HKCU\test</li> <li>• HKEY_USERS\test<br/>HKU\test</li> </ul> |
|             | IncludeSubkey | yes       | Include any subkeys   |
|             |               | no        | Do not include any subkeys  |

| PARAMETER   | SETTINGS         | VALUE           | DESCRIPTION  |
|---|------------------|-----------------|--|
| RegistryValue   | Key              | <reg_key>       | Registry key<br><reg_key> can be abbreviated or expanded as shown below: <ul style="list-style-type: none"> <li>• HKEY_LOCAL_MACHINE\test<br/>HKLM\test</li> <li>• HKEY_CURRENT_CONFIG\test<br/>HKCC\test</li> <li>• HKEY_CLASSES_ROOT\test<br/>HKCR\test</li> <li>• HKEY_CURRENT_USER\test<br/>HKCU\test</li> <li>• HKEY_USERS\test<br/>HKU\test</li> </ul> |
|   | Name             | reg_value_name> | Registry value name  |
| <b>ExceptionList: Container for the Write Protection Exception List</b> |                  |                 |  |
| Process   | Path             | <process_path>  | Path of the process  |
| File  | Path             | <file_path>     | File path  |
| Folder  | Path             | <folder_path>   | Folder path  |
|   | IncludeSubfolder | yes             | Use the files in the specified folder and its subfolders   |

| PARAMETER   | SETTINGS | VALUE                      | DESCRIPTION  |
|-------------|----------|----------------------------|--|
|             |          | no                         | Use the files in the specified folder  |
| RegistryKey | Key      | <reg_key>                  | Registry key<br><reg_key> can be abbreviated or expanded as shown below: <ul style="list-style-type: none"> <li>• HKEY_LOCAL_MACHINE\test</li> <li>   HKLM\test</li> <li>• HKEY_CURRENT_CONFIG\test</li> <li>   HKCC\test</li> <li>• HKEY_CLASSES_ROOT\test</li> <li>   HKCR\test</li> <li>• HKEY_CURRENT_USER\test</li> <li>   HKCU\test</li> <li>• HKEY_USERS\test</li> <li>   HKU\test</li> </ul> |
|             |          | yes                        | Include any subkeys  |
|             | no       | Do not include any subkeys |  |

| PARAMETER     | SETTINGS   | VALUE            | DESCRIPTION   |
|---------------|------------|------------------|---|
| RegistryValue | Key        | <reg_key>        | <p>Registry key</p> <p>&lt;reg_key&gt; can be abbreviated or expanded as shown below:</p> <ul style="list-style-type: none"> <li>• HKEY_LOCAL_MACHINE \testHKLM \test</li> <li>• HKEY_CURRENT_CONFIG \testHKCC \test</li> <li>• HKEY_CLASSES_ROOT \testHKCR \test</li> <li>• HKEY_CURRENT_USER \testHKCU \test</li> <li>• HKEY_USERS \testHKU\test</li> </ul> |
|               | Name       | <reg_value_name> | Registry value name   |
| CustomAction  | ActionMode | 0                | <p>Ignore blocked files or processes when Application Lockdown blocks any of the following events:</p> <ul style="list-style-type: none"> <li>• Process launch</li> <li>• DLL loading</li> <li>• Script file access</li> </ul>  |

| PARAMETER              | SETTINGS   | VALUE | DESCRIPTION   |
|------------------------|------------|-------|---|
|                        |            | 1     | Quarantine blocked files or processes when Application Lockdown blocks any of the following events: <ul style="list-style-type: none"> <li>• Process launch</li> <li>• DLL loading</li> <li>• Script file access</li> </ul>         |
|                        |            | 2     | Ask what to do for blocked files or processes when Application Lockdown blocks any of the following events: <ul style="list-style-type: none"> <li>• Process launch</li> <li>• DLL loading</li> <li>• Script file access</li> </ul> |
| UsbMalwareProtection   | Enable     | yes   | Enable USB Malware Protection   |
|                        |            | no    | Disable USB Malware Protection  |
|                        | ActionMode | 0     | Allow action by detected malware  |
|                        |            | 1     | Block action by detected malware  |
| DllInjectionPrevention | Enable     | yes   | Enable DLL Injection Prevention   |
|                        |            | no    | Disable DLL Injection Prevention  |

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



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

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

| PARAMETER | SETTINGS | VALUE                                   | DESCRIPTION   |
|-----------|----------|---|---|
| Parent4   |          | <great great<br>grandparent<br>process> | Great great<br>grandparent process<br>of the monitored<br>process |

## Log Section

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

**TABLE 5-5. Configuration File - Log Section Parameters**

| PARAMETER                                   | SETTINGS                                | VALUE | DESCRIPTION  |
|---|---|-------|--|
| Configuration                               | Container for the Configuration section |       |  |
| Feature                                     | Container for the Feature section       |       |  |
| Log   | Container for configuring logs          |       |  |
| EventLog                                    | Enable                                  | yes   | Log the StellarProtect (Legacy Mode) events specified in the following elements        |
|   |   | no    | Do not log the StellarProtect (Legacy Mode) events specified in the following elements |
| Level: Container for configuring log levels |   |       |  |
| WarningLog                                  | Enable                                  | yes   | Log "Warning" level events related to StellarProtect (Legacy Mode)                     |

| PARAMETER         | SETTINGS | VALUE | DESCRIPTION   |
|-------------------|----------|-------|---|
|                   |          | no    | Do not log "Warning" level events related to StellarProtect (Legacy Mode)     |
| InformationLog    | Enable   | yes   | Log "Information" level events related to StellarProtect (Legacy Mode)        |
|                   |          | no    | Do not log "Information" level events related to StellarProtect (Legacy Mode) |
| BlockedAccessLog  | Enable   | yes   | Log files blocked by StellarProtect (Legacy Mode)                             |
|                   |          | no    | Do not log files blocked by StellarProtect (Legacy Mode)                      |
| ApprovedAccessLog | Enable   | yes   | Log files approved by StellarProtect (Legacy Mode)                            |
|                   |          | no    | Do not log files approved by StellarProtect (Legacy Mode)                     |
| TrustedUpdaterLog | Enable   | yes   | Log Trusted Updater approved access   |
|                   |          | no    | Do not log Trusted Updater approved access                                    |
| DLLDriver Log     | Enable   | yes   | Log DLL/Driver approved access  |

| PARAMETER             | SETTINGS | VALUE | DESCRIPTION  |
|-----------------------|----------|-------|--|
|                       |          | no    | Do not log DLL/Driver approved access                          |
| Exception PathLog     | Enable   | yes   | Log Application Lockdown exception path approved access        |
|                       |          | no    | Do not log Application Lockdown exception path approved access |
| TrustedCertificateLog | Enable   | yes   | Log Trusted Certifications approved access                     |
|                       |          | no    | Do not log Trusted Certifications approved access              |
| 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                        |
| Exception PathLog     | Enable   | yes   | Log exceptions to Application Lockdown                         |
|                       |          | noe   | Do not log exceptions to Application Lockdown                  |
| WriteProtectionLog    | Enable   | yes   | Log Write Protection events                                    |

| PARAMETER  | SETTINGS | VALUE | DESCRIPTION   |
|--|----------|-------|---|
|  |          | no    | Do not log Write Protection events                    |
| ListLog  | Enable   | yes   | Log events related to the Approved list               |
|  |          | no    | Do not log events related to the Approved list        |
| UsbMalwareProtectionLog  | Enable   | yes   | Log events that trigger USB Malware Protection        |
|  |          | no    | Do not log events that trigger USB Malware Protection |
| ExecutionPreventionLog   | Enable   | yes   | Log events that trigger Execution Prevention          |
|  |          | no    | Do not log events that trigger Execution Prevention   |
| <b>IntegrityMonitoringLog: Container for configuring Integrity Monitoring logs</b> |          |       |   |
| FileCreatedLog   | Enable   | yes   | Log file and folder created events                    |
|  |          | no    | Do not log file and folder created events             |
| FileModifiedLog  | Enable   | yes   | Log file modified events                              |
|  |          | no    | Do not log file modified events                       |
| FileDeletedLog   | Enable   | yes   | Log file and folder deleted events                    |


| PARAMETER           | SETTINGS | VALUE | DESCRIPTION                               |
|---------------------|----------|-------|---|
|                     |          | no    | Do not log file and folder deleted events |
| FileRenamedLog      | Enable   | yes   | Log file and folder renamed events        |
|                     |          | no    | Do not log file and folder renamed events |
| RegValueModifiedLog | Enable   | yes   | Log registry value modified events        |
|                     |          | no    | Do not log registry value modified events |
| RegValueDeletedLog  | Enable   | yes   | Log registry value deleted events         |
|                     |          | no    | Do not log registry value deleted events  |
| RegKeyCreatedLog    | Enable   | yes   | Log registry key created events           |
|                     |          | no    | Do not log registry key created events    |
| RegKeyDeletedLog    | Enable   | yes   | Log registry key deleted events           |
|                     |          | no    | Do not log registry key deleted events    |
| RegKeyRenamedLog    | Enable   | yes   | Log registry key renamed events           |
|                     |          | no    | Do not log registry key renamed events    |
| DeviceControlLog    | Enable   | yes   | Log storage device control events         |

| PARAMETER | SETTINGS | VALUE | DESCRIPTION                              |
|-----------|----------|-------|--|
|           |          | no    | Do not log storage device control events |
| DebugLog  | Enable   | yes   | Log debugging information                |
|           |          | no    | Do not log debugging information         |



## Managed Mode Section

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



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

| PARAMETER  | SETTINGS   | VALUE  | DESCRIPTION   |
|--|--|--|---|
| Configuration  | Container for the Configuration section              |  |   |
| GroupPolicy  | Container for configuring group policy to StellarOne |  |   |
| SyncInterval   |  | 0 ~ 2147483647   | Agent information will be updated periodically according to this sync period          |
|  |  |  <b>Note</b><br>Unite:<br>Minutes |   |
| Agent: Container for configuring StellarProtect (Legacy Mode) agents |  |  |   |
| Port   |  | <server_messages_port>   | Specify the secure port for server communications (formerly the agent listening port) |
|  |  | no   | Do not log "Warning" level events related to StellarProtect (Legacy Mode)             |



| PARAMETER  | SETTINGS | VALUE   | DESCRIPTION  |
|--|----------|---|--|
| FixedIp  |          | <ul style="list-style-type: none"> <li>A . B . C . D / E</li> <li>A , B , C , D :<br/>0~255</li> <li>E : 1~32</li> </ul>                  | Specify the agent IP address (in Classless inter-domain routing (CIDR) format) to communicate with the StellarOne server   |
| server: Container for configuring StellarOne                         |          |   |  |
| HostName   |          | <hostname>  | Specify the host name of the StellarOne  |
| FastPort   |          | <logs_port>   | Specify secure port for collecting logs and status (formerly Fast Lane)  |
| Message : Container for configuring automated messages to StellarOne |          |   |  |
| InitialRetryInterval   |          | 0~2147483647<br><hr/>  <b>Note</b><br>Unit:<br>Seconds   | Starting interval, in seconds, between attempts to resend an event to StellarOne<br><br>This interval doubles in size for each unsuccessful attempt, until it exceeds the MaxRetryInterval value |
| MaxRetryInterval   |          | 0~2147483647<br><hr/>  <b>Note</b><br>Unit:<br>Seconds | Maximum interval between attempts to resend events to StellarOne   |

| <b>PARAMETER</b>    | <b>SETTINGS</b> | <b>VALUE</b>  | <b>DESCRIPTION</b>   |
|---------------------|-----------------|---|--|
| RegularStatusUpdate |                 | <ul style="list-style-type: none"><li>• 0</li><li>• 1</li></ul> | 0: Agent information will not be updated periodically during this sync period<br><br>1: Agent information will be updated periodically during this sync period |

| PARAMETER  | SETTINGS      | VALUE  | DESCRIPTION   |
|--|---------------|--|---|
| MessageRandomization<br><br><hr/>  <b>Note</b><br>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 ( $\geq 1$ )                                    | Specify the total number of message time groups   |
|  | OwnGroupIndex | Zero or Positive Integer, $\langle \text{TotalGroupNum} \rangle$ | 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<br><br><hr/>  <b>Note</b><br>Message time groups do not become active if their duration is set to zero (0). |
| Proxy  | Mode          | 0  | Do not use a proxy (direct access)  |
|  |               | 1  | Use a proxy (manual setting)  |

| PARAMETER | SETTINGS | VALUE              | DESCRIPTION                                       |
|-----------|----------|--------------------|---|
|           |          | 2                  | Synchronize proxy settings with Internet Explorer |
| HostName  |          | <proxy_hostname>   | Specify the proxy host name                       |
| Port      |          | <proxy_port>       | Specify the proxy port number                     |
| UserName  |          | <proxy_user_name > | Specify the proxy user name                       |
| Password  |          | <proxy_password>   | Specify the proxy password                        |


## AccountRef Section

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

Refer to [Password and Account Types on page 3-49](#) for more information about the StellarProtect (Legacy Mode) account types.

**TABLE 5-7. Configuration File - AccountRef Section Parameters**

| PARAMETER     | SETTINGS                                | VALUE         | DESCRIPTION   |
|---------------|---|---------------|---|
| Configuration | Container for the Configuration section |               |   |
| Permission    | Container for the Permission section    |               |   |
| AccountRef    | Container for the AccountRef section    |               |   |
| UIControl     | ID                                      | DetailSetting | Access the features and functions on the StellarProtect (Legacy Mode) console Settings page |

| PARAMETER | SETTINGS | VALUE                        | DESCRIPTION  |
|-----------|----------|------------------------------|--|
|           |          |                              |  <b>Note</b><br>The Password page is not available to the User account.                        |
|           |          | LockUnlock                   | Access the Application Lockdown setting on the <b>Overview</b> screen  |
|           |          | LaunchUpdater                | Access the <b>Automatically add files created or modified by the selected application installer</b> option when a User clicks <b>Add Item</b> on the <b>Approved List</b> screen |
|           |          | RecentHistoryUnapprovedFiles | Access the Block logs if a User clicks <b>Last application blocked</b> link on the <b>Overview</b> screen  |
|           |          | ImportExportList             | Access the <b>Import List</b> and <b>Export List</b> buttons   |
|           |          | ListManagement               | Access the following items on the <b>Approved List</b> screen: <ul style="list-style-type: none"> <li>• The <b>Delete Item</b> button</li> </ul>                                 |

| PARAMETER | SETTINGS | VALUE | DESCRIPTION  |
|-----------|----------|-------|--|
|           |          |       | <ul style="list-style-type: none"><li>• The <b>Update Hash</b> button</li><li>• The <b>Add Item &gt; Add Files/ Folders</b> menu</li></ul> |
|           | State    | yes   | Enable the permission specified by ID  |
|           |          | no    | Disable the permission specified by ID   |

# Chapter 6

## Agent Event Logs

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

- *Overview of Agent Event Logs on page 6-2*
- *StellarProtect Events on page 6-2*
- *StellarProtect (Legacy Mode) Events on page 6-24*

## Overview of Agent Event Logs

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

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

## StellarProtect Events

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

- [Accessing StellarProtect Event Logs on page 6-2](#)
- [Agent Event Log Descriptions for StellarProtect on page 6-2](#)

## Accessing StellarProtect Event Logs

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

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

## Agent Event Log Descriptions for StellarProtect

This table details the Windows event log descriptions for StellarProtect.

| EVENT ID | LEVEL       | CATEGORY | EVENT                | DETAILS |
|----------|-------------|----------|----------------------|---------|
| 256      | Information | System   | Service has started. |         |



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

| EVENT ID | LEVEL       | CATEGORY   | EVENT                                 | DETAILS   |
|----------|-------------|------------|---------------------------------------|---|
| 516      | Information | intelli_av | A scheduled scan has ended.           | Folders scanned: %1<br>Symbolic links: %2<br>Regular files: %3<br>Files scanned: %4<br>Files passed: %5<br>Threats detected: %6 |
| 517      | Information | intelli_av | A manually launched scan has started. |   |
| 518      | Information | intelli_av | A manually launched scan has ended.   | Folders scanned: %1<br>Symbolic links: %2<br>Regular files: %3<br>Files scanned: %4<br>Files passed: %5<br>Threats detected: %6 |
| 519      | Information | intelli_av | A scheduled scan has been enabled.    | Next scan will be on %NextScan %.   |
| 520      | Information | intelli_av | A scheduled scan has been disabled.   |   |

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

| EVENT ID | LEVEL       | CATEGORY       | EVENT  | DETAILS   |
|----------|-------------|----------------|--|---|
| 769      | Information | anomaly_detect | Script behavior has been added to the Situational Awareness baseline.        | Access User:<br>%USERNAME%<br><br>ID: %ID%<br><br>Target Process:<br>%PATH%<br>%ARGUMENT%<br><br>Parent Process<br>1: %PATH%<br>%ARGUMENT%<br><br>Parent Process<br>2: %PATH%<br>%ARGUMENT%<br><br>Parent Process<br>3: %PATH%<br>%ARGUMENT%<br><br>Parent Process<br>4: %PATH%<br>%ARGUMENT% |
| 770      | Information | anomaly_detect | A script behavior has been excluded from the Situational Awareness baseline. | ID: %ID%<br><br>Target Process:<br>%PATH%<br>%ARGUMENT%<br><br>Parent Process<br>1: %PATH%<br>%ARGUMENT%<br><br>Parent Process<br>2: %PATH%<br>%ARGUMENT%<br><br>Parent Process<br>3: %PATH%<br>%ARGUMENT%<br><br>Parent Process<br>4: %PATH%<br>%ARGUMENT%                                   |

| EVENT ID | LEVEL       | CATEGORY       | EVENT   | DETAILS  |
|----------|-------------|----------------|---|--|
| 771      | Information | anomaly_detect | Operations Behavior Anomaly Detection (User Login) has been enabled.            | Mode: %Mode%<br>Level: %Level%<br>Learning time: %LearningTime% day(s)               |
| 772      | Information | anomaly_detect | Operations Behavior Anomaly Detection (Application Behavior) has been enabled.  | Mode: %Mode%<br>Level: %Level%<br>Learning time: %LearningTime% day(s)               |
| 773      | Information | anomaly_detect | A user login account has been added to the Situational Awareness baseline.      | Domain: %Domain%<br>Account: %Account%<br>Login Type: %LoginType%<br>Source IP: %IP% |
| 774      | Information | anomaly_detect | A user login account has been excluded from the Situational Awareness baseline. | Domain: %Domain%<br>Account: %Account%<br>Login Type: %LoginType%<br>Source IP: %IP% |
| 775      | Information | anomaly_detect | An application has been added to the Situational Awareness baseline.            | Application Path: %Path%   |

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

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

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



| EVENT ID | LEVEL       | CATEGORY | EVENT                                       | DETAILS   |
|----------|-------------|----------|---|---|
| 2052     | Information | update   | Components updated successfully.            | Update Source:<br>%UPDATE_URL%<br><br>[Original Version]<br><br>%COMPONENTS_INFO%<br><br>[Updated Version]<br><br>%COMPONENTS_INFO% |
| 3840     | Information | misc     | User account has been enabled.              |   |
| 3841     | Information | misc     | User account has been disabled.             |   |
| 3842     | Information | misc     | User password has been changed.             |   |
| 4352     | Warning     | system   | Service has stopped.                        |   |
| 4353     | Warning     | system   | Unable to apply policy (Version: %version%) |   |
| 4354     | Warning     | system   | Unable to update file.                      | Source Path:<br>%src_path%<br><br>Destination Path: %dst_path%<br><br>Error Code:<br>%err_code%                                     |

| EVENT ID | LEVEL   | CATEGORY   | EVENT  | DETAILS   |
|----------|---------|------------|--|---|
| 4355     | Warning | system     | Unable to apply patch.                                       | File Name:<br>%file_name%<br><br>Error Code:<br>%err_code%  |
| 4609     | Warning | intelli_av | Incoming Files Scanned, Action Taken by Antivirus:<br>%PATH% | Incoming files were scanned by antivirus. Action was taken according to settings.<br><br>File Path: %PATH%<br><br>File Hash:<br>%STRING%<br><br>Threat Type:<br>%STRING%<br><br>Threat Name:<br>%STRING%<br><br>Action Result:<br>%INTEGER%<br><br>Quarantine Path:<br>%PATH% |

| EVENT ID | LEVEL   | CATEGORY   | EVENT   | DETAILS   |
|----------|---------|------------|---|---|
| 4610     | Warning | intelli_av | Incoming Files Scanned, Action Taken by Next-Generation Antivirus: %PATH% | <p>Incoming files were scanned by next-generation antivirus. Action was taken according to settings.</p> <p>File Path: %PATH%</p> <p>File Hash: %STRING%</p> <p>Threat Type: %STRING%</p> <p>Threat Name: %STRING%</p> <p>Action Result: %INTEGER%</p> <p>Quarantine Path: %PATH%</p> |

| EVENT ID | LEVEL   | CATEGORY   | EVENT  | DETAILS   |
|----------|---------|------------|--|---|
| 4611     | Warning | intelli_av | Local Files Scanned, Action Taken by Antivirus: %PATH% | Local files were scanned by antivirus. Action was taken according to settings.<br><br>File Path: %PATH%<br><br>File Hash: %STRING%<br><br>Threat Type: %STRING%<br><br>Threat Name: %STRING%<br><br>Action Result: %INTEGER%<br><br>Quarantine Path: %PATH% |

| EVENT ID | LEVEL   | CATEGORY   | EVENT  | DETAILS   |
|----------|---------|------------|--|---|
| 4612     | Warning | intelli_av | Local Files Scanned, Action Taken by Next-Generation Antivirus: %PATH% | Local files were scanned by next-generation antivirus. Action was taken according to settings.<br><br>File Path: %PATH%<br><br>File Hash: %STRING%<br><br>Threat Type: %STRING%<br><br>Threat Name: %STRING%<br><br>Action Result: %INTEGER%<br><br>Quarantine Path: %PATH% |
| 4613     | Warning | intelli_av | Suspicious Program Execution Blocked                                   | Suspicious program execution was blocked.<br><br>File Path: %PATH%<br><br>File Hash: %STRING%   |

| EVENT ID | LEVEL   | CATEGORY   | EVENT                                      | DETAILS  |
|----------|---------|------------|--|--|
| 4614     | Warning | intelli_av | Suspicious Program Currently Running       | Suspicious program is currently running.<br>Process ID: %PID %<br>File Path: %PATH %<br>File Hash: %STRING%<br>File Credibility: %STRING%              |
| 4615     | Warning | intelli_av | Application Execution Blocked By Antivirus | Application execution was blocked by antivirus.<br>Process Image Path: %PATH%<br>File Hash: %STRING%<br>Threat Type: %STRING%<br>Threat Name: %STRING% |

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

| EVENT ID | LEVEL   | CATEGORY       | EVENT   | DETAILS   |
|----------|---------|----------------|---|---|
| 4865     | Warning | anomaly_detect | Script Behavior has been allowed by Operations Behavior Anomaly Detection: %PATH% | Access User: %USERNAME%<br>Parent Process 1: %PATH% %ARGUMENT%<br>Parent Process 2: %PATH% %ARGUMENT%<br>Parent Process 3: %PATH% %ARGUMENT%<br>Parent Process 4: %PATH% %ARGUMENT%<br>Mode: %Mode%<br>Level: %LEVEL% |
| 4866     | Warning | anomaly_detect | Script Behavior has been blocked by Operations Behavior Anomaly Detection: %PATH% | Access User: %USERNAME%<br>Parent Process 1: %PATH% %ARGUMENT%<br>Parent Process 2: %PATH% %ARGUMENT%<br>Parent Process 3: %PATH% %ARGUMENT%<br>Parent Process 4: %PATH% %ARGUMENT%<br>Mode: %Mode%<br>Level: %LEVEL% |



| EVENT ID | LEVEL   | CATEGORY       | EVENT  | DETAILS   |
|----------|---------|----------------|--|---|
| 4867     | warning | anomaly_detect | Operations Behavior Anomaly Detection (User Login) has been disabled.              |   |
| 4868     | warning | anomaly_detect | Operations Behavior Anomaly Detection (Application Behavior) has been disabled.    |   |
| 4869     | warning | anomaly_detect | A user login failure has been detected by Operations Behavior Anomaly Detection.   | Domain:<br>%Domain%<br><br>Account:<br>%Account%<br><br>Login Type:<br>%LoginType%<br><br>Source IP: %IP% |
| 4870     | warning | anomaly_detect | An abnormal user Login has been detected by Operations Behavior Anomaly Detection. | Domain:<br>%Domain%<br><br>Account:<br>%Account%<br><br>Login Type:<br>%LoginType%<br><br>Source IP: %IP% |

| EVENT ID | LEVEL   | CATEGORY       | EVENT   | DETAILS  |
|----------|---------|----------------|---|--|
| 4871     | warning | anomaly_detect | Suspicious application behavior has been detected by Operations Behavior Anomaly Detection. | Program Path:<br>%Path%<br><br>Program Hash:<br>%SHA256%<br><br>Program Size:<br>%Size%<br><br>Certificate:<br>%CertificateSigner%<br><br>Vendor:<br>%VendorName%<br><br>Product:<br>%Product%                   |
| 4872     | warning | anomaly_detect | An unrecognized application has been detected by Operations Behavior Anomaly Detection.     | PID: %PID%<br><br>Program Path:<br>%Path%<br><br>Program Hash:<br>%SHA256%<br><br>Program Size:<br>%Size%<br><br>Certificate:<br>%CertificateSigner%<br><br>Vendor:<br>%VendorName%<br><br>Product:<br>%Product% |

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

| EVENT ID | LEVEL   | CATEGORY       | EVENT  | DETAILS   |
|----------|---------|----------------|--|---|
| 5377     | Warning | device_control | USB access has been blocked:<br>%PATH%         | Access Image Path: %PATH%<br><br>Access User: %USERNAME%<br><br>Vendor ID: %HEX %<br><br>Product ID: %HEX%<br><br>Serial Number: %STRING%                                       |
| 5378     | Warning | device_control | USB autorun.inf file has been blocked: %PATH % |   |
| 5888     | Warning | lockdown       | File access has been allowed:<br>%PATH%        | Access Image Path: %PATH%<br><br>Access User: %USERNAME%<br><br>Mode: %MODE%<br><br>Reason: %ALLOWED_REASON%<br><br>File hash allowed: %SHA256_HEXSTR%<br>%THROTTLING_INFO_MSG% |

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

| EVENT ID | LEVEL    | CATEGORY       | EVENT  | DETAILS  |
|----------|----------|----------------|--|--|
| 6144     | Warning  | update         | Component update unsuccessful. (%AU_ERROR_CODE%) | Update Source: %UPDATE_URL%<br>[Original Version]<br>%COMPONENTS_INFO%<br>[Updated Version]<br>%COMPONENTS_INFO% |
| 8706     | Critical | intelli_av     | Real-Time Scan has been disabled.                |  |
| 9216     | Critical | change_control | The Maintenance Mode has now started.            |  |
| 9217     | Critical | change_control | The Maintenance Mode has now ended.              |  |

## StellarProtect (Legacy Mode) Events

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

- [Agent Event Log Descriptions for StellarProtect \(Legacy Mode\) on page 6-24](#)
- [Agent Error Code Descriptions for StellarProtect \(Legacy Mode\) on page 6-72](#)

## Agent Event Log Descriptions for StellarProtect (Legacy Mode)

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

| EVENT ID | LEVEL       | CATEGORY | EVENT  | DETAILS |
|----------|-------------|----------|--|---------|
| 1000     | Information | System   | Service started                              |         |
| 1001     | Warning     | System   | Service stopped                              |         |
| 1002     | Information | System   | Application<br>Lockdown Turned<br>On         |         |
| 1003     | Warning     | System   | Application<br>Lockdown Turned<br>Off        |         |
| 1004     | Information | System   | Disabled                                     |         |
| 1005     | Information | System   | Administrator<br>password<br>changed         |         |
| 1006     | Information | System   | User password<br>changed                     |         |
| 1007     | Information | System   | User account<br>enabled                      |         |
| 1008     | Information | System   | User account<br>disabled                     |         |
| 1009     | Information | System   | Product activated                            |         |
| 1010     | Information | System   | Product<br>deactivated                       |         |
| 1011     | Warning     | System   | License Expired.<br>Grace period<br>enabled. |         |
| 1012     | Warning     | System   | License Expired.<br>Grace period<br>ended.   |         |
| 1013     | Information | System   | Product<br>configuration                     |         |

| EVENT ID | LEVEL       | CATEGORY | EVENT  | DETAILS |
|----------|-------------|----------|--|---------|
|          |             |          | import started:<br>%path%                                  |         |
| 1014     | Information | System   | Product<br>configuration<br>import<br>completed:<br>%path% |         |
| 1015     | Information | System   | Product<br>configuration<br>exported to:<br>%path%         |         |
| 1016     | Information | System   | USB Malware<br>Protection set to<br>Allow                  |         |
| 1017     | Information | System   | USB Malware<br>Protection set to<br>Block                  |         |
| 1018     | Information | System   | USB Malware<br>Protection<br>enabled                       |         |
| 1019     | Warning     | System   | USB Malware<br>Protection<br>disabled                      |         |
| 1025     | Information | System   | Memory<br>Randomization<br>enabled                         |         |
| 1026     | Warning     | System   | Memory<br>Randomization<br>disabled                        |         |
| 1027     | Information | System   | API Hooking<br>Prevention set to<br>Allow                  |         |



| EVENT ID | LEVEL       | CATEGORY | EVENT                                 | DETAILS |
|----------|-------------|----------|---------------------------------------|---------|
| 1028     | Information | System   | API Hooking Prevention set to Block   |         |
| 1029     | Information | System   | API Hooking Prevention enabled        |         |
| 1030     | Warning     | System   | API Hooking Prevention disabled       |         |
| 1031     | Information | System   | DLL Injection Prevention set to Allow |         |
| 1032     | Information | System   | DLL Injection Prevention set to Block |         |
| 1033     | Information | System   | DLL Injection Prevention enabled      |         |
| 1034     | Warning     | System   | DLL Injection Prevention disabled     |         |
| 1035     | Information | System   | Pre-defined Trusted Update enabled    |         |
| 1036     | Information | System   | Pre-defined Trusted Update disabled   |         |
| 1037     | Information | System   | DLL/Driver Lockdown enabled           |         |
| 1038     | Warning     | System   | DLL/Driver Lockdown disabled          |         |

| EVENT ID | LEVEL       | CATEGORY | EVENT                         | DETAILS   |
|----------|-------------|----------|-------------------------------|---|
| 1039     | Information | System   | Script Lockdown enabled       |   |
| 1040     | Warning     | System   | Script Lockdown disabled      |   |
| 1041     | Information | System   | Script added                  | File extension:<br>%extension%<br><br>Interpreter:<br>%interpreter% |
| 1042     | Information | System   | Script removed                | File extension:<br>%extension%<br><br>Interpreter:<br>%interpreter% |
| 1044     | Information | System   | Exception path enabled        |   |
| 1045     | Information | System   | Exception path disabled       |   |
| 1047     | Information | System   | Trusted certificate enabled   |   |
| 1048     | Information | System   | Trusted certificate disabled  |   |
| 1049     | Information | System   | Write Protection enabled      |   |
| 1050     | Warning     | System   | Write Protection disabled     |   |
| 1051     | Information | System   | Write Protection set to Allow |   |
| 1052     | Information | System   | Write Protection set to Block |   |

| EVENT ID | LEVEL       | CATEGORY | EVENT   | DETAILS |
|----------|-------------|----------|---|---------|
| 1055     | Information | System   | Added file to Write Protection List<br>Path: %path%                                     |         |
| 1056     | Information | System   | Removed file from Write Protection List<br>Path: %path%                                 |         |
| 1057     | Information | System   | Added file to Write Protection Exception List<br>Path: %path%<br>Process: %process%     |         |
| 1058     | Information | System   | Removed file from Write Protection Exception List<br>Path: %path%<br>Process: %process% |         |
| 1059     | Information | System   | Added folder to Write Protection List<br>Path: %path%<br>Scope: %scope%                 |         |
| 1060     | Information | System   | Removed folder from Write Protection List<br>Path: %path%<br>Scope: %scope%             |         |

| EVENT ID | LEVEL       | CATEGORY | EVENT   | DETAILS |
|----------|-------------|----------|---|---------|
| 1061     | Information | System   | Added folder to Write Protection Exception List<br><br>Path: %path%<br><br>Scope: %scope%<br><br>Process: %process%     |         |
| 1062     | Information | System   | Removed folder from Write Protection Exception List<br><br>Path: %path%<br><br>Scope: %scope%<br><br>Process: %process% |         |
| 1063     | Information | System   | Added registry value to Write Protection List<br><br>Registry Key: %regkey%<br><br>Registry Value Name: %regvalue %     |         |
| 1064     | Information | System   | Removed registry value from Write Protection List<br><br>Registry Key: %regkey%<br><br>Registry Value Name: %regvalue % |         |

| EVENT ID | LEVEL       | CATEGORY | EVENT   | DETAILS |
|----------|-------------|----------|---|---------|
| 1065     | Information | System   | Added registry value to Write Protection Exception List<br><br>Registry Key: %regkey%<br><br>Registry Value Name: %regvalue %<br><br>Process: %process%     |         |
| 1066     | Information | System   | Removed registry value from Write Protection Exception List<br><br>Registry Key: %regkey%<br><br>Registry Value Name: %regvalue %<br><br>Process: %process% |         |
| 1067     | Information | System   | Added registry key to Write Protection List<br><br>Path: %regkey%<br><br>Scope: %scope%   |         |
| 1068     | Information | System   | Removed registry key from Write Protection List<br><br>Path: %regkey%<br><br>Scope: %scope%   |         |

| EVENT ID | LEVEL       | CATEGORY | EVENT   | DETAILS  |
|----------|-------------|----------|---|--|
| 1069     | Information | System   | Added registry key to Write Protection Exception List<br><br>Path: %regkey%<br><br>Scope: %scope%<br><br>Process: %process%     |  |
| 1070     | Information | System   | Removed registry key from Write Protection Exception List<br><br>Path: %regkey%<br><br>Scope: %scope%<br><br>Process: %process% |  |
| 1071     | Information | System   | Custom Action set to Ignore   |  |
| 1072     | Information | System   | Custom Action set to Quarantine   |  |
| 1073     | Information | System   | Custom Action set to Ask StellarOne   |  |
| 1074     | Information | System   | Quarantined file is restored.   | Original Location: %path%<br><br>Source: %source % |
| 1075     | Information | System   | Quarantined file is deleted.  | Original Location: %path%<br><br>Source: %source % |

| EVENT ID | LEVEL       | CATEGORY | EVENT   | DETAILS                   |
|----------|-------------|----------|---|---------------------------|
| 1076     | Information | System   | Integrity Monitoring enabled  |                           |
| 1077     | Information | System   | Integrity Monitoring disabled   |                           |
| 1078     | Information | System   | Root cause analysis report unsuccessful                                   | Access Image Path: %path% |
| 1079     | Information | System   | Server certification imported: %path %                                    |                           |
| 1080     | Information | System   | Server certification exported: %path %                                    |                           |
| 1081     | Information | System   | Managed mode configuration imported: %path %                              |                           |
| 1082     | Information | System   | Managed mode configuration exported: %path %                              |                           |
| 1083     | Information | System   | Managed mode enabled  |                           |
| 1084     | Information | System   | Managed mode disabled   |                           |
| 1085     | Information | System   | Protection applied to Write Protection List and Approved List while Write |                           |

| EVENT ID | LEVEL       | CATEGORY | EVENT  | DETAILS |
|----------|-------------|----------|--|---------|
|          |             |          | Protection is enabled  |         |
| 1086     | Warning     | System   | Protection applied to Write Protection List while Write Protection is enabled. |         |
| 1088     | Information | System   | Windows Update Support enabled   |         |
| 1089     | Information | System   | Windows Update Support disabled  |         |
| 1094     | Information | System   | Applied a patch to agent by StellarOne<br><br>File applied: %file_name%        |         |
| 1096     | Information | System   | Trusted hash enabled   |         |
| 1097     | Information | System   | Trusted hash disabled  |         |
| 1099     | Information | System   | Storage device access set to Allow   |         |
| 1100     | Information | System   | Storage device access set to Block   |         |
| 1101     | Information | System   | Storage device control enabled   |         |
| 1102     | Warning     | System   | Storage device control disabled  |         |



| EVENT ID | LEVEL       | CATEGORY | EVENT                      | DETAILS  |
|----------|-------------|----------|----------------------------|--|
| 1103     | Information | System   | Event Log settings changed | Windows Event Log: %ON off%<br>Level: Warning Log: %ON off%<br>Information Log: %ON off%<br>System Log: %ON off%<br>Exception Path Log: %ON off%<br>Write Protection Log: %ON off%<br>List Log: %ON off%<br>Approved Access Log: DllDriver Log: %ON off%<br>Trusted Updater Log: %ON off%<br>Exception Path Log: %ON off%<br>Trusted Certification Log: %ON off%<br>Trusted Hash Log: %ON off%<br>Write Protection Log: %ON off%<br>Blocked Access Log: %ON off%<br>USB Malware Protection Log: %ON off% |

| EVENT ID | LEVEL   | CATEGORY | EVENT   | DETAILS   |
|----------|---------|----------|---|---|
|          |         |          |   | Execution Prevention Log: %ON off%<br>Integrity Monitoring Log<br>File Created Log: %ON off%<br>File Modified Log: %ON off%<br>File Deleted Log: %ON off%<br>File Renamed Log: %ON off%<br>RegValue Modified Log: %ON off%<br>RegValue Deleted Log: %ON off%<br>RegKey Created Log: %ON off%<br>RegKey Deleted Log: %ON off%<br>RegKey Renamed Log: %ON off%<br>Device Control Log: %ON off%<br>Debug Log: %ON off% |
| 1104     | Warning | System   | Memory Randomization is not available in this version of Windows. |   |

| EVENT ID | LEVEL       | CATEGORY | EVENT                                   | DETAILS |
|----------|-------------|----------|---|---------|
| 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      |         |
| 1112     | Warning     | System   | Fileless Attack Prevention disabled     |         |
| 1500     | Information | List     | Trusted Update started.                 |         |
| 1501     | Information | List     | Trusted Update stopped.                 |         |
| 1502     | Information | List     | Approved List import started: %path%    |         |
| 1503     | Information | List     | Approved List import complete: %path%   |         |
| 1504     | Information | List     | Approved List exported to: %path%       |         |
| 1505     | Information | List     | Added to Approved List: %path%          |         |

| EVENT ID | LEVEL       | CATEGORY | EVENT  | DETAILS  |
|----------|-------------|----------|--|--|
| 1506     | Information | List     | Added to Trusted Updater List:<br>%path%                   |  |
| 1507     | Information | List     | Removed from Approved List:<br>%path%                      |  |
| 1508     | Information | List     | Removed from Trusted Updater List: %path%                  |  |
| 1509     | Information | List     | Approved List updated: %path%                              |  |
| 1510     | Information | List     | Trusted Updater List updated:<br>%path%                    |  |
| 1511     | Warning     | List     | Unable to add to or update Approved List:<br>%path%        |  |
| 1512     | Warning     | List     | Unable to add to or update Trusted Updater List:<br>%path% |  |
| 1513     | Information | System   | Added to Exception Path List                               | Type:<br>%exceptionpath<br>type%<br><br>Path:<br>%exceptionpath<br>% |
| 1514     | Information | System   | Removed from Exception Path List                           | Type:<br>%exceptionpath<br>type%                                     |

| EVENT ID | LEVEL       | CATEGORY | EVENT                                   | DETAILS  |
|----------|-------------|----------|---|--|
|          |             |          |   | Path:<br>%exceptionpath<br>%   |
| 1515     | Information | System   | Added to Trusted Certification List     | Label: %label%<br>Hash:<br>%hashvalue%<br>Type: %type%<br>Subject: %subject<br>%<br>Issuer: %issuer%                         |
| 1516     | Information | System   | Removed from Trusted Certification List | Label: %label%<br>Hash:<br>%hashvalue%<br>Type: %type%<br>Subject: %subject<br>%<br>Issuer: %issuer%                         |
| 1517     | Information | System   | Added to Trusted Hash List.%n           | Label : %label%<br>Hash :<br>%hashvalue%<br>Type : %type%<br>Add to Approved List: %yes no%<br>Path : %path%<br>Note: %note% |
| 1518     | Information | System   | Removed from Trusted Hash List.%n       | Label : %label%<br>Hash :<br>%hashvalue%<br>Type : %type%  |

| EVENT ID | LEVEL       | CATEGORY | EVENT   | DETAILS  |
|----------|-------------|----------|---|--|
|          |             |          |   | Add to Approved List: %yes no%<br>Path : %path%<br>Note: %note%  |
| 1519     | Information | List     | Removed from Approved List remotely: %path %  |  |
| 1520     | Warning     | List     | Unable to create Approved List because an unexpected error occurred during enumeration of the files in %1 %<br>Error Code: %2 %<br>%n |  |
| 1521     | Information | System   | Added Fileless Attack Prevention exception  | Label : %label%<br>Target Process: %process_name %<br>Arguments: %arguments% %regex_flag%<br>Parent Process 1 Image Path: %path%<br>Parent Process 2 Image Path: %path%<br>Parent Process 3 Image Path: %path% |

| EVENT ID | LEVEL       | CATEGORY | EVENT   | DETAILS   |
|----------|-------------|----------|---|---|
|          |             |          |   | Parent Process 4<br>Image Path:<br>%path%   |
| 1522     | Information | System   | Removed Fileless<br>Attack Prevention<br>exception  | Label : %label%<br><br>Target Process:<br>%process_name<br>%<br><br>Arguments:<br>%arguments%<br>%regex_flag%<br><br>Parent Process 1<br>Image Path:<br>%path%<br><br>Parent Process 2<br>Image Path:<br>%path%<br><br>Parent Process 3<br>Image Path:<br>%path%<br><br>Parent Process 4<br>Image Path:<br>%path% |
| 1523     | Information | System   | Maintenance<br>Mode started                         |   |
| 1524     | Information | System   | Leaving<br>Maintenance<br>Mode                      |   |
| 1525     | Information | System   | Maintenance<br>Mode stopped                         |   |
| 1526     | Information | List     | Added to<br>Approved List in<br>Maintenance<br>Mode |   |

| EVENT ID | LEVEL       | CATEGORY        | EVENT   | DETAILS   |
|----------|-------------|-----------------|---|---|
|          |             |                 | Path: %1<br>Hash: %2  |   |
| 1527     | Information | List            | Approved List updated in Maintenance Mode<br>Path: %1<br>Hash: %2                           |   |
| 2000     | Information | Access Approved | File access allowed: %path%   | Access Image Path: %path%<br>Access User: %username%<br>Mode: %mode%<br>List: %list%              |
| 2001     | Warning     | Access Approved | File access allowed: %path%   | Access Image Path: %path%<br>Access User: %username%<br>Mode: %mode%<br>File Hash allowed: %hash% |
| 2002     | Warning     | Access Approved | File access allowed: %path%<br>Unable to get the file path while checking the Approved List | Access Image Path: %path%<br>Access User: %username%<br>Mode: %mode%                              |
| 2003     | Warning     | Access Approved | File access allowed: %path%<br>Unable to calculate hash                                     | Access Image Path: %path%<br>Access User: %username%  |




| EVENT ID | LEVEL       | CATEGORY        | EVENT  | DETAILS  |
|----------|-------------|-----------------|--|--|
|          |             |                 | while checking the Approved List   | Mode: %mode%   |
| 2004     | Warning     | Access Approved | File access allowed: %path%<br>Unable to get notifications to monitor process                  |  |
| 2005     | Warning     | Access Approved | File access allowed: %path%<br>Unable to add process to non exception list                     |  |
| 2006     | Information | Access Approved | File access allowed: %path%  | Access Image Path: %path%<br>Access User: %username%<br>Mode: %mode% |
| 2007     | Warning     | Access Approved | File access allowed: %path%<br>An error occurred while checking the Exception Path List        | Access Image Path: %path%<br>Access User: %username%<br>Mode: %mode% |
| 2008     | Warning     | Access Approved | File access allowed: %path%<br>An error occurred while checking the Trusted Certification List | Access Image Path: %path%<br>Access User: %username%<br>Mode: %mode% |
| 2011     | Information | Access Approved | Registry access allowed<br>Registry Key: %regkey%  | Access Image Path: %path%<br>Access User: %username%                 |

| EVENT ID | LEVEL       | CATEGORY        | EVENT  | DETAILS  |
|----------|-------------|-----------------|--|--|
|          |             |                 | Registry Value Name: %regvalue %   | Mode: %mode%   |
| 2012     | Information | Access Approved | Registry access allowed<br><br>Registry Key: %regkey%  | Access Image Path: %path%<br><br>Access User: %username%<br><br>Mode: %mode% |
| 2013     | Information | Access Approved | Change of File/ Folder allowed by Exception List: %path%   | Access Image Path: %path%<br><br>Access User: %username%<br><br>Mode: %mode% |
| 2015     | Information | Access Approved | Change of Registry Value allowed by Exception List<br><br>Registry Key: %regkey%<br><br>Registry Value Name: %regvalue % | Access Image Path: %path%<br><br>Access User: %username%<br><br>Mode: %mode% |
| 2016     | Information | Access Approved | Change of Registry Key allowed by Exception List<br><br>Registry Key: %regkey%   | Access Image Path: %path%<br><br>Access User: %username%<br><br>Mode: %mode% |
| 2017     | Warning     | Access Approved | Change of File/ Folder allowed: %path%   | Access Image Path: %path%<br><br>Access User: %username%                     |

| EVENT ID | LEVEL   | CATEGORY        | EVENT   | DETAILS  |
|----------|---------|-----------------|---|--|
|          |         |                 |   | Mode: %mode%   |
| 2019     | Warning | Access Approved | Change of Registry Value allowed<br><br>Registry Key: %regkey%<br><br>Registry Value Name: %regvalue% | Access Image Path: %path%<br><br>Access User: %username%<br><br>Mode: %mode%   |
| 2020     | Warning | Access Approved | Change of Registry Key allowed<br><br>Registry Key: %regkey%  | Access Image Path: %path%<br><br>Access User: %username%<br><br>Mode: %mode%   |
| 2021     | Warning | Access Approved | File access allowed: %path%<br><br>An error occurred while checking the Trusted Hash List             | Access Image Path: %path%<br><br>Access User: %username%<br><br>Mode: %mode%   |
| 2022     | Warning | Access Approved | Process allowed by Fileless Attack Prevention:<br>%path%<br>%argument%                                | Access User: %username%<br><br>Parent Process 1 Image Path: %path%<br><br>Parent Process 2 Image Path: %path%<br><br>Parent Process 3 Image Path: %path% |

| EVENT ID | LEVEL       | CATEGORY       | EVENT   | DETAILS  |
|----------|-------------|----------------|---|--|
|          |             |                |   | Parent Process 4<br>Image Path:<br>%path%<br><br>Mode: Unlocked<br><br>Reason: %reason%<br>% |
| 2503     | Warning     | Access Blocked | Change of File/<br>Folder blocked:<br>%path%  | Access Image<br>Path: %path%<br><br>Access User:<br>%username%<br><br>Mode: %mode%           |
| 2505     | Warning     | Access Blocked | Change of<br>Registry Value<br>blocked.<br><br>Registry Key:<br>%regkey%<br><br>Registry Value<br>Name: %regvalue%<br>% | Access Image<br>Path: %path%<br><br>Access User:<br>%username%<br><br>Mode: %mode%           |
| 2506     | Warning     | Access Blocked | Change of<br>Registry Key<br>blocked.<br><br>Registry Key:<br>%regkey%  | Access Image<br>Path: %path%<br><br>Access User:<br>%username%<br><br>Mode: %mode%           |
| 2507     | Information | Access Blocked | Action completed<br>successfully:<br>%path%   | Action: %action%<br><br>Source: %source%<br>%  |
| 2508     | Warning     | Access Blocked | Unable to take<br>specified action:<br>%path%   | Action: %action%<br><br>Source: %source%<br>%  |

| EVENT ID | LEVEL       | CATEGORY       | EVENT   | DETAILS   |
|----------|-------------|----------------|---|---|
| 2509     | Warning     | Access Blocked | File access blocked: %path%                                 | Access Image Path: %path%<br>Access User: %username%<br>Mode: %mode%<br>Reason: Not in Approved List<br>File Hash blocked: %hash%               |
| 2510     | Warning     | Access Blocked | File access blocked: %path%                                 | Access Image Path: %path%<br>Access User: %username%<br>Mode: %mode%<br>Reason: Hash does not match expected value<br>File Hash blocked: %hash% |
| 2511     | Information | Access Blocked | Change of File/ Folder blocked: %path%                      | Access Image Path: %path%<br>Access User: %username%<br>Mode: %mode%  |
| 2512     | Warning     | Access Blocked | Change of Registry Value blocked.<br>Registry Key: %regkey% | Access Image Path: %path%<br>Access User: %username%  |

| EVENT ID | LEVEL   | CATEGORY       | EVENT  | DETAILS   |
|----------|---------|----------------|--|---|
|          |         |                | Registry Value Name: %regvalue %                                       |  <b>Note</b><br>Enabling the Service Creation Prevention feature triggers Event ID 2512.   |
| 2513     | Warning | Access Blocked | Process blocked by Fileless Attack Prevention:<br>%path%<br>%argument% | Access User: %username%<br><br>Parent Process 1 Image Path: %path%<br><br>Parent Process 2 Image Path: %path%<br><br>Parent Process 3 Image Path: %path%<br><br>Parent Process 4 Image Path: %path%<br><br>Mode: locked<br><br>Reason: %reason% |
| 2514     | Warning | Access Blocked | File access blocked:<br>%BLOCKED_FILE_PATH%                            | Access Image Path: %PARENT_PROCESS_PATH%<br><br>Access User: %USER_NAME%  |

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

| EVENT ID | LEVEL       | CATEGORY                 | EVENT                            | DETAILS  |
|----------|-------------|--------------------------|----------------------------------|--|
|          |             |                          |                                  | Threat User:<br>%username%   |
| 4004     | Warning     | Process Protection Event | DLL Injection allowed: %path%    | Threat Image Path: %path%<br>Threat User: %username%                             |
| 4005     | Warning     | Process Protection Event | DLL Injection blocked: %path%    | Threat Image Path: %path%<br>Threat User: %username%                             |
| 4500     | Information | Changes in System        | File/Folder created: %path%      | Access Image Path: %path%<br>Access Process Id: %pid%<br>Access User: %username% |
| 4501     | Information | Changes in System        | File modified: %path%            | Access Image Path: %path%<br>Access Process Id: %pid%<br>Access User: %username% |
| 4502     | Information | Changes in System        | File/Folder deleted: %path%      | Access Image Path: %path%<br>Access Process Id: %pid%<br>Access User: %username% |
| 4503     | Information | Changes in System        | File/Folder renamed: %path%<br>% | Access Image Path: %path%<br>Access Process Id: %pid%                            |



| EVENT ID | LEVEL       | CATEGORY          | EVENT  | DETAILS  |
|----------|-------------|-------------------|--|--|
|          |             |                   | New Path: %path%   | Access User: %username%  |
| 4504     | Information | Changes in System | Registry Value modified.<br><br>Registry Key: %regkey%<br><br>Registry Value Name: %regvalue%<br><br>Registry Value Type: %regvaluetype% | Access Image Path: %path%<br><br>Access Process Id: %pid%<br><br>Access User: %username% |
| 4505     | Information | Changes in System | Registry Value deleted.<br><br>Registry Key: %regkey%<br><br>Registry Value Name: %regvalue%<br>%  | Access Image Path: %path%<br><br>Access Process Id: %pid%<br><br>Access User: %username% |
| 4506     | Information | Changes in System | Registry Key created.<br><br>Registry Key: %regkey%  | Access Image Path: %path%<br><br>Access Process Id: %pid%<br><br>Access User: %username% |
| 4507     | Information | Changes in System | Registry Key deleted.<br><br>Registry Key: %regkey%  | Access Image Path: %path%<br><br>Access Process Id: %pid%<br><br>Access User: %username% |

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

| EVENT ID | LEVEL | CATEGORY | EVENT | DETAILS   |
|----------|-------|----------|-------|---|
|          |       |          |       | Pattern:<br>%VERSION%                                   |
|          |       |          |       | Damage Cleanup<br>Template:<br>%VERSION%                |
|          |       |          |       | Damage Cleanup<br>Engine<br>Configuration:<br>%VERSION% |
|          |       |          |       | Virus Scan<br>Engine:<br>%VERSION%                      |
|          |       |          |       | Damage Cleanup<br>Engine:<br>%VERSION%                  |
|          |       |          |       | Scanner:<br>%VERSION%                                   |
|          |       |          |       | [Updated Version]                                       |
|          |       |          |       | Virus Pattern:<br>%VERSION%                             |
|          |       |          |       | Spyware Pattern:<br>%VERSION%                           |
|          |       |          |       | Digital Signature<br>Pattern:<br>%VERSION%              |
|          |       |          |       | Program<br>Inspection<br>Pattern:<br>%VERSION%          |
|          |       |          |       | Damage Cleanup<br>Template:<br>%VERSION%                |
|          |       |          |       | Damage Cleanup<br>Engine                                |

| EVENT ID | LEVEL   | CATEGORY | EVENT   | DETAILS   |
|----------|---------|----------|---|---|
|          |         |          |   | Configuration:<br>%VERSION%<br><br>Virus Scan<br>Engine:<br>%VERSION%<br><br>Damage Cleanup<br>Engine:<br>%VERSION%<br><br>Scanner:<br>%VERSION%  |
| 6001     | Warning | System   | Update failed:<br>%ERROR_MSG%<br>(%ERROR_CODE<br>%) | Update Source:<br>%SERVER%<br><br>[Original Version]<br><br>Virus Pattern:<br>%VERSION%<br><br>Spyware Pattern:<br>%VERSION%<br><br>Digital Signature<br>Pattern:<br>%VERSION%<br><br>Program<br>Inspection<br>Pattern:<br>%VERSION%<br><br>Damage Cleanup<br>Template:<br>%VERSION%<br><br>Damage Cleanup<br>Engine<br>Configuration:<br>%VERSION%<br><br>Virus Scan<br>Engine:<br>%VERSION% |

| EVENT ID | LEVEL | CATEGORY | EVENT | DETAILS   |
|----------|-------|----------|-------|---|
|          |       |          |       | Damage Cleanup Engine:<br>%VERSION%<br><br>Scanner:<br>%VERSION%<br><br>[Updated Version]<br><br>Virus Pattern:<br>%VERSION%<br><br>Spyware Pattern:<br>%VERSION%<br><br>Digital Signature Pattern:<br>%VERSION%<br><br>Program Inspection Pattern:<br>%VERSION%<br><br>Damage Cleanup Template:<br>%VERSION%<br><br>Damage Cleanup Engine Configuration:<br>%VERSION%<br><br>Virus Scan Engine:<br>%VERSION%<br><br>Damage Cleanup Engine:<br>%VERSION%<br><br>Scanner:<br>%VERSION% |

| EVENT ID | LEVEL       | CATEGORY | EVENT                                | DETAILS  |
|----------|-------------|----------|--------------------------------------|--|
| 6002     | Information | System   | Malware scan started:<br>%SCAN_TYPE% | Files to scan:<br>%SCAN_FOLDER_TYPE%<br><br>Scanned folders:<br>%PATHS%<br><br>Excluded paths:<br>%PATHS%<br><br>Excluded files:<br>%PATHS%<br><br>Excluded extensions:<br>%PATHS%<br><br>[Components]<br><br>Virus Pattern:<br>%VERSION%<br><br>Spyware Pattern:<br>%VERSION%<br><br>Digital Signature Pattern:<br>%VERSION%<br><br>Program Inspection Pattern:<br>%VERSION%<br><br>Damage Cleanup Template:<br>%VERSION%<br><br>Damage Cleanup Engine Configuration:<br>%VERSION%<br><br>Virus Scan Engine:<br>%VERSION% |

| EVENT ID | LEVEL       | CATEGORY | EVENT   | DETAILS   |
|----------|-------------|----------|---|---|
|          |             |          |   | Damage Cleanup Engine:<br>%VERSION%<br><br>Scanner:<br>%VERSION%  |
| 6003     | Information | System   | Malware scan completed:<br>%SCAN_TYPE%.<br><br>Number of infected files:<br>%NUM% | Files to scan:<br>%SCAN_FOLDER_TYPE%<br><br>Scanned folders:<br>%PATHS%<br><br>Excluded paths:<br>%PATHS%<br><br>Excluded files:<br>%PATHS%<br><br>Excluded extensions:<br>%PATHS%<br><br>Start date/time:<br>%DATE_TIME%<br><br>End date/time:<br>%DATE_TIME%<br><br>Number of scanned files:<br>%NUM%<br><br>Number of infected files:<br>%NUM%<br><br>Number of cleaned files:<br>%NUM%<br><br>Number of files cleaned after reboot: %NUM%<br><br>[Components] |

| EVENT ID | LEVEL   | CATEGORY | EVENT   | DETAILS  |
|----------|---------|----------|---|--|
|          |         |          |   | Virus Pattern:<br>%VERSION%<br><br>Spyware Pattern:<br>%VERSION%<br><br>Digital Signature<br>Pattern:<br>%VERSION%<br><br>Program<br>Inspection<br>Pattern:<br>%VERSION%<br><br>Damage Cleanup<br>Template:<br>%VERSION%<br><br>Damage Cleanup<br>Engine<br>Configuration:<br>%VERSION%<br><br>Virus Scan<br>Engine:<br>%VERSION%<br><br>Damage Cleanup<br>Engine:<br>%VERSION%<br><br>Scanner:<br>%VERSION% |
| 6004     | Warning | System   | Malware scan<br>unsuccessful:<br>%SCAN_TYPE%<br>%ERROR% | Files to scan:<br>%SCAN_FOLDER_<br>TYPE%<br><br>Scanned folders:<br>%PATHS%<br><br>Excluded paths:<br>%PATHS%  |



| EVENT ID | LEVEL | CATEGORY | EVENT | DETAILS   |
|----------|-------|----------|-------|---|
|          |       |          |       | Excluded files:<br>%PATHS%<br><br>Excluded extensions:<br>%PATHS%<br><br>Start date/time:<br>%DATE_TIME%<br><br>End date/time:<br>%DATE_TIME%<br><br>Number of scanned files:<br>%NUM%<br><br>Number of infected files:<br>%NUM%<br><br>Number of cleaned files:<br>%NUM%<br><br>Number of files cleaned after reboot: %NUM%<br><br>[Components]<br><br>Virus Pattern:<br>%VERSION%<br><br>Spyware Pattern:<br>%VERSION%<br><br>Digital Signature Pattern:<br>%VERSION%<br><br>Program Inspection Pattern:<br>%VERSION% |

| EVENT ID | LEVEL       | CATEGORY | EVENT   | DETAILS   |
|----------|-------------|----------|---|---|
|          |             |          |   | Damage Cleanup<br>Template:<br>%VERSION%<br><br>Damage Cleanup<br>Engine<br>Configuration:<br>%VERSION%<br><br>Virus Scan<br>Engine:<br>%VERSION%<br><br>Damage Cleanup<br>Engine:<br>%VERSION%<br><br>Scanner:<br>%VERSION%  |
| 6005     | Information | System   | Malware<br>detected:<br>%ACTION%<br><br>File path: %PATH<br>% | Reboot required:<br>%NEED_REBOOT<br>%<br><br>[Scan Result]<br><br>Threat type:<br>%TYPE%<br><br>Threat name:<br>%NAME%<br><br>[Components]<br><br>Virus Pattern:<br>%VERSION%<br><br>Spyware Pattern:<br>%VERSION%<br><br>Digital Signature<br>Pattern:<br>%VERSION%<br><br>Program<br>Inspection |

| EVENT ID | LEVEL   | CATEGORY | EVENT  | DETAILS   |
|----------|---------|----------|--|---|
|          |         |          |  | Pattern:<br>%VERSION%<br><br>Damage Cleanup<br>Template:<br>%VERSION%<br><br>Damage Cleanup<br>Engine<br>Configuration:<br>%VERSION%<br><br>Virus Scan<br>Engine:<br>%VERSION%<br><br>Damage Cleanup<br>Engine:<br>%VERSION%<br><br>Scanner:<br>%VERSION%                     |
| 6006     | Warning | System   | Malware<br>detected.<br><br>Unable to<br>perform scan<br>actions: %PATH% | First action:<br>%1ST_ACTION%<br><br>Second action:<br>%2ND_ACTION%<br><br>Threat type:<br>%TYPE%<br><br>Threat name:<br>%NAME%<br><br>[Components]<br><br>Virus Pattern:<br>%VERSION%<br><br>Spyware Pattern:<br>%VERSION%<br><br>Digital Signature<br>Pattern:<br>%VERSION% |

| EVENT ID | LEVEL   | CATEGORY         | EVENT   | DETAILS   |
|----------|---------|------------------|---|---|
|          |         |                  |   | Program Inspection Pattern: %VERSION%<br>Damage Cleanup Template: %VERSION%<br>Damage Cleanup Engine Configuration: %VERSION%<br>Virus Scan Engine: %VERSION%<br>Damage Cleanup Engine: %VERSION%<br>Scanner: %VERSION% |
| 6007     | Warning | Maintenance Mode | Malware detected in Maintenance Mode (file quarantine successful): %PATH% | Component versions: %VERSION%<br>Virus Pattern: %VERSION%<br>Spyware Pattern: %VERSION%<br>Digital Signature Pattern: %VERSION%<br>Program Inspection Pattern: %VERSION%  |

| EVENT ID | LEVEL   | CATEGORY         | EVENT   | DETAILS  |
|----------|---------|------------------|---|--|
|          |         |                  |   | Damage Cleanup<br>Template:<br>%VERSION%<br><br>Damage Cleanup<br>Engine<br>Configuration:<br>%VERSION%<br><br>Virus Scan<br>Engine:<br>%VERSION%<br><br>Damage Cleanup<br>Engine:<br>%VERSION%<br><br>Scanner:<br>%VERSION%   |
| 6008     | Warning | Maintenance Mode | Malware detected in Maintenance Mode (file quarantine unsuccessful): %PATH% | Component versions: Virus<br>Pattern:<br>%VERSION%<br><br>Spyware Pattern:<br>%VERSION%<br><br>Digital Signature<br>Pattern:<br>%VERSION%<br><br>Program<br>Inspection<br>Pattern:<br>%VERSION%<br><br>Damage Cleanup<br>Template:<br>%VERSION%<br><br>Damage Cleanup<br>Engine<br>Configuration:<br>%VERSION% |

| EVENT ID | LEVEL   | CATEGORY         | EVENT  | DETAILS   |
|----------|---------|------------------|--|---|
|          |         |                  |  | Virus Scan Engine:<br>%VERSION%<br><br>Damage Cleanup Engine:<br>%VERSION%<br><br>Scanner:<br>%VERSION%   |
| 6009     | Warning | Maintenance Mode | Malware detected in Maintenance Mode: %PATH% | Component versions: Virus Pattern:<br>%VERSION%<br><br>Spyware Pattern:<br>%VERSION%<br><br>Digital Signature Pattern:<br>%VERSION%<br><br>Program Inspection Pattern:<br>%VERSION%<br><br>Damage Cleanup Template:<br>%VERSION%<br><br>Damage Cleanup Engine Configuration:<br>%VERSION%<br><br>Virus Scan Engine:<br>%VERSION%<br><br>Damage Cleanup Engine:<br>%VERSION% |

| EVENT ID | LEVEL       | CATEGORY | EVENT  | DETAILS   |
|----------|-------------|----------|--|---|
|          |             |          |  | Scanner:<br>%VERSION%   |
| 7000     | Information | System   | Group policy applied                                   | Old Group Name:<br>%GROUP NAME%<br><br>Old Policy<br>Version:<br>%VERSION%<br><br>New Group<br>Name: %GROUP<br>NAME%<br><br>New Policy<br>Version:<br>%VERSION%                             |
| 7001     | Warning     | System   | Unable to<br>synchronize<br>group policy               | Old Group Name:<br>%GROUP NAME%<br><br>Old Policy<br>Version:<br>%VERSION%<br><br>New Group<br>Name: %GROUP<br>NAME%<br><br>New Policy<br>Version:<br>%VERSION%<br><br>Reason: %Reason<br>% |
| 8000     | Information | System   | Real Time Scan is<br>enabled.                          |   |
| 8001     | Warning     | System   | Real Time Scan is<br>disabled.                         |   |
| 8010     | Warning     | System   | Incoming files<br>were scanned by<br>antivirus. Action | File Path: %PATH<br>%   |

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



| EVENT ID | LEVEL       | CATEGORY       | EVENT   | DETAILS  |
|----------|-------------|----------------|---|--|
|          |             |                | Login) has been enabled.  | Learning time: %LearningTime% day(s)                                   |
| 8602     | Information | anomaly_detect | Operations Behavior Anomaly Detection (User Login) has been disabled.           |  |
| 8603     | Information | anomaly_detect | Operations Behavior Anomaly Detection (Application Behavior) has been enabled.  | Mode: %Mode%<br>Level: %Level%<br>Learning time: %LearningTime% day(s) |
| 8604     | Warning     | anomaly_detect | Operations Behavior Anomaly Detection (Application Behavior) has been disabled. |  |
| 8605     | Information | anomaly_detect | Operations Behavior Anomaly Detection (Script Behavior) has been enabled.       | Mode: %Mode%<br>Level: %Level%<br>Learning time: %LearningTime% day(s) |
| 8606     | Warning     | anomaly_detect | Operations Behavior Anomaly Detection (Script Behavior) has been disabled.      |  |

| EVENT ID | LEVEL   | CATEGORY       | EVENT   | DETAILS  |
|----------|---------|----------------|---|--|
| 8610     | warning | anomaly_detect | An abnormal user login has been detected by Operations Behavior Anomaly Detection.      | Domain: %Domain%<br>Account: %Account%<br>Login Type: %LoginType%<br>Source IP: %IP%   |
| 8611     | warning | anomaly_detect | A user login failure has been detected by Operations Behavior Anomaly Detection.        | Domain: %Domain%<br>Account: %Account%<br>Login Type: %LoginType%<br>Source IP: %IP%   |
| 8612     | warning | anomaly_detect | An unrecognized application has been detected by Operations Behavior Anomaly Detection. | PID: %PID%<br>Program Path: %Path%<br>Program Hash: %SHA256%<br>Program Size: %Size%<br>Certificate: %CertificateSigner%<br>Vendor: %VendorName%<br>Product: %Product% |
| 8613     | warning | anomaly_detect | Malicious application behavior has been detected by                                     | Program Path: %Path%   |

| EVENT ID | LEVEL   | CATEGORY       | EVENT  | DETAILS  |
|----------|---------|----------------|--|--|
|          |         |                | Operations Behavior Anomaly Detection  | Program Hash:<br>%SHA256%<br>Program Size:<br>%Size%<br>Certificate:<br>%CertificateSigner%<br>Vendor:<br>%VendorName%<br>Product:<br>%Product%                            |
| 8614     | warning | anomaly_detect | Suspicious application behavior has been detected by Operations Behavior Anomaly Detection.  | Program Path:<br>%Path%<br>Program Hash:<br>%SHA256%<br>Program Size:<br>%Size%<br>Certificate:<br>%CertificateSigner%<br>Vendor:<br>%VendorName%<br>Product:<br>%Product% |
| 8615     | warning | anomaly_detect | Script Behavior has been allowed by Operations Behavior Anomaly Detection: %PATH% %ARGUMENT% | Access User:<br>%USERNAME%<br>Parent Process 1:<br>%PATH%<br>%ARGUMENT%<br>Parent Process 2:<br>%PATH%<br>%ARGUMENT%   |

| EVENT ID | LEVEL       | CATEGORY           | EVENT   | DETAILS   |
|----------|-------------|--------------------|---|---|
|          |             |                    |   | Parent Process 3:<br>%PATH%<br>%ARGUMENT%<br><br>Parent Process 4:<br>%PATH%<br>%ARGUMENT%<br><br>Mode: %MODE%<br><br>Level: %LEVEL%<br>%THROTTLING_I<br>NFO_MSG%   |
| 8616     | warning     | anomaly_dete<br>ct | Script Behavior<br>has been blocked<br>by Operations<br>Behavior<br>Anomaly<br>Detection: %PATH<br>% %ARGUMENT% | Access User:<br>%USERNAME%<br><br>Parent Process 1:<br>%PATH%<br>%ARGUMENT%<br><br>Parent Process 2:<br>%PATH%<br>%ARGUMENT%<br><br>Parent Process 3:<br>%PATH%<br>%ARGUMENT%<br><br>Parent Process 4:<br>%PATH%<br>%ARGUMENT%<br><br>Mode: %MODE%<br><br>Level: %LEVEL%<br>%THROTTLING_I<br>NFO_MSG% |
| 8620     | Information | anomaly_dete<br>ct | A user login<br>account has been<br>added to the<br>Situational<br>Awareness<br>baseline.                       | Domain:<br>%Domain%<br><br>Account:<br>%Account%  |

| EVENT ID | LEVEL       | CATEGORY       | EVENT   | DETAILS  |
|----------|-------------|----------------|---|--|
|          |             |                |   | Login Type:<br>%LoginType%<br><br>Source IP: %IP%  |
| 8621     | Information | anomaly_detect | A user login account has been excluded from the Situational Awareness baseline. | Domain:<br>%Domain%<br><br>Account:<br>%Account%<br><br>Login Type:<br>%LoginType%<br><br>Source IP: %IP%  |
| 8622     | Information | anomaly_detect | An application has been added to the Situational Awareness baseline.            | Application Path:<br>%Path%  |
| 8623     | Information | anomaly_detect | An application has been excluded from the Situational Awareness baseline.       | Application Path:<br>%Path%  |
| 8624     | Information | anomaly_detect | A script behavior has been added to the Situational Awareness baseline.         | Access User:<br>%USERNAME%<br><br>ID:%ID%<br><br>Monitored Process / Script:<br>%PATH%<br>%ARGUMENT%<br><br>Parent Process 1:<br>%PATH%<br>%ARGUMENT%<br><br>Parent Process 2:<br>%PATH%<br>%ARGUMENT% |

| EVENT ID | LEVEL       | CATEGORY       | EVENT  | DETAILS  |
|----------|-------------|----------------|--|--|
|          |             |                |  | Parent Process 3:<br>%PATH%<br>%ARGUMENT%<br><br>Parent Process 4:<br>%PATH%<br>%ARGUMENT%   |
| 8625     | Information | anomaly_detect | A script behavior has been excluded from the Situational Awareness baseline. | ID:%ID%<br><br>Monitored Process / Script:<br>%PATH%<br>%ARGUMENT%<br><br>Parent Process 1:<br>%PATH%<br>%ARGUMENT%<br><br>Parent Process 2:<br>%PATH%<br>%ARGUMENT%<br><br>Parent Process 3:<br>%PATH%<br>%ARGUMENT%<br><br>Parent Process 4:<br>%PATH%<br>%ARGUMENT% |

## 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. |

| <b>CODE</b> | <b>DESCRIPTION</b>                                    |
|-------------|---|
| 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)                           |
| 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.                   |

| <b>CODE</b> | <b>DESCRIPTION</b>  |
|-------------|---|
| 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)   |
| 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.               |



| <b>CODE</b> | <b>DESCRIPTION</b>                |
|-------------|-----------------------------------|
| 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. |



# Chapter 7

## Troubleshooting Resources

This chapter provides available troubleshooting resources for the Agent.

Topics in this chapter include

- *Frequently Asked Questions (FAQ) on page 7-2*
- *Troubleshooting StellarProtect on page 7-2*
- *Troubleshooting StellarProtect (Legacy Mode) on page 7-5*

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

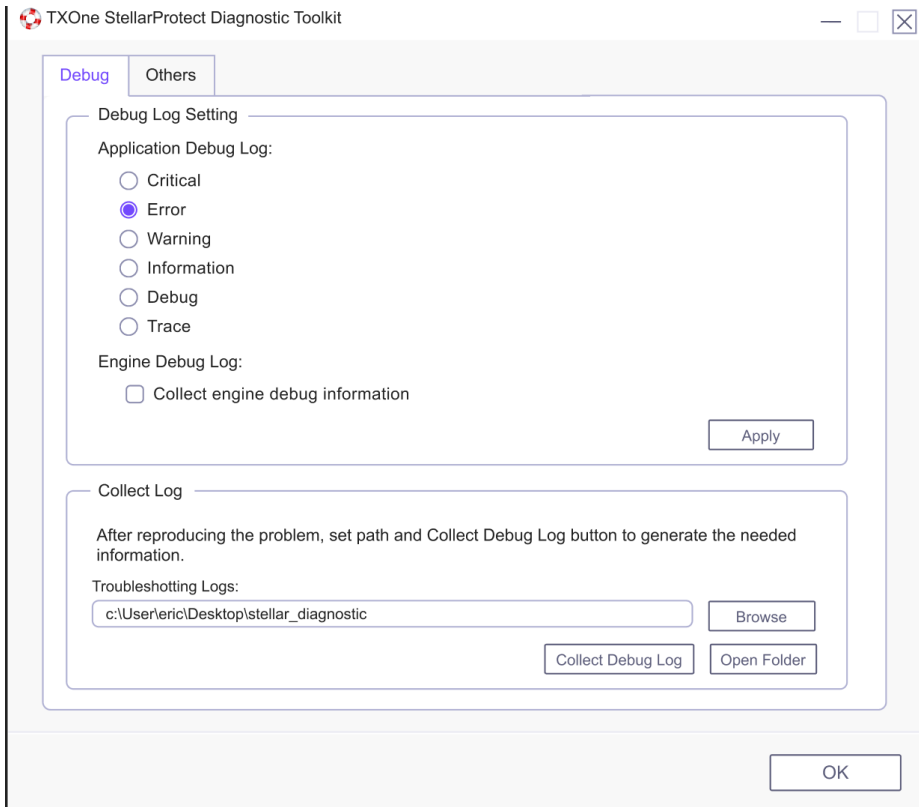
### Where can I get more help with TXOne StellarProtect/StellarProtect (Legacy Mode)?

To get the most up-to-date information and support, see [Technical Support on page 8-1](#).

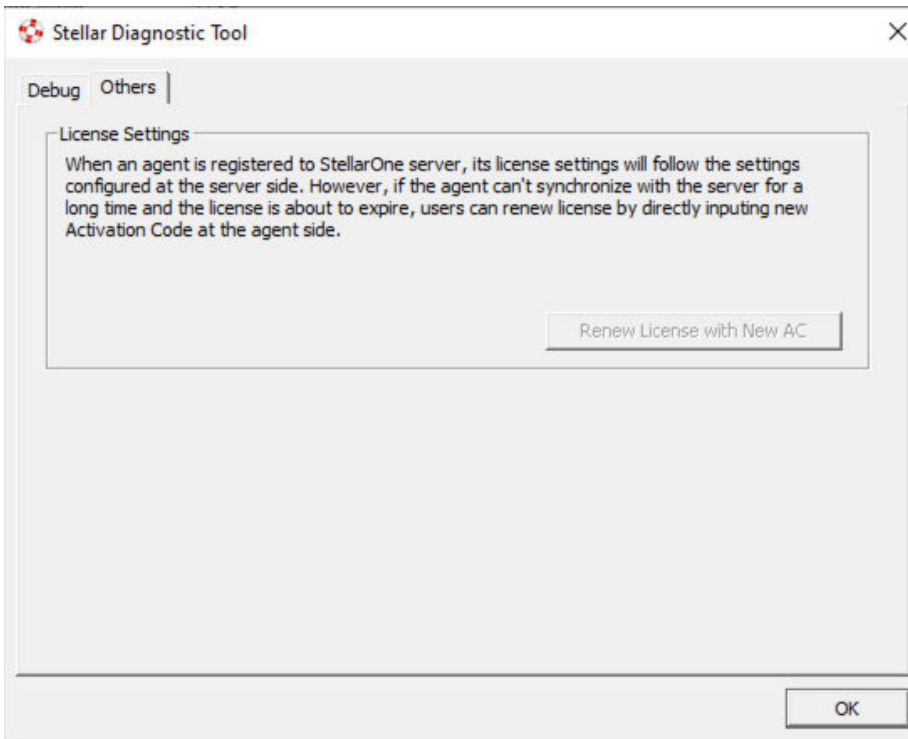
## Troubleshooting StellarProtect

The TXOne StellarProtect Diagnostic Toolkit offers administrators the ability to perform a number of diagnostic functions and license settings, including:

- Change debug log settings and collect debug logs
- Renew license for the agent that had registered to StellarOne but haven't sync with the server for a long time and its license is about to expire



**FIGURE 7-1. The TXOne StellarProtect Diagnostic Toolkit [Debug]**



**FIGURE 7-2.** The TXOne StellarProtect Diagnostic Toolkit Debug [Others]

## Using the StellarProtect Diagnostic Toolkit for Troubleshooting

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

### Procedure

1. Open the Diagnostic Toolkit and enable full logging:
  - a. Open the TXOne StellarProtect installation folder and run `op_diagnostic.exe`.

**Note**

The default installation location is c:\Program Files\TXOne\StellarProtect\.

---

- b. Provide the Administrator or User password and click **OK**.
  - c. On the **Debug** tab, specify the log level needed in the **Application Debug Log** section; enable **Collect engine debug information** if needed in the **Engine Debug Log** section, and click **Apply**.
2. Reproduce the problem.
  3. Collect the diagnostic logs:
    - a. Reopen the Diagnostic Toolkit.
    - b. On the **Debug** tab, click **Browse** to choose the location where TXOne StellarProtect saves the logs.
- 

**Note**

The default location for saved logs is: c:\Program Files\TXOne\StellarProtect\Log\Archive\.

---

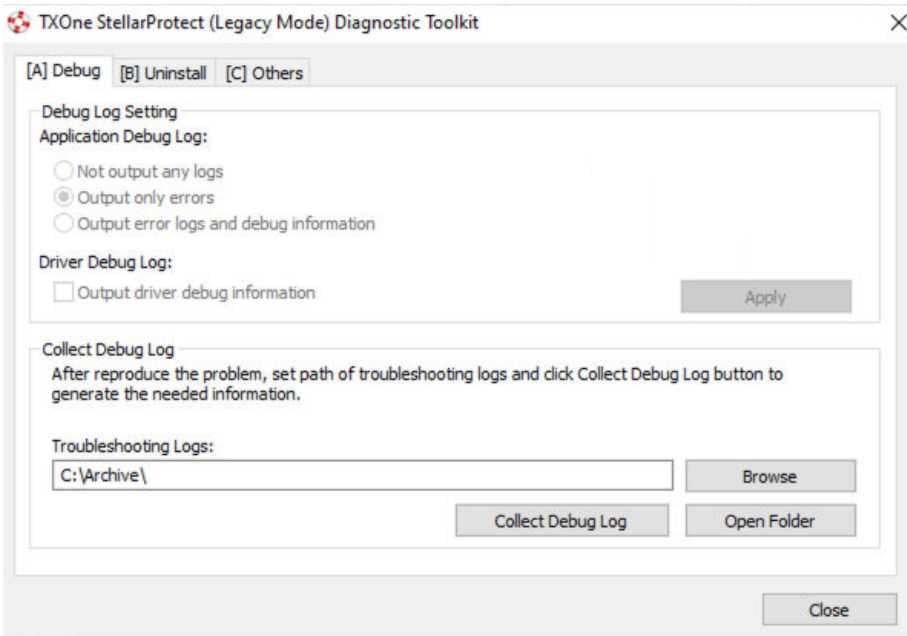
- c. Click **OK** when finished.
  - d. Click **Collect Debug Log**.
  - e. Once the Debug Logs have been collected, click **Open Folder** to access the zipped log files for review, or to send them to TXOne Networks Technical Support.
- 

## Troubleshooting StellarProtect (Legacy Mode)

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

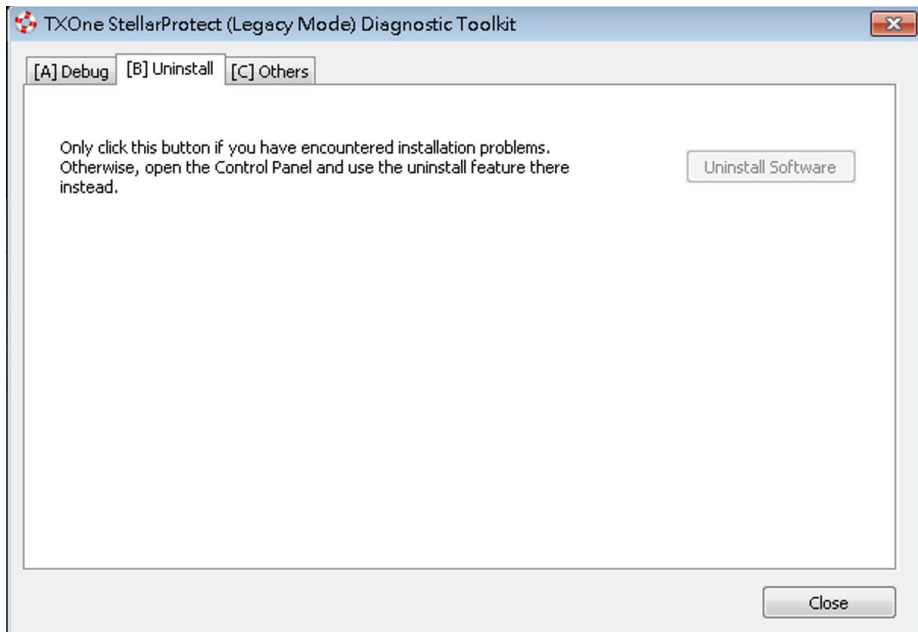
- Create, collect, and delete debugging logs

- Enable or disable Self Protection
- Uninstall the agent if the installation problems occur
- Renew license for the agent that had registered to StellarOne but haven't sync with the server for a long time and its license is about to expire

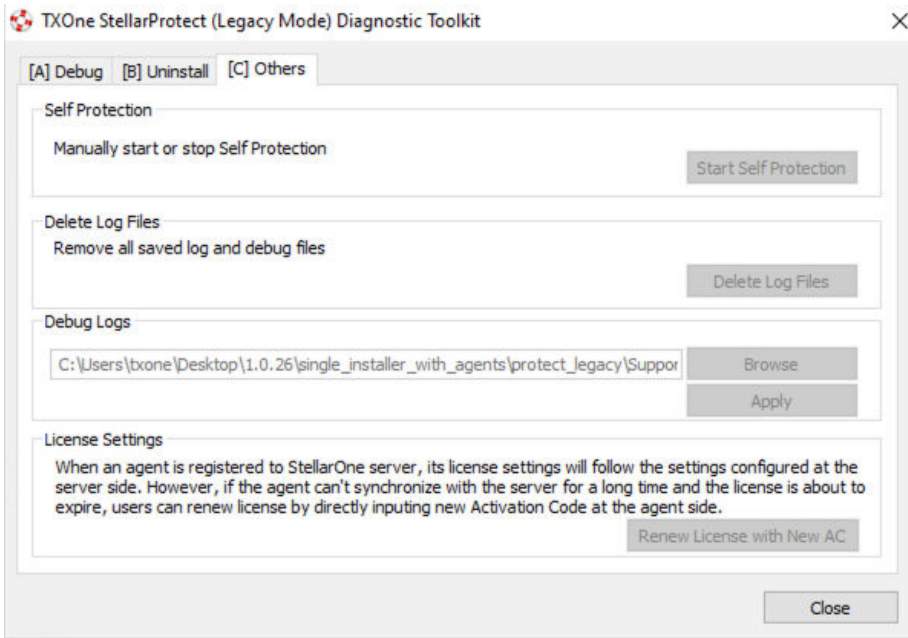


**FIGURE 7-3. The TXOne StellarProtect (Legacy Mode) Diagnostic Toolkit Debug Tab A [Debug]**





**FIGURE 7-4. The TXOne StellarProtect (Legacy Mode) Diagnostic Toolkit Debug Tab B [Uninstall]**



**FIGURE 7-5. The TXOne StellarProtect (Legacy Mode) Diagnostic Toolkit Debug Tab C [Others]**

## Using the StellarProtect (Legacy Mode) Diagnostic Toolkit for Troubleshooting

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

### Procedure

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

**Note**

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

---

- b. Provide the Administrator or User password and click **OK**.
  - c. On the **[A] Debug** tab, select **Output error logs and debug information** and **Output driver debug information**, and click **Apply**.
2. Reproduce the problem.
  3. Collect the diagnostic logs:
    - a. Reopen the Diagnostic Toolkit.
    - b. On the **[A] Debug** tab, click **Browse** to choose the location where TXOne StellarProtect (Legacy Mode) saves the logs.

**Note**

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

---

- c. Click **OK** when finished.
  - d. Click **Collect Debug Log**.
  - e. Once the Debug Logs have been collected, click **Open Folder** to access the zipped log files for review, or to send them to TXOne Networks Technical Support.
-



# Chapter 8

## Technical Support

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

Learn about the following topics:

- *[Troubleshooting Resources on page 8-2](#)*
- *[Contacting Trend Micro and TXOne on page 8-3](#)*
- *[Sending Suspicious Content to Trend Micro on page 8-4](#)*
- *[Other Resources on page 8-5](#)*

## Troubleshooting Resources

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

### Using the Support Portal

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

---

#### Procedure

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



#### Tip

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

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

---

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

---

### Threat Encyclopedia

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

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

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

## Contacting Trend Micro and TXOne

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

**TABLE 8-1. Trend Micro Contact Information**

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

**TABLE 8-2. TXOne Contact Information**

|               |  |
|---------------|--|
| Address       | TXOne Networks, Incorporated<br>222 West Las Colinas Boulevard, Suite 1650<br>Irving, TX 75039 U.S.A |
| Website       | <a href="https://www.txone.com">https://www.txone.com</a>  |
| Email address | <a href="mailto:support@txone.com">support@txone.com</a>   |

- Worldwide support offices:

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

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

- Trend Micro product documentation:

<https://docs.trendmicro.com>

## Speeding Up the Support Call

To improve problem resolution, have the following information available:

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

## Sending Suspicious Content to Trend Micro

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

### Email Reputation Services

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

<https://ers.trendmicro.com/>

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



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

## File Reputation Services

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

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

Record the case number for tracking purposes.

## Web Reputation Services

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

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

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

## Other Resources

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

## Download Center

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

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

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



# Appendix A

## StellarProtect (Legacy Mode) Limitations by Operating Systems

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

| OPERATING SYSTEMS               | LIMITATIONS   |
|---------------------------------|---|
| Windows 10                      | <ul style="list-style-type: none"><li>• 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.</li><li>• To improve performance, disable the following Windows 10 components:<ul style="list-style-type: none"><li>• Windows Defender Antivirus. This may be disabled via group policy.</li><li>• Windows Update. Automatic updates may require the download of large files, which may affect performance.</li><li>• Windows Apps (Microsoft Store) auto-update. Checking for frequent updates may cause performance issues.</li></ul></li></ul> |
| Windows 10 Fall Creators Update | OneDrive integration is not supported. Ensure that OneDrive integration is disabled before installing StellarProtect (Legacy Mode).   |

| OPERATING SYSTEMS  | LIMITATIONS   |
|--|---|
| Windows 10 April 2018 Update (Redstone 4) and later versions   | <ul style="list-style-type: none"> <li>• OneDrive integration is not supported. Ensure that OneDrive integration is disabled before installing StellarProtect (Legacy Mode).</li> <li>• See the following limitations when working with folders where the <i>case sensitive</i> attribute has been enabled: <ul style="list-style-type: none"> <li>• Enabling the <i>case sensitive</i> 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.</li> <li>• StellarProtect (Legacy Mode) blocks all processes started from folders where the <i>case sensitive</i> attribute is enabled. Additionally, StellarProtect (Legacy Mode) is unable to provide any information for the blocked processes, except for file path.</li> <li>• The StellarProtect (Legacy Mode) agent cannot verify file signatures of files saved in folders where the <i>case sensitive</i> attribute is enabled. As a result, DAC exceptions related to signatures cannot work.</li> </ul> </li> </ul> |
| Windows XP Embedded SP1  | The custom action of “quarantine” for Application Lockdown or Real-Time Scan is not supported   |
| <ul style="list-style-type: none"> <li>• Windows 2000 SP4 (without update rollup)</li> <li>• Windows XP SP1</li> <li>• Windows XP Embedded</li> <li>• Windows 2000 Server SP4</li> </ul> | <p>The following functions are not supported:</p> <ul style="list-style-type: none"> <li>• DLL/Driver Lockdown</li> <li>• Script Lockdown</li> <li>• Integrity Monitoring</li> <li>• USB Malware Protection</li> <li>• Storage Device Blocking</li> <li>• Maintenance Mode</li> <li>• Predefined Trusted Updater</li> </ul>   |

# Index

## A

about hashes, 3-14, 3-42

Agent console

    About StellarProtect, 3-33

    About StellarProtect (Legacy Mode), 3-64

Approved List

    Add or remove files, 3-45

    Check or update hashes, 3-42

    Configuration, 3-44

    StellarProtect, 3-11

    StellarProtect (Legacy Mode), 3-40

## C

Check connection

    StellarProtect, 3-24

    StellarProtect (Legacy Mode), 3-55

Command Line Interface (CLI)

    List of All Commands, 4-4

    Using SLCmd at CLI, 4-16

Config File

    Export/Import, 5-3

## D

Diagnostic toolkit, 7-4, 7-8

## F

Feature settings

    StellarProtect, 3-27

    StellarProtect (Legacy Mode), 3-59

## I

introduction, 1-1

    key features and benefits, 1-3

    what's new, 1-6

## M

Maintenance Mode

    StellarProtect, 3-25

    StellarProtect (Legacy Mode), 3-56

## O

Operations

    StellarProtect, 3-21

    StellarProtect (Legacy Mode), 3-52

Overview

    StellarProtect, 3-2

    StellarProtect (Legacy Mode), 3-34

## P

Password

    StellarProtect, 3-20

    StellarProtect (Legacy Mode), 3-51

## S

Scan now

    StellarProtect, 3-23

    StellarProtect (Legacy Mode), 3-54

StellarProtect

    OT Applications, 3-9

    OT Certificates, 3-10

StellarProtect (Legacy Mode)

    Approved List

        Export/Import, 3-48

        Update/install using Trusted

        Updater, 3-46

    StellarProtect (Legacy Mode) events, 6-24

## StellarProtect Approved List

- Add or remove files, 3-17

- Check or update hashes, 3-14

- Configuration, 3-16

- Export/Import file hashes, 3-18

## StellarProtect CLI

- Overview, 4-2

- Using OPCmd at CLI, 4-2

## StellarProtect events, 6-2

### support

- resolve issues faster, 8-4

### Sync now

- StellarProtect, 3-24

- StellarProtect (Legacy Mode), 3-55

## system requirements, 1-7

## T

### technical support, 8-1

- contact, 8-3

- troubleshooting resources, 8-2

## U

- Using agent console, 3-1

- using StellarProtect (Legacy Mode)

- agent console, 3-34

- Using StellarProtect agent console, 3-2



**TXONE NETWORKS INCORPORATED**

222 West Las Colinas Boulevard, Suite 1650  
Irving, TX 75039 U.S.A  
Email: [support@txone.com](mailto:support@txone.com)  
[www.txone.com](http://www.txone.com)

[www.txone.com](http://www.txone.com)

Item Code: APEM39832/230913