

3.1 TXOne StellarOne

Administrator's Guide

Unify your cyber security posture with one centralized console



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:

<https://my.txone.com/>

TXOne Networks, StellarOne, StellarProtect, and StellarProtect (Legacy Mode) 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 © 2024. TXOne Networks Incorporated. All rights reserved.

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.

Data collected by TXOne Networks is subject to the conditions stated in the TXOne Networks Global 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	1-5

Chapter 2: Getting Started

About the Web Console	2-2
Opening StellarOne Management Console	2-2

Chapter 3: Dashboard

About the Dashboard Screen	3-2
Widget Manager	3-5
About the Widget	3-6
Security Monitoring	3-7
Widget for CPSDR	3-7
Widgets for Monitoring Agents	3-9
Asset Management	3-12
Widgets displaying managed asset status	3-12
Deployment Status Widget	3-13
Agent Version Status Widget	3-14
Agent Component Status Widget	3-14

Agent Connection Status Widget	3-15
Widgets displaying key features settings	3-16
System Status	3-18
Widgets for Monitoring Disk Usage	3-19

Chapter 4: Agents Management

About the Agents Screen	4-2
Agent Status Settings	4-8
Manage Agent Connection Status	4-8
Manage Agent Component Status	4-9
Correlated Settings for Agent Component Status	4-11
Recommended Bandwidth for StellarOne	
Components Update	4-13
Configuring Agent Component Status Settings— Use	
Case	4-13
Add Groups	4-15
Edit Description for Agents	4-16
Organize Agents/Groups	4-16
Search for Agents/Groups	4-18
Filter Options for Agents/Groups	4-18
Protection	4-20
Configure Maintenance Mode	4-20
Update Approved List	4-24
Scan Now	4-25
Update	4-28
Update Agent Components	4-29
Deploy Agent Patches	4-29
Check Connections	4-31
Apply Policies	4-31
Collect Event Logs	4-32
Agent Export/Import Settings	4-35
Export Agent Settings	4-35
Export Agent Configurations	4-35
Export Approved List	4-36

Import Agent Settings	4-36
Import Agent Configurations	4-37
Import Approved List	4-38
Export Selected Agents Info	4-39
Export all Agents Info	4-39

Chapter 5: Policy Configuration

Settings for the Agent/Group Policy Screen	5-2
Set Policy Refresh Interval	5-4
Set Agent User Interface Preferences	5-5
Export/Import Exclusions Settings	5-6
Export Exclusions	5-7
Exclusions Configuration File	5-7
Exclusions Configuration File Parameters	5-8
Application Lockdown Section for StellarProtect	5-9
Application Lockdown Section for StellarProtect (Legacy Mode)	5-10
Real-Time Scan and Scheduled Scan Section	5-15
Operations Behavior Anomaly Detection Section	5-16
Device Control Section	5-19
OT Application Safeguard Section for StellarProtect	5-19
Import Exclusions	5-21
Agent View and Policy Settings	5-23
Go to the Agent View	5-23
Finding the Target Agent	5-25
Agent Policy Settings	5-27
Operations Behavior Anomaly Detection	5-27
Setting the Learning Time	5-34
Setting the Learning Time - Use Case	5-35
Policy-based Watchlist and Approved Items	5-36
Policy-based Watchlist	5-36
Policy-based Approved Login Accounts	5-37

Policy-based Approved Applications	5-38
Use Case	5-39
Strict Mode	5-41
Strict Mode - Use Case	5-44
Migration/Upgrade from Previous Version - Use Case	5-45
Sizing Table - 2nd Disk Space Requirement	5-48
Other Key Features for StellarProtect	5-49
Application Lockdown	5-49
Excluded Paths Settings	5-50
Trusted Hash Values Settings	5-52
Calculate Hash Values	5-52
Add Trusted Hash Values	5-54
Import Trusted Hash Values	5-55
Edit Trusted Hash Values	5-55
Remove Trusted Hash Values	5-56
Multi-Method Threat Prevention	5-57
Real-Time Scan	5-57
Predictive Machine Learning	5-58
Scheduled Scan	5-58
Advanced Settings	5-60
Advanced Options for Real-Time Scan ..	5-60
Advanced Options for Scheduled Scan ..	5-61
Scan Exclusions	5-63
OT Application Safeguard	5-64
DLL Injection Prevention	5-66
Other Key Features for StellarProtect (Legacy Mode) ..	5-67
Application Lockdown	5-67
Excluded Paths Settings	5-68
Add a File, Folder, or Regular Expression as an Excluded Path	5-69
Edit Excluded Path	5-69
Remove Excluded Path	5-70
Trusted Hash Values Settings	5-70
Calculate Hash Values	5-70
Add Trusted Hash Values	5-72
Import Trusted Hash Values	5-73

Edit Trusted Hash Values	5-73
Remove Trusted Hash Values	5-74
Write Protection Exclusions Settings	5-75
Add a File, Folder, Registry Key, or Registry Key and Value to Write Protection Exclusions	5-75
Edit Write Protection Exclusions	5-76
Remove Write Protection Exclusions	5-76
Threat Prevention	5-77
Real-Time Scan	5-77
Scheduled Scan	5-78
Advanced Settings	5-80
Advanced Options for Real-Time Scan ..	5-80
Advanced Options for Scheduled Scan ..	5-81
Scan Exclusions	5-83
Comman Policy Settings for StellarProtect/StellarProtect (Legacy Mode)	5-84
Agent Component Update Schedule	5-84
Device Control	5-86
Get Device Information	5-88
Edit/Add/Remove Trusted USB Devices by Importing Configuration File	5-89
User-Defined Suspicious Objects	5-90
Agent Password	5-91
Patch	5-92
Trusted Certificates Settings	5-94
Importing/Deleting Trusted Certificates	5-94
Situational Awareness	5-95
Situational Awareness for StellarProtect	5-95
Approved Script Behaviors	5-96
Approved Login Accounts	5-98
Approved Applications	5-99
Situational Awareness for StellarProtect (Legacy Mode)	5-101
Approved Script Behaviors	5-102
Approved Login Accounts	5-103
Approved Applications	5-104

Group Policy Settings	5-106
Go to the Group Policy Screen	5-107
Group Policy Settings	5-108
Create Custom Exceptions to the Inherited Policy ..	5-110

Chapter 6: Logs

Agent Events	6-2
About Agent Events Screen	6-2
Agent Events Filtering	6-4
Agent Event Actions	6-5
Add to Baseline	6-6
Add to Suspicious Objects Blocklist	6-7
Grant One-Time Access	6-8
Server Events	6-10
About Server Events Screen	6-10
Server Events Log Filtering	6-12
System Logs	6-13
About System Logs Screen	6-14
Audit Logs	6-15
About Audit Logs Screen	6-16
Audit Log Filtering	6-17

Chapter 7: Administration

Account	7-3
Account Management	7-3
Account Types	7-4
Server Accounts Overview	7-5
Add Accounts	7-7
Delete Accounts	7-9
Edit Accounts	7-9
Generate an API Key	7-10
Single Sign-On	7-11
Configuring ADFS as SAML IdP for SSO	7-13
Resolving the SSO Issue	7-14

Notification	7-16
SMTP Settings and Notification	7-16
Scheduled Report	7-17
Syslog Forwarding	7-19
Update	7-19
Proxy Settings	7-20
Downloads/Updates	7-21
Configuring Scan Component for StellarOne	7-21
Downloading Agent Installer Package/Group.ini File	7-23
Group Mapping	7-24
Importing/Deleting Agent's Patch	7-25
Importing Firmware	7-26
License	7-27
About the License Screen	7-28
License Management	7-30
License Renewal	7-30
Renew License with the same License Key .	7-31
Renew License by Importing License File ...	7-31
Getting the License File	7-31
New License Key/File	7-33
License Editions	7-34
Features of License Editions	7-36
System	7-36
System Time	7-37
Log Purge	7-37
Importing SSL Certificate	7-39
OT Intelligent Trust	7-40
Service Integration	7-40
Integrate with Trend Micro Vision One	7-41

Chapter 8: Getting Help and Troubleshooting

Troubleshooting Resources	8-2
Self-Diagnosis	8-2
Resolving Low Disk Space Issues	8-2
Using the Support Portal	8-3

Threat Encyclopedia	8-4
Contacting TXOne Networks	8-5
Speeding Up the Support Call	8-5
Other Resources	8-6
Download Center	8-6

Appendix A: Appendices

Log Descriptions	A-2
Log Descriptions for StellarProtect	A-2
Agent Event Log Descriptions for StellarProtect	A-2
Server Event Log Descriptions for StellarProtect	A-26
Log Descriptions for StellarProtect (Legacy Mode)	A-28
Agent Event Log Descriptions for StellarProtect (Legacy Mode)	A-28
Agent Error Code Descriptions for StellarProtect (Legacy Mode)	A-80
Server Event Log Descriptions for StellarProtect (Legacy Mode)	A-83
Server Event Log Descriptions for StellarOne	A-87
Syslog Content - CEF	A-88
StellarProtect/StellarProtect (Legacy Mode) Syslog Content - CEF	A-88
StellarProtect Agent Event Format	A-88
StellarProtect Server Event Format	A-91
StellarProtect (Legacy Mode) Agent/Server Event Format	A-92
StellarOne Syslog Content - CEF	A-94
StellarOne System Event Format	A-95
StellarOne System Event IDs and Messages	A-97
StellarOne Audit Event Format	A-97
StellarOne Audit Event IDs and Messages	A-100

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.

Preface

Preface

This Administrator's Guide introduces TXOne StellarOne™ and covers all aspects of product management.

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 StellarOne™ 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 StellarOne
Administrator's Guide	A PDF document that discusses StellarOne agent installation, getting started information, and server and agent management
Online Help	HTML files that provide "how to's", usage advice, and field-specific information
Knowledge Base	An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following websites: https://kb.txone.com/

Audience





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

Document Conventions

The documentation uses the following conventions.

TABLE 1. Document Conventions

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

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

Terminology

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

TERMINOLOGY	DESCRIPTION
server	The StellarOne console server program
server endpoint	The host where the StellarOne server is installed

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

Chapter 1

Introduction

This chapter introduces TXOne StellarOne™ and how it manages the agents providing Cyber-Physical System Detection and Response (CPSDR), Multi-Method Threat Prevention, Operations lockdown, and trusted peripheral control protection to your assets. StellarOne

An overview of management functions is provided. This manual will focus on its use for StellarProtect™: an OT/ICS-compatible, high performance and zero touch endpoint protection solution, and StellarProtect (Legacy Mode)™: a simple, no-maintenance solution to lock down and protect fixed-function computers, helping protect businesses against security threats and increase productivity.

Topics in this chapter include:

- *About TXOne Stellar on page 1-2*
- *Key Features and Benefits on page 1-3*
- *What's New on page 1-5*

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 incident before it could occur. The security team followed up and resolved the ransomware infection in a different part of the environment. The operation team could schedule the required update to run during planned maintenance period.

- **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 strengthen organization's security posture while maintaining its business operations stability.

Key Features and Benefits

The TXOne StellarOne™ management console provides following features and benefits.

TABLE 1-1. Features and Benefits

FEATURE	BENEFIT
Cyber-Physical System Detection and Response (CPSDR)	The CPSDR requires a deep understanding of what the expected behaviors for each device are. Embodied within the advanced Operations Behavior Anomaly Detection feature, which primarily defends against unexpected changes that may impact operational stability by comparing daily operation processes and behaviors with a unique baseline of each agent-device and performing comprehensive behavioral analysis not only via identifying baseline deviation but also using TXOne Networks' exclusive industrial application repository and ransomware detection engine.
Dashboard	The Dashboard provides an overview of the CPS situational awareness and agent deployment status at the centralized control level, along with the monitored asset status and StellarOne console's system status. Administrators can check deployed agent status easily, have quick access to the detected events for further investigation or actions if needed, and generate security reports related to specific agent activity for specified periods.

FEATURE	BENEFIT
Centralized Agent Management	<p>StellarOne allows administrators to perform the following tasks:</p> <ul style="list-style-type: none"> • Monitor StellarProtect/StellarProtect (Legacy Mode) agent status • Examine connection status • View configurations • Collect agent logs on-demand (Legacy Mode only) • Turn agent Application Lockdown on or off • Enable or disable agent Device Control • Configure agent Maintenance Mode settings • Update agent components • Initialize the Approved List • Deploy agent patches • Add trusted files and USB devices • Export agents information • Import/Export agents configuration settings and import agent Approved list (Legacy Mode only) • Export agents Approved List
Centralized Event Management	<p>On endpoints protected by StellarProtect/StellarProtect (Legacy Mode) agents, administrators can monitor status and events, as well as respond when files are blocked from running. StellarOne provides event management features that let administrators quickly know about and take action on the blocked-file events.</p>
Server Event Auditing	<p>Operations performed by StellarOne web console accounts are logged. StellarOne records an operating log for each account, tracking who logs on, who deletes event logs, and more.</p>

What's New

TXOne StellarOne™ 3.1 provides following new features and enhancements.

TABLE 1-2. What's New in TXOne StellarOne™ 3.1

FEATURE	BENEFIT
<p>Visibility enhancement:</p> <ul style="list-style-type: none"> • New widgets for security monitoring and asset management • Asset information 	<p>New dashboard widgets:</p> <ul style="list-style-type: none"> • Security monitoring: new widget for displaying Cyber-Physical Systems (CPS) situational awareness and security posture using a tiered structure from event triage to investigation. • Asset management: new widget for displaying managed asset status and associated features settings. <p>Asset information: you can view system data of each managed endpoint from the General Info page on the StellarOne console.</p>
<p>Enhanced dashboard management</p>	<p>You can add new dashboards and customize them by selecting which widgets to display based on different needs (e.g., security monitoring, asset management, or system status).</p>
<p>Customizable agent status settings</p>	<p>In addition to viewing the agent connection and component update statuses, you can also change the default configuration for proactive asset management.</p>
<p>Custom exceptions</p>	<p>By creating custom exceptions to the inherited policy, the selected exceptions settings will become customizable and associated changes will take precedence over the inherited policy; while the rest of the settings still remain inherited from the parent group.</p>
<p>Agent User Interface Preferences settings</p>	<p>The display of certain pop-up notifications or right-click scan accessibility on the agent console is customizable now.</p>
<p>New preventative action available for CPS detection</p>	<p>Provides the action setting that allows users to manually add detected applications to the blocklist.</p>
<p>Option for deferring agent component update</p>	<p>Provides the option to defer the policy-based agent component update. If enabled, StellarOne will deploy only the previous component version to the target endpoint or group of endpoints.</p>

FEATURE	BENEFIT
Option for suspending automatic patch update	StellarOne automatic patch update can be suspended if needed, allowing the local user to perform on-demand patch update manually on the agent console.
Command button of exporting Approved List for StellarProtect	Exporting the approved list of the selected StellarProtect agent is now available.
More Application Lockdown policy settings available for StellarProtect (Legacy Mode)	You can configure more policy settings of Application Lockdown for StellarProtect (Legacy Mode) via the StellarOne console.
Agent events enhancement	<ul style="list-style-type: none"><li data-bbox="655 540 1163 618">• Improves agent event search functionality, enabling you to set up a custom filter with criteria range and save a set of filters for use in different scenarios<li data-bbox="655 638 1116 688">• Provides a unified display of StellarProtect and StellarProtect (Legacy Mode) events.

Chapter 2

Getting Started

This chapter introduces how to access and configure the StellarOne web-based management console.

Topics in this chapter include:

- *[About the Web Console on page 2-2](#)*
- *[Opening StellarOne Management Console on page 2-2](#)*

About the Web Console

TXOne StellarOne is a management console with web GUI for users to access via web browsers. StellarOne is packaged in an Open Virtual Appliance (OVA) or Virtual Hard Disk v2 (VHDX) format and supports 4 types of platforms: VMware ESXi, VMware Workstation, Windows Hyper-V systems, and AWS EC2.

**Note**

Supported browsers:

- Google Chrome 87 or later versions
 - Microsoft Edge 79 or later versions
 - Mozilla Firefox 78 or later versions
-

For users who log on StellarOne for the first time, please refer to [Opening StellarOne Management Console on page 2-2](#).

For more details about the installation for StellarOne, please refer to the [StellarOne Installation Guide](#).

Opening StellarOne Management Console

Procedure

1. For VMware or Hyper-V system, launch the StellarOne instance and then run the OOB process in the setup CLI.
 - a. Use the default credentials when logging on for the first time:
 - Username: `root`
 - Password: `txone`
 - b. Change the default credentials to your desired username and password.

**Important**

To enhance security, it is recommended to create a safe username and strong password.

**Note**

For StellarOne instance deployed from AMI on AWS EC2 platform, the OOB process is not required.

2. Open a web browser and enter the StellarOne address in the following format: `https://<targetserver IP address>`. The log on screen appears.

3. Enter your credentials (user ID and password).

Use the default credentials of administrator when logging on for the first time:

- User ID: `admin`
- Password: `txone`

4. Click **Log On**.

5. If this is the first time the StellarOne instance being logged on, follow below procedures to complete the initial settings.

a. The **Login Information Setup** window appears and prompts you to change password. Confirm your password settings by:

- specifying your new password in the **New Password** text field.
- specifying the password again in the **Confirm Password** text field.

b. Click **Confirm**. You will be automatically logged out. The **Log On** screen will appear again.

c. Log on again using your new credentials. The **License Activation** window appears.

d. Choose one of the ways to activate the license based on your license data and network environment:

- **License Key**

1. Click **License Key**.
 2. Specify your license key in the text field.
-



Note

- The license key that contains more than 30 characters can be used for online or offline license activation.
- The license key that contains less than 30 characters can only be used for online license activation.

The license key with less than 30 characters can be used to download the license file, which can be used for offline license activation.

- **License File:**

1. Click **License File**.
 2. Select the license file (a .txt file) to import.
-



Note

- The license file can be used for license activation if the StellarOne has no Internet connection.
 - If you don't have the license file on hand, see [Getting the License File on page 7-31](#). A license file with less than 30 characters is required for downloading a license file.
-

- e. Click **Apply**.
-



Note

A full license can not be converted to a trial license.

- f. A success message appears. The license information also appears at the bottom of the **License Activation** window. Check if it matches the license data provided by your support provider.
- g. Click **Continue**.
- h. The **End User License Agreement and TXOne OT Intelligent Trust** window appears. Click the links to read the documents carefully and click the checkboxes to proceed to next step.

**Note**

It is recommended to enable **TXOne OT Intelligent Trust** to enhance security deployment. See *OT Intelligent Trust on page 7-40* for more details.

- i. Specify the time settings such as the **Date and Time** as well as the **Time Zone**, and then click **Continue**.
- j. The StellarOne console is ready for use now.

**Note**

After the initial settings are completed, the StellarOne allows various user accounts to log on remotely via a web browser.

6. (Optional) You can change your password by clicking the ID icon at the top right corner of the screen, and then selecting **Change Password**.
7. (Optional) For security reasons, you can manually log off by clicking the ID icon at the top right corner of the screen.
 - a. A pop-up **Log Off** window appears. Click **Yes** to log out of StellarOne.

**Note**

You will be automatically logged off the console if no operations are performed within 30 minutes.

Chapter 3

Dashboard

This chapter provides an overview of the StellarOne web console's dashboard and introduces how to configure the dashboard settings.

Topics in this chapter include:

- *About the Dashboard Screen on page 3-2*
 - *Widget for CPSDR on page 3-7*
 - *Widgets for Monitoring Agents on page 3-9*
 - *Widgets for Monitoring Disk Usage on page 3-19*
 - *Widget Manager on page 3-5*

About the Dashboard Screen

The **Dashboard** provides an overview of security monitoring, asset management, and StellarOne console's system status. Click the **Dashboard** tab in the top navigation bar of the StellarOne web console. The **Dashboard** screen with three tabs of **Security Monitoring**, **Asset Management**, and **System Status** appears.

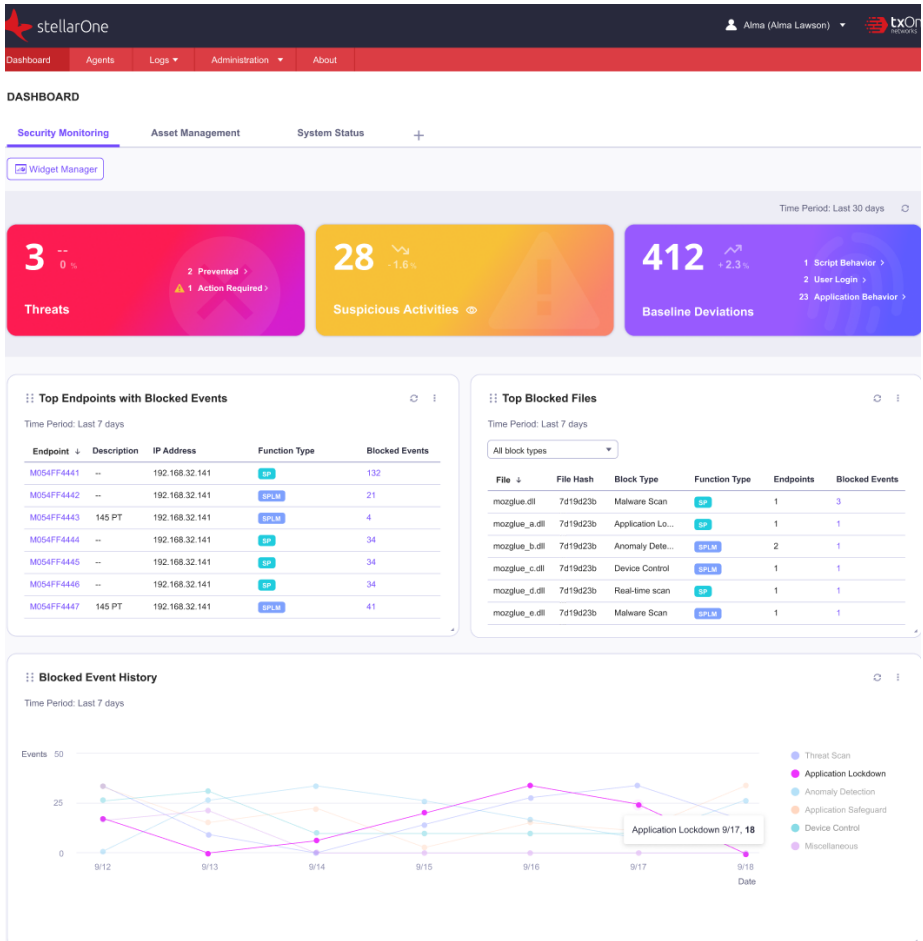

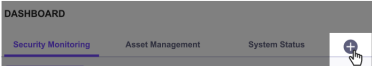

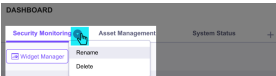


FIGURE 3-1. The Dashboard Screen

TABLE 3-1. About the Dashboard Screen

FUNCTION	DESCRIPTION
<p>Security Monitoring</p>	<p>This page displays one widget related to Cyber-Physical Systems (CPS) security monitoring, along with three widgets for monitoring the agent events:</p> <ul style="list-style-type: none"> • Dynamic Visibility of Cyber-Physical System Security • Top Endpoints with Blocked Events • Blocked Event History • Top Blocked Files <p>See Widget for CPSDR on page 3-7 and Widgets for Monitoring Agents on page 3-9 for more details.</p> <hr/> <p> Note</p> <p>By default the Security Monitoring tab page is set as the landing page of the Dashboard screen.</p>
<p>Asset Management</p>	<p>This page displays eight widget related to asset status and key features settings:</p> <ul style="list-style-type: none"> • Deployment Status • Agent Version Status • Agent Component Status • Agent Connection Status • Real-Time Scan Settings • Application Lockdown Settings • Operations Behavior Anomaly Detection Settings • Device Control Settings <p>See Widgets displaying managed asset status on page 3-12 and Widgets displaying key features settings on page 3-16 for more details.</p>

FUNCTION	DESCRIPTION
System Status	<p>Under this tab, you can check StellarOne console's system status related to:</p> <ul style="list-style-type: none"> • Disk Usage (1st HDD) • Disk Usage (2nd HDD) • CPU Usage • Memory Usage <p>See Widgets for Monitoring Disk Usage on page 3-19 for more details.</p>
Tab Settings	<ul style="list-style-type: none"> • : Add new dashboard by clicking the icon. <hr/> <p> Note</p> <p>You can have up to 10 dashboards. If the maximum number of dashboards exceeds, delete existing dashboards for creating new ones.</p> <hr/> <ul style="list-style-type: none"> • : To edit a dashboard, mouse over by the name of the target dashboard and click the arrow that appears. You can rename or delete the selected dashboard.
Widget Manager	<p>This button allows you to add desired widgets to the selected dashboard. See Widget Manager on page 3-5 for more details.</p>

Widget Manager

The number of widgets you can add to a dashboard depends on the dashboard page layout. Once the number of widgets exceeds the maximum number the dashboard can accommodate, you must remove a widget from the dashboard or add the widget to another dashboard.

Procedure

1. Go to **Dashboard** in the navigation at the top of the web console.
2. Click **Security Monitoring**, **Asset Management**, or **System Status** dashboard.

**Note**

You can add dashboard by clicking the **+**, specifying the dashboard title in the text field, and clicking **Add** to add a new dashboard.

3. Click the **Widget Manager** button, and then the screen for adding or removing widgets appears.
 4. Select to add one or more widgets to the dashboard. You can also deselect to remove one or more widgets from the dashboard.
 5. Click the **Apply Changes** button to complete the task.
-

About the Widget

You can determine how often the widget data will be updated and specify the time period of the data for the widgets to display.

Procedure

1. Click the **Refresh** icon at the top right corner of the target widget to display the up-to-date data.
2. The drop-down menu at the top right corner of each widget provides two functions:
 - a. **Widget Settings**
 - **Time Period:** allows you to select a specific timeframe, which determines the number of the detected threats or baseline deviations to display (The default value is **Last 7 days**).
 - **Auto Refresh Settings:** allows you to configure the auto refresh frequency (The default value is **Every 5 minutes**).

- b. **Remove Widget:** allows you to remove the widgets from the dashboard.
3. On the chart widgets such as **Blocked Event History** or **Operations Behavior Anomaly Detection Settings**, click an entry on the legend to show or hide data for the associated setting.



Tip

- To move a widget, click and hold on the title bar of the widget and drag it to various locations on the page.
- To resize a widget, mouse over the bottom right corner of the widget and a diagonal resize pointer appears. Drag it to resize the widget.

Security Monitoring

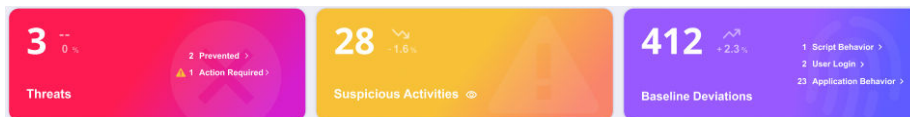
This section provides an overview of the **Security Monitoring** dashboard and introduces how to configure the associated settings.

Four widget for displaying Cyber-Physical Systems (CPS) situational awareness and security posture, or the critical agent events can be added to this dashboard.

Topics in this section includes:

- [Widget for CPSDR on page 3-7](#)
- [Widgets for Monitoring Agents on page 3-9](#)

Widget for CPSDR



Dynamic Visibility of Cyber-Physical Systems Security: This widget serves as the quantifying indicators of the detected threats and baseline deviations

collected from the managed agents with CPSDR features enabled. Not only does it dynamically display the number of agent events triggered by detected threats, suspicious activities, and baseline deviations detected within a specified time period, but also provide actionable alerts for detected threats, as well as prioritizes suspicious activities that require additional investigation.

This widget facilitates security monitoring by means of a tiered structure with funnel-based framework:

1. Event triage:

- **Baseline Deviations:** Based on the baseline fingerprint of each agent-device established during practicable operating states, baseline deviation analysis is performed using an expansive industrial application repository and exclusive threat detection engine to defend against unexpected changes that may impact stability.
- **Threats:** When potential threats are detected, preventative actions are taken on behalf of SOC analysts and alerts displayed if further actions are required, enabling security personnel to work efficiently by prioritizing their time on what matters most.
- **Suspicious Activities:** By filtering out most of the "noise" from a high volume of non-critical events and resolving the most critical incidents, suspicious activities that may lead to advanced persistent threat by a sophisticated adversary are escalated to the higher tier of investigation.

2. Investigation: The second tier for **Suspicious Activities** provides descriptive analysis for SOC analysts to track and identify the sources of these activities, facilitating the work of generating detailed report and recommendations for remediation.

The following table describes the items available on this widget:

ITEM	DESCRIPTION
Threats	<p>Click the links to be directed to the associated agent events for more details or actions:</p> <ul style="list-style-type: none"> • Prevented: The specified actions have been taken on the detected threats. • Actions required: The specified actions have been taken on the detected threats but more actions are required to prevent the threats.
Suspicious Activities	<p>Click Suspicious Activities to expand the content that prioritizes suspicious activities requiring additional investigation.</p> <ul style="list-style-type: none"> • Top Detection Rules Triggered: Displays the most detection rules triggered by the suspicious events, accompanied with the MITRE ID mapping, endpoints, and the triggering events. • Top Endpoints with Triggered Rules: Displays the endpoints with the most detection rules triggered, accompanied with the description, IP address, function type (StellarProtect or StellarProtect (Legacy Mode)), triggered rules, and triggering events.
Baseline Deviation	<p>Click the links to be directed to the associated agent events for more details or actions:</p> <ul style="list-style-type: none"> • Script Behavior: Displays detected anomalies associated with unrecognized monitored process or script-based fileless attacks. • User Login: Displays detected anomalies associated with unrecognized user accounts or unexpected login activities • Application Behavior: Displays detected anomalies associated with unrecognized applications or unexpected application running behaviors

Widgets for Monitoring Agents

Three widgets for monitoring agent events can be added to the **Security Monitoring** dashboard.

- **Top Endpoints with Blocked Events:** This widget displays the endpoints with the most blocked events.

Top Endpoints with Blocked Events

Time Period: Last 7 days

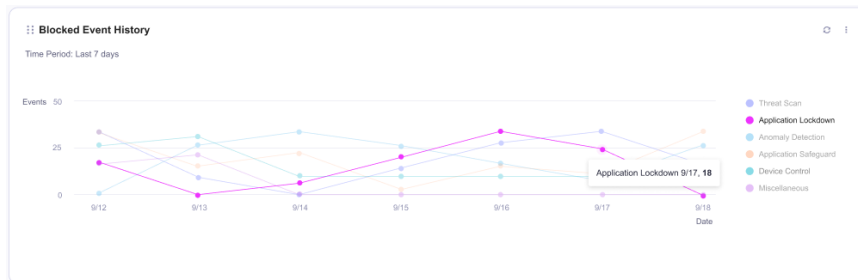
Endpoint ↓	Description	IP Address	Function Type	Blocked Events
M054FF4441	--	192.168.32.141	SP	132
M054FF4442	--	192.168.32.141	SPLM	21
M054FF4443	145 PT	192.168.32.141	SPLM	4
M054FF4444	--	192.168.32.141	SP	34
M054FF4445	--	192.168.32.141	SP	34
M054FF4446	--	192.168.32.141	SP	34
M054FF4447	145 PT	192.168.32.141	SPLM	41

1. Click an endpoint name to be directed to the **General Info** page for more details about the endpoint.
2. Click a value on the chart to be directed to the relevant agent events for more details..

TABLE 3-2. Widget: Top Endpoints with Blocked Events

COLUMN	DESCRIPTION
Endpoint Name	Name of the endpoint
Description	Description assigned to the endpoint
IP Address	IP address of the endpoint
Function Type	The agent installed on the endpoints <ul style="list-style-type: none"> • SP: StellarProtect • SPLM: StellarProtect (Legacy Mode)
Blocked Events	Total number of events blocked on the endpoint

- **Blocked Event History:** This widget displays a summary of blocked events for the specified time period.



1. Click a value on the chart to be directed to the relevant agent events for more details.
 2. Click an entry on the legend to show or hide data for that event type.
- **Top Blocked Files:** This widget displays a list of files that triggered the most blocked events.

Top Blocked Files
Time Period: Last 7 days

All block types

File ↓	File Hash	Block Type	Function Type	Endpoints	Blocked Events
mozglue.dll	7d19d23b	Malware Scan	SP	1	3
mozglue_a.dll	7d19d23b	Application Lo...	SP	1	1
mozglue_b.dll	7d19d23b	Anomaly Dete...	SPLM	2	1
mozglue_c.dll	7d19d23b	Device Control	SPLM	1	1
mozglue_d.dll	7d19d23b	Real-time scan	SP	1	1
mozglue_e.dll	7d19d23b	Malware Scan	SPLM	1	1

TABLE 3-3. Widget: Top Blocked Files

COLUMN	DESCRIPTION
File Name	Name of the file that triggered the blocked events
File Hash	SHA1 hash of the file that triggered the blocked events
Block Type	Protection feature that triggered the blocked events
Function Type	The agent installed on the endpoints <ul style="list-style-type: none"> • SP: StellarProtect • SPLM: StellarProtect (Legacy Mode)
Endpoints	Total number of the endpoints that reported the blocked events triggered by the file
Blocked Events	Total number of the blocked events triggered by the file

Asset Management

This section provides an overview of the **Asset Management** dashboard and introduces how to configure the associated settings.

Eight widget for displaying managed asset status and associated features settings can be viewed on this dashboard.

Topics in this section includes:

- [Widgets displaying managed asset status on page 3-12](#)
- [Widgets displaying key features settings on page 3-16](#)

Widgets displaying managed asset status

The following table describes the widgets used to display the status of the managed endpoints.

NAME	DESCRIPTION
Deployment Status	Displays and summarizes the current status of agent deployment on the managed endpoints. See Deployment Status Widget on page 3-13 for more details.
Agent Version Status	Provides an overview of the current agent versions installed on the managed endpoints. See Agent Version Status Widget on page 3-14 for more details.
Agent Component Status	Provides an overview of the component update status for agents installed on the managed endpoints. See Agent Component Status Widget on page 3-14 for more details.
Agent Connection Status	Provides an overview of the availability status for agents installed on the managed endpoints. See Agent Connection Status Widget on page 3-15 for more details.

Deployment Status Widget

This widget displays and summarizes the current status of agent deployment on the managed endpoints.

The following table describes the items available on this widget:

TABLE 3-4. About the Deployment Status Widget

ITEM	DESCRIPTION
Deployed	The number of the license seats used
Available Seats	The number of the remaining license seats
Over-deployed	The number of the endpoints that require additional license seats
Total Seats	The total number of the license seats
Total Assets	The total number of the managed assets
Status Bar	Displays current deployment status and license usage by number and percentage

Agent Version Status Widget

This widget provides an overview of the current agent versions installed on the managed endpoints.

The following table describes the items available on this widget:

TABLE 3-5. About the Agent Version Status Widget

ITEM	DESCRIPTION
Drop-down menu	Displays the agent versions installed on the managed endpoints
Pie chart	Displays the distribution of agent versions installed

Agent Component Status Widget

This widget provides an overview of the component update status for agents installed on the managed endpoints.


The data is represented in the pie chart and corresponding figures will appear when you mouse over the specific area of the pie chart.

See the following example to understand what the figures mean:

- **Up-to-date: 800 (80%):** The agent components are up to date on 800 endpoints (80% of 1,000 in total).
- **Out-of-date: 200 (20%):** The agent components are out of date on 200 endpoints (20% of 1,000 in total).

The following table describes the items available on this widget:

TABLE 3-6. About the Agent Component Status Widget

ITEM	DESCRIPTION
Pie Chart	<p>Displays the number and percentage of agent component update status categorized as Out-of-date and Up-to-date:</p> <ul style="list-style-type: none"> • Out-of-date: By default, the criteria of showing Out-of-date status is the agent components haven't been updated for more than one week. • Up-to-date: By default: the criteria of showing Up-to-date status is the agent components have been updated within one week. <hr/> <p> Note This widget displays only the agents that appear Online in the Agent Connection Status widget. See Agent Connection Status Widget on page 3-15 for more details.</p>
Manage Agent Component Status	The link will direct you to Manage Agent Component Status on page 4-9 to view or configure the agent component status settings.
Learn more	This link will direct you to the TXOne StellarOne Online Help for more details about the agent component status widget and associated settings.

Agent Connection Status Widget

This widget provides an overview of the availability status for agents installed on the managed endpoints..

The data is represented in the pie chart and corresponding figures will appear when you mouse over the specific area of the pie chart.

See the following example to understand what the figures mean:

- **Online: 800 (80%):** Agents installed on the 800 (80% of 1,000 in total) managed endpoints are online.
- **Offline: 200 (20%):** Agents installed on the 200 (20% of 1,000 in total) managed endpoints are offline.

The following table describes the items available on this widget:

TABLE 3-7. About the Agent Component Status Widget

ITEM	DESCRIPTION
Pie Chart	Displays the number and percentage of agent component update status categorized as Online and Offline : <ul style="list-style-type: none"> • Online: By default: the criteria of showing Online status is the agents have been connected with StellarOne within 7 days. • Offline: By default, the criteria of showing Offline status is the agents have been disconnected from StellarOne for more than 7 days.
Manage Agent Connection Status	The link will direct you to Manage Agent Connection Status for customizing the criteria of showing different agent connection status. See Manage Agent Connection Status on page 4-8 for more details.

Widgets displaying key features settings

Four widgets respectively provide an overview of the associated feature settings applied to the managed endpoints by number and percentage.

The data is represented in the pie chart and corresponding figures will appear when you mouse over the specific area of the pie chart. See the following examples to understand what the figures mean.


Example 1:

- **On: 800 (80%)**: The feature is enabled on 800 endpoints (80% of 1,000 in total).
- **Off: 200 (20%)**: The feature is disabled on 200 endpoints (20% of 1,000 in total).

Example 2:

- **Enforce: 500 (50%)**: The feature is enabled and set to "Enforce" mode on 500 endpoints (50% of 1,000 in total).
- **Detect: 400 (40%)**: The feature is enabled and set to "Detect" mode on 400 endpoints (40% of 1,000 in total).
- **Disable: 100 (10%)**: The feature is disabled on 100 endpoints (10% of 1,000 in total).

TABLE 3-8. About the Widgets Displaying Features Settings

NAME	DESCRIPTION
Real-Time Scan Settings	<p>Provides an overview of the Real-Time Scan settings applied to the managed endpoints by number and percentage.</p> <p>The Real-Time Scan settings include:</p> <ul style="list-style-type: none"> • On: The Real-Time Scan is enabled. Persistent and ongoing file scan is running on the group of endpoints. • Off: The Real-Time Scan is disabled.
Application Lockdown Settings	<p>Provides an overview of the Application Lockdown settings applied to the managed endpoints by number and percentage.</p> <p>The Application Lockdown settings include:</p> <ul style="list-style-type: none"> • Enforce: The files not in the Approved List will be blocked and corresponding events will be generated on the group of endpoints.. • Detect: The files not in the Approved List will be allowed and corresponding events will be generated on the group of endpoints.. • Disable: The Application Lockdown is turned off. <hr/> <p> Note The StellarProtect (Legacy Mode) provides only two modes for Application Lockdown settings, ON and OFF, which correspond respectively to Enforce and Detect in the widget.</p>

NAME	DESCRIPTION
Operations Behavior Anomaly Detection Settings	<p>Provides an overview of the Operations Behavior Anomaly Detection settings applied to the managed endpoints by number and percentage.</p> <p>The Operations Behavior Anomaly Detection Settings settings include:</p> <ul style="list-style-type: none"> • Learn: In the group of endpoints, the agents are collecting behavioral patterns from the installed devices to establish baseline fingerprints. • Detect: In the group of endpoints, the agents identify and send alerts for any unexpected changes or security threats by analyzing current behaviors against the baselines. • Enforce: In the group of endpoints, the agents take preventative action on detected baseline deviations to defend operation stability and security. • Disable: The Operations Behavior Anomaly Detection Settings is turned off.
Device Control Settings	<p>Provides an overview of the Device Control settings applied to the managed endpoints by number and percentage.</p> <p>The Device Control settings include:</p> <ul style="list-style-type: none"> • On: The Device Control is enabled. Only the devices added in the trusted list have permanent access to the group of endpoints. • Off: The Device Control is disabled.

System Status

This section provides an overview of the **System Status** dashboard and introduces how to configure the associated settings.

Four widget for displaying console's system status can be viewed on this dashboard.

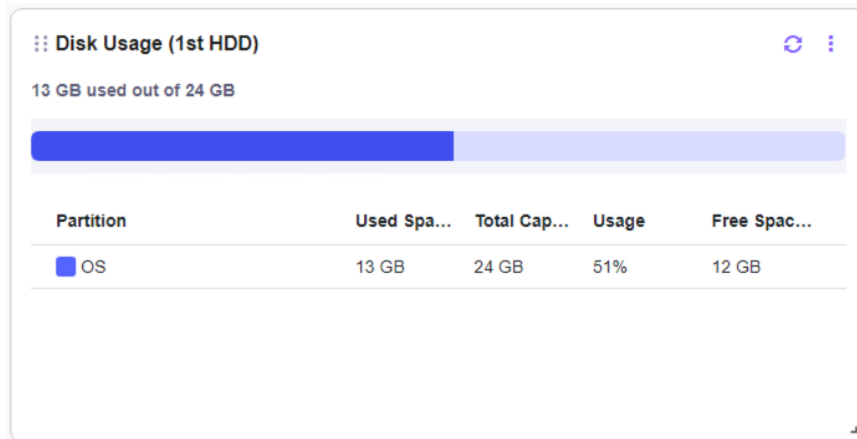
Topics in this section includes:

- [Widgets for Monitoring Disk Usage on page 3-19](#)

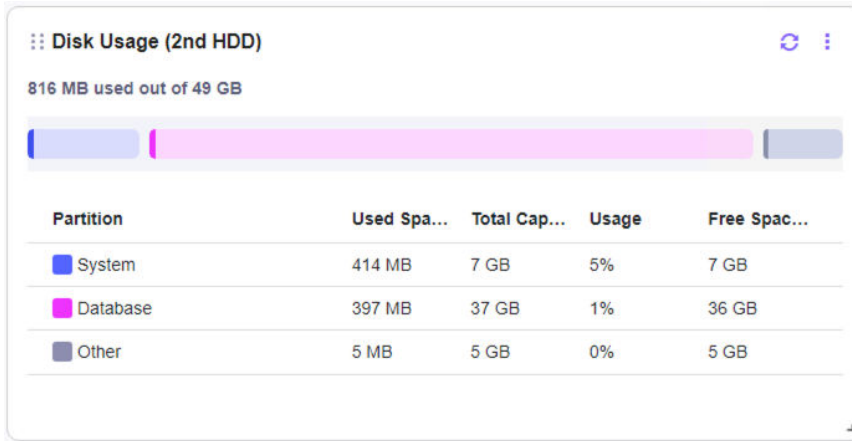
- CPU & Memory Usage

Widgets for Monitoring Disk Usage

- **Disk Usage (1st HDD):** This widget displays the current total size of the first disk and amount used for the OS partition.



- **Disk Usage (2nd HDD):** This widget displays the current total size of the second disk and amount used for the System, Database, and Other partition.



Chapter 4

Agents Management

This chapter introduces how to manage StellarProtect/StellarProtect (Legacy Mode) agents via StellarOne web console.

Topics in this chapter include:

- *About the Agents Screen on page 4-2*
- *Protection on page 4-20*
- *Update on page 4-28*
- *Agent Export/Import Settings on page 4-35*

About the Agents Screen

The StellarOne console facilitates agent management by allowing you to organize agents into various groups and build up multi-level hierarchy among the groups (parent groups above child groups), forming an agent/group tree structure. On the **Agents** screen, you can deploy one-time commands to the selected groups and/or agents for performing immediate actions.

Click the **Agents** tab in the top navigation bar of the StellarOne web console. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.



Note

All agents are under the **All** group by default.

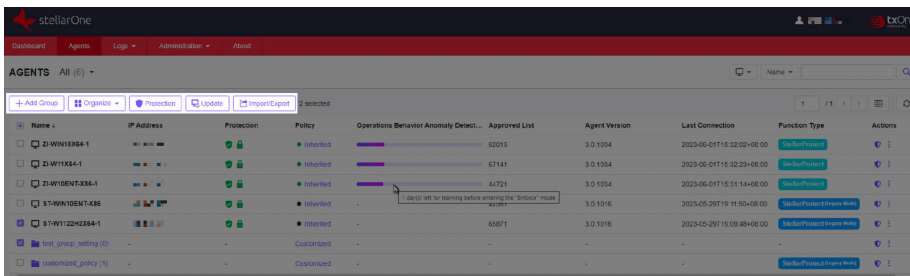
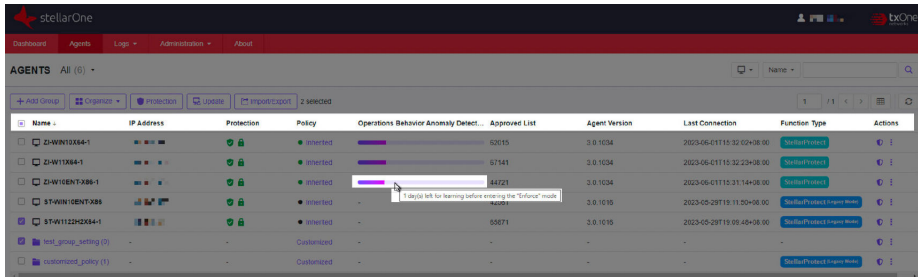


FIGURE 4-1. The Agents Screen - Toolbar

TABLE 4-1. Toolbar

TOOLS	DESCRIPTION
+Add Group	This tool allows you to create groups according to location, type, or purpose for better multi-agent management. See Add Groups on page 4-15 for more details.
Organize	This tool allows you to edit description for agent(s), move agent(s) to another group, and remove agent(s)/group(s). See Edit Description for Agents on page 4-16 and Organize Agents/Groups on page 4-16 for more details.

TOOLS	DESCRIPTION
Protection	This tool allows you to configure Maintenance Mode, update Approved List when the Application Lockdown feature is enabled, and customize file scan settings. See Configure Maintenance Mode on page 4-20 , Update Approved List on page 4-24 , and Scan Now on page 4-25 for more details.
Update	This tool allows you to update components and deploy patches for agents, as well as check connections with endpoints, apply group/agent policies immediately, and collect event logs (Legacy Mode only). See Update Agent Components on page 4-29 , Deploy Agent Patches on page 4-29 , Check Connections on page 4-31 , Apply Policies on page 4-31 , and Collect Event Logs on page 4-32 for more details.
Import/Export	This tool allows you to export an agent config file (Legacy Mode only) or Approved List (Legacy Mode only), and then import it to apply the settings specified in the config file or Approved List to a batch of target agents/groups. You can also export information about the selected or all agents. See Agent Export/Import Settings on page 4-35 for more details.

















The screenshot shows the StellarOne Agents Management interface. At the top, there are navigation tabs for Dashboard, Agents, Logs, Administration, and About. Below the navigation, there are buttons for Add Group, Organize, Protection, Update, Import/Export, and 2 selected. The main area displays a table of agents with the following column headings: Name, IP Address, Protection, Policy, Operations Behavior Anomaly Detect..., Approved List, Agent Version, Last Connection, Function Type, and Actions. The table contains several rows of agent data, including ZI-WIN12064-1, ZI-W113064-1, ZI-W10E17X86-1, ST-W11C2HTX88, and ST-W112ZH2K4-1. A tooltip is visible over the Policy column for the second row, stating "Tap/Click left for hearing before entering the 'Infrared' mode".





Name	IP Address	Protection	Policy	Operations Behavior Anomaly Detect...	Approved List	Agent Version	Last Connection	Function Type	Actions
ZI-WIN12064-1		Protected	Infrared		62615	3.0.1034	2023-06-01 11:32:02+08:00	StellarProtected	
ZI-W113064-1		Protected	Infrared		67541	3.0.1034	2023-06-01 11:32:23+08:00	StellarProtected	
ZI-W10E17X86-1		Protected	Infrared		84221	3.0.1034	2023-06-01 11:31:14+08:00	StellarProtected	
ST-W11C2HTX88		Protected	Infrared		66666	3.0.1016	2023-05-29 11:20:00+08:00	StellarProtected (Legacy Mode)	
ST-W112ZH2K4-1		Protected	Infrared		65671	3.0.1016	2023-05-29 11:00:46+08:00	StellarProtected (Legacy Mode)	
test_group_setting (3)			Customized						
customized_policy (1)			Customized						

FIGURE 4-2. The Agents Screen - Column Headings

TABLE 4-2. Column Headings

HEADINGS	DESCRIPTION
Name	<ul style="list-style-type: none"> •  : Indicates a group •  : Indicates an agent and its connection status is Online •  : Indicates an agent and its connection status is Offline <hr/> <p> Note The criteria of displaying Online and Offline status depend on how long the agent has been disconnected from StellarOne. By default, the agent will appear Offline after disconnected from StellarOne for more than 7 days. See Manage Agent Connection Status on page 4-8 for more details.</p>
IP Address	Displays the IP Address of the endpoint (one IP address corresponds to a single agent)
Protection	<ul style="list-style-type: none"> •  : Indicates the Application Lockdown is enabled •  : Indicates the Real-Time Scan is enabled •  : Indicates the agent is in maintenance mode •  : Indicates a maintenance period has been scheduled but not started yet •  : Indicates all the agent protection features are disabled and the endpoint may be vulnerable to security threats •  : Indicates the protection provided by the agent has been fully disabled, which is triggered by the local user via the Stop protection button on the local console. The endpoint may be vulnerable to security threats.

HEADINGS	DESCRIPTION
Policy Inheritance	<ul style="list-style-type: none"> • Inherited: Indicates the policy settings for the agent/group are inherited from its parent group • Customized: Indicates the policy settings for the agent/group are customized by administrators •  Self-managed: Indicates the agent/group is free from the StellarOne web console's policy management and its feature settings should be configured on the local console •  : Indicates the agent's feature settings synchronize with the StellarOne console policy settings •  : Indicates the agent's feature settings do not synchronize with the StellarOne console settings
Operations Behavior Anomaly Detection	<p>Displays the status of Operations Behavior Anomaly Detection:</p> <ul style="list-style-type: none"> • Learn: Indicates the agent is collecting behavioral patterns from the monitored device to establish a baseline. • Detect: Indicates the agent is checking and should send alerts for any unexpected changes or security threats. • Enforce: Indicates the agent should take preventative actions on any anomalies detected. • Disable: Indicates the Operations Behavior Anomaly Detection is disabled. •  : If the agent has not established a baseline yet but is set to the Detect or Enforce mode, it will learn first and automatically switch to the specified mode. The progress bar here indicates how many days left for learning before entering the specified mode. • - : Indicates the agent version or license edition does not support Operations Behavior Anomaly Detection.

HEADINGS	DESCRIPTION
Component Status	<p>Displays the component update status of the agent:</p> <ul style="list-style-type: none"> •  Up-to-date: Indicates the components installed on the agent have been updated within a specified duration •  Out-of-date: Indicates the components installed on the agent have not been updated for more than a specified duration <hr/> <p> Note By default, the component status will appear Out-of-date after 1 week. See Manage Agent Component Status on page 4-9 for more details.</p>
Approved List	<p>Displays the total number of applications added in the Approved List. If the endpoint is creating its Approved List, a progress bar instead will appear.</p>
Agent Version	<p>Displays the firmware version of the agent</p>
Last Connection	<p>Displays the last time the agent was connected with StellarOne</p>
Function Type	<p>Displays two function types of StellarProtect:</p> <ul style="list-style-type: none"> • StellarProtect: for devices with Windows 7 or later versions • StellarProtect (Legacy Mode): for devices with legacy platforms such as Windows XP/2000
Actions	<p>Under this heading, you can:</p> <ul style="list-style-type: none"> • click  , the Policy icon, for linking to the General Info policy page. • click the three dots More actions menu, for organizing agents and renaming/removing groups. See Edit Description for Agents on page 4-16 and Organize Agents/Groups on page 4-16 for more details.

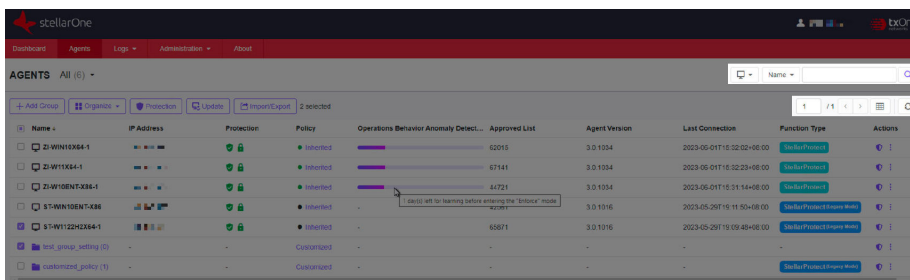


FIGURE 4-3. The Agents Screen - Other Tools

TABLE 4-3. Other Tools

TOOL	DESCRIPTION
Filter	This tool allows you to quickly find the agents/groups by sorting and searching. See Filter Options for Agents/Groups on page 4-18 for more details.
Table Display Settings	This tool allows you to customize the table display settings by: <ul style="list-style-type: none"> going back and forth between the display pages selecting how many agents/groups to be displayed per page and specifying only certain contents to be displayed in the Customize Table Display setting
Agent Status Settings	This tool allows you to view or change current configuration for the agent status settings, which determines the associated agent status displayed on the Agents screen and the information displayed in the corresponding widgets on the Dashboard screen. Available options include: <ul style="list-style-type: none"> Manage Agent Connection Status: Specify the duration (by days) to determine whether the agents should be categorized as Online, Offline, or removed from StellarOne. See Manage Agent Connection Status on page 4-8 for more details. Manage Agent Component Status: Specify the duration (by a day, week, or month) to determine whether the agent component update status should be categorized as Up-to-date or Out-of-date. See Manage Agent Component Status on page 4-9 for more details. Refresh: Manually refreshing the agent status for the latest outputs

Agent Status Settings

This section introduces how to configure the following agent status settings:

- [Manage Agent Connection Status on page 4-8](#)
- [Manage Agent Component Status on page 4-9](#)
 - [Correlated Settings for Agent Component Status on page 4-11](#)
 - [Configuring Agent Component Status Settings— Use Case on page 4-13](#)



Manage Agent Connection Status

The configuration of **Manage Agent Connection Status** determines the connection status of each single agent displayed on the **Agents** screen, as well as the overall availability status of all the managed agents displayed in **Agent Connection Status** widget on the **Dashboard** screen.

The criteria of displaying **Online**, **Offline**, and removal of the agent depend on how long the agent has been disconnected from StellarOne. By default, the agent will appear **Offline** after disconnected from StellarOne for more than 7 days and basically never be removed from StellarOne no matter how long the disconnection lasts. In other words, by default the agent will always appear **Online** if it has been connected to StellarOne within 7 days.

You can also customize the settings to fit your environment needs. See the following instructions for how to change the configuration:

Procedure

1. Go to **Agents** in the top navigation bar of the StellarOne web console.
2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.
3. Find the settings icon  on the right side of the screen.
4. Click  and select **Manage Agent Connection Status** from the drop-down menu.
5. The configuration window appears. In **Appear Offline after** drop-down menu, specify the time frame after which the agent connection status

will display offline if the agent has been disconnected. Available time period for selection includes:

- 1 day
- 2 days
- 3 days
- 7 days (Default)
- 14 days
- 30 days

6. In **Remove from StellarOne after**, specify the time frame after which the agent will be removed from StellarOne managed agents list if disconnected for more than the specified duration. Available time period for selection includes:

- Never (Default)
- 1 month
- 2 months
- 3 months
- 6 months
- 12 months

See the sections below for more details about the correlated settings to consider and use case when configuring the agent connection status settings.



Manage Agent Component Status

The configuration of **Manage Agent Component Status** determines the component update status of each single agent displayed on the **Agents** screen, as well as the overall component update status of all the managed agents displayed in **Agent Component Status** widget on the **Dashboard** screen.

The criteria of displaying **Up-to-date** or **Out-of-date** depend on how long the agent components have or have not been updated. By default, the status of agent components will always appear **Up-to-date** if they have been updated within 1 week. In other words, by default the status of agent components will appear **Out-of-date** if they haven't been updated for more than 1 week.

You can also customize the settings to fit your environment needs. See the following instructions for how to change the configuration:

Procedure

1. Go to **Agents** in the top navigation bar of the StellarOne web console.
2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.
3. Find the settings icon  on the right side of the screen.
4. Click  and select **Manage Agent Component Status** from the drop-down menu.
5. The configuration window appears. In the **Appear Out-of-date after** drop-down menu, specify the time frame after which the status of agent components will display out-of-date if they haven't been updated. Available time period for selection includes:
 - 1 day
 - 1 week (Default)
 - 1 month
 - 2 months

**Important**


- It is recommended to take the agent component update schedule specified in the agent/group policy settings into consideration before you adjust the configuration of **Manage Agent Component Status**. See *Correlated Settings for Agent Component Status on page 4-11* and *Configuring Agent Component Status Settings— Use Case on page 4-13* for more details.
 - If you enable **Defer Component Update** in the agent component update schedule, the agent or group deployed with the previous components version will be categorized as **Up-to-date** in the widget. See *Agent Component Update Schedule on page 5-84* for more details.
-


Correlated Settings for Agent Component Status

Changes of several settings can impact the **Agent Component Status** widget. Properly configuring the correlated settings determines if the widget can accurately reflect your environment.

See the following table for an overview of the correlated settings and factors to consider:

TABLE 4-4. Correlated Settings and Relevant Details

SETTING	LOCATION	FREQUENCY OR DURATION	FACTOR TO CONSIDER
Scan Component Update Schedule (StellarOne)	Administration > Downloads/Updates > StellarOne	Frequency options: <ul style="list-style-type: none"> • Daily (Default) • Weekly • Monthly • Start Time: 20:00 (Default) 	Data transmission bandwidth  Note See Recommended Bandwidth for StellarOne Components Update on page 4-13 for more details.
Agent Component Update Schedule	Agents > All: target agent/group Policy page	Frequency options: <ul style="list-style-type: none"> • Daily (Default) • Weekly • Monthly • Start Time: 00:00 (Default) 	
Manage Agent Component Status	Agents > Status Settings	Duration options: <ul style="list-style-type: none"> • 1 day • 1 week (Default) • 1 month • 2 months  Note By default, the agent component status will appear out-of-date after 1 week.	The frequency specified in Agent Component Update Schedule

SETTING	LOCATION	FREQUENCY OR DURATION	FACTOR TO CONSIDER
Manage Agent Connection Status	Agents > Status Settings	Duration options: <ul style="list-style-type: none"> • 1 day • 2 days • 3 days • 7 days (Default) • 30 days <hr/>  Note By default, the agent connection status will appear Offline after 7 days.	The duration specified in Manage Agent Component Status

Recommended Bandwidth for StellarOne Components Update

See the following table for the recommended data transmission bandwidth for StellarOne components update.

METHOD	RECOMMENDED BANDWIDTH (ON AVERAGE)
Full load	75 MB (if the components loading takes place every 15 days)
Incremental load	200 KB (if the components loading takes place within 14 days)

Configuring Agent Component Status Settings— Use Case

The following section describes a use case that requires the StellarOne admin to configure the correlated components update and agent component status settings.

Scenario: You have a group of agents that are scheduled for maintenance **at the first day of every month**. Since the update frequency is fixed to "monthly", you'll need to change the default settings (daily) to **Monthly** for the **Agent Component Update Schedule**, to prevent the updates from impacting on the

asset operations. Furthermore, since monthly component update is viewed "normal" for this group of assets, you'll also need to change the default settings (1 week) to at least **1 month** for the **Agent Component Status** widget, so the group of assets can appear up-to-date within the determined update frequency that fits your environment.

See the following procedures as the recommended practice:

Procedure

1. Go to **Scan Component Update Schedule (StellarOne)**, select the frequency you want StellarOne to download the latest scan component. It is recommended to select **Daily** or **Weekly** if the data transmission bandwidth is limited. Refer to [Recommended Bandwidth for StellarOne Components Update on page 4-13](#) for more information.

**Note**

See [Configuring Scan Component for StellarOne on page 7-21](#) for more detailed configuration procedures.

2. Go to **Agent Component Update Schedule**, specify the frequency StellarOne will apply the latest scan components to the managed group of agents. It is recommended to select **Monthly**. However, you may need to adjust the network bandwidth between the agents and StellarOne for smooth updates. Refer to [Recommended Bandwidth for StellarOne Components Update on page 4-13](#) for more information.

**Note**

See [Agent Component Update Schedule on page 5-84](#) for more detailed configuration procedures.

3. Go to **Agents > Settings > Manage Agent Component Status** to specify **1 month**. The agent component status will appear up-to-date if the components have been deployed to the managed agents within 1 month.

**Note**

It is recommended to specify a larger or the same value for the time frame compared with that of the frequency set in **Agent Component Update Schedule**; otherwise, the group of the agents would appear out-of-date.

4. Since the **Agent Component Status** widget only displays agents that appear **Online** in the **Agent Connection Status** widget, if the group of agents may be disconnected to StellarOne for more than the duration specified in the **Manage Agent Connection Status** settings, it'd be better to go to **Agents > Settings > Manage Agent Connection Status** to specify **30 days** after which the agents will appear offline if disconnected with StellarOne.
-

Add Groups

Procedure

1. Go to **Agents** in the top navigation bar of the StellarOne web console.
 2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.
 3. Click the **+Add Group** button in the toolbar.
 4. The **Add New Agent Group** window appears. Specify the group name in the text field.
-

**Note**

- The maximum length limitation of a group name is 50 characters.
 - The maximum number of group levels is 15 levels.
-

5. Click **Confirm** to add the group.
-

Edit Description for Agents

To edit description for agents, which will appear on the main screen of the local agent, follow below procedures.

Procedure

1. Go to **Agents** in the top navigation bar of the StellarOne web console.
 2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.
 3. There are two ways to edit descriptions for agent(s):
 - To edit description for multiple agents at the same time, click the checkboxes next to the target agents. Click the **Organize** tool on the toolbar.
 - To edit description for a single agent, find the target agent and click its three dots **More actions** menu under the **Actions** header.
 4. A drop-down menu appears. Click **Edit Description** and then a window appears.
 5. Specify the description for the agent(s) in the text field.
 6. Click **Confirm** to complete this task.
-

Organize Agents/Groups

You can organizing agents/groups by:

- renaming groups
- removing groups
- removing agents from groups
- moving agents to another group

Procedure

1. Go to **Agents** in the top navigation bar of the StellarOne web console.
2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.
3. To rename a group, click the three dots **More actions** menu of the target group under the **Actions** header. A drop-down menu appears. Select **Rename** and then a pop-up window appears. Delete the old group name and replace it with a new one. Click **Confirm** to complete this task.

**Note**

Groups at the same level can not have the same group name.

4. There are two ways to remove groups or agents:
 - To remove multiple agents or groups at the same time, click the checkboxes next to the target agents or groups. Click the **Organize** tool on the toolbar and select **Remove**. Click **Confirm** to remove the agents/groups.

**Important**

- To remove agent(s): The agent(s) will be unregistered from the server.
 - To remove group(s): The group(s) and the configuration of the group(s) will be removed.
-
- To remove a single agent or group, click the three dots **More actions** menu of the target agent/group under the **Actions** header. A drop-down menu appears. Select **Remove** to remove the agent/group.

**Important**

To remove groups with child groups/agents, please remove the child groups/agents from the target groups first.

5. There are two ways to move agent(s) to another group:

- To move multiple agents to another group at the same time, click the checkboxes next to the target agents. Click the **Organize** tool on the toolbar.
- To move a single agent to another group, click the three dots **More actions** menu of the target agent under the **Actions** header.

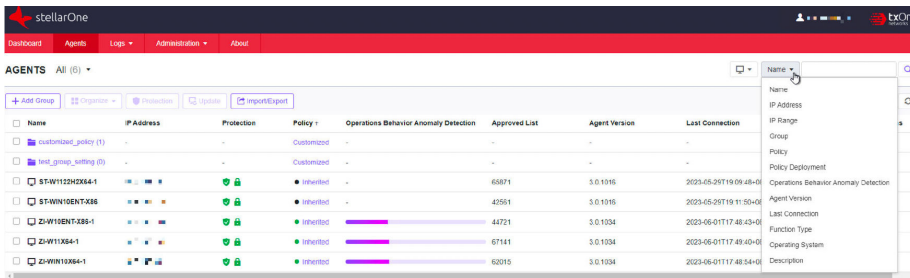
A drop-down menu appears. Select **Move** and then a pop-up window appears. Select the group and click **Confirm** to complete this task.

Search for Agents/Groups

Procedure

1. Go to **Agents** in the top navigation bar of the StellarOne web console.
2. At the top-right corner of the screen, search for specific endpoints by selecting criteria from the drop-down list and specify additional search criteria as required.

Filter Options for Agents/Groups




The screenshot shows the StellarOne web console interface. The top navigation bar includes 'Dashboard', 'Agents', 'Log', 'Administration', and 'About'. The main content area is titled 'AGENTS All (6)'. A search filter dropdown menu is open, showing a list of filter options: Name, IP Address, IP Range, Group, Policy, Policy Deployment, Operations Behavior Anomaly Detection, Agent Version, Last Connection, Function Type, Operating System, and Description. The table below the dropdown lists several agents with columns for Name, IP Address, Protection, Policy, Operations Behavior Anomaly Detection, Approved List, Agent Version, and Last Connection.

Name	IP Address	Protection	Policy	Operations Behavior Anomaly Detection	Approved List	Agent Version	Last Connection
customized_policy (1)	-	-	Customized	-	-	-	-
test_group_setting (0)	-	-	Customized	-	-	-	-
ST-WIN1122H2X64-1	-	Green Lock	Inherited	-	65871	3.0.1036	2023-05-26T19:09:48-01
ST-WIN10ENTX386	-	Green Lock	Inherited	-	42561	3.0.1036	2023-05-26T19:11:50-01
ZI-WIN10ENTX86-1	-	Green Lock	Inherited	Progress Bar	44721	3.0.1034	2023-05-01T17:48:43-01
ZI-WIN11X64-1	-	Green Lock	Inherited	Progress Bar	67141	3.0.1034	2023-05-01T17:49:40-01
ZI-WIN11X64-1	-	Green Lock	Inherited	Progress Bar	62015	3.0.1034	2023-05-01T17:48:54-01

FIGURE 4-4. Filter Options for Agents/Groups

TABLE 4-5. Filter Options for Agents/Groups

OPTIONS	DESCRIPTIONS
	<p>This icon provides three filter options:</p> <ul style="list-style-type: none"> • Active Agents: the agents with license seats • Inactive Agents: the agents without license seats • Ungrouped Agents: the agents that are not grouped.
Name	The name of the agent. Type the full or partial endpoint host name to locate the specific agent.
IP Address	Type the IPv4 address.
IP Range	Type the IPv4 address range.
Group	The name of the group. Please ensure that you select the available group.
Policy	Three options -- Customized , Inherited , and Self-managed , are available for selection.
Policy Deployment	The status of policy deployment from StellarOne to Agents. Select Completed or In Progress .
Operations Behavior Anomaly Detection	Find the target agents by the modes of the Operations Behavior Anomaly Detection. Four modes are available for selection: Learn , Detect , Enforce , or Disabled .
Agent Version	Type the build version of the target agents.
Last Connection	<p>The last time the agents were connected with StellarOne. Select the default time period or select Custom range to specify a time period. Default time period available for selection includes:</p> <ul style="list-style-type: none"> • Last 1 hour • Last 24 hours • Last 7 days • Last 30 days
Function Type	Select StellarProtect or StellarProtect (Legacy Mode) .

OPTIONS	DESCRIPTIONS
Operating System	Select an operating system of the target endpoints.
Description	Type the full or partial description to query specific endpoints.

Protection

The **Protection** tool sends one-time commands to endpoints for triggering immediate actions, allowing you to configure Maintenance Mode, update Approved List when the Application Lockdown feature is enabled, and customize file scan settings.

Topics in this chapter include:

- [Configure Maintenance Mode on page 4-20](#)
- [Update Approved List on page 4-24](#)
- [Scan Now on page 4-25](#)

Configure 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, the agents allows all file executions and adds all files that are created, executed, or modified to the Approved List. Besides, the agents 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. You can also define the action to take after suspicious files are detected.

**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 policy settings of Application Lockdown, Multi-Method Threat Prevention (StellarProtect), OT Application Safeguard (StellarProtect), or Threat Prevention (StellarProtect (Legacy Mode)) during maintenance period, the policy settings will not be implemented until the maintenance period is ended.
 - During the maintenance period, you cannot perform agent patch updates on endpoints. In addition, the StellarProtect (Legacy Mode) agent 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.
-

Procedure

1. Go to **Agents > All**.
2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.
3. Select one or more endpoints (agents or groups) by clicking the checkboxes next to them.
4. Click the **Protection** button from the Tool Bar at the top of the **Agents** screen.

5. A pop-up window appears. Click the **Configure Maintenance Mode** option.
6. Click **Confirm**.
7. The configuration window appears. Please read the notice carefully before you check the **Disable** or **Enable** radio button.
 - Click **Disable** > **OK** to end Maintenance Mode. This will cancel the scheduled maintenance period on endpoints.
 - a. A warning message appears. Please read carefully before proceeding to next step.



Important

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

- b. Click **OK** to end Maintenance Mode. A pop-up window appears showing the deployment status of stopping Maintenance Mode on endpoints.
- Click **Enable** to start the Maintenance Mode settings. Please go to *Step 8* for next procedure.



Important

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

8. The schedule configuration window appears. Do one of the following for scheduling Maintenance Mode.

**Note**

- Agents can start one scheduled maintenance period at a time. If you configure a new maintenance period, the system overwrites the existing maintenance schedule that has not started yet.
 - 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.
-

- Click the **Schedule** radio button, and then click the edit icon to select the start date and specify the start time for Maintenance Mode. After that, specify the duration of the maintenance period in **Maintenance Mode will be ended after**.
 - Click the **Start now** radio button, and then specify the duration of the maintenance period in **Maintenance Mode will be ended after**.
9. A **Scan** toggle switch is added at the bottom and is set **enabled** by default.
-

**Note**



- If you disable scan feature in the policy settings, TXOne Networks suggests you enable the scan function here to ensure all the new or changed files go through the malware scanning before they're added to the Approved List. After the maintenance, the original policy settings (in which the scan feature is disabled) will still apply.
 - The scan toggle should not appear on the StellarOne console with StellarOEM license edition. See [License Editions on page 7-34](#) for more details.
-

10. Select one of the actions to take if suspicious files are detected during scanning:
- **Quarantine detected files**
 - **Add detected files to Approved List**

11. Click **OK** to deploy the settings to the selected agents or groups.
12. The **Command Deployment** window appears showing the deployment status. Click the **Close** button to close the window.

**Note**

On the **Agents** screen, in the **Protection** column of the selected agents/groups:

- The  will appear indicating a maintenance period has been scheduled but not started yet if you select **Schedule** in *Step 8* and deploy related settings.
 - The  icon will appear indicating the agents/groups are currently in maintenance mode if you select **Start now** in *Step 8* and deploy related settings.
-

Update Approved List

This function allows you to update the Approved List on selected agents/groups by several simple clicks. Updating the Approved List performs an inventory scan on selected endpoints and adds any new applications found on the endpoints to the global Approved List. The Approved List must be periodically updated so the newly-added applications can run on the endpoints when the Application Lockdown feature is turned on.

After setting up the Approved List, you can also add new programs by enabling Maintenance Mode, and the new or modified files will be added to the Approved List.

Procedure

1. Go to **Agents > All**.
2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.
3. Select one or more endpoints (agents or groups) by clicking the checkboxes next to them.

4. Click the **Protection** button from the Tool Bar at the top of the **Agents** screen.
5. A pop-up window appears. Click the **Update Approved List** option.
6. Click **Confirm**.
7. A pop-up **Update Approved List** window appears. Click **OK** to start the Approved List update process.

**WARNING!**

Do not restart or turn off the endpoint(s) during the update. The update process may take more than 30 minutes to complete.

8. The **Update Approved List** window appears showing the update status. Click the **Close** button to close the window.
-

Scan Now

You can manually initiate **Scan Now** on selected endpoints and deploy the scan settings on one or several target endpoints.

Procedure

1. Go to **Agents > All**.
2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.
3. Select one or more endpoints (agents or groups) by clicking the checkboxes next to them.
4. Click the **Protection** button from the Tool Bar at the top of the **Agents** screen.
5. A pop-up window appears. Click the **Scan Now** option.
6. Click **Confirm**.
7. The configuration window appears.

8. The configuration window consists of four sections: **Files to Scan**, **CPU Usage**, **Scan Action**, and **Scan Exclusions**.

**Note**

The StellarProtect (Legacy Mode) agents will automatically attempt to download the latest components before starting a scan. A **Component Update** toggle is available for you to determine whether the endpoints should continue with the scan if the component update is unsuccessful.

- a. In the **Files to Scan** section, click **All local folders** to scan all files in detail; click **Default folders (Quick Scan)** for a general scan; or click **Specific folders** to specify the paths to the folders for scan.

**Tip**

Under the **Specific folders** option, click the "+" or "-" icon to add or delete paths to the specific folders.

- (Optional) Check **Scan removable drives** to allow scanning files in removable drives
 - (Optional) Check **Scan compressed files** and select the **Maximum layers** between 1 and 20 for the compressed files.
 - (Optional) To skip files over a certain size, check **Skip files larger than** and specify the file size between 1 and 2048 MB. Files exceeding the specified file size will not be scanned.
 - (Optional and StellarProtect only) Check **Aggressive scan (include all OT applications and CA files)** to allow scanning files in existing trusted list.
- b. The **CPU Usage** settings allow you to select the appropriate mode of CPU usage to balance between the scan and the available CPU resources depending on situations. There are two options available:

- Click **Normal** to reduce the impact on the service performance, which allows you to perform other tasks while scanning but the scan may take longer to complete.
 - Click **High** to reduce scan time, which requires higher CPU usage and may affect the system performance.
- c. In the **Scan Action** section, you can pre-define the action to take after threats are detected. Select **Quarantine** to place the suspicious or infected files detected in an isolated folder for further checking. Select **No action** to produce only a readout of results with no actions taken on the suspicious files.

**Note**

The StellarProtect (Legacy Mode) agents provide more choices such as:

- **Use ActiveAction:** The pre-configured scan actions, which are best to use if you are not familiar with scan actions or if you are not sure which scan action is suitable.
 - **Clean, or delete if the clean action is unsuccessful:** To delete the target file if it cannot be recovered.
 - **Clean, or quarantine if the clean action is unsuccessful:** To quarantine the target file if it cannot be recovered.
 - **Clean, or ignore if the clean action is unsuccessful:** To ignore the target file if it cannot be recovered.
-
- d. (Optional) The **Scan Exclusions** section allows you to exclude certain folders, files, or file extensions from being scanned.
- **Folders:** specify a path to the folders that do not require scanning.
 - **Files:** specify a path to the files that do not require scanning.
 - **File Extensions:** specify the file extension of certain files that do not require scanning.



Note

- StellarProtect supports only local paths for **Scan Exclusions**. Remote paths such as an URL or \\ [Hostname] are not supported.
 - It is not required to add "." or "*" in front of the file extension.
-



Tip

Click the "+" or "-" icon to add or delete paths to the specific folders/ files or file extensions for specific file types .

9. Click **Confirm** to deploy the settings to the selected endpoints.
 10. The **Command Deployment** window appears showing the deployment status. Click **Close** to close the window.
-

Update

This section introduces how to implement immediate update for the agents via StellarOne web console.

Topics in this section include:

- [Update Agent Components on page 4-29](#)
 - [Deploy Agent Patches on page 4-29](#)
 - [Check Connections on page 4-31](#)
 - [Apply Policies on page 4-31](#)
 - [Collect Event Logs on page 4-32](#)
-



Note

Only StellarProtect (Legacy Mode) supports the Collect Event Logs feature.

Update Agent Components

You can update agent components on selected endpoints via StellarOne web console. TXOne Networks recommends updating agent components regularly to protect the endpoints against the latest security threats.

Procedure

1. Click the **Agents** tab in the top navigation bar of the StellarOne web console.
2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.
3. Select one or more endpoints (agents or groups) by clicking the checkboxes next to them.
4. Click the **Update** button from the Tool Bar at the top of the **Agents** screen.
5. A pop-up window appears. Click **Update Agent Components** option.
6. Click **Confirm**.
7. The **Update Agent Components** window appears. Click **OK** to start the update.



Important

Do not restart or turn off the endpoints during the update. The update process may take some time to complete.

8. The **Command Deployment** window appears showing the update status. Click the **Close** button to close the window.
-

Deploy Agent Patches

You can deploy patch files for agents on selected endpoints via StellarOne web console. TXOne Networks recommends updating agent patches regularly to protect the endpoints against the latest security threats.

Procedure

1. Go to **Agents > All**.
2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.
3. Select one or more endpoints (agents or groups) by clicking the checkboxes next to them.
4. Click the **Update** button from the Tool Bar at the top of the **Agents** screen.
5. A pop-up window appears. Click the **Deploy Agent Patches** option.
6. Click **Confirm**.
7. A pop-up **Deploy Agent Patches** window with the patch list appears. Select the version of the patch for deployment and click the checkbox next to it.

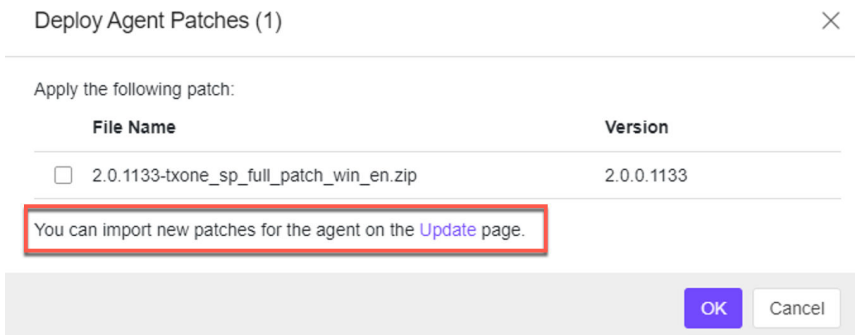


FIGURE 4-5. Select the Patch Version



Note

By clicking the **Update** link, you will be directed to the [Downloads/Updates on page 7-21](#) page for importing new patches for agents.

8. Click **OK** to start the patch deployment process for the agents. Click the **Close** button to close the window.
-

Check Connections

You can check the connection status of the selected agents.

Procedure

1. Go to **Agents > All**.
2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.
3. Select one or more endpoints (agents or groups) by clicking the checkboxes next to them.
4. Click the **Update** button from the Tool Bar at the top of the **Agents** screen.
5. A pop-up window appears. Click the **Check Connections** option.
6. Click **Confirm**.
7. A pop-up **Command Deployment** window with the endpoint list appears. The **Status** column shows if the agents are successfully connected to the StellarOne server.



Note

If the status shows **Unsuccessful**, check the network connectivity of the disconnected agents.

8. Click **Close** to close the window.
-

Apply Policies

You can manually apply policy updates to the selected endpoints.

Procedure

1. Go to **Agents > All**.
2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.
3. Select one or more endpoints (agents or groups) by clicking the checkboxes next to them.
4. Click the **Update** button from the Tool Bar at the top of the **Agents** screen.
5. A pop-up window appears. Click the **Apply Policies** option.
6. Click **Confirm**.
7. A pop-up **Command Deployment** window with the endpoint list appears. The **Status** column shows if the StellarOne policies are successfully applied to the target agents.



Note

- If the status shows **Unsuccessful**, check the network connectivity of the disconnected agents.
- By default, agents automatically synchronize with StellarOne policies every 20 minutes. If you want to adjust the policy sync interval, see [Set Policy Refresh Interval on page 5-4](#) for specifying how often the StellarOne policy is applied to selected agent/group.

-
8. Click **Close** to close the window.
-

Collect Event Logs

Logs contain information about agent activity. **Collect Event Logs** updates the StellarOne database with the latest information from the selected agents.



Note

Only StellarProtect (Legacy Mode) supports this function.

Procedure

1. Go to **Agents > All**.
2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.
3. Select the target agents by clicking the checkboxes next to them.
4. Click the **Update** button from the Tool Bar at the top of the **Agents** screen.
5. A pop-up window appears. Click the **Collect Event Logs** option.
6. Click **Confirm**.
7. A pop-up **Command Deployment** window with the endpoint list appears. The **Status** column shows if the event logs are successfully collected.
8. Click **Close** to close the window.

**Note**

StellarOne will update the date and time displayed in the **Last Connection** column on the **Agents** screen after each StellarProtect (Legacy Mode) agent successfully sends logs and status to StellarOne.

-
9. Go to **Logs > Agent Events** for viewing the collected event logs of the selected agents. Refer to [Agent Events on page 6-2](#) for more detailed instructions if needed.

**Note**

By default, the selected agents will only send back the **Warning** and **Critical** level logs.

-
10. (Optional) Choose one of the ways to add the **Information** level logs in the collected event logs.

**Note**

The log volume may surge if the **Information** level logs are included in the collected event logs.

- On the StellarOne console, export the agent's configuration file and change the value of `InformationLog Enable` to `yes`. Import the modified configuration file to the selected agent. Refer to [Export Agent Configurations on page 4-35](#) and [Import Agent Configurations on page 4-37](#) for more detailed instructions.

```
<Log>
  <EventLog Enable="yes">
    <Level>
      <WarningLog Enable="yes"/>
      <InformationLog Enable="yes"/>
    </Level>
  </EventLog>
</Log>
```

FIGURE 4-6. Snippet of the Configuration File

- On the target StellarProtect (Legacy Mode) agent, open the `StellarSetup.ini` file in the installer package and change the value of `Level_InformationLog` to 1. Be sure to save the changed file and run the installation again.

```
[Legacy_EventLog]
Enable = 1
Level_WarningLog = 1
Level_InformationLog = 1
```

FIGURE 4-7. Snippet of the StellarSetup.ini File**Note**

Only after you change the event log setting for the target agents and apply the **Collect Event Logs** action to them, will the **Information** level logs be sent to StellarOne.

Agent Export/Import Settings

This section introduces how to apply the import/export actions to the agents via StellarOne web console.

Topics in this section include:

- [Export Agent Settings on page 4-35](#)
- [Import Agent Settings on page 4-36](#)
- [Export Selected Agents Info on page 4-39](#)
- [Export all Agents Info on page 4-39](#)



Note

- Except for exporting Approved List, StellarProtect does not support the export or import of other agent settings.
 - The export of agent settings are only available for individual agents. When you select any group from the list, the functions are unavailable.
-

Export Agent Settings

You can remotely obtain the StellarProtect (Legacy Mode) agent configuration settings or the StellarProtect/StellarProtect (Legacy Mode) Approved List by exporting and downloading them from the StellarOne console.

Export Agent Configurations

Procedure

1. Go to **Agents > All**.
2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.
3. Select the target agent by clicking the checkbox next to it.

4. Click the **Import/Export** button from the Tool Bar at the top of the **Agents** screen.
 5. Click the **Export Agent Configurations** option.
 6. Click **Confirm**.
 7. A pop-up **Command Deployment** window appears. The **Status** shows if the agent configuration is exported successfully.
 8. Click the **Download** link to download the target agent's configuration file.
-

Export Approved List

Procedure

1. Go to **Agents > All**.
 2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.
 3. Select the target agent by clicking the checkbox next to it.
 4. Click the **Import/Export** button from the Tool Bar at the top of the **Agents** screen.
 5. Click the **Export Approved List** option.
 6. Click **Confirm**.
 7. A pop-up **Command Deployment** window appears. The **Status** shows if the agent's Approved List is exported successfully.
 8. Click the **Download** link to download the target agent's Approved List.
-

Import Agent Settings

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

- Remotely overwrite the agent configuration
- Remotely overwrite the Approved List

Remember to prepare a customized agent configuration or Approved List file first before you start the import:

1. Export and download an agent configuration file or the Approved List.
2. Customize the downloaded file.

**Note**

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

- The Approved List file must be in the CSV format with UTF-8 encoding and file size ideally less than **120 MB**.
- The agent configuration file must be in the XML format with the file size ideally less than **1 MB**.

Import Agent Configurations

Procedure

1. Go to **Agents > All**.
2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.
3. Select the target agents by clicking the checkboxes next to them.
4. Click the **Import/Export** button from the Tool Bar at the top of the **Agents** screen.
5. Click the **Import Agent Configurations** option.
6. Click **Confirm**.
7. A pop-up **Import Agent Configurations** window appears. Click **Select File**.

8. Select the file to import and click **OK**.
 9. A pop-up **Command Deployment** window appears. The **Status** shows if the agent configurations are imported to the target endpoints successfully.
 10. Click **Close** to close the window.
-

Import Approved List

Procedure

1. Go to **Agents > All**.
 2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.
 3. Select the target agents by clicking the checkboxes next to them.
 4. Click the **Import/Export** button from the Tool Bar at the top of the **Agents** screen.
 5. Click the **Import Approved List** option.
 6. Click **Confirm**.
 7. A pop-up **Import Approved List** window appears. Click **Select File**.
 8. Select the file to import and click **OK**.
-



Note

The switch toggle, **Replace the trusted hash value of existing applications with that in the imported Approved List.**, is used for overwriting the existing trusted hash values in the original Approved List. By default, the toggle is switched off.

9. A pop-up **Command Deployment** window appears. The **Status** shows if the new Approved List is imported to the target endpoints successfully.

10. Click **Close** to close the window.
-

Export Selected Agents Info

This function allows you to export selected agents' information about endpoint description, IP address, license status, policy settings, etc.

Procedure

1. Go to **Agents > All**.
 2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.
 3. Select one or more endpoints (agents or groups) by clicking the checkboxes next to them.
 4. Click the **Import/Export** button from the Tool Bar at the top of the **Agents** screen.
 5. A pop-up window appears. Click the **Export Selected Agents Info** option.
 6. Click **Confirm**.
 7. A `.csv` file is downloaded.
-

Export all Agents Info

This function allows you to export all agents' information about endpoint description, IP address, license status, policy settings, etc.

Procedure

1. Go to **Agents > All**.
2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.
3. Click the **Import/Export** button from the Tool Bar at the top of the **Agents** screen.

4. A pop-up window appears. Click the **Export all Agents Info** option.
 5. Click **Confirm**.
 6. A .csv file is downloaded.
-

Chapter 5

Policy Configuration

This chapter introduces how to configure StellarProtect/StellarProtect (Legacy Mode) policy settings at the agent and/or group level via StellarOne web console.

Topics in this chapter include:

- *Settings for the Agent/Group Policy Screen on page 5-2*
- *Agent View and Policy Settings on page 5-23*
- *Group Policy Settings on page 5-106*

Settings for the Agent/Group Policy Screen

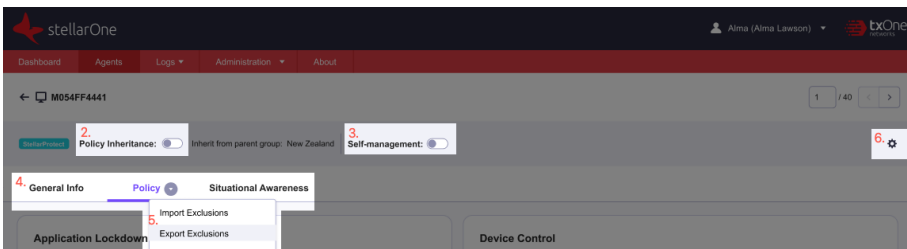


FIGURE 5-1. Options Available in the Agent View

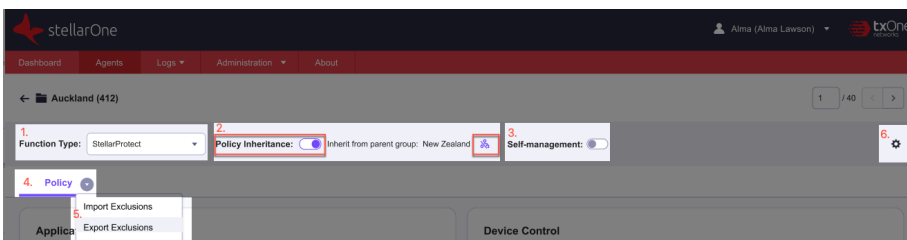


FIGURE 5-2. Options Available on the Group Policy Screen

ITEM	OPTIONS	AGENT	GROUP
1	Function Type	N/A	The dropdown menu allows you to switch between StellarProtect and StellarProtect (Legacy Mode) .

ITEM	OPTIONS	AGENT	GROUP
2	Policy Inheritance	<p>The toggle allows you to enable or disable the policy inheritance from the parent group.</p> <ul style="list-style-type: none"> If this toggle is on, policy settings for the agents/groups are inherited from the parent group. The Inherited status will be displayed in the Policy column on the Agents screen. If this toggle is off, the StellarOne administrators can create a custom policy based on current policy settings. The Customized status will be displayed in the Policy column on the Agents screen. 	
	Custom Exceptions	N/A	<p>At the group level, after enabling Policy Inheritance, the Custom Exceptions option will appear, which is used to create custom exceptions to the inherited policy. See Create Custom Exceptions to the Inherited Policy on page 5-110 for more details.</p>
3	Self-management	<p>The toggle allows you to enable or disable the agent's self-management. When the toggle is on, the agent will be set free from StellarOne console's policy management and the on-site operators can configure the agent's policy settings on their own.</p>	
4	Tab pages	<p>You can switch among the pages related to the General Info, Policy page, and Situational Awareness baseline at the agent level.</p>	<p>Only the Policy page is available at the group level.</p>
5	<p>Import Exclusions</p> <p>Export Exclusions</p>	<p>You can export and import the policy-based exceptions list used for Application Lockdown, (Multi-Method) Threat Prevention, OT Application Safeguard (StellarProtect only), Operations Behavior Anomaly Detection, and Device Control.</p> <p>See Export/Import Exclusions Settings on page 5-6 for more information.</p>	

ITEM	OPTIONS	AGENT	GROUP
6	Settings	<ul style="list-style-type: none"> • Set Policy Refresh Interval: You can specify how often the StellarOne policy, dashboard and Situational Awareness data sync are applied to the agent/group. See Set Policy Refresh Interval on page 5-4 for more details. • Agent User Interface Preferences: You can customize the user interface settings, such as the display of pop-up notifications and right-click scan accessibility on the managed endpoints. See Set Agent User Interface Preferences on page 5-5 for more information. 	

Set Policy Refresh Interval

You can specify how often the StellarOne policy, dashboard and the Situational Awareness data sync are applied to the specific agent.

Procedure

1. See [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group setting.
2. Find the settings icon in the upper-right corner of the screen.
3. Click the settings icon and the **Set Policy Refresh Interval** window appears.
4. Click the **Refresh Interval** menu and select among the given options:
 - **5 Minutes**
 - **10 Minutes**
 - **20 Minutes** (default setting)
 - **60 Minutes**



Important

Frequent refresh might interfere with your work and increase network traffic. See the following table as the recommended policy refresh interval regarding the number of agents managed:

POLICY REFRESH INTERVAL	NO. OF AGENTS MANAGED
5 minutes	5,000
10 minutes	10,000
20 minutes	20,000
60 minutes	60,000

5. Click **Save** to complete the setting.

Set Agent User Interface Preferences

You can customize the user interface settings, such as the display of pop-up notifications and right-click scan accessibility on the managed endpoints via StellarOne at the agent or group level.

Procedure

1. See [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group setting.
2. Find the settings icon in the upper-right corner of the screen.
3. Click the settings icon and the **Agent User Interface Preferences** window appears.
4. Three preference settings are available:
 - **Display a pop-up notification for a detected threat:** If enabled, a pop-up window will appear on the local console whenever a threat is detected. More details about the threat the the infected file will be provided to the local user for further investigation.
 - **Display a pop-up notification for a blocked USB device:** If enabled, a pop-up window will appear on the local console whenever a blocked USB device is detected. The local administrator can grant one-time access to the blocked USB device via the pop-up notification.

**Note**

The blocking occurs when USB device control has been enabled. See [Device Control on page 5-86](#) for more details.

- **Add a scan option to the Windows context menu:** If enabled, a scan option will be added to the right-click context menu. Agent users can run a right-click scan for the selected file, folder, or drive.

5. Click **Save** to complete the setting.

Export/Import Exclusions Settings

Exporting and importing exclusions settings allow you to move the associated settings listed below from one group to another:

- **Application Lockdown**
 - Excluded Paths
 - Trusted Hash Values
 - Write Protection (StellarProtect (Legacy Mode) only)
- **(Multi-Method) Threat Prevention**
 - Real-Time Scan Exclusions
 - Scheduled Scan Exclusions
- **OT Application Safeguard** (StellarProtect only)
 - Files / Folders
 - Authorized Process
- **Operations Behavior Anomaly Detection**
 - Policy-based Watchlist
 - Policy-based Approved Login Accounts
 - Policy-based Approved Applications
- **Device Control**

- Trusted USB Device

It is recommended to refer to the [Agent Policy Settings on page 5-27](#) to configure the associated exclusions settings first, and then export the exclusions file from the agent/group as a template to modify (if needed) and import it to a batch of target agents/groups.

Export Exclusions

You can remotely obtain the policy-based exclusions list of a single agent or group of agents by exporting and downloading it from StellarOne.

Procedure

1. Navigate to the target agent or group, and then go to its **Policy** page. For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.
2. Click the **Policy** tab and a downward arrow appears.
3. Click the arrow and a drop-down menu appears.
4. Select **Export Exclusions**.
5. Find the exported exclusions list in your downloads folder.



Note

The exported exclusions list is editable depending on your needs. See ... for the complete exclusions configuration file and associated parameters as a reference to modify the exclusions list.

Exclusions Configuration File

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

**Important**

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


Exclusions Configuration File Parameters

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

The `Product` parameter defines the configuration file is used by StellarProtect or StellarProtect (Legacy Mode).

TABLE 5-1. Configuration File Sections and Descriptions

SECTION	DESCRIPTION	ADDITIONAL INFORMATION
Configuration	Container for the Configuration section	
Feature	Container for the Feature section	
ApplicationLockDown	Parameters to configure the agent features and functions	StellarProtect and StellarProtect (Legacy Mode) contain slightly different parameter settings. See: Application Lockdown Section for StellarProtect on page 5-9 or Application Lockdown Section for StellarProtect (Legacy Mode) on page 5-10 for more details.
RealTimeScan		Real-Time Scan and Scheduled Scan Section on page 5-15
ScheduleScan		
Obad		Operations Behavior Anomaly Detection Section on page 5-16

SECTION	DESCRIPTION	ADDITIONAL INFORMATION
DeviceControl		Device Control Section on page 5-19
OtApplication		OT Application Safeguard Section for StellarProtect on page 5-19 <hr/>  Note Only StellarProtect supports this function.

Application Lockdown Section for StellarProtect

The following table lists the parameters to configure StellarProtect Application Lockdown exclusions.

TABLE 5-2. StellarProtect Application Lockdown Section Parameters

PARAMETER	SETTINGS	VALUE	DESCRIPTION
ExceptionPathList: Container for the exceptions list			
ExceptionPath	Type	LOCKDOWN_EXCEPTI ON_PATH_TYPE_ECM ASCRIP_T_REGEX	Use the regular expression to specify the file that will be excluded from Application Lockdown monitoring
		LOCKDOWN_EXCEPTI ON_PATH_TYPE_FIL E	Use the file path to specify the file that will be excluded from Application Lockdown monitoring

PARAMETER	SETTINGS	VALUE	DESCRIPTION
		LOCKDOWN_EXCEPTI ON_PATH_TYPE_FOL DER	Use the folder path to specify the files within the folder that will be excluded from Application Lockdown monitoring
	Path	<exception_path>	Files specified by using regular expressions or file/folder paths are treated as lockdown exclusions
TrustedHash: Container for the trusted hash list			
PredefinedTruste dHash	Type	HASH_TYPE_SHA256	File matched by this hash value (SHA-2) is treated as a trusted file
	Hash	<SHA-2_hash_valu e>	SHA-2 hash value of this file
	Note	<note>	Add a note for the file matched by this hash value

Application Lockdown Section for StellarProtect (Legacy Mode)

The following table lists the parameters to configure StellarProtect (Legacy Mode) Application Lockdown exclusions.

TABLE 5-3. StellarProtect (Legacy Mode) Application Lockdown Section Parameters

PARAMETER	SETTINGS	VALUE	DESCRIPTION
ExceptionPathList: Container for the exceptions list			

PARAMETER	SETTINGS	VALUE	DESCRIPTION
ExceptionPath	Type	regex	Use the regular expression to specify the file that will be excluded from Application Lockdown monitoring
		file	Use the file path to specify the file that will be excluded from Application Lockdown monitoring
		folder	Use the folder path to specify the files within the folder that will be excluded from Application Lockdown monitoring
		folderandsub	Use the folder path to specify the files within the folder and its subfolders that will be excluded from Application Lockdown monitoring
	Path	<exception_path>	Files specified by using regular expressions or file/folder paths are treated as lockdown exclusions
TrustedHash: Container for the trusted hash list			

PARAMETER	SETTINGS	VALUE	DESCRIPTION
PredefinedTruste dHash	Type	updater	File matched by this hash value (SHA-1) is treated as a Trusted Update
		lockdown	File matched by this hash value (SHA-1) is not treated as a Trusted Update
	Hash	<SHA-1_hash_valu e>	SHA-1 hash value of this file
	Note	<note>	Add a note for the file matched by this hash value
WriteProtection: Container for the Write Protection section			
ExceptionList: Container for the Write Protection exceptions list			
Exceptionlist	Type	TYPE_FILE	Use the file path to specify the file that can be written by all processes or specific process
		TYPE_FOLDER	Use the folder path to specify the files within the folder that can be written by all processes or specific process
		TYPE_FOLDER_AND_ SUBFOLDER	Use the folder path to specify the files within the folder and its subfolders that can be written by all processes or specific process

PARAMETER	SETTINGS	VALUE	DESCRIPTION
		TYPE_REGKEY	<p>Use the registry key to specify the files within the folder that can be written by all processes or specific process</p> <p>The registry key can be abbreviated or expanded as shown below:</p> <ul style="list-style-type: none"> • HKEY_LOCAL_MACHINE\test • HKEY_CURRENT_CONFIG\test • HKEY_CLASSES_ROOT\test • HKEY_CURRENT_USER\test • HKEY_USERS\test
		TYPE_REGKEY_AND_SUBKEY	<p>Use the registry key and its subkeys to specify the files within the folder and its subfolders that can be written by all processes or specific process</p>

PARAMETER	SETTINGS	VALUE	DESCRIPTION
		TYPE_REGVALUE	Use the registry value to specify the files that can be written by all processes or specific process
	Path	<exception_path>	Use the corresponding path type to specify Write Protection exclusions
	Process	<process_path>	Use the process path to specify specific process that can write the specified file
List: Container for the Write Protection List			
List	Type	TYPE_FILE	Use the file path to specify the file
		TYPE_FOLDER	Use the folder path to specify the file
		TYPE_FOLDER_AND_SUBFOLDER	Use the folder path to specify the files within the folder and its subfolders
		TYPE_REGKEY	Use the registry key to specify the files within the folder
		TYPE_REGKET_AND_SUBKEY	Use the registry key and its subkeys to specify the files within the folder and its subfolders
		TYPE_REGVALUE	Use the registry value to specify the file

PARAMETER	SETTINGS	VALUE	DESCRIPTION
	Path	<path>	Use the corresponding path type to specify Write Protection list

Real-Time Scan and Scheduled Scan Section

The following table lists the parameters to configure StellarProtect or StellarProtect (Legacy Mode) Real-Time Scan exclusions.

TABLE 5-4. Real-Time Scan and Scheduled Scan Section Parameters

PARAMETER	SETTINGS	VALUE	DESCRIPTION
RealTimeScan: Container for the Real-Time Scan exceptions list			
ExceptionPath	Type	EXCLUDE_PATH_TYPE_FOLDER	Use the folder path to specify the files within the folder that will be excluded from Real-Time Scan monitoring
		EXCLUDE_PATH_TYPE_FILE	Use the file path to specify the file that will be excluded from Real-Time Scan monitoring
		EXCLUDE_PATH_TYPE_EXT	Use the file extension to specify the file that will be excluded from Real-Time Scan monitoring
	Path	<exception_path>	Files specified by using file extensions or file/folder paths are treated as real-time scan exclusions
ScheduledScan: Container for the Scheduled Scan exceptions list			



PARAMETER	SETTINGS	VALUE	DESCRIPTION
ExceptionPath	Type	EXCLUDE_PATH_TYP E_FOLDER	Use the folder path to specify the files within the folder that will be excluded from Scheduled Scan monitoring
		EXCLUDE_PATH_TYP E_FILE	Use the file path to specify the file that will be excluded from Scheduled Scan monitoring
		EXCLUDE_PATH_TYP E_EXT	Use the file extension to specify the file that will be excluded from Scheduled Scan monitoring
	Path	<file_path>	Files specified by using file extensions or file/folder paths are treated as scheduled scan exclusions

Operations Behavior Anomaly Detection Section

The following table lists the parameters to configure StellarProtect or StellarProtect (Legacy Mode) Operations Behavior Anomaly Detection exclusions.

TABLE 5-5. Operations Behavior Anomaly Detection Section Parameters

PARAMETER	SETTINGS	VALUE	DESCRIPTION
Obad: Container for the Operations Behavior Anomaly Detection exceptions list			
ScriptOperation: Container for the Policy-based Watchlist settings in Operations Behavior Anomaly Detection			

PARAMETER	SETTINGS	VALUE	DESCRIPTION
AnomalyDetection	Id	<Integer>	<p>Used to specify the list of monitored process or script.</p> <hr/> <p> Note Please do not repeat the same number.</p> <hr/>
	MonitoredProcess	<process_path>	<p>Used to specify commonly-abused applications.</p> <hr/> <p> Note By default, the agent monitors the specific high-risk applications such as Powershell.exe, wscript.exe, cscript.exe, mshta.exe, and psexec.exe.</p> <hr/>

PARAMETER	SETTINGS	VALUE	DESCRIPTION
Account: Container for the Policy-based Approved Login Accounts in Operations Behavior Anomaly Detection			
AccountConfigByPassed	Domain	<domain>	Use to specify the domain from where the user logs in
	User	<user name>	Use to specify the user name of the logged-in user
	IpAddress	<ip address>	Use to specify the IP address from where the user logs in
	LogonType	<logon type>	Use to specify the logon type
	CreatedTime	<timestamp>	The timestamp when the exclusion setting is configured
SystemOperation: Container for the Policy-based Approved Applications in Operations Behavior Anomaly Detection			
SystemOperationConfigByPassed	Path	<file_path>	Use a file or folder path to specify the application that will be excluded from monitoring
		<folder_path>	
	PathType	PATH_TYPE_FOLDER	Use the folder path to specify the files within the folder that will be excluded from monitoring
		PATH_TYPE_FILE	Use the file path to specify the file that will be excluded from monitoring

PARAMETER	SETTINGS	VALUE	DESCRIPTION
	CreatedTime	<timestamp>	The timestamp when the exclusion setting is configured

Device Control Section

The following table lists the parameters to configure StellarProtect or StellarProtect (Legacy Mode) Device Control exclusions.

TABLE 5-6. Device Control Section Parameters

PARAMETER	SETTINGS	VALUE	DESCRIPTION
DeviceControl: Container for the Device Control exceptions list			
TrustedUsbDevice	VendorId	<device vendor ID>	Specify at least one of the device information for USB that will be excluded from monitoring.
	ProductId	<device product ID>	
	SerialNumber	<device serial number>	


OT Application Safeguard Section for StellarProtect

The following table lists the parameters to configure StellarProtect OT Application Safeguard exclusions.

TABLE 5-7. OT Application Safeguard Section Parameters

PARAMETER	SETTINGS	VALUE	DESCRIPTION
OtApplication: Container for the OT Application Safeguard settings			
FilesFolderList: Container for the OT Application Safeguard list			
FilesFolders	ProtectionType	PROTECTION_TYPE_FILE	Use a file or folder path to specify the file(s) to protect
		PROTECTION_TYPE_FOLDER	

PARAMETER	SETTINGS	VALUE	DESCRIPTION
	ProtectionPath	<file_path>	Use the file/folder path to specify the file(s) that will be excluded from monitoring
		<folder_path>	
	Flags	EXECUTABLES_ONLY	By default, StellarProtect will only protect the PE files (.exe and .dll) under the selected folder and its subfolder(s). If you remove the value of the Flags, all files inside the selected folder will be protected.
AuthorizedProcessList: Container for the OT Application Safeguard exceptions list			
AuthorizedProcesses	SubjectType	SUBJECT_TYPE_PROCESS	Use a full path to specify specific process that can modify the protected OT applications

PARAMETER	SETTINGS	VALUE	DESCRIPTION
	SubjectPath	<process_path>	<p>Used to specify an authorized process that can modify the protected OT applications.</p> <hr/> <p> Important By adding the authorized process, you may set other applications to be trusted and change the protected files/folders previously defined as well as the PE files for OT applications detected by agents.</p>

Import Exclusions

You can remotely apply new exclusions list to the selected agents from StellarOne. This feature allows you to remotely overwrite the exclusions list of the target agents/group.

Remember to prepare an exclusions list before you start the import:

1. Export and download an exclusions list.
2. Customize the downloaded file if needed.



Procedure


1. Navigate to the target agent or group, and then go to its **Policy** page. For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.
2. Mouse over the **Policy** tab and a downward arrow appears.
3. Click the arrow and a drop-down menu appears.
4. Select **Import Exclusions**.
5. A pop-up window appears. Click **Select File**.

**Note**

The imported file will overwrite only the customized exclusions. The exclusions inherited from the parent group will not be overwritten.

6. Select the file to import and click **Import**.
7. The **View Import Result** window appears indicating the result of importing the exclusions list. The following table describes the status icons:

ICON	DESCRIPTION
	Successfully overwrote the corresponding exclusions of the target agents/group.
	Failed to overwrite the corresponding exclusions of the target agents/group.

ICON	DESCRIPTION
	Unable to overwrite the corresponding exclusions of the target agents/group because they are inherited exclusions, which cannot be overwritten.

Agent View and Policy Settings

The agent view provides three tab pages at the agent level, including:

- **General Info:** Displays the system information, scan components, applied policy settings (Legacy Mode only), and installed path/hotfix (Legacy Mode only).
- **Policy:** Provides the configuration page for policy settings. See [Agent Policy Settings on page 5-27](#) for more details.
- **Situational Awareness:** Displays the agent baseline established during the learning period set from the **Operations Behavior Anomaly Detection**. See [Situational Awareness on page 5-95](#) for more details.

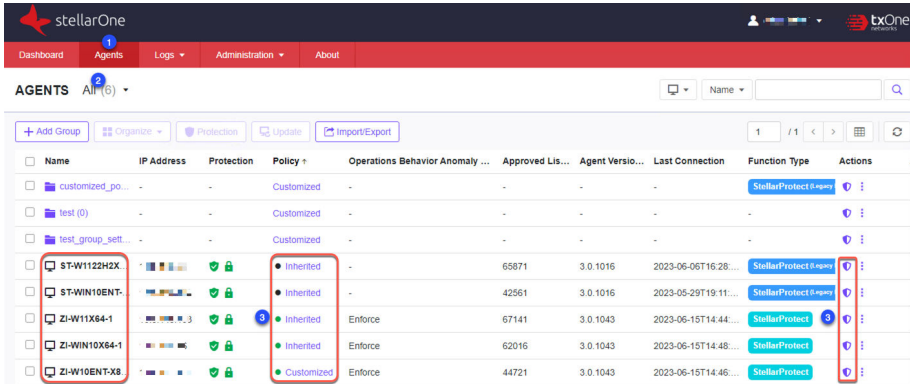
Topics in this chapter include:

- [Go to the Agent View on page 5-23](#)
- [Agent Policy Settings on page 5-27](#)
- [Situational Awareness on page 5-95](#)


Go to the Agent View

Go to a specific agent view to check the agent details or configure the agent policy settings.

Follow the instructions below to go to the agent view.



Procedure

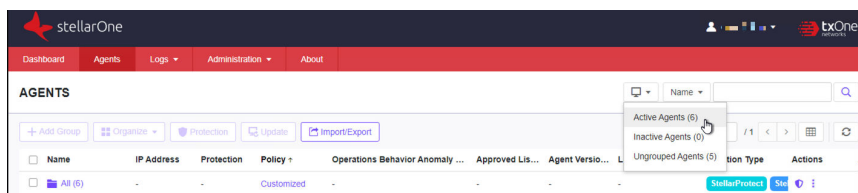
1. Click the **Agents** tab in the top navigation bar of the StellarOne web console.
2. Click the **All** group, and then a screen displays the second level of groups/agents managed by StellarOne.
3. Navigate to the target agent.
 - To view the agent policy settings, click the link (**Inherited**, **Customized**, or **Self-managed**) in the **Policy Inheritance** column. The **Policy** tab page appears.
 - To view the agent inherited information, click the  Policy icon in the **Actions** column. The **General Info** tab page appears.
4. You can switch between the **General Info**, **Policy**, or **Situational Awareness** tab pages as needed.
5. See *Settings for the Agent/Group Policy Screen on page 5-2* for more information.

Finding the Target Agent

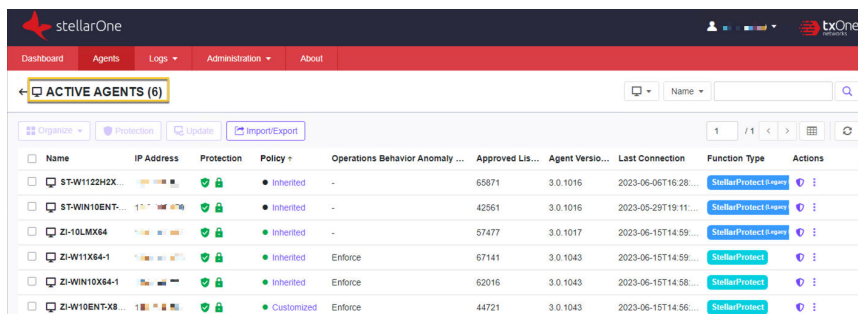
You can use the filter tool provided on the **Agents** screen to list all the **Active Agents**, and then do an advanced search to quickly find the target agent for checking its details or policy configuration.

Procedure

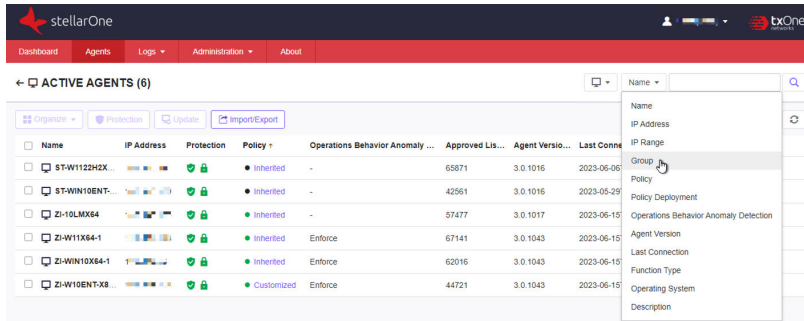
1. On the **Agents** screen, click the  icon and select the **Active Agents**.



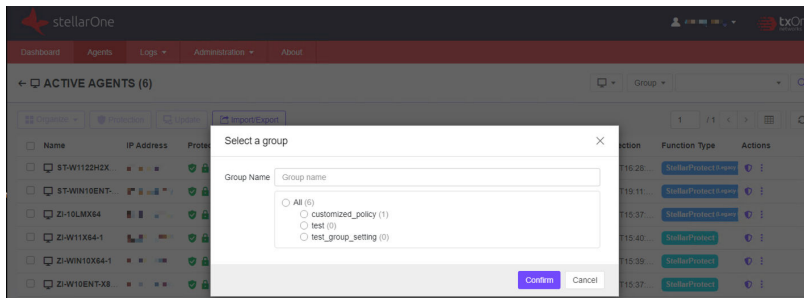
2. The screen displays all the active agents.



3. Click the filter dialog box for an advanced search. You'll need to type directly in the search box or choose from the filter menu depending on the selected filter option.
4. See below as an example of how to find a specific agent in the specified group.
 - a. Select **Group** from the filter menu.



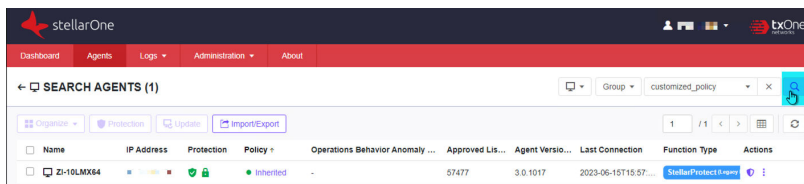
b. Click the filter menu and a **Select a group** window appears.




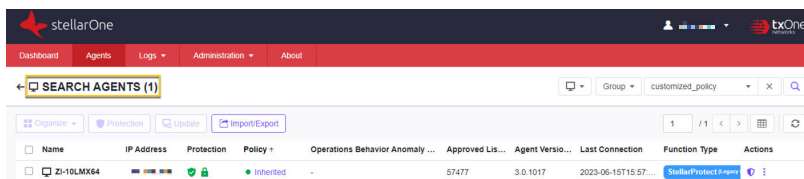
c. Click the radio button next to the target group or type the group name in the **Group Name** text field.

d. Click **Confirm**.

e. Click the search icon.



- f. The screen displays the target agent. Click the link in the **Policy** column or  icon in the **Actions** column for checking the agent details or policy configuration.



Agent Policy Settings

This section introduces the configuration page for policy settings at the agent level.

Topics in this section include:

- [Operations Behavior Anomaly Detection on page 5-27](#)
- [Other Key Features for StellarProtect on page 5-49](#)
- [Other Key Features for StellarProtect \(Legacy Mode\) on page 5-67](#)
- [Common Policy Settings for StellarProtect/StellarProtect \(Legacy Mode\) on page 5-84](#)

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 feature 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's exclusive industrial application repository and ransomware detection engine.

Navigate to the target agent or group, and then go to its **Policy** page. For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

Scroll down and find the **Operations Behavior Anomaly Detection** pane.

Operations Behavior Anomaly Detection NEW ⓘ

- Learn: Collect behavioral patterns from the monitored agent-devices to establish baseline fingerprints
- Detect: Identify and send 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 ⓘ
- Enforce: Take preventative action on detected fingerprint deviations to defend operation stability and security
- Disable

[> Learn more](#)

⚠ All agent-devices must start with the "Learn" mode to establish their own baseline fingerprints before entering the "Detect" or "Enforce" mode. The agents (e.g. newly-added agents) will learn first and then automatically switch to the specified mode according to the policy.

Learning time: 7 Days

- Script Based: Protect the endpoints against script-based or fileless attacks.
- User Login: Defend the endpoints against credential-based attacks.
- Application Behavior: Keep the endpoints secure against malicious application attacks.

FIGURE 5-3. Operations Behavior Anomaly Detection

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

Four Normal Modes:

- **Learn:** In this mode, the agents collect behavioral patterns from the monitored devices to establish baseline fingerprints.



Important

TXOne Networks recommends setting 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. See [Use Case on page 5-39](#) for more details.

- **Detect:** In this mode, the agents identify and send alerts for any unexpected changes or 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, the agents take 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.

Learning time:

When **Detect** or **Enforce** mode is selected, the **Learning time** option becomes available. You can specify the learning period for the target agents/group from the **Learning time** menu. The agents that have not established their own baselines will then start learning and once the learning period ends, they will automatically switch to the predefined **Detect** or **Enforce** mode.

See [Setting the Learning Time on page 5-34](#) and [Setting the Learning Time - Use Case on page 5-35](#) for more information.

Three Pillars of Protection:

- **Script Behavior:** Protects the endpoints against script-based 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.
 - **Approved Script Behaviors in Baseline:** Click this link to go to the **Situational Awareness** page for viewing the approved script behaviors and relevant details stored in the baseline at the agent level. See [Approved Applications on page 5-99](#) for more information.
 - **Policy-based Watchlist:** Click this link to manually add commonly-abused applications used in operations and processes to the Monitored Application list for strengthening security monitoring. See [Policy-based Watchlist on page 5-36](#) for more information.
- **User Login:** Defends the endpoints against credential-based attacks when enabled. By comparing the list of user accounts and login activities in the baseline with those used for daily operations, unrecognized user accounts or unexpected login activities will be detected as anomalies and trigger events.

- **Approved Login Accounts in Baseline:** Click this link to go to the **Situational Awareness** page for viewing the approved user accounts and relevant details stored in the baseline at the agent level. See [Approved Login Accounts on page 5-98](#) for more information
- **Policy-based Approved Login Accounts:** Click this link to manually add approved user accounts and relevant details used in operations and processes to avoid false alerts. See [Policy-based Approved Login Accounts on page 5-37](#) for more information.
- **Application Behavior:** Safeguards the endpoints against malicious application attacks. By comparing the list of applications and application behaviors in the baseline with those running for daily operations, unrecognized applications or unexpected application behaviors will be detected as anomalies and trigger incident notifications.
- **Suspicious Objects Blocklist:** Click this link to view the applications that have been added to the Suspicious Objects Blocklist, which will be blocked from running on the endpoint unless removed from the blocklist.

**Note**

The **Suspicious Objects Blocklist** appears only when **Operations Behavior Anomaly Detection** is set to **Enforce** mode.

- **Approved Applications in Baseline:** Click this link to go to the **Situational Awareness** page for viewing the approved applications and relevant details stored in the baseline at the agent level. See [Approved Applications on page 5-99](#) for more information.
- **Policy-based Approved Applications:** Click this link to manually add approved applications and relevant details used in operations and processes to avoid false alerts. See [Policy-based Approved Applications on page 5-38](#) for more information.

The three pillars of protection can be individually toggled on for guarding separate vulnerability points, or you can choose to enable them all and set in the **Strict mode** for maximum defense.


**Note**

For more details on how the **Strict mode** works for the three pillars, see [Strict Mode on page 5-41](#) and [Strict Mode - Use Case on page 5-44](#).

The following table illustrates how the three pillars work in the **Learn**, **Detect**, and **Enforce** modes.

TABLE 5-8. An example of how Operations Behavior Anomaly Detection works

OPERATIONS BEHAVIOR ANOMALY DETECTION	SCRIPT BEHAVIORS	USER LOGIN	APPLICATION BEHAVIOR
Learn	Stores the approved script behavior listed below in the baseline: For example: explorer.exe→cmd.exe→ (monitored process or script)	Stores the login account listed below in the baseline: For example: • Username: admin • Domain: TXOne	Stores the application behavior listed below in the baseline: For example: • Application: Google Chrome • Behavior: 1
Detect	Sends alerts for the unexpected change: For example: cmd.exe → explorer.exe→ (monitored process or script)	Sends alerts for the unexpected change: For example: Username: admin1	Sends alerts for the unexpected changes: For example: Behavior: 2

OPERATIONS BEHAVIOR ANOMALY DETECTION	SCRIPT BEHAVIORS	USER LOGIN	APPLICATION BEHAVIOR
<p>Enforce</p>	<ul style="list-style-type: none"> • Sends alerts for the unexpected changes • Automatically blocks the unexpected changes <p>For example:</p> <p>cmd.exe → explorer.exe → (monitored process or script)</p>	<p>Sends alerts for the unexpected change:</p> <p>For example:</p> <p>Username: admin1</p>	<ul style="list-style-type: none"> • Sends alerts for the unexpected changes • Provides the action that allows users to manually add detected applications to the Suspicious Objects Blocklist from the generated events <p>For example:</p> <p>Behavior: 2</p> <hr/> <p> Note See Add to Suspicious Objects Blocklist on page 6-7 for how to add the applications to the Suspicious Objects Blocklist</p>

Setting the Learning Time

When the **Detect** or **Enforce** mode of **Operations Behavior Anomaly Detection** is selected, the **Learning time** option becomes available. You can specify the learning period for the target agents/group from the **Learning time** menu. The agents that have not established their own baselines will then start learning and once the learning period ends, they will automatically switch to the predefined **Detect** or **Enforce** mode.

See the following instructions for how to set the learning time.

Procedure

1. Go to **Agents > Policy**, scroll down and find the **Operations Behavior Anomaly Detection** pane. Select **Detect** or **Enforce**.
2. The **Learning time** section appears.
3. Scroll down and determine which security pillars (**Script Behavior**, **User Login**, or **Application Behavior**) you want to enable. Ensure you toggle on at least one of them for the agent-device to establish the associated baseline.



Note

The three security pillars can be individually toggled on for guarding separate vulnerability points, or you can choose to enable them all for the complete protection.

-
4. Specify the learning period for the target agent-device from the **Learning time** menu.
 5. A progress bar displaying how many days left for learning will appear on the **Agents** screen or the **General Info** page for the agent-device. See [About the Agents Screen on page 4-2](#) for more information.

**Note**

- The learning time counts only when the target agent-device is powered on.
 - If you toggle on the security pillars separately, though the learning period is specified and fixed, the actual learning time displayed on the progress bar varies depending on when the last pillar is enabled. Besides, the agent switches to the predefined **Detect** or **Enforce** mode for the security pillars separately. See the following use case for more details.
-

Setting the Learning Time - Use Case

See the example below for how the learning time works if the security pillars are enabled separately.

Procedure

1. Three days ago, you've enabled the **Detect** mode for **Operations Behavior Anomaly Detection**, toggled on the **Script Behavior**, and set the **Learning time** to 3 days.
2. This morning, you enabled the **User Login** and then the agent started establishing the baseline of the approved login accounts.
3. If you had not enabled the **User Login** today, the learning progress bar displayed on the **Agents** screen should have disappeared and the status should have changed to **Detect**. However, the progress bar still exists because you enabled the **User Login** today (without changing the learning period, which was set to 3 days).
4. For now, the agent is multitasking for the **Operations Behavior Anomaly Detection** function:
 - The **Script Behavior** baseline has been established and the agent is actually detecting any anomalies now. You may find relevant events on the [Agent Events](#).

- The agent is now establishing the **User Login** baseline. The learning progress bar on the **Agents** screen indicates there are 3 days left for learning before entering the **Detect** mode.
5. Moreover, if you changed the learning time to 7 days while enabling the **User Login** today, the agent would start updating the baseline for **Script Behavior**; on the other hand, it would start establishing the baseline for **User Login**. To elaborate, since the agent has already collected the script behaviors for 3 days, the actual learning time for **Script Behavior** was extended to 4 days only. As for the **User Login**, the actual learning time was set to 7 days.
-

Policy-based Watchlist and Approved Items

You can specify policy-based watchlist for monitoring fileless attacks, or policy-based approved login accounts or applications to avoid false alerts at the agent or group level.

Related settings include:

- [Policy-based Watchlist on page 5-36](#)
- [Policy-based Approved Login Accounts on page 5-37](#)
- [Policy-based Approved Applications on page 5-38](#)

Policy-based Watchlist

By default, Stellar agents monitor Powershell.exe, wscript.exe, cscript.exe, mshta.exe, and psexec.exe when the **Operations Behavior Anomaly Detection "Detect" or "Enforce"** mode is enabled with the **Script Behavior** toggled on. In addition to the default monitored applications, you can also manually add commonly-abused applications used in operations and processes to the **Policy-based Watchlist** for strengthening security monitoring.

See the following instructions for how to add applications to the **Policy-based Watchlist**.

Procedure

1. Go to **Agents > Policy**, scroll down and find the **Operations Behavior Anomaly Detection** pane. Select **Operations Behavior Anomaly Detection Learn, Detect, or Enforce**.
2. Toggle on the **Script Behavior**.
3. Click **Script Behavior** to expand this section.
4. Find and click the **Policy-based Watchlist**.
5. Click **+Add** and then specify the application to be monitored.
6. Click **Add** and the added application appears in the **Monitored Application** list.
7. Click **Close** to close the window.



Tip

To delete the added application one by one, click the Delete icon in the **Actions** column; to delete multiple applications, click the checkboxes next to them and then click **Delete > Confirm**.

Policy-based Approved Login Accounts

You can manually add approved user accounts and relevant details used in operations and processes into the **Policy-based Approved Login Accounts** to avoid false alerts.

See the following instructions for how to add the approved user accounts to the **Policy-based Approved Login Accounts**.

Procedure

1. Go to **Agents > Policy**, scroll down and find the **Operations Behavior Anomaly Detection** pane. Select **Operations Behavior Anomaly Detection Learn, Detect, or Enforce**.
2. Toggle on the **User Login**.

3. Click **User Login** to expand this section.
4. Find and click the **Policy-based Approved Login Accounts**.
5. Click **+Add** and then specify the user account and relevant information.
6. Click **Add** to add the approved user account.
7. Click **Close** to close the window.

**Tip**

To delete the added user accounts one by one, click the Delete icon in the **Actions** column; to delete multiple user accounts, click the checkboxes next to them and then click **Delete > Confirm**.

Policy-based Approved Applications

You can manually add approved applications used in operations and processes into the **Policy-based Approved Applications** to avoid false alerts.

See the following instructions for how to add the approved applications to the **Policy-based Approved Applications**.

Procedure

1. Go to **Agents > Policy**, scroll down and find the **Operations Behavior Anomaly Detection** pane. Select **Operations Behavior Anomaly Detection Learn, Detect, or Enforce**.
2. Toggle on the **Application Behavior**.
3. Click **Application Behavior** to expand this section.
4. Find and click the **Policy-based Approved Applications**.
5. Click **+Add** and then specify the path to the application and relevant information.
6. Click **Add** to add the approved application.
7. Click **Close** to close the window.

**Tip**

To delete the added applications one by one, click the Delete icon in the **Actions** column; to delete multiple user accounts, click the checkboxes next to them and then click **Delete > Confirm**.

Use Case

The **Operations Behavior Anomaly Detection** embodies the CPSDR concept and has a deep understanding of what the expected behaviors for each device are from learning the behaviors of each agent-device first. Every agent continuously analyzes its host device to establish and maintain a unique baseline fingerprint. Then in real-time, unexpected behaviors and deviations from this fingerprint can be detected at the individual agent level and then secondarily at the centralized control level to inform wider instability issues and prompt preventative actions.

See the following procedures as the recommended practice when you start using the **Operations Behavior Anomaly Detection**:

Procedure

1. Toggle on the **Learn** mode of the **Operations Behavior Anomaly Detection** on the Policy page. Ensure that you toggle on the **Script Behaviors**, **User Login**, and **Application Behavior** as well.
 2. Deploy all the required configuration, features, updates, or fixes, and run all the daily operation processes during the **Learn** mode.
-

**Note**

If the Application Lockdown is enabled, ensure you turn on the maintenance mode when performing these deployments.

- a. Toggle on the **User Login**:
 1. Use the required user accounts to log into the agent-device.

2. Ensure you also log in from different IP addresses or domains if it is required during your daily operation processes.

**Note**

You can also manually add approved user accounts and relevant details used in the operations and processes into the **Policy-based Approved Login Accounts**.

- b. Toggle on the **Application Behaviors**:

- Run the applications required for daily operation processes.
- Download required applications or execute updates or fixes required for existing applications on the agent-device.

**Note**

You can also manually add approved applications used in the operations and processes into the **Policy-based Approved Applications**.

- c. Toggle on the **Script Behavior**:

- Run the scripts required for your daily operation processes.
- Run the scripts accompanied with parameters.

**Note**

By default, StellarProtect monitors the commonly-abused script running applications such as `Powershell.exe`, `wscript.exe`, `cscript.exe`, `mshta.exe`, and `psexec.exe`. Ensure you manually add other commonly-abused applications used in your daily operation processes to the **Policy-based Watchlist** for strengthening security monitoring.

3. After all the operation processes have been executed and learned, switch to the **Detect** mode and check if any events will be triggered by the normal daily operations.

**Note**

- You can check the Agent event logs to see if there's any anomalous operation or process detected. See [Agent Events on page 6-2](#) for more details.
 - See [Strict Mode on page 5-41](#) and [Strict Mode - Use Case on page 5-44](#) for more details on using the **Strict mode**.
-

4. Switch to the **Enforce** mode for activating preventative actions (Script Behaviors only). If any unexpected script execution occurs, it should be blocked.
-

**Note**

If you also enable the **Strict mode**, only the exact script running processes (with exact parameters) that have been learned and stored in the baseline will be allowed. You can check the **Situational Awareness > Script Behaviors** page to make sure the specific full operation processes (parameters included) have been added in the agent baseline.

Strict Mode

The **Strict mode** under the **Detect** or **Enforce** mode is used for stronger threat protection. Enabling **Strict mode** reduces the level of baseline fingerprint deviation allowed; in other words, it performs stricter comparison between the established baseline and currently-running operational behaviors.

**Note**

In more dynamic processes where devices and access behaviors are more subject to change, this may generate more events. See [Strict Mode - Use Case on page 5-44](#) for information.

To enable **Strict mode**, set the **Operations Behavior Anomaly Detection** to **Detect** or **Enforce** mode, and then toggle on specific pillars of protection for

guarding separate vulnerability points or simply enable them all for maximum defense.

See below for more details on how the three pillars work in **Strict mode**.

Script Behaviors: In the **Strict mode**, the operation process and the monitored process or script must exactly match the approved full operation process stored in the baseline; otherwise, events will be generated or the process will be blocked.

See below as an example of how the **Strict mode** works for the **Script Behaviors**.

1. When you select the **Learn** mode under the **Operations Behavior Anomaly Detection**, the following full operation process is learned:
 - explorer.exe → cmd.exe → powershell.exe → script.ps1
2. When you switch to the **Detect** or **Enforce** mode without turning on the **Strict Mode**, StellarProtect will not block recognized program calls with unidentified script; the following process is allowed:
 - explorer.exe → cmd.exe → powershell.exe → NEWscript.ps1

**Note**

The NEWscript.ps1 does not count as an unrecognized script in the process when the **Strict Mode** is turned off.

3. When the **Strict Mode** is turned on, no matter it's under the **Detect** or **Enforce** mode, the following process is not allowed:
 - explorer.exe → cmd.exe → powershell.exe → NEWscript.ps1

**Note**

The NEWscript.ps1 is detected as an unrecognized script that will trigger alerts or be blocked when **Strict Mode** is enabled.

4. In conclusion, when **Strict Mode** is turned on, only the exact process (the process learned in *Step 1*) is allowed:

- explorer.exe → cmd.exe → powershell.exe → script.ps1

TABLE 5-9. Example: Script Behaviors - Strict Mode ON/OFF

	SCRIPT BEHAVIORS			OPERATIONS BEHAVIOR ANOMALY DETECTION			
	APPROVED OPERATION	MONITORED PROCESS		DETECT	ENFORCE	DETECT	ENFORCE
		MONITORED APPLICATION	SCRIPT	STRICT MODE: OFF		STRICT MODE: ON	
Process learned and stored in the baseline	explorer.exe→cmd.exe→	powershell.exe→	script.ps1	Allowed			
Operation process changed	cmd.exe→explorer.exe→	powershell.exe→	script.ps1	Events	Blocked	Events	Blocked
Monitored application changed	explorer.exe→cmd.exe→	cscript.exe →	script.ps1	Events	Blocked	Events	Blocked
Script changed	explorer.exe→cmd.exe→	powershell.exe→	NEWscript.ps1	Allowed		Events	Blocked

User Login: In the **Strict mode**, the user accounts and the login activities must exactly match the approved user accounts stored in the baseline; otherwise, events will be generated.

Application Behavior: In the **Strict mode**, the application behaviors must exactly match the approved application behaviors stored in the baseline; otherwise, events will be generated.

See [Strict Mode - Use Case on page 5-44](#) for the description of how you can use the **Strict mode** to maximize its effectiveness.

Strict Mode - Use Case

As **Strict mode** performs stricter comparison between the established baseline and currently-running operational behaviors, it does not allow too much deviations from the baseline and thus may be more appropriate to be used for static environments that is intended to remain unchanged by users and administrators. For example, it may be a shared deployment environment with permanent infrastructure, where all the features and fixes are deployed once at the end of a planned release cycle.

Facing the growing prevalence of script-based attacks such as fileless malware or PowerShell abuse, the behavioral pattern identification along with parameter recognition for defending unknown threats adds an extra layer of protection without impacting the operational stability.

To illustrate: the global policy may restrict the use of PowerShell. However, one device uses PowerShell for regular system updates and there is a specific command run to complete the process. The agent for this device can allow PowerShell to be used for this specific process. No individual policy override is needed, and any other use of PowerShell on other devices will still be blocked.

See the following procedures as the recommended practice:

1. Organize the agents in the static environment as a group and set the **Operations Behavior Anomaly Detection "Learn"** mode as one of the group policy settings. Ensure that you toggle on the **Script Behaviors**.
2. Deploy all the required configuration, features, updates, or fixes, and run all the daily operation processes during the learning period.



Note

If the Application Lockdown is enabled, ensure you turn on the maintenance mode when performing the deployments.

3. For the specific agent-device that uses PowerShell as the regular system update tool, check the **Situational Awareness > Approved Script**

Behaviors page to make sure the specific full operation process with parameter identification has been included in the agent baseline.

4. After all the operation processes have been executed and learned, switch to the **Detect** mode and check if any events will be triggered by the normal daily operations. When you run the PowerShell command on the specific agent and other agent-devices in the same group; one should treat it as a normal behavior and the other ones should treat it as anomalies and trigger events.

**Note**

You can check the Agent event logs to see if there's any anomalous operation or process detected. See [Agent Events on page 6-2](#) for more details.

5. Switch to the **Enforce** mode and enable the **Strict mode** for activating preventative actions. For most of the devices, the use of PowerShell should be blocked; for the specific device, only the exact process for running the PowerShell that have been learned and stored in the baseline will be allowed.

Migration/Upgrade from Previous Version - Use Case

For StellarOne migrated or upgraded from previous versions to 3.0, see the following use case.

**Note**

After you migrate or upgrade StellarOne to version 3.0, please also upgrade the managed agents to the latest version. Though StellarOne provides backward compatibility to support agents with earlier version, new features or enhanced functionality should not be applicable on some agents with earlier versions.

1. If the original policy setting of the **Operations Behavior Anomaly Detection** was set to the **Detect** or **Enforce** mode, after migrated or

upgraded to version 3.0, the StellarOne would retain the previous setting and the **Script Behavior** toggle would be automatically turned on.

2. After then, if you enable the **User Login** or **Application Behavior**, the agent automatically starts learning by collecting the related behavioral patterns performed on the device to establish its baseline fingerprint for **User Login** or **Application Behavior**.



Note

The learning of the **User Login** or **Application Behavior** does not change the original policy setting of the **Operations Behavior Anomaly Detection**.

3. In the **Operations Behavior Anomaly Detection** pane, find and set the **Learning time**.

Operations Behavior Anomaly Detection NEW

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

Strict mode (i)
 Disable

⚠ All agent-devices must start with the "Learn" mode to establish their own baseline fingerprints before entering the "Detect" or "Enforce" mode. The agents (e.g. newly-added agents) will learn first and then automatically switch to the specified mode according to the policy.

Learning time 1 Day

1 Day
 1 Day
 3 Days
 7 Days
 14 Days

Script Based [Toggle]
 Protect the endpoints against script-based or fileless attacks.

User Login [Toggle]
 Defend the endpoints against credential-based attacks.

Application Behavior [Toggle]
 Keep the endpoints secure against malicious application attacks.



Note

- See the [Use Case on page 5-39](#) for the recommended practice as you start using the **Operations Behavior Anomaly Detection** and evaluate the proper learning period for the agent-device.
- The learning time counts only when the agent-device is powered on.

4. Go to the **Agents** screen. You can find the the learning progress bar displayed in the **Operations Behavior Anomaly Detection** column for the agent-device. Mouse over the progress bar to check how many days

left for learning. See [About the Agents Screen on page 4-2](#) for more information.



Note

In addition to the progress bar displayed on the **Agents** screen, you can also check the learning progress on the **General Info** page for the agent-device.

5. After learning, the agent-device will automatically switch to the specified mode according to the original policy settings.

Sizing Table - 2nd Disk Space Requirement

The StellarOne requires an external disk for storing system configurations and event logs. To ensure the storage requirement for the agent baselines is fulfilled, see the following table for the required external disk space depending on the number of the installed agents and for executing the **Operations Behavior Anomaly Detection** feature.

TABLE 5-10. Sizing Table - 2nd Disk Space Requirement for Operations Behavior Anomaly Detection

MAX. NO. OF AGENTS	MIN NO. OF vCORES	MEMORY SIZE	1ST HDD SPACE	2ND HDD SPACE (RECOMMENDED)*
30,000	10	32 GB	25 GB	500 GB
20,000	8	16 GB		400 GB
15,000	8	16 GB		300 GB
10,000	8	16 GB		200 GB
5,000	8	16 GB		150 GB
1,000	4	16 GB		100 GB
500	4	12 GB		100 GB

**Note**

According to the table, If you want to deploy 25,000 agents and run **Operations Behavior Anomaly Detection**, you'll need to prepare a 2nd HDD of 500 GB capacity.

Other Key Features for StellarProtect

Other key features provided by StellarProtect agent include:

- [Application Lockdown on page 5-49](#)
- [Multi-Method Threat Prevention on page 5-57](#)
- [OT Application Safeguard on page 5-64](#)
- [DLL Injection Prevention on page 5-66](#)

See [Comman Policy Settings for StellarProtect/StellarProtect \(Legacy Mode\) on page 5-84](#) for how to configure Agent Component Update Schedule, Device Control, User-Defined Suspicious Objects, Agent Password, Agent Patch deployment, and Trusted Certificate Settings for StellarProtect agent.

Application Lockdown

When Application Lockdown is turned on, the agent will only be able to access applications that are in the Approved List.

Procedure

1. Go to **Agents > All**.
2. Navigate to the target agent or group, and then go to its **Policy** page.

**Note**

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

3. Go to the **Application Lockdown** pane.

4. Three modes are available for selection:
- **Detect:** When an application not in the Approved List launches, it is allowed and users will receive a notification.
 - **Enforce:** When an application not in the Approved List launches, it is blocked and users will receive a notification.
 - **Disable:** Application Lockdown is turned off.

**Note**

- For how to configure exclusion settings for the Approved List, see [Excluded Paths Settings on page 5-50](#) and [Trusted Hash Values Settings on page 5-52](#).
- For how to configure trusted hash values settings for the Approved List, see [Trusted Hash Values Settings on page 5-52](#).

-
5. If you enable the "Detect" mode or "Enforce" mode, the sub-features listed below will appear. By default, the sub-features are enabled. Click the toggles to disable them if needed.
- **DLL/Driver Lockdown:** Prevents unapproved DLLs or drivers from being loaded into the memory of protected endpoints.
 - **Script Lockdown:** Prevents unapproved script files from being run on protected endpoints.
 - **Intelligent Runtime Learning:** Allows runtime executable files that are generated by applications in the Approved List.

Excluded Paths Settings

When **Application Lockdown** is enabled, the Agent will only be able to access applications that are in the Approved List. However, the **Excluded Paths** allows you to configure lockdown exclusion settings for the Approved List.

Procedure

1. Go to **Agents > All**.
2. Navigate to the target agent or group, and then go to its **Policy** page.

**Note**

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

3. Find and click the **Excluded Paths** at the bottom of the **Application Lockdown** pane.
 - For adding exception paths:
 - a. Click the **+Add** button, and then a pop-up window appears.
 - b. Select among **File**, **Folder**, or **Regular Expression** and input the required information in the corresponding text field.

**Note**

The **Excluded Paths** function supports only the real path and hardlink path.

- c. Click **Add** to complete adding the exception paths for the Approved List.
- For editing existing exception paths:
 - a. Find the exception path to be edited and click the corresponding Edit icon under the **Actions** header.
 - b. A pop-up window appears. Select among **Folder**, **File**, or **Regular Expression** and edit in the corresponding text field.
 - c. Click **Save** to complete editing the exception paths for the Approved List.
 - For deleting multiple existing exception paths:

- a. Click the checkboxes next to the existing exception paths.
 - b. Click the **Delete** button next to the **+Add** button.
 - c. A warning message window appears. Click **Confirm** to delete the selected items.
- For deleting single existing exception path:
 - a. Find the exception path to be deleted and click the corresponding Delete icon in the **Actions** column.
 - b. A warning message window appears. Click **Confirm** to delete the selected item.
-

Trusted Hash Values Settings

When **Application Lockdown** is enabled, the Agent will only be able to access applications that are in the Approved List. However, the **Trusted Hash Values** allows you to configure trusted hash values for the Approved List.

Calculate Hash Values

Use **File Hash Generator** to calculate hash values before adding trusted hash values.

Procedure

1. Go to **Agents > All**.
 2. Navigate to the target agent or group, and then go to its **Policy** page.
-



Note

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

3. Find and click the **Trusted Hash Values** at the bottom of the **Application Lockdown** pane.

4. The **Trusted Hash Values** windows appears. Find and click **File Hash Generator** to download the tool.
5. Execute `WKFileHashGen.exe` from the downloaded folder. The **File Hash Generator** screen will appear.
6. Use any of the following methods to select files and calculate hash values:
 - Drag and drop folders or files to the **File Hash Generator** screen.
 - Click the drop-down button and click **Add Files** to select the files to add.
 - Click the drop-down button and click **Add Folder** to add all the files in the selected folder.

**Tip**

Only executable, script, and installer files are supported. Mouse over the **Supported file types** for more details.

**Note**

Hash values will appear in the SHA-1 and SHA-256 columns.

7. For a single file, right-click the item and select **Copy SHA-1** or **Copy SHA-256**. For multiple files, click **Export All** to generate a list of hash values

**Note**

- To ensure that all necessary files are calculated for hash values, it is advisable to add the root folder of the target application(s) to the **File Hash Generator** for calculation.
 - By clicking the **Add Folder** button, only the installer files, script files, and files in the PE (Portable Executable) format will be calculated.
 - For the single hash value, see [Add Trusted Hash Values on page 5-54](#) for how to add the copied hash value to the trusted hash value list.
 - For multiple hash values, see [Import Trusted Hash Values on page 5-55](#) for how to import the file containing the hash values to the trusted hash value list.
-

8. Click **Exit** to close the tool.
-

Add Trusted Hash Values

Procedure

1. Go to **Agents > All**.
 2. Navigate to the target agent or group, and then go to its **Policy** page.
-

**Note**

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

3. Find and click the **Trusted Hash Values** at the bottom of the **Application Lockdown** pane.
 4. Click the **Add** button and fill in the hash values and notes.
-

Import Trusted Hash Values

Procedure

1. Go to **Agents > All**.
2. Navigate to the target agent or group, and then go to its **Policy** page.

**Note**

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

3. Find and click the **Trusted Hash Values** at the bottom of the **Application Lockdown** pane.
4. Click the **Import** button to import the .txt file containing a batch of hash values.

**Note**

See [Calculate Hash Values on page 5-70](#) for generating the file containing the list of multiple hash values

Edit Trusted Hash Values

Procedure

1. Go to **Agents > All**.
2. Navigate to the target agent or group, and then go to its **Policy** page.

**Note**

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

3. Find and click the **Trusted Hash Values** at the bottom of the **Application Lockdown** pane.
 4. Find the trusted hash value to be edited and click the corresponding Edit icon in the **Actions** column.
 5. The **Edit Trusted Hash Value** dialog window appears.
 6. After modification, click the **Save** button to complete the settings.
-

Remove Trusted Hash Values

Procedure

1. Go to **Agents > All**.
2. Navigate to the target agent or group, and then go to its **Policy** page.



Note

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

3. Find and click the **Trusted Hash Values** at the bottom of the **Application Lockdown** pane.
4. To delete multiple existing trusted hash values:
 - a. Click the checkboxes next to the existing trusted hash values.
 - b. Click the **Delete** button next to the **Import** button.
 - c. A warning message window appears. Click **Confirm** to delete the selected items.
5. To delete single existing trusted hash values:
 - a. Find the trusted hash value to be deleted and click the corresponding Delete icon in the **Actions** column.

- b. A warning message window appears. Click **Confirm** to delete the selected item.
-

Multi-Method Threat Prevention

The Multi-Method Threat Prevention provides advanced threat scan to secure the endpoints without interrupting the endpoints's operations via machine learning and ICS root of trust. Related settings include:

- [Real-Time Scan on page 5-57](#)
- [Scheduled Scan on page 5-58](#)
- [Advanced Settings on page 5-60](#)

Real-Time Scan

Real-Time Scan provides persistent and ongoing file scan for the endpoints. Each time a file is received, opened, downloaded, copied, or modified, **Real-Time Scan** always scans the file for security assessment. After performing the **Real-Time Scan**, users can proceed to access the file if it does not pose a security threat. However, if a security risk or possible virus/malware has been detected during the scanning, associated events indicating the name of the infected file and the specific security risk will be generated for further investigation.

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.

Procedure

1. Go to **Agents > All**.
2. Navigate to the target agent or group, and then go to its **Policy** page.

**Note**

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

3. Go to the **Real-Time Scan** section in the **Multi-Method Threat Prevention** pane.
 4. Toggle on the **Real-Time Scan**.
-

**Note**

See [Advanced Settings on page 5-60](#) for instructions on how to configure the types of the files to be scanned, the action to take after possible security risk is detected, and the scan exclusion list.

Predictive Machine Learning

The **Predictive Machine Learning** uses intelligent machine learning technology to correlate threat information and perform an in-depth file analysis for emerging unknown security risk detection through digital DNA fingerprinting, API mapping, and other file properties. **Predictive Machine Learning** also performs a behavioral analysis on unknown or low-prevalence processes to determine if an emerging or unknown threat is attempting to infect your network. **Predictive Machine Learning** is a powerful tool that helps protect your assets and network environment against unidentified threats and zero-day attacks.

To enable **Predictive Machine Learning**, find and click the check box next to it in the section of **Real-Time Scan** in the **Multi-Method Threat Prevention** pane.

Scheduled Scan

You can customize a regular antivirus scan schedule for elevating vulnerability scanning to its potential, as well as providing less burden on technical operators.

Procedure

1. Go to **Agents > All**.
2. Navigate to the target agent or group, and then go to its **Policy** page.

**Note**

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

3. Go to the **Scheduled Scan** in the **Multi-Method Threat Prevention** pane.
4. Toggle the **Scheduled Scan** on.
5. Click the **Schedule** button. A **Schedule** window appears.
6. Select one of the radio buttons listed below for determining the scan frequency.
 - **Daily**: Perform scanning every day
 - **Weekly**: Perform scanning every week (by default it's set as **every Sunday**)
 - **Monthly**: Perform scanning every month (by default it's set as **on day 01**)

**Important**

Since not every month contains the date 29th, 30th, or 31st, e.g., February only has 28 days (29 days on a leap year), TXOne Networks recommends NOT selecting the date 29th, 30th, or 31st for monthly update frequency. This helps prevent the system from bypassing the update in the month that does not contain the date 29th, 30th, or 31st.

7. Specify the scan start time in the **Start Time** field (by default it's set as **00:00**).
8. Click **Confirm** to complete the setting.

**Note**

See [Advanced Settings on page 5-60](#) for instructions on how to configure the types of the files to be scanned, the action to take after possible security risk is detected, and the scan exclusion list.

Advanced Settings

The **Advanced Options** allows you to configure the types of the files to be scanned, CPU usage setting, the action to take after possible security risk is detected, and the scan exclusion list.

**Note**

CPU usage setting is not available for **Real-Time Scan**.

Advanced Options for Real-Time Scan

Procedure

1. Go to **Agents > Policy > Multi-Method Threat Prevention**.
2. Click the **Advanced Settings** in the **Real-Time Scan** section.
3. The **Advanced Settings** configuration window appears.
4. The configuration window consists of two sections: **Files to Scan** and **Scan Action**.
5. In the **Files to Scan** section:
 - Check **Scan compressed files** and then select **Maximum layers** between 1 and 20 for the compressed files.
 - To skip scanning files over a certain size, check **Skip files larger than** and specify the file size between 1 and 2048 MB. Files exceeding the specified file size will not be scanned.
6. In the **Scan Action** section, you can pre-define the action to take after threats are detected during the scanning. Select **Quarantine** to place the suspicious files detected in an isolated folder for further checking. Select

No action to produce only a readout of results with no actions taken on the suspicious files.

7. Click **Confirm** to complete the settings.

Advanced Options for Scheduled Scan

Procedure

1. Go to **Agents > Policy > Multi-Method Threat Prevention**.
2. Click the **Advanced Settings** in the **Scheduled Scan** section:
3. The **Advanced Settings** configuration window appears.
4. The configuration window consists of three sections: **Files to Scan**, **CPU Usage**, and **Scan Action**.
 - a. In the **Files to Scan** section, click **All local folders** to scan all files in detail; click **Default folders (Quick Scan)** for a general scan; or click **Specific folders** to specify the paths to the folders for scan.



Tip

Under the **Specific folders** option, click the "+" or "-" icon to add or delete paths to the specific folders.

- (Optional) Check **Scan removable drives** to allow scanning files in removable drives
 - (Optional) Check **Scan compressed files** and select the **Maximum layers** between 1 and 20 for the compressed files.
 - (Optional) To skip files over a certain size, check **Skip files larger than** and specify the file size between 1 and 2048 MB. Files exceeding the specified file size will not be scanned.
- b. The **CPU Usage** settings allow you to select the appropriate mode of CPU usage to balance between the scan and the available CPU resources depending on situations. There are two options available:

- Click **Normal** to reduce the impact on the service performance, which allows you to perform other tasks while scanning but the scan may take longer to complete.
 - Click **High** to reduce scan time, which requires higher CPU usage and may affect the system performance.
- c. In the **Scan Action** section, you can pre-define the action to take after threats are detected. Select **Quarantine** to place the suspicious or infected files detected in an isolated folder for further checking. Select **No action** to produce only a readout of results with no actions taken on the suspicious files.
- d. (Optional) The **Scan Exclusions** section allows you to exclude certain folders, files, or file extensions from being scanned.
- **Folders:** specify a path to the folders that do not require scanning.
 - **Files:** specify a path to the files that do not require scanning.
 - **File Extensions:** specify the file extension of certain files that do not require scanning.

**Note**

- StellarProtect supports only local paths for **Scan Exclusions**. Remote paths such as an URL or \\ [Hostname] are not supported.
- It is not required to add "." or "*" in front of the file extension.

**Tip**

Click the "+" or "-" icon to add or delete paths to the specific folders/ files or file extensions for specific file types .

5. Click **Confirm** to complete the settings.
-

Scan Exclusions

The **Scan Exclusions** settings allow you to exclude certain files, folders, or file extensions from being scanned when running **Real-Time Scan** or **Scheduled Scan**

Procedure

1. Go to **Agents > Policy > Multi-Method Threat Prevention**.
-

**Note**

For StellarProtect (Legacy Mode), go to **Agents > Policy > Threat Prevention**

2. Find and click the **Real-Time Scan Exclusions** or **Scheduled Scan Exclusions**.
 3. The configuration window appears. Click **Add** to add certain file, folder, or file extension that will be excluded from being scanned.
 4. The configuration window appears. Choose from the menu to add scan exclusions:
 - **File:** Specify a path to the file that does not require scanning.
 - **Folder and subfolder:** Specify a path to the folder that does not require scanning.
 - **File Extension:** Specify the file extension of certain files that do not require scanning.
-

**Note**

- StellarProtect supports only local paths for Scan Exclusions. Remote paths such as an URL or `\\[Hostname]` are not supported.
 - It is not required to add "." or "*" in front of the file extension.
-

**Tip**

Click the "+" or "-" icon to add or delete the folder/file paths or file extensions.

OT Application Safeguard

OT Application Safeguard is an industrial-based change control protection. This feature ensures the StellarProtect-recognized OT applications can be updated without being blocked or restricted. In addition, you can enable OT application protection to secure recognized OT application executable binary files.

To enable **OT Application Safeguard**, go to **Agent > Policy**, scroll down to find and toggle on the **OT Application Safeguard** at the left side of the screen.

Upon launch, StellarProtect will auto-detect currently-installed OT applications and put them under protection. The recognized OT applications will be shown on the **Situational Awareness** tab page. Follow the instructions to view the identified OT applications.

Procedure

1. Go to **Agent > Policy**, scroll down to find and toggle on the **OT Application Safeguard** at the left side of the screen.
2. Find and click the **OT Applications**
3. The **Situational Awareness** screen appears.
4. Check the OT Applications automatically recognized by the StellarProtect agent.

**Important**

- Be sure to enable the **Maintenance Mode** before installing new OT applications. After the installation process completes, disable the **Maintenance Mode** and then StellarProtect will auto re-scan the newly-added OT applications. Any new applications found will be added into the OT Application Safeguard list. See [Configure Maintenance Mode on page 4-20](#) for how to enable this function.
- Be sure to enable the **Learn** mode of **Operations Behavior Anomaly Detection** before installing new OT applications. After the installation process completes, the StellarProtect agent will add the new OT applications into the **OT Applications** list displayed on the agent's **Situational Awareness** page. See [Operations Behavior Anomaly Detection on page 5-27](#) for more details.

-
5. You can also manually add the installation path for the application into the Safeguard's protection list.
 - a. Go to the **Policy** page and scroll down and find the **OT Application Safeguard** at the left side of the screen.
 - b. Make sure the **OT Application Safeguard** toggle is switched on.
 - c. Click **File/Folder**, and then the configuration window appears.
 - d. Click the **+Add** button, and then select **Folder** or **File** and specify the folder or file path in the corresponding text fields.

**Note**

By default, StellarProtect will only protect the PE files (.exe and .dll) under the selected folder and its subfolder(s).

-
- e. (Optional) If you want to protect all files inside the selected folder, please uncheck the **Executable files only**.

**Tip**

By unchecking the **Executable files only**, users can prevent their own secret files, configurations, or other files under the selected folder from being modified.

- f. Click **Add** to complete the setting.
6. You can also add user-defined authorized processes.
 - a. Go to **Policy > OT Application Safeguard**, and then click the **Authorized Processes**.
 - b. The configuration window appears. Click the **+Add** button, and then specify the authorized processes in the corresponding text fields.
-

**Important**

By adding the authorized process, you may set other applications to be trusted and change the protected files/folders previously defined as well as the PE files for OT applications detected by agents. Please note if any malicious file has been set into the authorized process, StellarProtect cannot prevent this file from modifying the OT applications since it has been already excluded from the StellarProtect's monitoring process. Make sure the user-defined authorized process is safe before adding it.

- c. Click **Add** to complete the setting.
-

DLL Injection Prevention

The **DLL Injection Prevention** provides protection against DLL hijacking attacks.

**Note**

Only x86 platform supports DLL injection Prevention.

Procedure

1. Go to **Agents > All**.
2. Navigate to the target agent or group, and then go to its **Policy** page.



Note

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

-
3. Scroll down and find the **DLL Injection Prevention** at the left side of the screen.
 4. Toggle on **Block DLL Injection** to enable it.
-

Other Key Features for StellarProtect (Legacy Mode)

Other key features provided by StellarProtect (Legacy Mode) agent include:

- [Application Lockdown on page 5-67](#)
- [Threat Prevention on page 5-77](#)

See [Comman Policy Settings for StellarProtect/StellarProtect \(Legacy Mode\) on page 5-84](#) for how to configure Agent Component Update Schedule, Device Control, User-Defined Suspicious Objects, Agent Password, Agent Patch deployment, and Trusted Certificates Settings for StellarProtect (Legacy Mode) agent.

Application Lockdown

When Application Lockdown is turned on, the agent will only be able to access applications that are in the Approved List.

Procedure

1. Go to **Agents > All**.

2. Navigate to the target agent or group, and then go to its **Policy** page.

**Note**

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

3. Go to the **Application Lockdown** pane, and then toggle on **Application Lockdown**.

**Note**

See the [Excluded Paths Settings on page 5-68](#), [Trusted Hash Values Settings on page 5-70](#), and [Write Protection Exclusions Settings on page 5-75](#) for how to configure the exclusions for the Approved List.

4. If you enable **Application Lockdown**, the sub-features listed below will appear. Select to enable them if needed.
 - **DLL/Driver Lockdown:** Prevents unapproved DLLs or drivers from being loaded into the memory of protected endpoints.
 - **Script Lockdown:** Prevents unapproved script files from being run on protected endpoints.
 - **Write Protection:** Blocks modification and deletion of files, folders, and registry entries and optionally prevents write access to files in the Approved List.
 - **Fileless Attack Prevention:** Detects and blocks unapproved process chains and arguments that may lead to a fileless attack event.
 - **Intelligent Runtime Learning:** Allows runtime executable files that are generated by applications in the Approved List.
-

Excluded Paths Settings

Excluded paths are used to point StellarProtect (Legacy Mode) to your file or file folder directly so that it can approve the file's execution.

Add a File, Folder, or Regular Expression as an Excluded Path

Procedure

1. Go to **Agents > All**.
2. Navigate to the target agent or group, and then go to its **Policy** page.

**Note**

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

3. Find the **Excluded Paths** section from the **Application Lockdown** pane.
 4. Click the **Add** button and the **Add Excluded Path** dialog window will appear.
 5. Select one of the exception types: **File**, **Folder**, or **Regular Expression**.
 6. Input the file system path for your exception.
 7. Click the **Add** button to add a single exception path and the settings will be saved.
-

Edit Excluded Path

Procedure

1. Go to **Agents > All**.
2. Navigate to the target agent or group, and then go to its **Policy** page.

**Note**

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

3. Find the **Excluded Paths** section from the **Application Lockdown** pane.
 4. Check the check box next to the exception path you want to edit.
 5. Click the **Edit** button and the **Add Excluded Path** dialog window will appear.
 6. After modification, click the **Save** button to save the settings.
-

Remove Excluded Path

Procedure

1. Go to **Agents > All**.
 2. Navigate to the target agent or group, and then go to its **Policy** page.
-



Note

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

3. Find the **Excluded Paths** section from the **Application Lockdown** pane.
 4. Check the check box next to the Exception Path you want to remove.
 5. Click the **Delete** button and the **Remove Excluded Path** dialog window will appear.
 6. Click the **Confirm** button to remove the selected entries.
-

Trusted Hash Values Settings

When **Application Lockdown** is enabled, the Agent will only be able to access applications that are in the Approved List. Use hash values to remotely allow applications and files to run on managed endpoints.

Calculate Hash Values

Use **File Hash Generator** to calculate hash values before adding trusted hash values.

Procedure

1. Find and click the **Trusted Hash Values** in the **Application Lockdown** pane.
2. A pop-up window appears. Find and download the **File Hash Generator** tool.
3. Execute `WKFileHashGen.exe` from the downloaded folder. The **File Hash Generator** screen will appear.
4. Use any of the following methods to select files and calculate hash values:
 - Drag and drop folders or files to the **File Hash Generator** screen.
 - Click the drop-down button and click **Add Files** to select the files to add.
 - Click the drop-down button and click **Add Folder** to add all the files in the selected folder.



Tip

Only executable, script, and installer files are supported. Mouse over the **Supported file types** for more details.



Note

Hash values will appear in the SHA-1 and SHA-256 columns.

5. For a single file, right-click the item and select **Copy SHA-1** or **Copy SHA-256**. For multiple files, click **Export All** to generate a list of hash values

**Note**

- To ensure that all necessary files are calculated for hash values, TXOne Networks suggests adding the root folder of the target application to the **File Hash Generator** for calculation.
 - By clicking the **Add Folder** button, only the installer files, script files, and files in the PE (Portable Executable) format will be calculated.
 - For the single hash value, see [Add Trusted Hash Values on page 5-72](#) for how to add the copied hash value to the trusted hash value list.
 - For multiple hash values, see [Import Trusted Hash Values on page 5-73](#) for how to import the file containing the hash values to the trusted hash value list.
-

6. Click **Exit** to close the tool.
-

Add Trusted Hash Values

Procedure

1. Go to **Agents > All**.
 2. Navigate to the target agent or group, and then go to its **Policy** page.
-

**Note**

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

3. Find and click the **Trusted Hash Values** in the **Application Lockdown** pane.
4. Click the **Add** button and fill in the hash values and notes.

5. (Optional) Select **Installer** to automatically add all files created or modified by the trusted installer to the Approved List.

Import Trusted Hash Values

Procedure

1. Go to **Agents > All**.
2. Navigate to the target agent or group, and then go to its **Policy** page.

**Note**

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

3. Find and click the **Trusted Hash Values** in the **Application Lockdown** pane.
4. Click the **Import** button to import the .txt file containing a batch of hash values.

**Note**

See [Calculate Hash Values on page 5-70](#) for generating the file containing the list of multiple hash values.

Edit Trusted Hash Values

Procedure

1. Go to **Agents > All**.
2. Navigate to the target agent or group, and then go to its **Policy** page.

**Note**

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

3. Find and click the **Trusted Hash Values** in the **Application Lockdown** pane.
 4. Find the trusted hash value to be edited and click the corresponding Edit icon in the **Actions** column.
 5. The **Edit Trusted Hash Value** dialog window appears.
 6. After modification, click the **Save** button to complete the settings.
 7. (Optional) Select **Installer** to automatically add all files created or modified by the trusted installer to the Approved List.
-

Remove Trusted Hash Values

Procedure

1. Go to **Agents > All**.
 2. Navigate to the target agent or group, and then go to its **Policy** page.
-

**Note**

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

3. Find and click the **Trusted Hash Values** in the **Application Lockdown** pane.
4. To delete multiple existing trusted hash values:
 - a. Click the checkboxes next to the existing trusted hash values.
 - b. Click the **Delete** button next to the **Import** button.

- c. A warning message window appears. Click **Confirm** to delete the selected items.
 5. To delete single existing trusted hash values:
 - a. Find the trusted hash value to be deleted and click the corresponding Delete icon in the **Actions** column.
 - b. A warning message window appears. Click **Confirm** to delete the selected item.
-

Write Protection Exclusions Settings

Write Protection allows you to protect the details in certain files or folders from being changed by unauthorized users or applications. Set **Write Protection** exclusions to remotely allow changes to certain files or folders on managed endpoints.

Add a File, Folder, Registry Key, or Registry Key and Value to Write Protection Exclusions

Procedure

1. Go to **Agents > All**.
 2. Navigate to the target agent or group, and then go to its **Policy** page.
-



Note

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

3. Find the **Write Protection Exclusions** section from the **Application Lockdown** pane.
4. Click the **Add** button and the **Add Write Protection Exclusions** dialog window will appear.
5. Select one of the protection types: **File**, **Folder**, **Registry Key** or **Registry Key and Value**.

6. Input the path to the target object to be write protected.
 7. Set the **Exception Process Type**.
 - No processes can write
 - All processes can write
 - Specify a process that can write by inputting the path.
 8. Click the **Add** button and the settings will be saved.
-

Edit Write Protection Exclusions

Procedure

1. Go to **Agents > All**.
 2. Navigate to the target agent or group, and then go to its **Policy** page.
-



Note

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

3. Find the **Write Protection Exclusions** section from the **Application Lockdown** pane.
 4. Check the check box next to the protection type you want to edit.
 5. Click the **Edit** button and the **Add Write Protection Exclusions** dialog window will appear.
 6. After modification, click the **Save** button to save the settings.
-

Remove Write Protection Exclusions

Procedure

1. Go to **Agents > All**.

2. Navigate to the target agent or group, and then go to its **Policy** page.

**Note**

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

3. Find the **Write Protection Exclusions** section from the **Application Lockdown** pane.
 4. Check the check box next to the protection type you want to remove.
 5. Click the **Delete** button and the **Remove Write Protection Exclusions** dialog window will appear.
 6. Click the **Confirm** button to remove the selected entries.
-

Threat Prevention

The **Threat Prevention** persistently scan new and changed files, along with system memory, to provide security assessment for maximum protection against malware. Related settings include:

- [Real-Time Scan on page 5-77](#)
- [Scheduled Scan on page 5-78](#)
- [Advanced Settings on page 5-80](#)

Real-Time Scan

Real-time Scan provides persistent and ongoing file scan for the endpoints. Each time a file is received, opened, downloaded, copied, or modified, **Real-time Scan** always scans the file for security assessment. After performing the **Real-Time Scan**, users can proceed to access the file if it does not pose a security threat. However, if a security risk or possible virus/malware has been detected during the scanning, associated events indicating the name of the infected file and the specific security risk will be generated for further investigation.

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.

Procedure

1. Go to **Agents > All**.
 2. Navigate to the target agent or group, and then go to its **Policy** page.
-



Note

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

3. Find the **Real-Time Scan** in the **Threat Prevention** pane.
 4. Toggle **Real-Time Scan** on to enable the function.
-



Note

See the [Advanced Settings on page 5-80](#) for instructions on how to configure the types of the files to be scanned, the action to take after possible security risk is detected, and the scan exclusion list.

Scheduled Scan

You can customize a regular antivirus scan schedule for elevating vulnerability scanning to its potential, as well as providing less burden on technical operators.

Procedure

1. Go to **Agents > All**.
2. Navigate to the target agent or group, and then go to its **Policy** page.

**Note**

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

3. Go to the **Scheduled Scan** in the **Threat Prevention** pane.
 4. Toggle the **Scheduled Scan** on.
 5. Click the **Schedule** button. A **Schedule** window appears.
 6. Select one of the radio buttons listed below for determining the scan frequency.
 - **Daily**: Perform scanning every day
 - **Weekly**: Perform scanning every week (by default it's set as **every Sunday**)
 - **Monthly**: Perform scanning every month (by default it's set as **on day 01**)
-

**Important**

Since not every month contains the date 29th, 30th, or 31st, e.g., February only has 28 days (29 days on a leap year), TXOne Networks recommends NOT selecting the date 29th, 30th, or 31st for monthly update frequency. This helps prevent the system from bypassing the update in the month that does not contain the date 29th, 30th, or 31st.

7. Specify the scan start time in the **Start Time** field (by default it's set as **00:00**).
8. Click **Confirm** to complete the setting.

**Note**

See [Advanced Settings on page 5-80](#) for instructions on how to configure the types of the files to be scanned, the action to take after possible security risk is detected, and the scan exclusion list.

Advanced Settings

The **Advanced Settings** allows you to configure the types of the files to be scanned, CPU usage setting, the action to take after possible security risk is detected, and the scan exclusion list.

**Note**

CPU usage setting is not available for **Real-Time Scan**.

Advanced Options for Real-Time Scan

Procedure

1. Go to **Agents > Policy > Threat Prevention**.
2. Click the **Advanced Settings** in the **Real-Time Scan** section.
3. The **Advanced Settings** configuration window appears.
4. The configuration window consists of three sections: **Files to Scan**, **Scan Action**, and **Scan Exclusions**.
5. In the **Files to Scan** section:
 - Check **Scan compressed files** and select the **Maximum layers** between 1 and 20 for the compressed files.
 - To skip scanning files over a certain size, check **Skip files larger than** and specify the file size between 1 and 2048 MB. Files exceeding the specified file size will not be scanned.
6. In the **Scan Action** section, you can pre-define the action to take after threats are detected during the scanning. Select **Quarantine** to place the suspicious files detected in an isolated folder for further checking. Select

No action to produce only a readout of results with no actions taken on the suspicious files.

7. Click **Confirm** to complete the settings.

Advanced Options for Scheduled Scan

Procedure

1. Go to **Agents > Policy > Threat Prevention**.
2. Click the **Advanced Settings** in the **Scheduled Scan** section:
3. The **Advanced Settings** configuration window appears.
4. The configuration window consists of three sections: **Files to Scan**, **CPU Usage**, and **Scan Action**.



Note

The StellarProtect (Legacy Mode) agents will automatically attempt to download the latest components before starting a scan. A **Component Update** toggle is available for you to determine whether the endpoints should continue with the scan if the component update is unsuccessful.

- a. In the **Files to Scan** section, click **All local folders** to scan all files in detail; click **Default folders (Quick Scan)** for a general scan; or click **Specific folders** to specify the paths to the folders for scan.



Tip

Under the **Specific folders** option, click the "+" or "-" icon to add or delete paths to the specific folders.

- (Optional) Check **Scan removable drives** to allow scanning files in removable drives
- (Optional) Check **Scan compressed files** and select the **Maximum layers** between 1 and 20 for the compressed files.

- (Optional) To skip files over a certain size, check **Skip files larger than** and specify the file size between 1 and 2048 MB. Files exceeding the specified file size will not be scanned.
- b. The **CPU Usage** settings allow you to select the appropriate mode of CPU usage to balance between the scan and the available CPU resources depending on situations. There are two options available:
- Click **Normal** to reduce the impact on the service performance, which allows you to perform other tasks while scanning but the scan may take longer to complete.
 - Click **High** to reduce scan time, which requires higher CPU usage and may affect the system performance.
- c. In the **Scan Action** section, you can pre-define the action to take after threats are detected. Select **Quarantine** to place the suspicious or infected files detected in an isolated folder for further checking. Select **No action** to produce only a readout of results with no actions taken on the suspicious files.

**Note**

The StellarProtect (Legacy Mode) agents provide more choices such as:

- **Use ActiveAction:** The pre-configured scan actions, which are best to use if you are not familiar with scan actions or if you are not sure which scan action is suitable.
- **Clean, or delete if the clean action is unsuccessful:** To delete the target file if it cannot be recovered.
- **Clean, or quarantine if the clean action is unsuccessful:** To quarantine the target file if it cannot be recovered.
- **Clean, or ignore if the clean action is unsuccessful:** To ignore the target file if it cannot be recovered.

-
5. Click **Confirm** to complete the settings.
-

Scan Exclusions

The **Scan Exclusions** settings allow you to exclude certain files, folders, or file extensions from being scanned when running **Real-Time Scan** or **Scheduled Scan**

Procedure

1. Go to **Agents > Policy > Multi-Method Threat Prevention**.

**Note**

For StellarProtect (Legacy Mode), go to **Agents > Policy > Threat Prevention**

2. Find and click the **Real-Time Scan Exclusions** or **Scheduled Scan Exclusions**.
3. The configuration window appears. Click **Add** to add certain file, folder, or file extension that will be excluded from being scanned.
4. The configuration window appears. Choose from the menu to add scan exclusions:
 - **File:** Specify a path to the file that does not require scanning.
 - **Folder and subfolder:** Specify a path to the folder that does not require scanning.
 - **File Extension:** Specify the file extension of certain files that do not require scanning.

**Note**

- StellarProtect supports only local paths for Scan Exclusions. Remote paths such as an URL or `\\[Hostname]` are not supported.
 - It is not required to add "." or "*" in front of the file extension.
-

**Tip**

Click the "+" or "-" icon to add or delete the folder/file paths or file extensions.

Common Policy Settings for StellarProtect/StellarProtect (Legacy Mode)

Common policy settings for StellarProtect/StellarProtect (Legacy Mode) agent include:

- [Agent Component Update Schedule on page 5-84](#)
- [Device Control on page 5-86](#)
- [User-Defined Suspicious Objects on page 5-90](#)
- [Agent Password on page 5-91](#)
- [Patch on page 5-92](#)
- [Trusted Certificates Settings on page 5-94](#)

Agent Component Update Schedule

You can configure the component update schedule for the agents via the StellarOne web console; thus the system can run component update automatically at the assigned time frequency.

**Note**

StellarOEM license edition does not support this function.

Procedure

1. Go to **Agents > All**.
2. Navigate to the target agent or group, and then go to its **Policy** page.

**Note**

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

3. On the **Policy** page, find the **Schedule Update** in the **Agent Component Update Schedule** pane.
 4. (Optional) Click **Go to StellarOne Scan Component Update Schedule** and view the current settings of StellarOne's component update schedule.
-

**Tip**

You can determine the agent's component update schedule by referring to the StellarOne console's component update schedule first.

**Note**

Only users logged in with administrator or operator account can edit the StellarOne component update schedule.

5. Toggle on the **Schedule Update**. Radio buttons for setting the **Frequency** and **Start Time** appear.
 - Click **Daily** to perform the agent component update every day
 - Click **Weekly** to perform the agent component update every week
-

**Note**

The default setting for **Weekly** update is **every Sunday**.

- Click **Monthly** to perform the agent component update every month
-

**Note**

The default setting for **Monthly** update is **on day 01**.

**Important**

Since not every month contains the date 29th, 30th, or 31st, e.g., February only has 28 days (29 days on a leap year), TXOne Networks recommends selecting **The last day of the month** for monthly update frequency. This helps prevent the system from bypassing the update in the month that does not contain the date 29th, 30th, or 31st.

6. Click **Start Time** to specify the exact time to perform the agent component update based on the defined frequency.
-

**Note**

The default setting for **Start Time** is **00:00**.

7. (Optional) If you do not want StellarOne to automatically deploy the latest component update to the agent/group, toggle on **Defer Component Update**. StellarOne will manage to deploy only the previous version.
-

**Note**

The configuration of agent component update will somehow impact the component update status displayed on the **Agents** screen and the **Agent Component Status** widget on **Dashboard**. See [Manage Agent Component Status on page 4-9](#) for more details.

Device Control

With **Device Control** enabled, every time the local user connects an unrecognized USB device to the protected endpoint, a pop-up notification will be displayed on the StellarProtect/StellarProtect (Legacy Mode) agent console for the local user to check and confirm if the USB device access is allowed. In addition, the associated event log will also be generated to notify the StellarOne administrator.

The StellarOne admin can grant one-time access to the unrecognized USB via the event action available on the blocked USB event. The USB will then be temporarily recognized as a trusted USB device and granted access until

disconnected from the endpoint. On top of that, the StellarOne admin can choose to add the USB to the **Trusted USB Device** list via the policy settings, allowing it to access directly and permanently without further check.

**Note**

In addition to USB devices, StellarProtect (Legacy Mode) also supports blocking CD/DVD drives and floppy disks on managed endpoints with **Device Control** enabled.

Procedure

1. Go to **Agents > All**.
2. Navigate to the target agent or group, and then go to its **Policy** page.

**Note**

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

3. Make sure the **Device Control** toggle is switched on.
4. Click **Trusted USB Device** and a pop-up window appears.
5. Specify at least one of the following information for the trusted USB device.
 - **Vendor ID**
 - **Product ID**
 - **Serial number**
6. Click **OK** to complete the setting.
7. Check if the USB device is successfully added in the trusted USB device list.
8. (Optional) To edit the USB device information, select the USB device and click the edit icon in the **Actions** column. A pop-up window appears.

Edit the USB device information in the related text fields and then click **OK**.

9. (Optional) To remove a USB device from trusted list, choose either way listed below.
 - For removing multiple USB devices at the same time, select the USB devices and click the **Delete** button next to the **+Add** button.
 - For removing only one USB device, click the Delete icon in the **Actions** column.

A pop-up **Notification** window appears. Click **Confirm** to delete the USB device(s).

Get Device Information

To get Device Information, use one of the following methods:

- Open the **Device Manager** on the endpoint.
- For StellarProtect (Legacy Mode) agent, use the `SLCmd.exe` command on the endpoint. Refer to [StellarProtect \(Legacy Mode\) Administrator's Guide](#) for more details.
- On StellarOne, go to the **Logs > Agent Events** on StellarOne console to check the event details about removable devices with Agent Event ID 1281/1282 (StellarProtect) or 5000/5001 (StellarProtect (Legacy Mode)).

For StellarProtect (Legacy Mode) agent, you can view the list of trusted USB devices on an endpoint by exporting the agent settings. To manually configure the trusted USB device list on an endpoint, do one of the following:

- Export the agent's settings, make changes, and then import the modified settings back to the agent via StellarOne
- Import an updated settings file via StellarOne
- Use the `SLCmd.exe` command on the StellarProtect (Legacy Mode) agent

Edit/Add/Remove Trusted USB Devices by Importing Configuration File

Procedure

1. Go to **Agents > All**.
2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.
3. Select the target agent by clicking the checkbox next to it.
4. Click the **Import/Export** button from the Tool Bar at the top of the **Agents** screen.
5. Click the **Export Agent Configuration** option.
6. Click **Confirm**.
7. A pop-up **Command Deployment** window appears. The **Status** shows if the agent configuration is exported successfully.
8. Click the **Download** link to download the target agent's configuration file.
9. Open the agent configuration file in a text editor and find the DeviceException section.

```
<StorageDeviceBlocking Enable="no" ActionMode="1" AllowNonMassStorageUSBDevice="no">
  <DeviceException>
    <DeviceGroup name="UserDefined"/>
  </DeviceException>
</StorageDeviceBlocking>
```

FIGURE 5-4. DeviceException section

10. The following figure shows an example where the section contains two entries for the added trusted USB devices.

```
<StorageDeviceBlocking Enable="no" ActionMode="1" AllowNonMassStorageUSBDevice="no">
  <DeviceException>
    <DeviceGroup name="UserDefined">
      <Device vid="781" pid="5151" sn="2444130A5442A4F5"/>
      <Device vid="951" pid="1666" sn="E03F49AECDDDF351E913003F"/>
    </DeviceGroup>
  </DeviceException>
</StorageDeviceBlocking>
```

FIGURE 5-5. Devices added in DeviceException section

11. You can edit, add, or remove the trusted USB devices by modifying, adding, or deleting the entries for the trusted USB devices and save the agent configuration file.
 12. Import the updated agent configuration file to the target agents.
-

User-Defined Suspicious Objects

The **User-Defined Suspicious Object** allows users to manually add the file hashes (SHA-1 or SHA-2) or paths of new IOC (Indicators of Compromise) into the blocked-file list, which prevents all managed endpoints from being infected by the malicious files.

**Note**

The StellarProtect (Legacy Mode) only supports SHA-1 file hash.

Procedure

1. Go to **Agents > All**.
 2. Navigate to the target agent or group, and then go to its **Policy** page.
-

**Note**

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

3. Find the **User-Defined Suspicious Object** at the right side of the screen.
4. Click **Add**. The **Add Item to User-Defined Suspicious Objects** window appears.
5. Select **Hash** or **File Path** as the suspicious file type.
6. Specify the file hash or path in the corresponding text field.
7. (Optional) Specify notes in the **Notes** text field.

8. Click **OK** to complete this task.
 9. (Optional) To remove a user-defined suspicious object, select the target hash/file path and click the **Delete** button next to the **+Add** button.
 10. A pop-up **Notification** window appears. Click **Confirm** to delete the selected item.
-

Agent Password

This function allows StellarOne administrators to remotely change the Agent's Administrator or User password required for logging on the StellarProtect/StellarProtect (Legacy Mode) local consoles. It does not require the old agent password to create a new one.



Note

This function is only available for users with privileges of Admins or Operators.

Procedure

1. Go to **Agents > All**.
 2. Navigate to the target agent or group, and then go to its **Policy** page.
-



Note

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

3. Scroll down and find the **Agent Password** at the right side of the screen.
4. Select the **ADMINISTRATOR** or **USER** tab.
5. Input the new password twice and click **Save** to finish this policy setting.

**Note**

- The password must be 8 to 64 alphanumeric characters. The following characters are not supported: | > " : < \ spaces
 - If the group/agent policy has been changed to customized, make sure you reset the agent password for better password management.
-

Patch

The **Patch** function allows the administrator to deploy a patch file upgrade on all agents under the same group policy. The patching process can be conducted remotely and automatically using policy synchronization. Only one patch file (Agent version) is allowed to be upgraded each time under each group policy.

**Important**

A patch is generally used to fix or enhance the current version. If you accidentally patch an older version, the patch deployment should not work and the agent status will keep un-synced with the StellarOne console. Meanwhile, other policy settings can't be deployed, either. After 20 minutes the agents will resynchronize with StellarOne; until then can the policy settings be applied to the agent.

Procedure

1. Go to **Agents > All**.
 2. Navigate to the target agent or group, and then go to its **Policy** page.
-

**Note**

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

3. Scroll down and find the **Patch** at the bottom right corner of the screen.
4. Click the checkbox next to the version of the patch file for deployment.

**Note**

You can import new patches for the agent on the [Importing/Deleting Agent's Patch on page 7-25](#) page.

5. The selected patch file will be deployed on the agents under the same group policy.

**Note**

Since StellarOne can apply global policy to all managed agents or certain group policies to group-owned endpoints for conducting the patching process on multiple devices at the same time, before you select agent version, please be aware that:

- By default, the global policy should be applied to every agent. TXOne Networks suggests that you keep lower agent version in the global policy settings.
 - If you don't want to set any agent version for patch deployment, do not select any of the checkboxes next to the agent version patch files in the **Patch** pane.
-

**Important**

StellarProtect Agent 1.0 does not support remote patch because it does not have any available remote patch files.

6. By default, StellarOne will automatically deploy the selected patch to the group of agents. However, if you toggle off the **Allow automatic updates**, the agents will only download the latest patch from StellarOne without installing. The local users can choose to run on-demand patch update manually on the agent console.
-

Trusted Certificates Settings

Similar to hash values, trusted certificates are made by the application vendors or organizations to allow the agent to know which applications are trustworthy. **Trusted Certificates** provides an import function allowing the administrator to add new trusted certificates. The trusted certificates defined by users and the corresponding applications will be bypassed during scanning and will not be blocked by Application Lockdown.

Importing/Deleting Trusted Certificates

Procedure

1. Go to **Agents > All**.
2. Navigate to the target agent or group, and then go to its **Policy** page.

**Note**

For instructions on how to go to the **Policy** page, see [Go to the Agent View on page 5-23](#) for a single agent or [Go to the Group Policy Screen on page 5-107](#) for a group of agents.

3. Scroll down and find the **Trusted Certificates** at the right side of the screen.
4. Click **Import** to import the selected trusted certificate file.
5. (StellarProtect (Legacy Mode) only) Enable the **Installer** toggle switch to automatically add all files created or modified by the trusted installer to the Approved List.

**Note**

By default, the **Installer** toggle is turned off.

6. Click **Import** to add the trusted certificate and the settings will be saved.
7. To remove the trusted certificate(s), choose either way listed below.
 - For removing multiple trusted certificates at the same time, select them and click the **Delete** button next to the **+Add** button.

- For removing only one trusted certificate, click the Delete icon in the **Actions** column.

A pop-up **Notification** window appears. Click **Confirm** to delete the selected certificate(s).

Situational Awareness

The Situational Awareness page displays a unique baseline fingerprint of each agent-device, which is generated via TXOne cyber-physical system (CPS) detection methods.

Topics in this section include:

- [Situational Awareness for StellarProtect on page 5-95](#)
- [Situational Awareness for StellarProtect \(Legacy Mode\) on page 5-101](#)

Situational Awareness for StellarProtect

The StellarProtect **Situational Awareness** page displays the baseline fingerprint at the agent level.



Note

The baseline data are transmitted at the default or specified policy refresh interval. See [Set Policy Refresh Interval on page 5-4](#) for more information.

See the following table for more details about this page.

TABLE 5-11. About the StellarProtect Situational Awareness Page

ITEM	DESCRIPTION
OT Applications	Upon launch, StellarProtect will auto-detect currently-installed OT applications and put them under protection. The recognized OT applications will be shown on the Situational Awareness tab page. See OT Application Safeguard on page 5-64 for more information.

ITEM	DESCRIPTION
OT Certificates	Upon launch and running pre-scan during the agent installation, StellarProtect will auto-detect currently-accepted OT certificates. The recognized OT certificates will be shown on the Situational Awareness tab page.
Approved Script Behaviors	Once you enable the Script Behavior of the Operations Behavior Anomaly Detection , the agent automatically learns and allows the approved scripts to run on the endpoints. See Approved Script Behaviors on page 5-96 for more details.
Approved Login Accounts	Once you enable the User Login of the Operations Behavior Anomaly Detection , the agent automatically learns and allows the approved user accounts and related login behaviors to run on the endpoints. See Approved Login Accounts on page 5-98 for more details.
Approved Applications	Once you enable the Application Behavior of the Operations Behavior Anomaly Detection , the agent automatically learns and allows the approved applications to run on the endpoints. See Approved Applications on page 5-99 for more information.

See [Operations Behavior Anomaly Detection on page 5-27](#) for more details about the **Approved Script Behaviors**, **Approved Login Accounts**, and **Approved Applications**.

Approved Script Behaviors

If you enable the **Operations Behavior Anomaly Detection > Script Behavior** function, script behaviors found on the StellarProtect agent-device will be added to its baseline and displayed on the **Situational Awareness > Approved Script Behaviors** page.

See the following table for more information about the **Approved Script Behaviors** page.

TABLE 5-12. About the Situational Awareness > Approved Script Behaviors Page

ITEM	DESCRIPTION
Baseline Toggle	<p>Allows you to determine if you want to include specific approved script behaviors in the baseline. If you turn the toggle off, the target script behaviors will be viewed as unexpected changes; alerts or preventative actions will be triggered depending on the selected Operations Behavior Anomaly Detection mode:</p> <ul style="list-style-type: none"> • In Detect mode: relevant events will be generated. • In Enforce mode: target script behaviors will be blocked.
Monitored Process / Script	<p>Displays the monitored operation process containing certain applications and accompanied parameters. By default, StellarProtect monitored 5 applications as listed below. You can also specify other commonly-abused applications in the Operations Behavior Anomaly Detection > Script Behavior > Policy-based Watchlist.</p> <ul style="list-style-type: none"> • powershell.exe • wscript.exe • cscript.exe • mshta.exe • psexec.exe <p>See Policy-based Watchlist on page 5-36 for more details.</p>
Approved Operation	<p>Displays the approved operations stored in the baseline. The approved operations can be viewed as the full execution process for triggering the monitored process mentioned above.</p> <p>See Operations Behavior Anomaly Detection on page 5-27 for more details.</p>
Added From	<p>Displays the sources the approved script behaviors are added from:</p> <ul style="list-style-type: none"> • Learn mode: the approved script behaviors have been detected and added to the baseline during Operations Behavior Anomaly Detection Learn mode. • Event action: the approved script behaviors have been added to the baseline by StellarOne administrator manually from the agent events (by clicking the Add to Baseline action button). See Add to Baseline on page 6-6 for more details.

ITEM	DESCRIPTION
Time Added	Displays the time when the approved script behaviors were added to the baseline.

**Note**

TXOne Networks recommends switching back to **Operations Behavior Anomaly Detection Learn** mode before adding new script behaviors or modifying existing ones.

Approved Login Accounts

If you enable the **Operations Behavior Anomaly Detection > User Login** function, user accounts and related login activities found on the StellarProtect agent-device will be added to its baseline and displayed on the **Situaional Awareness > Approved Login Accounts** page.

See the following table for more details about the **Approved Login Accounts** page.

TABLE 5-13. About the Situaional Awareness > Approved Login Accounts Page

ITEM	DESCRIPTION
Baseline Toggle	Allows you to determine if you want to include the approved login accounts in the baseline. If you turn it off, the corresponding login accounts will be viewed as not allowed and relevant events will be generated.
Domain	Displays the approved domains for the user to log in from.
Username	Displays the approved usernames stored in the baseline.
Source IP	Displays the approved IP addresses for the user to log in from.
Login Type	Displays the approved login type stored in the baseline.

ITEM	DESCRIPTION
Added From	<p>Displays the sources the approved login accounts are added from:</p> <ul style="list-style-type: none"> Learn mode: the approved login accounts have been detected and added to the baseline during Operations Behavior Anomaly Detection Learn mode. Event action: the approved login accounts have been added to the baseline by StellarOne administrator manually from the agent events (by clicking the Add to Baseline action button). See Add to Baseline on page 6-6 for more details.
Time Added	Displays the time when the approved login accounts were added to the baseline.

**Note**

TXOne Networks recommends switching back to **Operations Behavior Anomaly Detection Learn** mode before adding new user accounts or modifying existing ones.


Approved Applications

If you enable the **Operations Behavior Anomaly Detection > Application Behavior** function, applications found on the StellarProtect agent-device will be added to its baseline and displayed on the **Situational Awareness > Approved Applications** page.

See the following table for more details about the **Approved Applications** page.

TABLE 5-14. About the Situational Awareness > Approved Applications Page

ITEM	DESCRIPTION
Baseline Toggle	Allows you to determine if you want to include the approved applications in the baseline. If you turn it off, the running of the corresponding application will be viewed as unexpected changes and relevant events will be generated.

ITEM	DESCRIPTION
Application	Displays the product name of the approved application stored in the baseline.
Size	Displays the size of the approved application.
SHA-1	Displays the SHA-1 file hash value of the approved application
SHA-256	Displays the SHA-256 file hash value of the approved application
path	Displays the file path to the approved application
Version	Displays the version of the approved application when it was added to the baseline
Added From	<p>Displays the sources the approved applications are added from:</p> <ul style="list-style-type: none"> • Learn mode: the approved applications have been detected and added to the baseline during Operations Behavior Anomaly Detection "Learn" mode. • Event action: the approved applications have been added to the baseline by StellarOne administrator manually from the agent events (by clicking the Add to Baseline action button). See Add to Baseline on page 6-6 for more details. <hr/> <p> Note</p> <ul style="list-style-type: none"> • If the approved applications are added during the "Learn" mode, the agent learns not only the applications but also the relevant behaviors; different application behaviors may be detected as anomalies. • If the approved applications are added from the event action "Add to Baseline", the applications will be viewed as "exceptions" and associated behavior changes will be treated as acceptable.
Time Added	Displays the time when the approved applications were added to the baseline.

**Note**

TXOne Networks recommends switching back to **Operations Behavior Anomaly Detection Learn** mode before running the application updates.

Situational Awareness for StellarProtect (Legacy Mode)

The StellarProtect (Legacy Mode) **Situational Awareness** page displays the baseline fingerprint at the agent level.

**Note**

The baseline data are transmitted at the default or specified policy refresh interval. See [Set Policy Refresh Interval on page 5-4](#) for more information.

See the following table for more details about this page.

TABLE 5-15. About the StellarProtect (Legacy Mode) Situational Awareness Page

ITEM	DESCRIPTION
Approved Script Behaviors	Once you enable the Script Behavior of the Operations Behavior Anomaly Detection , the agent automatically learns and allows the approved scripts to run on the endpoints. See Approved Script Behaviors on page 5-102 for more details.
Approved Login Accounts	Once you enable the User Login of the Operations Behavior Anomaly Detection , the agent automatically learns and allows the approved user accounts and related login behaviors to run on the endpoints. See Approved Login Accounts on page 5-103 for more details.
Approved Applications	Once you enable the Application Behavior of the Operations Behavior Anomaly Detection , the agent automatically learns and allows the approved applications to run on the endpoints. See Approved Applications on page 5-104 for more information.

See [Operations Behavior Anomaly Detection on page 5-27](#) for more details about the **Approved Script Behaviors**, **Approved Login Accounts**, and **Approved Applications**.

Approved Script Behaviors

If you enable the **Operations Behavior Anomaly Detection > Script Behavior** function, script behaviors found on the StellarProtect (Legacy Mode) agent-device will be added to its baseline and displayed on the **Situational Awareness > Approved Script Behaviors** page.

See the following table for more information about the **Approved Script Behaviors** page.

TABLE 5-16. About the Situational Awareness > Approved Script Behaviors Page

ITEM	DESCRIPTION
Baseline Toggle	<p>Allows you to determine if you want to include specific approved script behaviors in the baseline. If you turn the toggle off, the target script behaviors will be viewed as unexpected changes; alerts or preventative actions will be triggered depending on the selected Operations Behavior Anomaly Detection mode:</p> <ul style="list-style-type: none"> • In Detect mode: relevant events will be generated. • In Enforce mode: target script behaviors will be blocked.
Monitored Process / Script	<p>Displays the monitored operation process containing certain applications and accompanied parameters. By default, StellarProtect (Legacy Mode) monitored 5 applications as listed below. You can also specify other commonly-abused applications in the Operations Behavior Anomaly Detection > Script Behavior > Policy-based Watchlist.</p> <ul style="list-style-type: none"> • powershell.exe • wscript.exe • cscript.exe • mshta.exe • psexec.exe <p>See Policy-based Watchlist on page 5-36 for more details.</p>

ITEM	DESCRIPTION
Approved Operation	<p>Displays the approved operations stored in the baseline. The approved operations can be viewed as the full execution process for triggering the monitored process and/or script mentioned above.</p> <p>See Operations Behavior Anomaly Detection on page 5-27 for more details.</p>
Added From	<p>Displays the sources the approved script behaviors are added from:</p> <ul style="list-style-type: none"> • Learn mode: the approved script behaviors have been detected and added to the baseline during Operations Behavior Anomaly Detection Learn mode. • Event action: the approved script behaviors have been added to the baseline by StellarOne administrator manually from the agent events (by clicking the Add to Baseline action button). See Add to Baseline on page 6-6 for more details.
Time Added	<p>Displays the time when the approved script behaviors were added to the baseline.</p>

**Note**

TXOne Networks recommends switching back to **Operations Behavior Anomaly Detection Learn** mode before adding new script behaviors or modifying existing ones.

Approved Login Accounts

If you enable the **Operations Behavior Anomaly Detection > User Login** function, user accounts and related login activities found on the StellarProtect (Legacy Mode) agent-device will be added to its baseline and displayed on the **Situational Awareness > Approved Login Accounts** page.

See the following table for more details about the **Approved Login Accounts** page.

TABLE 5-17. About the Situational Awareness > Approved Login Accounts Page

ITEM	DESCRIPTION
Baseline Toggle	Allows you to determine if you want to include the approved login accounts in the baseline. If you turn it off, the running of the corresponding login accounts will be viewed as not allowed and relevant events will be generated.
Domain	Displays the approved domains for the user to log in from.
Username	Displays the approved usernames stored in the baseline.
Source IP	Displays the approved IP addresses for the user to log in from.
Login Type	Displays the approved login type stored in the baseline.
Added From	Displays the sources the approved login accounts are added from: <ul style="list-style-type: none"> • Learn mode: the approved login accounts have been detected and added to the baseline during Operations Behavior Anomaly Detection Learn mode. • Event action: the approved login accounts have been added to the baseline by StellarOne administrator manually from the agent events (by clicking the Add to Baseline action button). See Add to Baseline on page 6-6 for more details.
Time Added	Displays the time when the approved login accounts were added to the baseline.

**Note**

TXOne Networks recommends switching back to **Operations Behavior Anomaly Detection Learn** mode before adding new user accounts or modifying existing ones.


Approved Applications

If you enable the **Operations Behavior Anomaly Detection > Application Behavior** function, applications found on the StellarProtect (Legacy Mode) agent-device will be added to its baseline and displayed on the **Situational Awareness > Approved Applications** page.

See the following table for more details about the **Approved Applications** page.

TABLE 5-18. About the Situational Awareness > Approved Applications Page

ITEM	DESCRIPTION
Baseline Toggle	Allows you to determine if you want to include the approved applications in the baseline. If you turn it off, the running of the corresponding application will be viewed as unexpected changes and relevant events will be generated.
Application	Displays the product name of the approved application stored in the baseline.
Size	Displays the size of the approved application.
SHA-1	Displays the SHA-1 file hash value of the approved application
SHA-256	Displays the SHA-256 file hash value of the approved application
path	Displays the file path to the approved application
Version	Displays the version of the approved application when it was added to the baseline

ITEM	DESCRIPTION
Added From	<p>Displays the sources the approved applications are added from:</p> <ul style="list-style-type: none"> • Learn mode: the approved applications have been detected and added to the baseline during Operations Behavior Anomaly Detection "Learn" mode. • Event action: the approved applications have been added to the baseline by StellarOne administrator manually from the agent events (by clicking the Add to Baseline action button). See Add to Baseline on page 6-6 for more details. <hr/> <p> Note</p> <ul style="list-style-type: none"> • If the approved applications are added during the "Learn" mode, the agent learns not only the applications but also the relevant behaviors; different application behaviors may be detected as anomalies. • If the approved applications are added from the event action "Add to Baseline", the applications will be viewed as "exceptions" and associated behavior changes will be treated as acceptable.
Time Added	Displays the time when the approved applications were added to the baseline.

**Note**

TXOne Networks recommends switching back to **Operations Behavior Anomaly Detection Learn** mode before running the application updates.

Group Policy Settings

The StellarOne console combines agents management and policy deployment by allowing you to organize agents into various groups, build up multi-level hierarchy among the groups, and deploy different policies to different groups when needed.

Two types of policy management are available for choice:

- Policy **Inherited**: The group policy is inherited from the parent group
- Policy **Customized**: The group policy is customized for specific groups by the StellarOne administrators



Note

Self-managed: This special policy setting allows local agents to be free from StellarOne's policy management and instead, to be managed directly by the on-site operators. Though it's a policy setting, once enabled, the **Self-managed** status will be shown in the **Policy** column on the **Agents** screen.

Topics in this chapter include:


- [Go to the Group Policy Screen on page 5-107](#)
- [Group Policy Settings on page 5-108](#)

Go to the Group Policy Screen


Name	IP Address	Protection	Policy	Operations Behavior Anomaly ...	Approved Lis...	Agent Versio...	Last Connection	Function Type	Actions
customized_po	-	-	Customized	-	-	-	-	StellarProtect (6-mem)	ⓘ ⚙
test (0)	-	-	Customized	-	-	-	-	StellarProtect (6-mem)	ⓘ ⚙
test_group_set	-	-	Customized	-	-	-	-	StellarProtect (6-mem)	ⓘ ⚙
ST-W1122H2X...	-	🟢	Inherited	-	65871	3.0.1016	2023-05-06T16:28...	StellarProtect (6-mem)	ⓘ ⚙
ST-W10ENT...	-	🟢	Inherited	-	42561	3.0.1016	2023-05-29T19:11...	StellarProtect (6-mem)	ⓘ ⚙
ZI-W11X84-1	-	🟢	Inherited	Enforce	67141	3.0.1043	2023-06-15T14:44...	StellarProtect	ⓘ ⚙
ZI-WIN10X84-1	-	🟢	Inherited	Enforce	62016	3.0.1043	2023-06-15T14:48...	StellarProtect	ⓘ ⚙
ZI-W10ENT-X8...	-	🟢	Customized	Enforce	44721	3.0.1043	2023-06-15T14:46...	StellarProtect	ⓘ ⚙

Procedure

1. Click the **Agents** tab in the top navigation bar of the StellarOne web console.

2. Click the **All** group, and then a screen displays the second level of groups/agents managed by StellarOne.
3. Navigate to the target group. Choose one of the ways to go to the group policy configuration page.
 - Click the link (**Inherited, Customized, or Self-managed**) in the **Policy** column.
 - Click the  Policy icon in the **Actions** column, and then click the **Policy** tab.
4. The **Policy** screen appears.

**Note**

You can also click the  Policy icon of the **All** group to check its policy settings.

Group Policy Settings

Unlike the agent policy page, the group policy configuration page allows you to manage policy at the group level. Also, the group policy page displays information at the group level, so some links for directing users to the **General Info** or **Situational Awareness** at the agent level are not available.

At the group level, if the **Policy Inheritance** is toggled on, the custom exceptions menu appears and allows you to customize specific settings that will take precedence over the inherited policy.

The following image shows the differences between the agent and group policy pages:

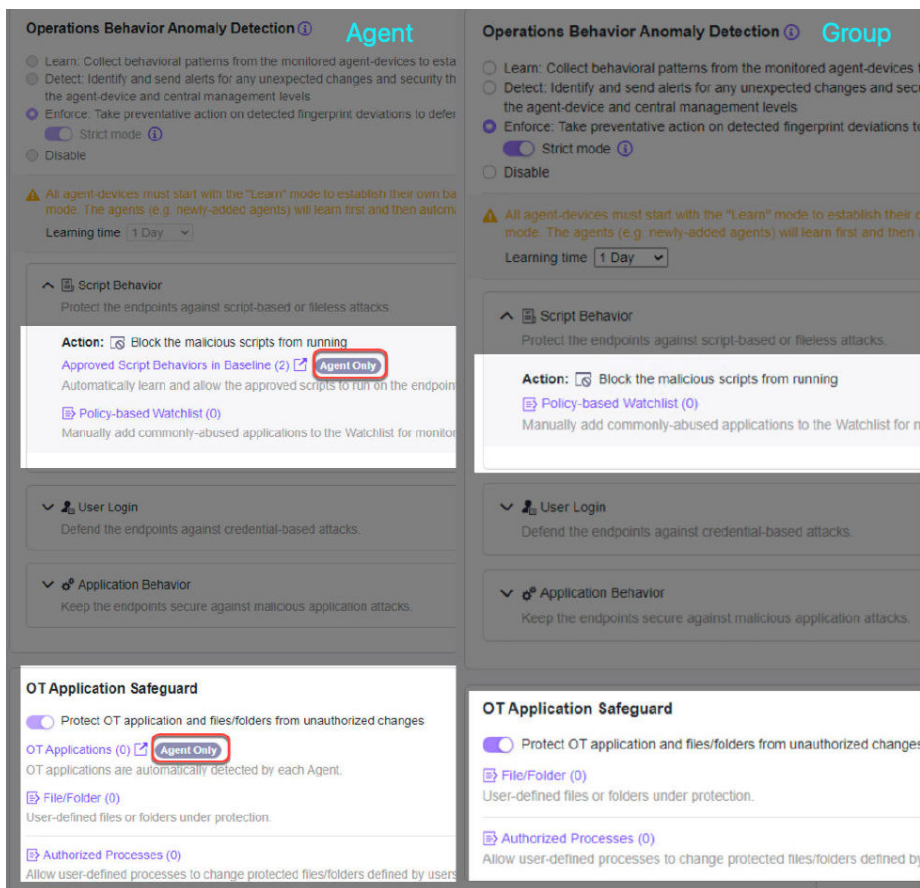




FIGURE 5-6. Differences between the Agent & Group Policy Pages

Refer to the *Agent Policy Settings* on page 5-27 for how to configure group policy settings.

Create Custom Exceptions to the Inherited Policy


You can create custom exceptions to the inherited policy at the group level, which transform the selected settings to customizable and associated changes will take precedence over the inherited policy. Meanwhile, the rest of the settings still remain inherited from the parent group

Procedure

1. Go to the group policy page and toggle on **Policy Inheritance**.
2. The **Custom Exceptions** icon  appears.
3. Click the  and a pop-up window appears.
4. Select the settings you want to make customizable, and then click **Save**.

**Note**

Only the enabled features are available for selection in the custom exceptions list.

-
5. On the **Policy** page, the **Custom Exception** icon  **Custom Exception** appears by the selected items.
 6. You can now edit the selected items. The associated changes will take precedence over the inherited group policy.
-

Chapter 6

Logs

This chapter describes how to access StellarOne-generated logs and the logs related to the agents, as well as includes detailed log information for advanced administrator management. Topics in this chapter include:

- *Agent Events on page 6-2*
- *Server Events on page 6-10*
- *System Logs on page 6-13*
- *Audit Logs on page 6-15*

Agent Events

The StellarOne collects activities on agents and log them in the **Agent Events**.

Procedure

1. Mouse over the **Logs** tab in the top navigation bar of the StellarOne web console. A drop-down menu appears.
2. Click the **Agent Events**.
3. The **Agent Events** screen appears.
4. You can search for the most relevant events for troubleshooting or analysis by using the filter tool in the upper-right corner of the screen. See [Agent Events Filtering on page 6-4](#) for more details.



Note

- For StellarProtect's event IDs and corresponding log information, see [Log Descriptions for StellarProtect on page A-2](#).
- For StellarProtect (Legacy Mode)'s event IDs and corresponding log information, see [Log Descriptions for StellarProtect \(Legacy Mode\) on page A-28](#)

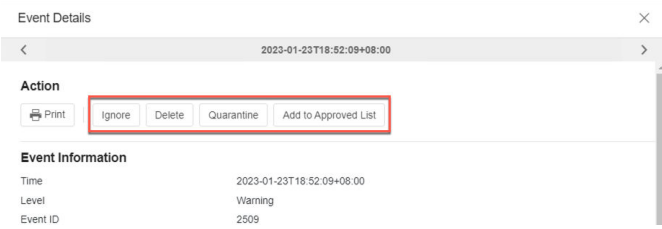
About Agent Events Screen

Time	Level	Event	Function Type	Endpoint	Action
2024-02-01T16:04:03+08:00	Warning	2509 File access blocked. File not found in Approved List	StellarProtect (Frame Map)	AD-WIN10X66-V2	6
2024-02-01T16:04:03+08:00	Warning	5889 File Access Blocked	StellarProtect	ST-WIN10X64	6
2024-02-01T16:04:03+08:00	Warning	5889 File Access Blocked	StellarProtect	ST-WIN10X64	6
2024-02-01T16:04:03+08:00	Warning	5889 File Access Blocked	StellarProtect	ST-WIN10X64	6

FIGURE 6-1. Agent Events Logs

TABLE 6-1. About Agent Events Screen


ITEM	DESCRIPTION
(1) Export	<p>You can export log list as an .csv file by clicking the Export button. It provides a drop-down menu consisting of:</p> <ul style="list-style-type: none"> • Export Selected: This button is activated when you select the checkbox(es) next to the logs to export. • Export: This button is always activated for exporting a maximum of 10,000 log entries.
(2) Filter	<p>Provides the filter tool for finding the most relevant event logs for troubleshooting or analysis. See Agent Events Filtering on page 6-4 for more details.</p>
(3) Log display setting	<p>You can specify the time range for viewing the logs generated within the specific period.</p>
(4) Screen display setting	<p>By clicking this button, you can customize the screen display by:</p> <ul style="list-style-type: none"> • selecting how many logs to display per page • hiding certain contents by unselecting Time, Level, Event, Function Type, or Endpoint in the Customize Table Display window.
(5) Refresh	<p>Provides manual refresh of the screen for the latest log outputs</p>


ITEM	DESCRIPTION
(6) View Details	<p>In Information or Critical level logs, you can view and print event details such as event information and agent information.</p> <p>In some of the Warning level logs, in addition to viewing and printing event details such as event information and agent information, you can also apply certain action to the detected files or blocked devices, such as Ignore, Delete, Quarantine, Add to Approved List, Grant One-Time Access, or Add to Baseline.</p> <p>See Agent Event Actions on page 6-5 for more details.</p>  <p>FIGURE 6-2. An Example of Available Event Actions in Certain Warning Level Logs</p>

Agent Events Filtering

This section describes how to filter the **Agent Events** logs to find the most relevant log messages.

Procedure

1. Go to **Logs > Agent Events**. Click the filter tool  in the upper-right corner of the screen, and then a drop-down menu appears.
2. Select **Add Filter**, and then the option menu appears.
3. Select the desired search criteria from the menu. The selected criteria will appear on the left side of the screen.
4. Click the criteria and specify the value by typing in the text field or selecting from the option menu.

5. Click **Apply** and then the screen will display the search result.
6. Click the close icon to remove the selected criteria one by one, or click **Clear all** to remove all of the selected criteria.
7. You can save the selected criteria as a filter by clicking the **Save filter** on the right side of the screen.
 - a. The **Save Filter** window appears. Specify the name of the filter in the **Filter Name** text field.
 - b. Click **Save** to complete the setting.
 - c. Click the filter tool  in the upper-right corner of the screen and the **Saved Filter** is available for selection.
 - d. Click the **Saved Filter** and then the target filter. The screen will display the search result.

**Note**

You can change the name of the saved filter or delete it by clicking the **edit** or **remove** icon beside it.

Agent Event Actions

The following table shows the actions you can apply to certain warning level events.

ACTION	DESCRIPTION
Ignore	Performs no action to the detected file.
Delete	Deletes the detected file.
Quarantine	Moves the detected file to a quarantine folder on the agent-device.
Add to Approved List	Adds the detected file to the Approved List. See StellarProtect Application Lockdown on page 5-49 or StellarProtect (Legacy Mode) Application Lockdown on page 5-67 for more details.

ACTION	DESCRIPTION
Add to Baseline	Adds the detected file to the baseline. See Add to Baseline on page 6-6 for more details.
Add to Suspicious Objects Blocklist	Adds the detected file to the blocklist. See Add to Suspicious Objects Blocklist on page 6-7 for more details.
Grant One-Time Access	Allow the blocked USB to access the endpoint temporarily until the USB is disconnected. See Grant One-Time Access on page 6-8 for more details.

Add to Baseline

This section describes how to apply the **Add to Baseline** action when the relevant event occurs and the associated outcomes. By applying this action, you allow the detected anomalies to run on the device without further check.

Procedure

1. To check agent events, go to **Logs > Agent Events**.
2. Find the **Warning** level events related to the Operations Behavior Anomaly Detection, and then click the **Event Details** icon in the **Action** column.
3. The **Event Details** window appears.
4. Click **Add to Baseline** to apply this action. The unrecognized application detected as shown in the following example will be added to the agent baseline as an approved application.

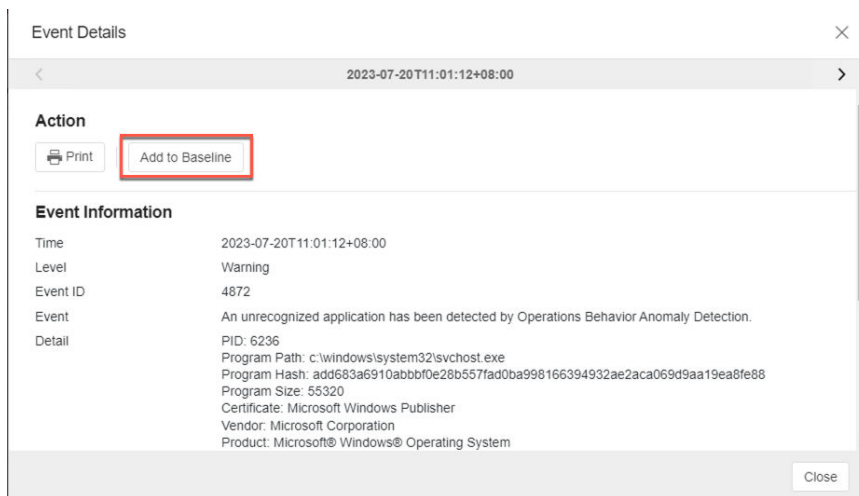


FIGURE 6-3. An example of the event with "Add to Baseline" action

5. To check if the application has been added to the agent baseline, go to the **Situational Awareness** page.
6. Find the search and filter tool, select **Added From** and **Event action** as the criteria and click the search icon.
7. As a result, the table displays a list of the approved applications added from the event action "**Add to Baseline**".



Note

Since the baseline data are transmitted at the default or specified policy refresh interval, the result of the applied action may not appear in the **Situational Awareness** baseline immediately. You can shorten the policy refresh interval to make the result appear earlier. See [Set Policy Refresh Interval on page 5-4](#) for how to configure the settings.

Add to Suspicious Objects Blocklist

This section describes how to apply the **Add to Suspicious Objects Blocklist** action when the relevant event occurs and the associated outcomes. By

applying this action, you block the application associated with the detected anomalies to run on the device without further check.

Procedure

1. To check agent events, go to **Logs > Agent Events**.
 2. Find the **Warning** level events related to the Operations Behavior Anomaly Detection – Application Behavior, and then click the **Event Details** icon in the **Action** column.
 3. The **Event Details** window appears.
 4. Click **Add to Suspicious Objects Blocklist** to apply this action. The application associated with the detected anomalies will be added to the Suspicious Objects Blocklist.
 5. A confirmation window appears. Read it carefully and click **Confirm** if you decide to add the application to the Suspicious Objects Blocklist.
-



Important

Once added, the application will be blocked from running on the endpoint unless removed from the Suspicious Objects Blocklist.

6. To check if the application has been added to the Suspicious Objects Blocklist, navigate to the target agent and then go to its **Policy** page.
 7. Go to **Operations Behavior Anomaly Detection > Application Behavior**.
 8. Find and click **Suspicious Objects Blocklist**. A pop-up window appears and displays a list of the blocked applications added from the event action "**Add to Suspicious Objects Blocklist**".
-

Grant One-Time Access

This section describes how to apply the **Grant One-Time Access** action when the relevant event occurs and the associated outcomes. By applying this action, you temporarily allow the blocked USB device to access until disconnected from the endpoint.

Procedure

1. To check agent events, go to **Logs > Agent Events**.
2. Find the **Warning** level events related to blocked USB devices, and then click the **Event Details** icon in the **Action** column.
3. The **Event Details** window appears.
4. Click **Grant One-Time Access** to apply this action. The blocked USB as shown in the following example will be temporarily recognized as a trusted USB device and granted access until disconnected from the endpoint.

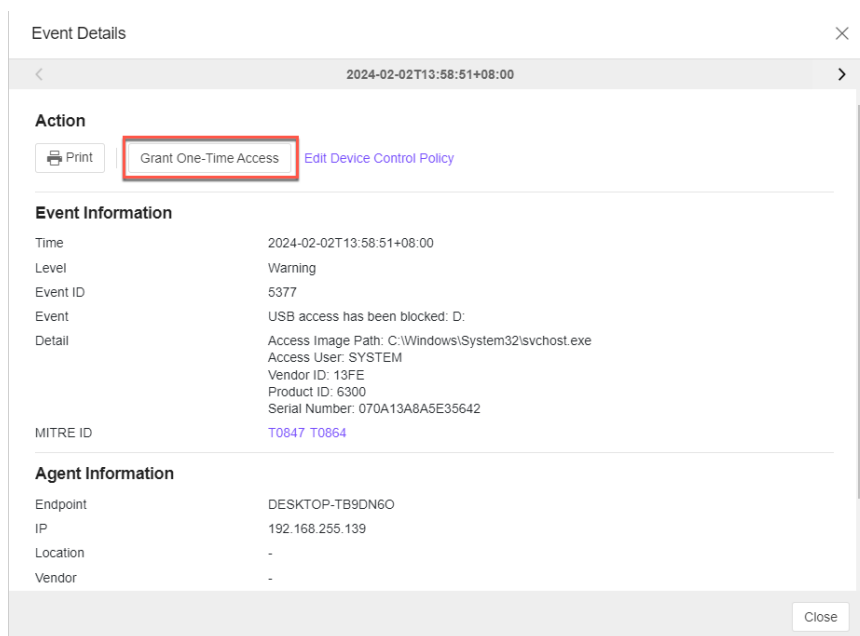


FIGURE 6-4. An example of the event with "Grant One-Time Access" action

**Note**

By clicking **Edit Device Control Policy**, you will be directed to the policy page where you can add the blocked USB device to a policy-based trusted device list. The device added will then have permanent access to the target endpoint or group of endpoints.

Server Events

Activities on StellarOne Servers and configuration deployed on the Agents by StellarOne are logged and shown in the **Server Events** screen.

Procedure

1. Mouse hover the **Logs** tab in the top navigation bar of the StellarOne web console. Click the **Server Events** option.
2. Click the StellarProtect or StellarProtect (Legacy Mode) tab, the configuration events deployed on the Agents by StellarOne appear.
3. Click the **StellarOne** tab, the StellarOne server event logs appear.

About Server Events Screen

Time	User ID	Event	Endpoint[Groups]	Status
2023-06-14T18:26:34+08:00		33029 Deploy policy with version: 1686738394452790452	ZI-W10ENT-X86-1	Successful
2023-06-14T18:26:33+08:00		33029 Deploy policy with version: 1686738392984832985	ZI-W10ENT-X86-1	Successful

FIGURE 6-5. Server Events Logs for StellarProtect

TABLE 6-2. About StellarProtect Server Events Screen

ITEM	DESCRIPTION
(1) Export	<p>Users can export log list as an .csv file by clicking the Export button. It provides a drop-down menu consisting of:</p> <ul style="list-style-type: none"> • Export Selected: This button is activated when users select the checkbox(es) next to the logs to be exported. • Export All: This button is always activated for users to export all logs.
(2) Filter	<p>This tool allows users to search for the relevant log messages for troubleshooting or analysis. Please refer to Server Events Log Filtering on page 6-12 for procedures.</p>
(3) Log display setting	<p>Users can customize how many logs to be displayed either by:</p> <ul style="list-style-type: none"> • the number of the latest log records • the logs generated within a particular period
(4) Screen display setting	<p>By clicking this button, users can customize the screen display by:</p> <ul style="list-style-type: none"> • selecting how many logs to be displayed on one page • hiding certain contents by unchecking Time, User ID, Event, Endpoint/[Groups], or Status in the Cusomize Table Display window.
(5) Refresh	<p>The button allows users to manually refresh the screen for the latest log outputs.</p>

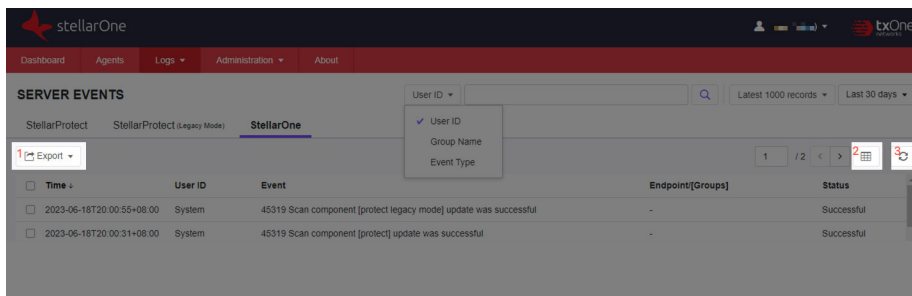


FIGURE 6-6. Server Events Logs for SterllarOne

TABLE 6-3. About StellarOne Server Events Screen

ITEM	DESCRIPTION
(1) Export	<p>Users can export log list as an .csv file by clicking the Export button. It provides a drop-down menu consisting of:</p> <ul style="list-style-type: none"> • Export Selected: This button is activated when users select the checkbox(es) next to the logs to be exported. • Export All: This button is always activated for users to export all logs.
(2) Screen display setting	<p>By clicking this button, users can customize the screen display by:</p> <ul style="list-style-type: none"> • selecting how many logs to be displayed per page • hiding certain contents by unchecking Time, User ID, Event, Endpoint/[Groups], or Status in the Customize Table Display window.
(3) Refresh	<p>The button allows users to manually refresh the screen for the latest log outputs.</p>

Server Events Log Filtering

This section describes how to filter the **Server Events** logs to find the most relevant log messages.

Procedure

1. Go to **Logs > Server Events > StellarProtect**. Click the **User ID** next to the search bar, and then a drop-down menu appears.
2. There are two types of log filtering based on the drop-down menu. Choose from either one listed below depending on your needs.
 - Select the **User ID** or **Endpoint Name**, and then type the search strings in the search field.
 - Select the **Group Name** or **Event Type**, a search box with an arrow pointing downwards appears. Tap on it to see the options under different categories.
 - **Group Name:** The **Select a group** window appears. Select one group and click **Confirm** for viewing its log records.

- **Event Type:** A drop-down menu with options of event types appears. Select one of them for viewing the relevant log records.

**Note**

Please refer to [Server Event Log Descriptions for StellarProtect on page A-26](#) for more details on various event types.

3. Click the search icon next to the search bar and then the screen will display the search result.
4. To clear the search criteria, close the filtering criteria appears above the **Export** button.

**Note**

Please refer to [Server Event Log Descriptions for StellarProtect on page A-26](#) and [Server Event Log Descriptions for StellarOne on page A-87](#) in the Appendices for more details about event IDs and corresponding log information..

System Logs

Internal system processes generated by StellarOne Servers are logged and shown in the **System Logs**.

Procedure

1. Mouse over the **Logs** tab in the top navigation bar of the StellarOne web console.
 2. Click the **System Logs** option.
 3. The **System Logs** screen appears.
-

About System Logs Screen

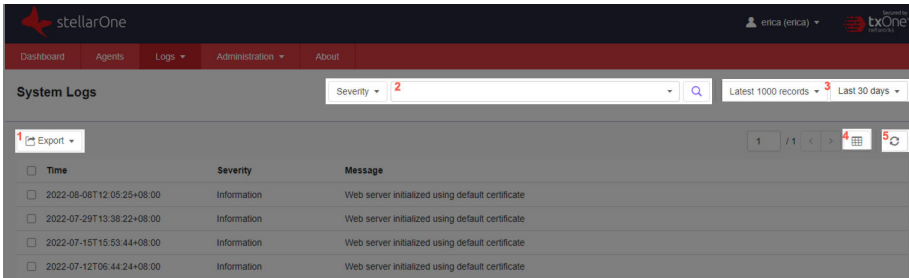


FIGURE 6-7. System Logs Screen

TABLE 6-4. About System Logs Screen

ITEM	DESCRIPTION
Export	<p>Users can export log list as an .csv file by clicking the Export button. It provides a drop-down menu consisting of:</p> <ul style="list-style-type: none"> • Export Selected: This button is activated when users select the checkbox(es) next to the logs to be exported. • Export All: This button is always activated for users to export all logs.

ITEM	DESCRIPTION
Filter	<p>Users can filter logs by selecting or specifying certain severity level directly in the search bar. The severity levels are listed as below:</p> <ul style="list-style-type: none"> • Emergency • Alert • Critical • Error • Warning • Notice • Information • Debug <p>After users set the search criteria and click the search button, the screen displays the search result. Meanwhile, the filtering criteria appears above the Export button. Close it to clear the search criteria and return to the initial screen.</p>
Log display setting	<p>Users can customize how many logs to be displayed either by:</p> <ul style="list-style-type: none"> • the number of the latest logs records • the logs generated within a particular period
Screen display setting	<p>By clicking this button, users can customize the screen display by:</p> <ul style="list-style-type: none"> • selecting how many logs to be displayed per page • hiding certain contents by unchecking Time, Severity, or Message in the Customize Table Display window.
Refresh	<p>The button allows users to manually refresh the screen for the latest log outputs.</p>

Audit Logs

The **Audit Logs** screen displays the user activities such as login, logout, or account creation/deletion.

Procedure

1. Mouse over the **Logs** tab in the top navigation bar of the StellarOne web console.
2. Click the **Audit Logs** option.
3. The **Audit Logs** screen appears.

About Audit Logs Screen

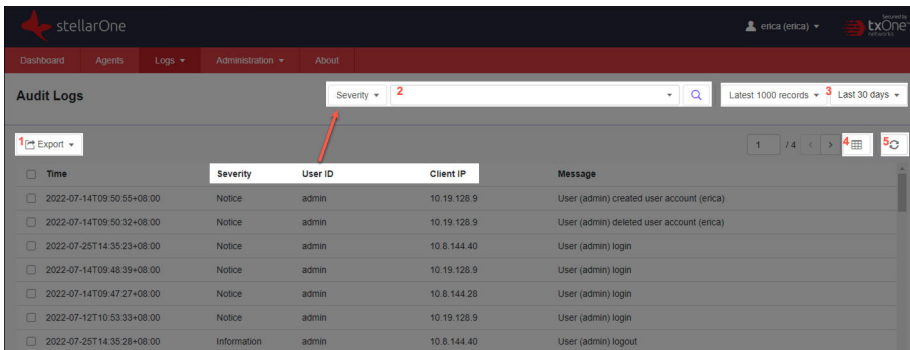


FIGURE 6-8. Audit Logs Screen

TABLE 6-5. About Audit Logs Screen

ITEM	DESCRIPTION
(1) Export	<p>Users can export log list as an .csv file by clicking the Export button. It provides a drop-down menu consisting of:</p> <ul style="list-style-type: none"> • Export Selected: This button is activated when users select the checkbox(es) next to the logs to be exported. • Export All: This button is always activated for users to export all logs.
(2) Filter	<p>This tool allows users to search for the relevant log messages for troubleshooting or analysis. Please refer to Audit Log Filtering on page 6-17 for procedures.</p>

ITEM	DESCRIPTION
(3) Log display setting	Users can customize how many logs to be displayed either by: <ul style="list-style-type: none"> • the number of the latest logs records • the logs generated within a particular period
(4) Screen display setting	By clicking this button, users can customize the screen display by: <ul style="list-style-type: none"> • selecting how many logs to be displayed per page • hiding certain contents by unchecking Time, Severity, User ID, Client IP, or Message in the Customize Table Display window.
(5) Refresh	The button allows users to manually refresh the screen for the latest log outputs.

Audit Log Filtering

This section describes how to filter the **Audit Log** to find the most relevant log messages.

Procedure

1. Go to **Logs > Audit Log**. Click the **Severity** next to the search bar, and then a drop-down menu appears.
2. There are two types of log filtering based on the drop-down menu. Choose from either one listed below depending on your needs.
 - Select the **User ID** or **Client IP**, and then type the search strings in the search field for viewing logs related to certain user account or IP address.
 - Select the **Severity**, a search box with an arrow pointing downwards appears. Tap on it to see the options listed below. Select one of them for viewing the log records by different levels.
 - Emergency
 - Alert
 - Critical

- Error
 - Warning
 - Notice
 - Information
 - Debug
3. Click the search icon next to the search bar, and then the screen will display the search result.
 4. To clear the search criteria, close the filtering criteria appears above the **Export** button.
-

Chapter 7

Administration

This chapter introduces the StellarOne web console's administration settings, mainly grouped into four categories: **Account**, **Notification**, **Update**, and **System**.

Topics in this chapter includes:

- **Account**
 - *Account Management on page 7-3*
 - *Single Sign-On on page 7-11*
- **Notification**
 - *SMTP Settings and Notification on page 7-16*
 - *Scheduled Report on page 7-17*
 - *Syslog Forwarding on page 7-19*
- **Update**
 - *Proxy Settings on page 7-20*
 - *Downloads/Updates on page 7-21*
 - *Importing Firmware on page 7-26*
 - *About the License Screen on page 7-28*

- **System**

- *System Time on page 7-37*
- *Log Purge on page 7-37*
- *Importing SSL Certificate on page 7-39*
- *OT Intelligent Trust on page 7-40*
- *Service Integration on page 7-40*

Account

Topics in this section includes

- [Account Management on page 7-3](#)
- [Single Sign-On on page 7-11](#)

Account Management

Go to **Administration > Account Management** to manage user accounts for accessing the StellarOne web console.

The **Account Management** screen have two tabs: **Users** and **Roles**. One allows users to manage accounts; the other one provides information about different privileges for different accounts.

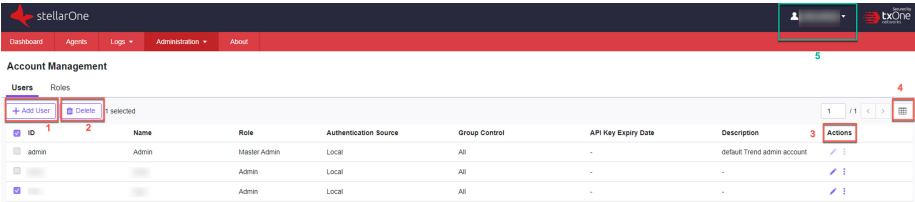


FIGURE 7-1. Account Management Screen

TABLE 7-1. About Account Management Screen - Users

ITEM	DESCRIPTION
(1) +Add User	This button allows you to add account(s) for accessing StellarOne web console. See Add Accounts on page 7-7 for instructions.
(2) Delete	This button allows you to delete account(s). See Delete Accounts on page 7-9 for instructions.

ITEM	DESCRIPTION
(3) Actions	<p>The Edit button allows you to edit a single user account. See Edit Accounts on page 7-9 for instructions.</p> <p>The three dots More Actions button allows you to:</p> <ul style="list-style-type: none"> • Generate an API Key: see Generate an API Key on page 7-10 for instructions. • Delete a single user account: see Delete Accounts on page 7-9 for instructions.
(4) Screen display setting	<p>By clicking this button, you can customize the screen display by:</p> <ul style="list-style-type: none"> • selecting how many items to be displayed on one page • hiding certain contents by unchecking items related to the titles in the Customize Table Display window.
(5) Account icon	<p>Click the account icon at the top-right corner of the screen to change your password or log off.</p>

See [Account Types on page 7-4](#) for more information about the **Roles** page.

Account Types

StellarOne user accounts are categorized into three types as listed below.

TABLE 7-2. StellarOne Account Types

ACCOUNT TYPES	ACCESS RIGHTS	PRIVILEGES
Admin	Full control	<ul style="list-style-type: none"> • Manage StellarOne: The privilege of configuring system settings • Manage Group: The privilege of creating, moving, or deleting groups • Account Management: The privilege of managing StellarOne accounts • Policy Configuration: The privilege of defining policy for Agents such as USB Control and Intelligent Runtime Learning

ACCOUNT TYPES	ACCESS RIGHTS	PRIVILEGES
Operator	Asset control	<ul style="list-style-type: none"> • Manage Group: The privilege of creating, moving, or deleting groups • Policy Configuration: The privilege of defining policy for Agents such as USB Control and Intelligent Runtime Learning
Viewer	Read only	<ul style="list-style-type: none"> • Read only for the dashboard, agent events logs, agent policy configurations, and StellarOne information. • Allowed to change his/her own account password.

Server Accounts Overview

TXOne StellarOne features web console accounts with different privileges and limitations. Use these accounts to configure StellarOne and to monitor or manage StellarProtect agents. The following table outlines typical StellarOne tasks and the account privileges required to perform them.

TABLE 7-3. StellarOne Account Types

TASK	ACCOUNT PRIVILEGE ALLOWED		
	ADMIN	OPERATOR	VIEWER
Dashboard	√	√	√
Configure Application Lockdown	√	√	
Configure Maintenance Mode	√	√	
Configure Device Control	√	√	
Add trusted files	√	√	
Add trusted USB devices	√	√	

TASK	ACCOUNT PRIVILEGE ALLOWED		
	ADMIN	OPERATOR	VIEWER
Scan now	√	√	
Update Approved List	√	√	
Update agent components	√	√	
Deploy agent patch	√	√	
Check connection	√	√	
Deploy policies	√	√	
Policy refresh interval	√	√	
Collect event logs	√	√	
Import / Export (Approved List / agent configuration)	√	√	
Organize (edit description / move / delete)	√	√	
Configure group policy	√	√	
Configure global policy	√	√	
Monitor agent event logs	√	√	√
Monitor server event logs	√	√	
Monitor system logs	√	√	

TASK	ACCOUNT PRIVILEGE ALLOWED		
	ADMIN	OPERATOR	VIEWER
Monitor audit logs	√	√	
Account management	√		
Single Sign-On	√		
System time settings	√		
Syslog forwarding	√		
Log purge	√		
Scheduled report	√		
Notification settings	√		
SMTP settings	√		
Proxy settings	√		
Downloads / Updates	√		
Firmware update	√		
SSL Certificate	√		
License management	√		

Add Accounts

This section describes how to add user accounts for accessing StellarOne web console.

Procedure

1. Log on to the web console using an account with the **Admin** role.

**Note**

- The logon credentials entered here are case-sensitive.
 - Only the account with the **Admin** role can manage user accounts.
-

2. Go to **Administration > Account Management**.
3. Click **Add User** button, and then the **Add User Account** window appears.
4. Specify the **Authentication Source (Local or SAML Identity Provider)**.
 - To add a **Local** user, specify the **ID** and **Name**.
 - To add an **SAML Identity Provider** user, specify **Email for SAML Account Mapping** and **Name**.

**Note**

To allow an SAML Identity Provider user to log in using Single Sign-On (SSO), click the **Single Sign On Configuration** link. Please refer to [Single Sign-On on page 7-11](#) for procedures.

**Note**

The **ID**, **Name**, and **Email for SAML Account Mapping** entered here are case-sensitive.

5. **Role:** Select among the account roles **Admin**, **Operator** or **Viewer** (Default). Please refer to [Account Types on page 7-4](#) for more details on the account privileges.
 - For a **Local** user, specify the **Local Password** and re-type it for confirmation.
6. **Group Control:** Select the groups the target account is allowed to access or view.

7. Click **Confirm** to complete the user account creation.
-

Delete Accounts

This section describes how to delete user accounts that are no longer needed.

Procedure

1. Log on to the web console using an account with the **Admin** role.
-



Note

- The logon credentials entered here are case-sensitive.
 - Only users logged on with the **Admin** role can manage user accounts.
-

2. Go to **Administration > Account Management**.
 3. There are two ways of deleting user accounts.
 - To delete only one user account at a time, under the **Actions** column, click the trash-can icon corresponding to the target user account.
 - To delete multiple user accounts at a time, click the checkboxes next to the user accounts you want to delete, and then click the **Delete** button next to the **Add User** button.
 4. The **Delete User Account** window appears.
 5. Click **Confirm** to delete the user account(s).
-

Edit Accounts

This section describes how to edit user accounts that have been created.

Procedure

1. Log on to the web console using an account with the **Admin** role.

**Note**

- The logon credentials entered here are case-sensitive.
 - Only the account with the **Admin** role can manage user accounts.
-

2. Go to **Administration > Account Management**.
3. Under the **Actions** column, click the edit icon corresponding to the target user account.
4. The **Edit User Account** window appears.
 - For a **Local** user, the **Role, Name, Password, Group Control,** and **Description** of an account can be edited.
 - For an **SAML Identity Provider** user, the **Role, Name, Group Control,** and **Description** of an account can be edited.

**Note**

To allow an SAML Identity Provider user to log in using Single Sign-On (SSO), click the **Single Sign On Configuration** link. Please refer to [Single Sign-On on page 7-11](#) for procedures.

5. Click **Confirm** to complete editing user account(s).
-

Generate an API Key

Users can generate API keys and query data from agents via the open API. The expiration dates of the API keys can be set for different user accounts to increase account management efficiency.

Procedure

1. Log on to the web console using an account with the **Admin** role.

**Note**

- The logon credentials entered here are case-sensitive.
-

2. Go to **Administration > Account Management**.
 3. Under the **Users** tab, find the user ID you want to modify and go to the kebab menu under **Actions** at the right of the screen.
 4. Click on the kebab menu, and then select the **Generate an API Key** option.
 5. The **Generate an API Key** window appears. Click the date picker and choose an expiration date on the pop-up calendar. Click **Confirm**.
 6. An API key is generated. Click the clipboard for copying the generated API key.
-

**Important**

Make sure to back up the copied API key before proceeding to the next step. The API key will not be displayed again for security reasons.

7. Click **OK**.
 8. Check the result under the **API Key Expiry Date** or mouse over above the kebab menu of the user account, and the expiration date of the API key will appear.
-

Single Sign-On

Users who log on with the SAML Identity Provider (IdP) user account can choose to complete the Single Sign-On (SSO) configuration, which allows to access multiple applications and services using a single set of login credentials.

Procedure

1. Log on to the web console using an account with the **Admin** role.



Note

The logon credentials entered here are case-sensitive.

2. Go to **Administration** > **Single Sign-On**.
 3. Click the **Download** button to download the StellarOne metadata XML file.
 4. Import the StellarOne metadata XML file to your IdP.
-



Note

See [Configuring ADFS as SAML IdP for SSO on page 7-13](#) to configure the specific settings required to integrate your IdP with StellarOne SSO.

5. Download the IdP metadata XML file from the following URL on a computer connected with the IdP server:

```
https://<adfs hostname>/federationmetadata/2007-06/  
federationmetadata.xml
```

6. Click the **Upload** button to upload the IdP metadata XML file to StellarOne web console to complete the SAML 2.0 SSO configuration.
-



Important

The IdP metadata XML file must be re-uploaded if there is a configuration change on the IdP.

7. After the IdP metadata XML file is uploaded, the **Test Connection** button will appear.
8. Click **Test Connection** to test the connectivity between the StellarOne and IdP servers.

**Note**

If the IdP and StellarOne servers are connected to different networks, the IdP connection test may fail, yet the SAML SSO may still work. Try logging in with SSO and if invalid logon error message appears, see [Resolving the SSO Issue on page 7-14](#) to check the email settings in IdP server or the system time synchronization in IdP and StellarOne servers.

Configuring ADFS as SAML IdP for SSO

The following instructions takes Windows ADFS server as an example for how to integrate your SAML IdP with StellarOne SSO.

Procedure

1. Open Windows **Server Manager** and go to **Tools > AD FS Management**.
2. Right-click on **Relying Party Trusts** and select **Add Relying Party Trusts**.
3. The **Add Relying Party Trust Wizard** appears. Go through the steps and ensure you configure the specific settings as described below:
 - a. **Import StellarOne file:** In **Select Data Source** step, select **Import data about the relying party from a file** and import the StellarOne metadata xml file.
 - b. Proceed with the steps and in the **Finish** step, ensure you select **Open the Edit Claim Rules dialog...** and click **Close**.
 - c. **Add rules:** The **Edit Claim Rules for...** window appears. Click **Add Rule...** and the **Add Transform Claim Rule Wizard** appears.
 1. In **Choose Rule Type**, select **Send LDAP Attributes as Claims**.
 2. In **Configure Claim Rule**, select **Active Directory** from the **Attribute store** menu. Ensure you select **E-Mail-Addresses** and **E-Mail Address** as the LDAP attributes and outgoing claim types, and then click **Finish**.

3. Click **Add Rule** to add the second rule.
 4. In **Choose Rule Type**, select **Transform an Incoming Claim** and proceed. Ensure you select **E-Mail Address**, **Name ID**, and **Email** as the incoming claim type, outgoing claim type, and outgoing name ID format, and then click **Finish**.
4. The window displaying the two rules configured for StellarOne SSO will appear. Proceed with downloading the IdP metadata file. See [Single Sign-On on page 7-11 Step 5](#) for more details.

Resolving the SSO Issue

Procedure

1. Open the **Users** folder under the **Active Directory Users and Computers** in IdP server.
2. Right-click on the user account used for SSO, and then go to **Properties** > **General**.
3. Check the **E-mail** field. Make sure the email input here is consistent with the account email used for accessing StellarOne web console.

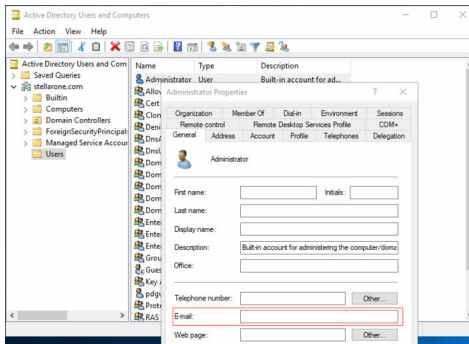


FIGURE 7-2. Resolving SSO Issue - Email Check

4. Make sure the system time in IdP and StellarOne servers is synchronized. You can choose one of the ways listed below to configure the associated settings.

- a. Sync time with an NTP server via StellarOne:
 1. Log on StellarOne and go to **Administration > System Time**.
 2. Click the **Synchronize system time with an NTP server** to enable it.
 3. Click **Test Synchronization** to check if the sync was successful.

**Note**

The default NTP server is pool.ntp.org.

- b. Sync time via VMware Tools:
 1. Ensure the time in the IdP server and the host PC running the StellarOne Virtual Machine (VM) is synchronized.
 2. Open the VM settings of StellarOne and go to **Options > VMware Tools**.
 3. Click the checkbox of **Synchronize guest time with host**, and then click **OK**.

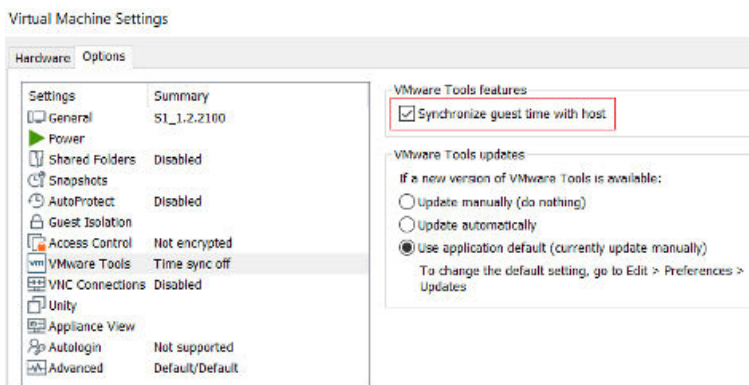


FIGURE 7-3. Virtual Machine Settings - Time Synchronization

Notification

Topics in this section includes:

- [SMTP Settings and Notification on page 7-16](#)
- [Scheduled Report on page 7-17](#)
- [Syslog Forwarding on page 7-19](#)

SMTP Settings and Notification

The settings allow users to receive notifications of warning or outbreak events by emails.

Procedure

1. Go to **Administration > SMTP Settings** for specifying the SMTP server setting required for notification sending.
2. Specify the **Server address**, **Port**, and **Sender**.
3. Specify the **Security Mode** by clicking **STARTTLS**, **SMTPS**, or **None**.
4. (Optional) If the SMTP server requires authentication, toggle on **SMTP server requires authentication**. Specify the **User name** and **Password** as the SMTP server authentication credential.
5. Click the **Send Test Email** button to send a test email from StellarOne (This step is essential for *Step 13*).
6. Click **Save** to complete the SMTP setting.
7. Go to **Administration > Notification** for notification criteria and email setting.
8. Under the **Warning Level Agent Events**, click the **Send warning level agent events** toggle to enable it.

**Note**

When the toggle is enabled, StellarOne console will send a notification to the specified email when an incident that triggers a **Warning** level events occurs.

9. Under the **Outbreak**, click the **Send outbreak notifications** toggle to enable it.
-

**Note**

When the toggle is enabled, StellarOne console will send a notification to the specified email when more than a specified number of open warning messages have appeared in a specified time period.

10. Define an outbreak by the number of detections and the detection period.
 - Specify the number of occurrences of an event in the field of **Number of warnings in a time period** (1- 20000).
 - Specify the time frame during which the event has occurred in the field of **The time period of those warnings** (1 - 60 minutes).
 11. Under **Email Notifications**, specify the email address for receiving the notifications in the **Send to** field.
 12. Click **Save** to complete the setting.
 13. Go to the specified email box to check if you receive the test email sent from StellarOne (see *Step 5*).
-

Scheduled Report

By configuring the **Scheduled Report**, users can receive a list of all reports that automatically generate on a user-defined schedule. The **Scheduled Report** screen also provides basic information about previously configured schedules and recipients, as well as allows users to enable and disable sending scheduled reports.


Procedure


1. Go to **Administration > Scheduled Report**.
2. Toggle on **Send scheduled reports**.

**Note**

By default, the **Scheduled Report** is disabled.

3. Three available settings appear on the **Scheduled Report** screen.

SETTINGS	DESCRIPTION
Report content	<p>Event Type:</p> <ul style="list-style-type: none"> • Blocked Event History • Top 10 Endpoints with Blocked Events • Top 10 Blocked Files <p>Time Period: A drop-down menu for users to choose preferred time period during which the above-mentioned events occur</p> <ul style="list-style-type: none"> • Last 7 days • Last 14 days • Last 30 days • Last 3 months • Last 6 months
Schedule	<p>Set the frequency and start time for the scheduled reports on a daily, weekly, or monthly basis.</p> <hr/> <p> Note It is recommended not to select the date 29th, 30th, or 31st for monthly update frequency. This helps prevent the system from bypassing the update in the month that does not contain the date 29th, 30th, or 31st.</p> <hr/>

SETTINGS	DESCRIPTION
Recipients	<p>A valid email address is required for specifying the report recipient.</p> <hr/> <p> Note When entering multiple email addresses, be sure to use the semicolon character to separate them.</p>

4. Click **Save** to save the settings.

Syslog Forwarding

Users can forward the Server and Agent Event logs to an external Syslog server for increasing monitoring and management capabilities. TXOne StellarOne console forwards logs in the Common Event Format (CEF). Make sure your Syslog server supports the Common Event Format (CEF).

Procedure

1. Go to **Administration > Syslog Forwarding**.
2. Click the **Forward logs to syslog server (CEF only)** toggle to switch on the function.
3. Specify the **Server Address**, **Port**, and **Protocol** of the Syslog server.
4. Click **Save** to complete the settings.

See [StellarProtect/StellarProtect \(Legacy Mode\) Syslog Content - CEF on page A-88](#) or [StellarOne Syslog Content - CEF on page A-94](#) in the Appendices for details about the logs forwarded in the Common Event Format (CEF).

Update

Topics in this section includes:

- [Proxy Settings on page 7-20](#)
- [Downloads/Updates on page 7-21](#)

- [Importing Firmware on page 7-26](#)
- [License on page 7-27](#)

Proxy Settings

There are three proxy settings: Proxy Settings for StellarOne to internet, Proxy settings for StellarOne to Agent communications, and Proxy Settings for Agent to StellarOne communicates.

Procedure

1. Go to **Administration > Proxy**.
 2. Toggle on the **Proxy Settings...** to enable below settings.
 - **Proxy Settings for StellarOne to internet**
 - **Proxy Settings for StellarOne to Agent communications**
 - **Proxy Settings for Agent to StellarOne communications**
 3. To configure proxy settings for updates:
 - a. Select the HTTPS or HTTP protocol.
-



Note

For **Proxy Settings for Agent to StellarOne communications**, since currently the StellarProtect does not support HTTPS proxy, if the destination is an HTTPS server, please use the HTTP proxy for connection.

- b. In the **Server Address** field, specify the IPv4 address or FQDN of the proxy server.
- c. Specify the **Port**.
- d. If your proxy server requires authentication, select **Proxy server requires authentication** and enter your credentials.
- e. Click **Save**.

**Tip**

To configure the proxy settings used by StellarOne when sending messages to StellarProtect:

- **Before installation:** Add the proxy information to the configuration file in the Agent's installer package and save the proxy settings. The settings will then be included in the Agent's installer package after the Agent's installer package is repacked.
 - **After installation:** Use the `opcnd.exe` or `SLCmd.exe` Command Line Interface tool on the local StellarProtect or StellarProtect (Legacy Mode) Agent.
-

Downloads/Updates

The **Downloads/Updates** page allows users to execute below tasks:

- Configuring scan component for StellarOne
- Downloading the Agent Installer Package or `Group.ini` file for [Group Mapping on page 7-24](#).
- Importing or deleting patch files for the agents

Configuring Scan Component for StellarOne

Procedure

1. Go to **Administration > Downloads/Updates > StellarOne**.
2. To start the component update for StellarOne immediately, click the **Update Now** button in the **Scan Component** section.

**Note**

- By clicking the **Update Now**, StellarOne will download and update the latest components. All of the pattern and engine versions available are listed under the **Update Now** button.
 - You can refer to the **Last Updated:** near the **Update Now** button for the last time the scan component was updated.
-

3. To schedule for the component update, find and click the **Scan Component Update Schedule (StellarOne)** at the bottom of the screen.
 - a. The **Scan Component Update Schedule (StellarOne)** window appears.
 - b. Toggle on the **Schedule Update**.
 - c. Click the radio buttons next to **Frequency** to set the frequency by **Daily**, **Weekly**, or **Monthly**.
-

**Important**

It is recommended NOT to select the date 29th, 30th, or 31st for monthly update frequency. This helps prevent the system from bypassing the update in the month that does not contain the date 29th, 30th, or 31st.

- d. Click the **Start Time** to determine when to start the scheduled scan component update.
4. To specify the download source for StellarOne regarding different network configurations, find and click the **Scan Component Update Source** at the bottom of the screen.
 - a. The **Scan Component Update Source** window appears.
 - b. In the **Scan Component Update Source (StellarOne)** section:
 - If the StellarOne server can connect to the ActiveUpdate server, select the **ActiveUpdate server**, the component update will be downloaded directly from the ActiveUpdate server.

- If the StellarOne server can not connect to the ActiveUpdate server or if users host an update server in an internal network, select **Other update source** and specify the URL address in the text field.
5. To specify the download source for agents regarding different network configurations or agent types, find and click the **Scan Component Update Source** at the bottom of the screen.
 - a. The **Scan Component Update Source** window appears.
 - b. In the **Scan Component Update Source (Agents)** section:
 - If the agents can connect to StellarOne server, select **Update from StellarOne** to download the component update directly from the StellarOne server.
 - If the agents can not connect to StellarOne server or if they are standalone agents, select **Other update source** and specify the URL address in the text field.
-

Downloading Agent Installer Package/Group.ini File

Procedure

1. Go to **Administration > Downloads/Updates > Agent**.
2. To download the latest Agent Installer Package. Click **Download**.

StellarOne **Agent**

Download Installer Package

① If the communication between StellarOne and Agents uses proxy, configure the settings on the [Proxy](#) page before downloading the installer package.

② To register Agent to a specific group directly, you can [download Group.ini](#) with the group ID and name, then add it into the installer package.

> [Learn More](#)

English

Patch

① New patch can be imported here, please deploy it to target endpoint on [Agents](#) page.

StellarProtect

<input type="checkbox"/> File Name	Version
<input type="checkbox"/> txone_sp_full_patch_win_en.zip	2.2.0.1040
<input type="checkbox"/> txone_sp_2.2.1039_full_patch_win_en.zip	2.2.0.1039

FIGURE 7-4. Downloads/Updates Screen

A zipped folder is downloaded. Extract the folder and proceed with the installation for the agents. Please refer to the [StellarProtect Installation Guide](#) for more details.

3. (Optional) If the StellarOne uses proxy to communicate with the agents, click the **Proxy** link or go to **Administration > Proxy** to complete the proxy configuration before downloading the installer package. Please refer to [Proxy Settings on page 7-20](#) for detailed procedures.
4. (Optional) To directly register the agent to a specific group via StellarOne console, click the **download a Group.ini** link and add it into the agent's installer package. Please refer to [Group Mapping on page 7-24](#) for more details.

Group Mapping

This function allows users to directly register agent to a specific group via the StellarOne web console.

Procedure

1. Go to **Administration > Downloads/Updates**.
 2. Select the **Agent** tab.
 3. Click **Download** to download the Installer Package.
 4. Click the **download Group.ini** link.
 5. The **Select a group** window appears.
 6. Select a group for the target agent and click **Download**. Click the **Close** button to close the window.
 7. A file named `Group.ini` has been downloaded. Place the `Group.ini` file as the top-level file in the installer package of the target agent.
 8. Run the installation on the target agent. Make sure the agent is connected to StellarOne console during the installation process.
 9. Users can check the StellarOne console and the on-site target agent to see if the agent is successfully registered.
-

Importing/Deleting Agent's Patch

Procedure

1. Go to **Administration > Downloads/Updates > Agent > Patch**.
2. Select **StellarProtect** or **StellarProtect (Legacy Mode)** to determine the target agent.
3. Click **Import** to import the target patch file.
4. A **Import Patch** window appears. Click the radio button to determine the target agent.
5. Click **Select File** to select the patch file to import.



Important

Be sure to select the patch file that matches the target agent.



Tip

Click the **Agents** link to be directed to the **Agents** screen, and then use the **Update** button to deploy the imported patch to the target agents. See [Deploy Agent Patches on page 4-29](#) for instructions.

6. To remove existing patch files on StellarOne, select the target files and then the **Delete** button appears next to the **Import** button. Click **Delete** to remove the selected entries.
-

Importing Firmware

Procedure

1. Go to **Administration > Firmware**.
2. Click the **Import** button to import the firmware patch file (e.g. acus.fw_2.0.xxxx.acf) to StellarOne.
3. The **Firmware Update** window appears. The **Version** shows the current StellarOne build version, the **Release Date** and **Description** show the information for the StellarOne patch file.
4. Click **Apply** to apply the patch to StellarOne.
5. Read the upgrade notice carefully.
6. Click **Install Now** to implement the update or **Abort** to stop the update.

FIRMWARE

Update downloaded. StellarOne is ready to install. Please click the Install button to start the installation. After completing installation, the system may restart all services.

⚠ Notice

- The installation may take 5 to 10 minutes to finish. Please do not shut down the StellarOne during the installation.
- We highly recommended you to back up your data before starting the installation.
- The system will not support downgrading to an earlier version.

📄 Install Now

⏹ Abort

FIGURE 7-5. Firmware Update Notice



Note

Before executing the firmware upgrade, please create a back up of the VM files first.

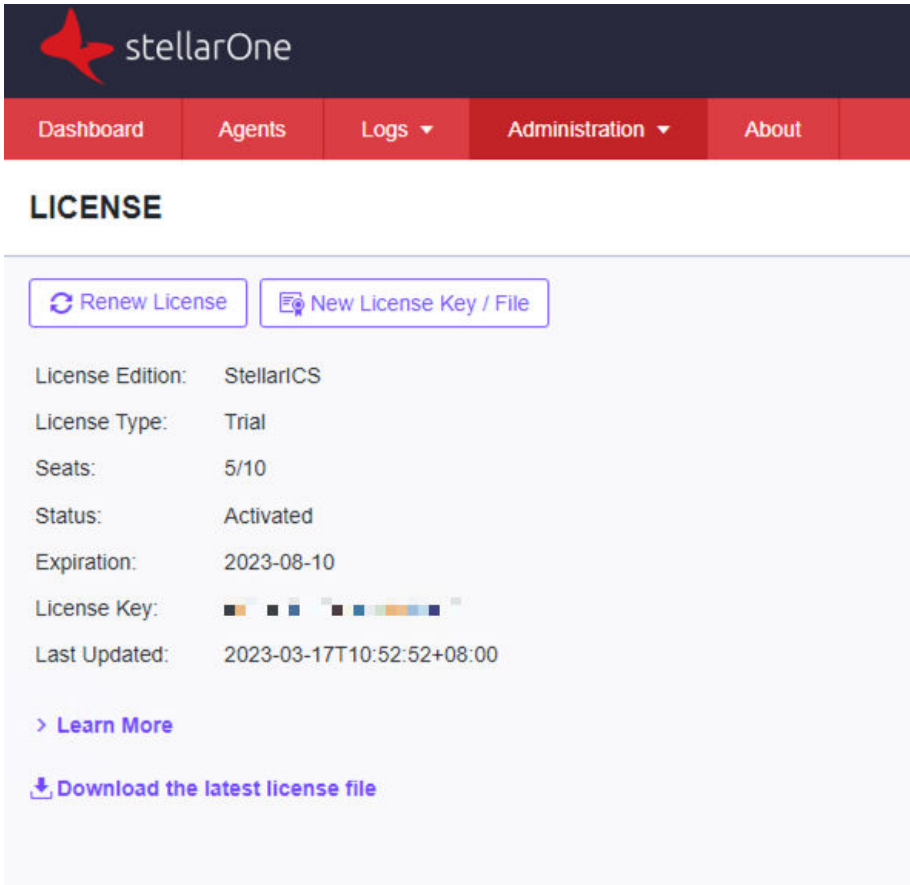
License

Topics in this section includes:

- [About the License Screen on page 7-28](#)
- [License Management on page 7-30](#)
- [License Editions on page 7-34](#)

About the License Screen

Go to **Administration** > **License**. The following table lists details about the **License** page.



stellaOne

Dashboard Agents Logs Administration About

LICENSE

[Renew License](#) [New License Key / File](#)

License Edition: StellarICS

License Type: Trial

Seats: 5/10

Status: Activated

Expiration: 2023-08-10

License Key: [masked]



Last Updated: 2023-03-17T10:52:52+08:00


[> Learn More](#)

[Download the latest license file](#)

FIGURE 7-6. The License Screen

TABLE 7-4. About the License Screen

ITEM	DESCRIPTION
Renew License Key	This button is for license renewal using the same license key. Refer to Renew License with the same License Key on page 7-31 for more details.
New License Key/ File	<p>This button is for license activation using new license key or license file. Refer to New License Key/File on page 7-33 for more details.</p> <hr/> <p> Note This button can also be used for other purpose: license renewal using the license file. Refer to Renew License by Importing License File on page 7-31 for more details.</p>
License Edition	Displays current license edition for Stellar product. Refer to License Editions on page 7-34 for more details.
License Type	<ul style="list-style-type: none"> • Full: a full version that is officially authorized. • Trial: a trial version with excluded features or limited functions. • Perpetual: provides permanent use and 5-year technical support.
Seats	<p>Specifies current number of agents managed by StellarOne and the total number of agents that can be managed by StellarOne. For example, Seats: 2/10 means:</p> <ul style="list-style-type: none"> • 2 agents are currently managed • Up to 10 agents can be managed <hr/> <p> Note Overseat is triggered when seat in use exceeds the seat count; the agents that can not be managed by StellarOne due to overseat will be classified as "Inactive Agents" on the Agents screen. See Filter Options for Agents/Groups on page 4-18 for more details.</p>

ITEM	DESCRIPTION
Status	<ul style="list-style-type: none"> • Activated: The existing license is effective. • Expired: The existing license is out of date. <hr/> <div style="display: flex; align-items: flex-start;">  <div> <p>Note</p> <p>It is recommended to renew license promptly to protect your devices against cybersecurity threats. Refer to one of the methods listed below for license renewal.</p> <ul style="list-style-type: none"> • Renew License with the same License Key on page 7-31 • Renew License by Importing License File on page 7-31 </div> </div> <hr/>
Expiration	Displays the effective date of existing license.
License Key	The license key that is required for activating StellarOne.
Last Updated	Displays the last time the License Key is updated.
Learn More	The link directs users to the Online Help web page for more details on license.
Download the Latest License File	The link is used to download the latest license file to renew license for standalone agents.

License Management

Users can renew license or activate new license via the StellarOne web console.

License Renewal

Choose one of the ways to renew license based on the license data available from your support provider:

- [Renew License with the same License Key on page 7-31](#)
- [Renew License by Importing License File on page 7-31](#)

Renew License with the same License Key

Procedure

1. Go to **Administration > License**
 2. Click the **Renew License Key** button.
 3. A message with **The License has been updated successfully** appears. The **Last Updated** shows the latest license renewal date and time.
-

Renew License by Importing License File

Procedure

1. Go to **Administration > License**
 2. Click the **New License Key / File** button.
 3. The **New License** window appears.
 4. Click **License File**.
 5. Select the license file (a .txt file) to import.
-

**Note**

If you don't have the license file on hand, refer to [Getting the License File on page 7-31](#).

6. Click **Apply**.
 7. A success message appears. The updated license information will be shown on the **License** page.
-

Getting the License File

The license file can be used for license renewal or new license activation. To get a license file, follow below procedures.

Procedure

1. Go to **Administration > License**
2. Click the **New License Key / File** button.
3. The **New License** window appears.
4. Click **License File**.
5. Click **Copy Download Link for getting the License File** at the bottom of the **New License** window.



Important

A license key is required for downloading a license file.

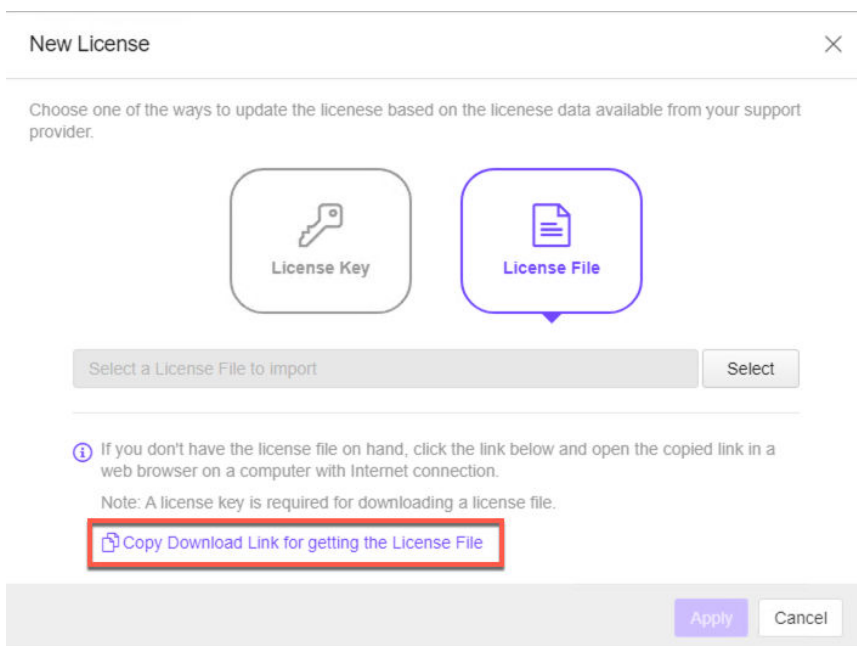
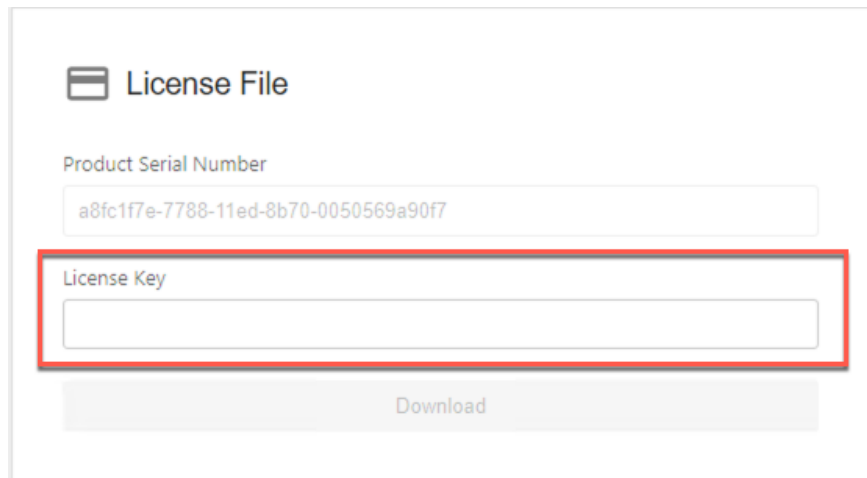


FIGURE 7-7. Copy Download Link for License File

6. **The Download Link has been copied** toast message appears.
7. Open the copied link in a web browser on a computer with Internet connection.
8. You will be directed to the TXOne **License File Management** screen. Specify your license key in the **License Key** field, and then click **Download**.



The screenshot shows a web interface for 'License File Management'. At the top, there is a header 'License File' with a menu icon. Below it, there is a 'Product Serial Number' field containing the text 'a8fc1f7e-7788-11ed-8b70-0050569a90f7'. Underneath that is a 'License Key' field, which is highlighted with a red rectangular border. At the bottom of the form is a 'Download' button.

FIGURE 7-8. TXOne License File Management

9. A pop-up window appears showing the license information. Read it carefully and click **Yes** for downloading the license file.

New License Key/File

If users need to activate a new license key or license file, follow below procedures.

Procedure

1. Go to **Administration > License**.
2. Click **New License Key / File**.

3. The **New License** window appears. Choose one of the ways:
 - Click **License Key** and specify the new license key in the text field below.
 - Click **License File** and select the license file (a .txt file) to import.

**Note**

If you don't have the license file on hand, refer to [Getting the License File on page 7-31](#).



4. Click **Apply**.
5. A message with **The License is activated successfully** appears.

License Editions

See below as the three kinds of license editions for the TXOne Stellar 3.1. The StellarProtect supports Windows 7 or later versions; the StellarProtect (Legacy Mode) supports legacy platforms such as Windows XP/2000.

TABLE 7-5. License Editions

EDITION	PRIMARY FUNCTION	DURATION
StellarICS	StellarProtect Agent: <ul style="list-style-type: none"> • Multi-Method Threat Prevention (Real-Time Scan) • Application Lockdown 	Annual
	StellarProtect (Legacy Mode) Agent: <ul style="list-style-type: none"> • Threat Prevention (Real-Time Scan) • Application Lockdown 	

EDITION	PRIMARY FUNCTION	DURATION
StellarKiosk	StellarProtect Agent: <ul style="list-style-type: none"> • Multi-Method Threat Prevention (Real-Time Scan) 	Annual <hr/>  Note StellarKiosk was named StellarMix before the TXOne Stellar version 2.0.
	StellarProtect (Legacy Mode) Agent: <ul style="list-style-type: none"> • Threat Prevention (Real-Time Scan) • Application Lockdown 	
StellarOEM	StellarProtect Agent: <ul style="list-style-type: none"> • Application Lockdown 	Perpetual <hr/>  Note <ul style="list-style-type: none"> • StellarOEM provides permanent use and 5-year technical support for the TXOne Stellar. • This license edition does not support features such as scan and agent component update. • StellarOEM was named Perpetual before the TXOne Stellar version 2.0.
	StellarProtect (Legacy Mode) Agent: <ul style="list-style-type: none"> • Application Lockdown 	

Features of License Editions

StellarICS, StellarKiosk, and StellarOEM license editions provides different features, allowing users in diverse industries to select based on their specific needs.

TABLE 7-6. Features of License Editions

FEATURES	STELLARICS	STELLARKIOSK	STELLAROEM
Multi-Method Threat Prevention	√	√	-
Operation/Application Lockdown	√	Windows XP/2000 only	√
Operations Behavior Anomaly Detection	√	√	√
Industrial Application and Certificate Repository	√	-	√
OT Application Safeguard	√	-	√
Intelligent Runtime Learning (Predictive Machine Learning)	√	-	√
Trusted USB Device Control	√	√	√
Legacy Systems Compatibility	√	√	√

System

Topics in this section includes:

- [System Time on page 7-37](#)
- [Log Purge on page 7-37](#)

- [Importing SSL Certificate on page 7-39](#)
- [OT Intelligent Trust on page 7-40](#)
- [Service Integration on page 7-40](#)

System Time

You can configure the system time settings for the StellarOne web console.

Procedure

1. Go to **Administration > System Time**.
2. Two options are available for configuring StellarOne system time. In the **Date and Time** section:
 - If you want to set the system time manually, click the Edit icon to specify the date and time, and then click **Apply** to save the setting.
 - If you want to align StellarOne system time with an NTP server, click the **Synchronize system time with an NTP server** toggle to enable it. Click **Test Synchronization** to check if the sync was successful.



Note

The default NTP server is pool.ntp.org.

3. In the **Time Zone** section, click the downward arrow in the blank bar. A drop-down menu with global time zone appears.
 4. Select the appropriate time zone for the system, and then click **Save** to complete the settings.
-

Log Purge

This feature allows users to manage the volume of log files for optimizing the disk space usage for StellarOne.

Procedure

1. Go to **Administration > Log Purge**.
2. Choose one of the ways listed below for log purge settings.

- **Purge Now:**

Use this setting to purge logs immediately.

- a. Click the drop-down menu next to **Purge**, and then select the log types to be purged.
 - All Logs
 - Agent Events
 - Server Events
 - System Log
 - Audit Log
- b. Click the drop-down menu next to **older than**, and then select a specified time frame. The files generated before the selected time frame will be removed.
 - No limit
 - 1 month(s), 2 months(s), 3 months(s), 6 months(s), 12 months(s), 18 months(s), 24 months(s), 36 months(s), 48 months(s), 60 months(s)
- c. Click the drop-down menu next to **keep at least**, and then select the minimum number of log entries to keep.
 - 0 entries
 - 10,000 entries, 50,000 entries, 100,000 entries, 500,000 entries, 1,000,000 entries, 5,000,000 entries, 10,000,000 entries
- d. Click **Purge Now** and the event logs will be immediately purged.

- **Automatic Purge:**

Use this setting to set an automatic purge once per day.

- a. Specify the log types you want to purge: **Agent Events, Server Events, System Log, or Audit Log.**
 - b. Specify one of the criteria listed below for the automatic log purge:
 - Click the drop-down menu next to **older than**, and then select a specified time frame. The files generated before the time frame will be removed.
 - No limit
 - 1 month(s), 2 months(s), 3 months(s), 6 months(s), 12 months(s), 18 months(s), 24 months(s), 36 months(s), 48 months(s), 60 months(s)
 - Click the drop-down menu next to **Keep at least**, and then select the minimum number of log entries to keep.
 - 10,000 entries, 50,000 entries, 100,000 entries, 500,000 entries, 1,000,000 entries, 5,000,000 entries, 10,000,000 entries
 - c. Click **Save**, and the event logs will be automatically purged once per day.
-

Importing SSL Certificate

Procedure

1. Go to **Administration > SSL Certificate.**
2. Click **Import Certificate**, and then the **Import Certificate** window appears.
 - Click the **Select file...** next to the **Certificate** option to select the target certificate.

- Click the **Select file...** next to the **Private Key** option to select the target private key.
- (Optional) Specify the passphrase in the **Passphrase** text field.

**Note**

Supported certificate and private key formats include:

- Certificate and private key in PEM format
- Private key in PKCS #1 format with or without encryption
- Private key in PKCS #8 format without encryption

-
3. Click **Import and Restart** to start importing the target certificate.

**Note**

Importing the certificate requires restarting the StellarOne console.

OT Intelligent Trust

When enabled, TXOne OT Intelligent Trust shares anonymous threat information with the Smart Protection Network, allowing TXOne to rapidly identify and address new threats. You can disable TXOne OT Intelligent Trust anytime on this console.

Procedure

1. Go to **Administration > OT Intelligent Trust** .
 2. Click the **Learn More** for visiting TXOne's OT threat research website.
 3. To enable TXOne OT Intelligent Trust, toggle on the **Enable TXOne OT Intelligent Trust (recommended)**.
-

Service Integration

Integrate with Trend Micro Vision One

Users can query for StellarOne malware detection logs via Trend Micro Vision One Search app.



Important

Be sure to complete the deployment of Trend Micro Vision One Service Gateway and enable **Forward proxy** function first, and then obtain the information for Service Gateway settings required in *Step 2* and *Step 3*. Please contact your support provider for more information.

Procedure

1. On StellarOne console, go to **Administration** > **Service Integration**.
2. Specify the IP address and API key of Trend Micro Vision One Service Gateway in **Service Gateway Address** and **Service Gateway API Key**.



Note

The IP address and API key should be obtained from the Trend Micro Vision One Service Gateway Virtual Appliance.

3. Specify the Trend Micro Vision One enrollment token in **Product Connector Enrollment Token**.



Note

The enrollment token is required to register StellarOne to Trend Micro Vision One. The enrollment token will expire within 24 hours if not used after generated from the Vision One Product Connector app.

4. Click **Test Connection** and a success message should appear.
5. Find **Forward Logs to Vision One** section, and then toggle on **Send StellarOne malware detection logs to Vision One**.

6. The **Log Sending Interval** menu appears. Select the frequency in the drop-down menu for sending StellarOne detection logs to Trend Micro Vision One.
7. Click **Save** to complete the settings.



Note

If StellarOne has connected with Trend Micro Vision One successfully, the **Vision One Onboarding Status** should display **Connected**.

Chapter 8

Getting Help and Troubleshooting

Learn about the following topics:

- *Troubleshooting Resources on page 8-2*
- *Contacting TXOne Networks on page 8-5*
- *Other Resources on page 8-6*

Troubleshooting Resources

Before contacting technical support, consider visiting the following TXOne Networks online resources.

Self-Diagnosis

Identify and troubleshoot low disk space issues with StellarOne.

- [Resolving Low Disk Space Issues on page 8-2](#)

Resolving Low Disk Space Issues

To keep you informed of your disk usage, and any potential issues that may arise, StellarOne displays banners or modal windows at certain disk usage thresholds. When encountering such errors, you can check the following table for the features affected and take actions as suggested in the **Workaround** column.

However, the most efficient way to get rid of low disk space error caused by the 2nd HDD is to add more space to the drive or partition. Follow the procedures:

1. Go to **Dashboard** to check [Widgets for Monitoring Disk Usage on page 3-19](#) for the current disk usage.
2. Check the following table for the features that will become unavailable at certain usage thresholds.
3. Extend the drive or partition which is running out of space.

**Note**

- If you take snapshots for the StellarOne virtual machine, ensure the snapshot files be consolidated before extending the partition space.
 - Contact your support provider if you need to fix the low disk space error caused by the 1st HDD.
-

TABLE 8-1. Unavailable Features List due to Low Disk Space

UNAVAILABLE FEATURES	MENU PATH	DESCRIPTION	USAGE THRESHOLD	WORKAROUND
Firmware upgrade	Administration > Update > Firmware	Unable to import the StellarOne firmware for upgrade	<ul style="list-style-type: none"> • 1st HDD disk space less than 3 GB • 2nd HDD disk space on System partition less than 3 GB 	Free up the 2nd HDD disk space on System partition by: <ul style="list-style-type: none"> • Deleting unused patch files • Purging unwanted agent debug logs
Agent patch file import	Administration > Downloads/ Updates > Agent	Unable to import Agent patch files	<ul style="list-style-type: none"> • 2nd HDD disk usage on System partition less than 20% 	
Agent debug tool collection	StellarOne debug page (for SEG purpose)	Unable to collect the debug logs for StellarProtect or StellarProtect (Legacy Mode)	<ul style="list-style-type: none"> • 2nd HDD disk usage on Database partition less than 20% 	
Debug log level selection		Unable to select the Info or Verbose log level. Only the Warn (Default) level logs can be collected.		
Server debug tool collection		Unable to collect the debug logs for the StellarOne server		

Using the Support Portal

The TXOne Networks 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://help.txone.com/>.
2. Click the appropriate button to search for solutions.
3. Use the **Search** box to search for available solutions.
4. If no solution is found, click **Live Chat** or **VoIP** service to submit a support case online.

A TXOne Networks support engineer investigates the case and responds in 24 hours or less.



Important

If the StellarOne virtual machine has been encrypted, ensure that you decrypt it for problem analysis.

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. TXOne Networks 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.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 TXOne Networks

TXOne Networks representatives are available by phone or chat/VoIP services:

TABLE 8-2. TXOne Networks Contact Information

U.S.	+1 (346) 586-7975
Netherland	+31 402-310-122
Taiwan	+886 (2) 7727-5120
Chat/VoIP services	https://help.txone.com/
Website	https://www.txone.com/contact/

- TXOne Networks product documentation:

<https://my.txone.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
- Product serial number and license file, or license key
- Detailed description of the environment where the agent is installed
- Exact text of any error message received

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://my.txone.com/>

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

Appendices

Topics in this section include:

- *Log Descriptions on page A-2*
- *Syslog Content - CEF on page A-88*

Log Descriptions

Topics in this section include:

- [Log Descriptions for StellarProtect on page A-2](#)
- [Log Descriptions for StellarProtect \(Legacy Mode\) on page A-28](#)
- [Server Event Log Descriptions for StellarOne on page A-87](#)

Log Descriptions for StellarProtect

Topics in this section include:

- [Agent Event Log Descriptions for StellarProtect on page A-2](#)
- [Server Event Log Descriptions for StellarProtect on page A-26](#)

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 started	
257	Information	System	Policy applied successfully (Version: %version%)	
258	Information	System	Patch applied File Name: %file_name%	

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
259	Information	System	Patching in progress	After the earlier-applied patch is completed, the system will automatically try to apply this patch: %deferred_file_name%.
513	Information	intelli_av	Application vault update was successful	
514	Information	intelli_av	Real Time Scan enabled	
515	Information	intelli_av	A scheduled scan started	
516	Information	intelli_av	A scheduled scan ended	Folders scanned: %1 Symbolic links: %2 Regular files: %3 Files scanned: %4 Files passed: %5 Threats detected: %6
517	Information	intelli_av	A manually launched scan started	

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
518	Information	intelli_av	A manually launched scan ended	Folders scanned: %1 Symbolic links: %2 Regular files: %3 Files scanned: %4 Files passed: %5 Threats detected: %6
519	Information	intelli_av	A scheduled scan enabled	Next scan will be on %NextScan %.
520	Information	intelli_av	A scheduled scan disabled	
521	Information	intelli_av	A scan manually launched by local user started	
522	Information	intelli_av	A scan manually launched by local user ended	Folders scanned: %1 Symbolic links: %2 Regular files: %3 Files scanned: %4 Files passed: %5 Threats detected: %6

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
523	Information	intelli_av	Incoming file detected malicious and quarantined successfully	File Path: %PATH% File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING% Quarantine Path: %PATH% Reboot Required: %NEED_REBOOT%
524	Information	intelli_av	Local file detected malicious and quarantined successfully	File Path: %PATH% File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING% Quarantine Path: %PATH% Reboot Required: %NEED_REBOOT%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
525	Information	intelli_av	Malicious file execution detected. Infected executable file quarantined successfully	File Path: %PATH% File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING% Quarantine Path: %PATH% Reboot Required: %NEED_REBOOT%
768	Information	anomaly_detect	Operations Behavior Anomaly Detection (Script Behavior) enabled	Mode: %Mode% Level: %Level% Learning time: %LearningTime% day(s)

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
769	Information	anomaly_detect	Script behavior added to baseline	Access User: %USERNAME% ID: %ID% Target Process: %PATH% %ARGUMENT% Parent Process 1: %PATH% %ARGUMENT% Parent Process 2: %PATH% %ARGUMENT% Parent Process 3: %PATH% %ARGUMENT% Parent Process 4: %PATH% %ARGUMENT%
770	Information	anomaly_detect	Script behavior excluded from baseline.	ID: %ID% Target Process: %PATH% %ARGUMENT% Parent Process 1: %PATH% %ARGUMENT% Parent Process 2: %PATH% %ARGUMENT% Parent Process 3: %PATH% %ARGUMENT% Parent Process 4: %PATH% %ARGUMENT%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
771	Information	anomaly_detect	Operations Behavior Anomaly Detection (User Login) enabled	Mode: %Mode% Level: %Level% Learning time: %LearningTime% day(s)
772	Information	anomaly_detect	Operations Behavior Anomaly Detection (Application Behavior) enabled	Mode: %Mode% Level: %Level% Learning time: %LearningTime% day(s)
773	Information	anomaly_detect	Login account added to baseline	Domain: %Domain% Account: %Account% Login Type: %LoginType% Source IP: %IP%
774	Information	anomaly_detect	Login account excluded from baseline	Domain: %Domain% Account: %Account% Login Type: %LoginType% Source IP: %IP%
775	Information	anomaly_detect	Application added to baseline	Application Path: %Path%
776	Information	anomaly_detect	Application excluded from baseline	Application Path: %Path%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
784	Information	anomaly_detect	DLL Injection Prevention enabled	
1280	Information	device_control	Device Control enabled	
1281	Information	device_control	USB device added into trusted device list	Vendor ID: %HEX% Product ID: %HEX% Serial Number: %STRING% Type: permanent or one time
1282	Information	device_control	USB device removed from trusted device list	Vendor ID: %HEX% Product ID: %HEX% Serial Number: %STRING%
1283	Information	device_control	Trusted USB device connected	Vendor ID: %HEX% Product ID: %HEX% Serial Number: %STRING% Active User: %STRING%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
1284	Information	device_control	Trusted USB device disconnected	Vendor ID: %HEX% Product ID: %HEX% Serial Number: %STRING% Active User: %STRING%
1792	Information	lockdown	File access allowed: %PATH%	Access Image Path: %PATH% Access User: %USERNAME% Mode: %MODE% List: %LIST%
1793	Information	lockdown	A new file added to Approved List in Maintenance Mode.	Path: %PATH% Hash: %SHA256_HEXSTR%
1794	Information	lockdown	The hash of an existing file in Approved List was updated in Maintenance Mode	Path: %PATH% Hash: %SHA256_HEXSTR%
1795	Information	lockdown	Approved List initialization started	
1796	Information	lockdown	Approved List initialization completed	Count: %COUNT%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
1797	Information	lockdown	Application Lockdown enabled	Mode: %MODE%
1798	Information	lockdown	DLL/Driver Lockdown enabled	
1799	Information	lockdown	Script Lockdown enabled	
1800	Information	lockdown	Intelligent Runtime Learning enabled	
2048	Information	update	Component update started	
2049	Information	update	Component update ended	
2050	Information	update	Scheduled component update enabled. Next update will be on %NEXT_UPDATE_LOCAL_TIME_STR% (agent's local system time).	
2051	Information	update	Scheduled component update disabled	

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

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

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
4610	Warning	intelli_av	Incoming files scanned, action taken by Next-Generation Antivirus: %PATH%	<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%	<p>Local files were scanned by 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
4612	Warning	intelli_av	Local files scanned, action taken by Next-Generation Antivirus: %PATH%	Local files were scanned by next-generation antivirus. Action was taken according to settings. File Path: %PATH% File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING% Action Result: %INTEGER% Quarantine Path: %PATH%
4613	Warning	intelli_av	Suspicious program execution blocked	Suspicious program execution was blocked. File Path: %PATH% File Hash: %STRING%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
4614	Warning	intelli_av	Suspicious program currently running	Suspicious program is currently running. Process ID: %PID % File Path: %PATH % File Hash: %STRING% File Credibility: %STRING%
4615	Warning	intelli_av	Application execution blocked by Antivirus	Application execution was blocked by antivirus. Process Image Path: %PATH% File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
4617	Warning	intelli_av	Application execution blocked by Next-Generation Antivirus	Application execution was blocked by next-generation antivirus. Process Image Path: %PATH% File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING%
4618	Warning	intelli_av	Failed to quarantine incoming file detected malicious	File Path: %PATH% % File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING%
4619	Warning	intelli_av	Failed to quarantine local file detected malicious	File Path: %PATH% % File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
4620	Warning	intelli_av	Malicious file execution detected. Failed to quarantine the infected executable file	File Path: %PATH% File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING%
4864	Warning	anomaly_detect	Operations Behavior Anomaly Detection (Script Behavior) disabled	
4865	Warning	anomaly_detect	Script Behavior allowed by Operations Behavior Anomaly Detection: %PATH% %ARGUMENT%	Access User: %USERNAME% Parent Process 1: %PATH% %ARGUMENT% Parent Process 2: %PATH% %ARGUMENT% Parent Process 3: %PATH% %ARGUMENT% Parent Process 4: %PATH% %ARGUMENT% Mode: %Mode% Level: %LEVEL%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
4866	Warning	anomaly_detect	Script Behavior blocked by Operations Behavior Anomaly Detection:%PATH% %ARGUMENT%	Access User: %USERNAME% Parent Process 1: %PATH% %ARGUMENT% Parent Process 2: %PATH% %ARGUMENT% Parent Process 3: %PATH% %ARGUMENT% Parent Process 4: %PATH% %ARGUMENT% Mode: %Mode% Level: %LEVEL%
4867	warning	anomaly_detect	Operations Behavior Anomaly Detection (User Login) disabled	
4868	warning	anomaly_detect	Operations Behavior Anomaly Detection (Application Behavior) disabled	

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
4869	warning	anomaly_detect	A user login failure detected by Operations Behavior Anomaly Detection	Domain: %Domain% Account: %Account% Login Type: %LoginType% Source IP: %IP%
4870	warning	anomaly_detect	An abnormal user login detected by Operations Behavior Anomaly Detection	Domain: %Domain% Account: %Account% Login Type: %LoginType% Source IP: %IP%
4871	warning	anomaly_detect	Suspicious application behavior detected by Operations Behavior Anomaly Detection	Program Path: %Path% Program Hash: %SHA256% Program Size: %Size% Certificate: %CertificateSigner% Vendor: %VendorName% % Product: %Product%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
4872	warning	anomaly_detect	An unrecognized application detected by Operations Behavior Anomaly Detection	PID: %PID% Program Path: %Path% Program Hash: %SHA256% Program Size: %Size% Certificate: %CertificateSigner% Vendor: %VendorName% Product: %Product%
4873	warning	anomaly_detect	Malicious application behavior detected by Operations Behavior Anomaly Detection	Program Path: %Path% Program Hash: %SHA256% Program Size: %Size% Certificate: %CertificateSigner% Vendor: %VendorName% Product: %Product%
4880	Warning	anomaly_detect	DLL Injection Prevention disabled	

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
4881	Warning	anomaly_detect	DLL Injection Prevention blocked: %OBJ_PATH%	Threat Image Path: %SUBJ_PATH% Threat User: %USER%
5120	Warning	change_control	Change to an ICS file blocked by OT Application Safeguard.	Blocked Process: %PATH% Target File: %PATH%
5376	Warning	device_control	Device Control disabled	
5377	Warning	device_control	USB access blocked: %PATH %	Access Image Path: %PATH% Access User: %USERNAME% Vendor ID: %HEX % Product ID: %HEX% Serial Number: %STRING%
5378	Warning	device_control	USB autorun.inf file blocked: %PATH%	

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
5379	Warning	device_control	Untrusted USB device connected	Vendor ID: %HEX% Product ID: %HEX% Serial Number: %STRING% Active User: %STRING%
5380	Warning	device_control	Untrusted USB device disconnected	Vendor ID: %HEX% Product ID: %HEX% Serial Number: %STRING% Active User: %STRING%
5888	Warning	lockdown	File access allowed: %PATH%	Access Image Path: %PATH% Access User: %USERNAME% Mode: %MODE% Reason: %ALLOWED_REASON% File hash allowed: %SHA256_HEXSTR% %THROTTLING_INFO_MSG%

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

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
6144	Warning	update	Component update unsuccessful (%AU_ERROR_CODE%)	Update Source: %UPDATE_URL% [Original Version] %COMPONENTS_INFO% [Updated Version] %COMPONENTS_INFO%
8448	Critical	system	Protection stopped manually via protection stop button or CLI	
8449	Critical	system	Protection resumed manually via protection resume button or CLI	
8706	Critical	intelli_av	Real-Time Scan disabled	
9216	Critical	change_control	Maintenance Mode started	
9217	Critical	change_control	Maintenance Mode ended	

Server Event Log Descriptions for StellarProtect

This table lists the server event log descriptions for StellarProtect.

EVENT ID	EVENT
33027	Switch agent (%s) to policy mode
33028	Switch agent (%s) to individual mode
33029	Deploy policy with version: %s
33041	Modify in common use (DLL Injection Prevention, Device Control, OT Application Safeguard, OBAD) setting for [%s] group policy with version: %s
33042	Modify real-time scan settings for [%s] group policywith version: %s
33043	Modify schedule scan settings for [%s] group policywith version: %s
33044	Maintain Device Control list for [%s] group policy with version: %s
33045	Maintain User-Defined Suspicious Object list for [%s] group policy with version: %s
33046	Maintain Operations Behavior Anomaly Detection Watch List for [%s] group policy with version: %s
33047	Maintain Trusted Certification list for [%s] group policy with version: %s
33048	Maintain OT Application Safeguard list for [%s] group policy with version: %s
33049	Modify agent password for [%s] group policy with version: %s
33056	Modify available patch setting for [%s] group policy with version: %s
33057	Maintain an authorized process for [%s] group policy with version: %s
33058	Modify schedule update settings for [%s] group policy with version: %s
33059	Modify lockdown config for [%s] group policy with version: %s
33105	Send individual command to agent (%s)
33106	Send protection command <Configure Maintenance Mode> to agents
33107	Send protection command <Scan Now> to agents
33108	Send update command <Update Agent Component> to agents

EVENT ID	EVENT
33109	Send update command <Deploy Agent Patches> to agents
33110	Send protection command <Initialize Lockdown Approved List> to agents
33111	Send update command <Check Connections> to agents
33112	Send update command <Apply Policies> to agents
33121	Apply event action to agent (%AGENT_NAME%)
33122	Apply event action <%ACTION_TYPE%> to agent(s)
37122	Set activation code with policy version: %s
37123	Active agents
37124	Inactive agents

Log Descriptions for StellarProtect (Legacy Mode)

Topics in this section include:

- [Agent Event Log Descriptions for StellarProtect \(Legacy Mode\) on page A-28](#)
- [Agent Error Code Descriptions for StellarProtect \(Legacy Mode\) on page A-80](#)

Agent Event Log Descriptions for StellarProtect (Legacy Mode)

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

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
1000	Information	System	Service started	
1001	Warning	System	Service stopped	
1002	Information	System	Application Lockdown turned on	

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
1003	Warning	System	Application Lockdown turned off	
1005	Information	System	Administrator password changed	
1006	Information	System	User password changed	
1007	Information	System	User account enabled	
1008	Information	System	User account disabled	
1009	Information	System	Product activated	
1010	Information	System	Product deactivated	
1011	Warning	System	License Expired. Grace period enabled	
1012	Warning	System	License Expired. Grace period ended	
1013	Information	System	Product configuration import started: %path%	
1014	Information	System	Product configuration import completed: %path%	
1015	Information	System	Product configuration	

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
			exported to: %path%	
1016	Information	System	USB Malware Protection set to Allow	
1017	Information	System	USB Malware Protection set to Block	
1018	Information	System	USB Malware Protection enabled	
1019	Warning	System	USB Malware Protection disabled	
1025	Information	System	Memory Randomization enabled	
1026	Warning	System	Memory Randomization disabled	
1027	Information	System	API Hooking Prevention set to Allow	
1028	Information	System	API Hooking Prevention set to Block	
1029	Information	System	API Hooking Prevention enabled	
1030	Warning	System	API Hooking Prevention disabled	

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
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	
1039	Information	System	Script Lockdown enabled	
1040	Warning	System	Script Lockdown disabled	
1041	Information	System	Script added	File extension: %extension% Interpreter: %interpreter%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
1042	Information	System	Script removed	File extension: %extension% Interpreter: %interpreter%
1044	Information	System	Exception path enabled	
1045	Information	System	Exception path disabled	
1047	Information	System	Trusted certificate enabled	
1048	Information	System	Trusted certificate disabled	
1049	Information	System	Write Protection enabled	
1050	Warning	System	Write Protection disabled	
1051	Information	System	Write Protection set to Allow	
1052	Information	System	Write Protection set to Block	
1055	Information	System	Added file to Write Protection List Path: %path%	
1056	Information	System	Removed file from Write Protection List Path: %path%	
1057	Information	System	Added file to Write Protection Exception List	

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

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
			Path: %path% Scope: %scope% Process: %process%	
1063	Information	System	Added registry value to Write Protection List Registry Key: %regkey% Registry Value Name: %regvalue %	
1064	Information	System	Removed registry value from Write Protection List Registry Key: %regkey% Registry Value Name: %regvalue %	
1065	Information	System	Added registry value to Write Protection Exception List Registry Key: %regkey% Registry Value Name: %regvalue % Process: %process%	
1066	Information	System	Removed registry value from Write	

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
			Protection Exception List Registry Key: %regkey% Registry Value Name: %regvalue % Process: %process%	
1067	Information	System	Added registry key to Write Protection List Path: %regkey% Scope: %scope%	
1068	Information	System	Removed registry key from Write Protection List Path: %regkey% Scope: %scope%	
1069	Information	System	Added registry key to Write Protection Exception List Path: %regkey% Scope: %scope% Process: %process%	
1070	Information	System	Removed registry key from Write Protection Exception List Path: %regkey%	

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
			Scope: %scope% Process: %process%	
1071	Information	System	Custom Action set to Ignore	
1072	Information	System	Custom Action set to Quarantine	
1073	Information	System	Custom Action set to Ask StellarOne	
1074	Information	System	Quarantined file is restored.	Original Location: %path% Source: %source %
1075	Information	System	Quarantined file is deleted.	Original Location: %path% Source: %source %
1076	Information	System	Integrity Monitoring enabled	
1077	Information	System	Integrity Monitoring disabled	
1079	Information	System	Server certification imported: %path %	
1080	Information	System	Server certification exported: %path %	

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
1081	Information	System	Managed mode configuration imported: %path %	
1082	Information	System	Managed mode configuration exported: %path %	
1083	Information	System	Managed mode enabled	
1084	Information	System	Managed mode disabled	
1085	Information	System	Protection applied to Write Protection List and Approved List while Write Protection was enabled	
1086	Warning	System	Protection applied to Write Protection List while Write Protection was 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 File applied: %file_name%	

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
1096	Information	System	Trusted hash enabled	
1097	Information	System	Trusted hash disabled	
1099	Information	System	Storage device access set to Allow	
1100	Information	System	Storage device access set to Block	
1101	Information	System	Storage device control enabled	
1102	Warning	System	Storage device control disabled	
1103	Information	System	Event Log settings changed	Windows Event Log: %ON off% Level: Warning Log: %ON off% Information Log: %ON off% System Log: %ON off% Exception Path Log: %ON off% Write Protection Log: %ON off% List Log: %ON off% Approved Access Log: DllDriver Log: %ON off%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
				Trusted Updater Log: %ON off%
				Exception Path Log: %ON off%
				Trusted Certification Log: %ON off%
				Trusted Hash Log: %ON off%
				Write Protection Log: %ON off%
				Blocked Access Log: %ON off%
				USB Malware Protection Log: %ON off%
				Execution Prevention Log: %ON off%
				Integrity Monitoring Log
				File Created Log: %ON off%
				File Modified Log: %ON off%
				File Deleted Log: %ON off%
				File Renamed Log: %ON off%
				RegValue Modified Log: %ON off%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
				RegValue Deleted Log: %ON off% RegKey Created Log: %ON off% RegKey Deleted Log: %ON off% RegKey Renamed Log: %ON off% Device Control Log: %ON off% Debug Log: %ON off%
1104	Warning	System	Memory Randomization is not available in this version of Windows.	
1105	Information	System	Blocked File Notification enabled	
1106	Information	System	Blocked File Notification disabled	
1107	Information	System	Administrator password changed remotely	
1108	Information	System	Prescan completed successfully	Prescan log: %PATH% Scanned files: %NUM% Infected files: %NUM%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
				Files with resolved threats: %NUM%
1109	Warning	System	Prescan completed successfully; system restart required	Prescan log: %PATH% Scanned files: %NUM% Infected files: %NUM% Files with resolved threats: %NUM% Files with resolved threats after restart: %NUM%
1110	Warning	System	Prescan unsuccessful	Prescan log: %PATH% Scanned files: %NUM% Infected files: %NUM% Files with resolved threats: %NUM% Files with resolved threats after restart: %NUM% Files with unresolved threats: %NUM%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
1111	Information	System	Fileless Attack Prevention enabled	
1112	Warning	System	Fileless Attack Prevention disabled	
1113	Warning	System	Intelligent Runtime Learning enabled	
1114	Warning	System	Intelligent Runtime Learning disabled	
1115	Critical	System	Protection stopped manually via protection stop button or CLI	
1116	Critical	System	Protection resumed manually via protection resume button or CLI	
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%	

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
1504	Information	List	Approved List exported to: %path%	
1505	Information	List	Added to Approved List: %path%	
1506	Information	List	Added to Trusted Updater List: %path%	
1507	Information	List	Removed from Approved List: %path%	
1508	Information	List	Removed from Trusted Updater List: %path%	
1509	Information	List	Approved List updated: %path%	
1510	Information	List	Trusted Updater List updated: %path%	
1511	Warning	List	Unable to add to or update Approved List: %path%	
1512	Warning	List	Unable to add to or update Trusted Updater List: %path%	
1513	Information	System	Added to Exception Path List	Type: %exceptionpath type%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
				Path: %exceptionpath%
1514	Information	System	Removed from Exception Path List	Type: %exceptionpathtype% Path: %exceptionpath%
1515	Information	System	Added to Trusted Certification List	Label: %label% Hash: %hashvalue% Type: %type% Subject: %subject% Issuer: %issuer%
1516	Information	System	Removed from Trusted Certification List	Label: %label% Hash: %hashvalue% Type: %type% Subject: %subject% Issuer: %issuer%
1517	Information	System	Added to Trusted Hash List.%n	Label : %label% Hash : %hashvalue% Type : %type% Add to Approved List: %yes no% Path : %path%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
				Note: %note%
1518	Information	System	Removed from Trusted Hash List.%n	Label : %label% Hash : %hashvalue% Type : %type% Add to Approved List: %yes no% Path : %path% Note: %note%
1519	Information	List	Removed from Approved List remotely: %path %	
1520	Warning	List	Unable to create Approved List because an unexpected error occurred during enumeration of the files in %1 %n Error Code: %2 %n	
1521	Information	System	Added Fileless Attack Prevention exception	Label : %label% Target Process: %process_name % Arguments: %arguments% %regex_flag% Parent Process 1 Image Path: %path%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
				Parent Process 2 Image Path: %path% Parent Process 3 Image Path: %path% Parent Process 4 Image Path: %path%
1522	Information	System	Removed Fileless Attack Prevention exception	Label : %label% Target Process: %process_name % Arguments: %arguments% %regex_flag% Parent Process 1 Image Path: %path% Parent Process 2 Image Path: %path% Parent Process 3 Image Path: %path% Parent Process 4 Image Path: %path%
1523	Information	System	Maintenance Mode started	
1524	Information	System	Leaving Maintenance Mode	

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
1525	Information	System	Maintenance Mode stopped	
1526	Information	List	Added to Approved List in Maintenance Mode Path: %1 Hash: %2	
1527	Information	List	Approved List updated in Maintenance Mode Path: %1 Hash: %2	
1528	Information	List	Maintenance Mode Summary	
1529	Information	List	Approved List initialization started	
1530	Information	List	Approved List initialization completed	
1531	Warning	List	Approved List initialization canceled	
2000	Information	Access Approved	File access allowed: %path%	Access Image Path: %path% Access User: %username% Mode: %mode% List: %list%


EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
2001	Warning	Access Approved	File access allowed: %path%	Access Image Path: %path% Access User: %username% Mode: %mode% File Hash allowed: %hash%
2002	Warning	Access Approved	File access allowed: %path% Unable to get the file path while checking the Approved List	Access Image Path: %path% Access User: %username% Mode: %mode%
2003	Warning	Access Approved	File access allowed: %path% Unable to calculate hash while checking the Approved List	Access Image Path: %path% Access User: %username% Mode: %mode%
2004	Warning	Access Approved	File access allowed: %path% Unable to get notifications to monitor process	
2005	Warning	Access Approved	File access allowed: %path% Unable to add process to non exception list	
2006	Information	Access Approved	File access allowed: %path%	Access Image Path: %path%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
				Access User: %username% Mode: %mode%
2007	Warning	Access Approved	File access allowed: %path% An error occurred while checking the Exception Path List	Access Image Path: %path% Access User: %username% Mode: %mode%
2008	Warning	Access Approved	File access allowed: %path% An error occurred while checking the Trusted Certification List	Access Image Path: %path% Access User: %username% Mode: %mode%
2011	Information	Access Approved	Registry access allowed Registry Key: %regkey% Registry Value Name: %regvalue %	Access Image Path: %path% Access User: %username% Mode: %mode%
2012	Information	Access Approved	Registry access allowed Registry Key: %regkey%	Access Image Path: %path% Access User: %username% Mode: %mode%
2013	Information	Access Approved	Change of File/ Folder allowed by Exception List: %path%	Access Image Path: %path% Access User: %username% Mode: %mode%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
2015	Information	Access Approved	Change of Registry Value allowed by Exception List Registry Key: %regkey% Registry Value Name: %regvalue %	Access Image Path: %path% Access User: %username% Mode: %mode%
2016	Information	Access Approved	Change of Registry Key allowed by Exception List Registry Key: %regkey%	Access Image Path: %path% Access User: %username% Mode: %mode%
2017	Warning	Access Approved	Change of File/ Folder allowed: %path%	Access Image Path: %path% Access User: %username% Mode: %mode%
2019	Warning	Access Approved	Change of Registry Value allowed Registry Key: %regkey% Registry Value Name: %regvalue %	Access Image Path: %path% Access User: %username% Mode: %mode%
2020	Warning	Access Approved	Change of Registry Key allowed Registry Key: %regkey%	Access Image Path: %path% Access User: %username%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
				Mode: %mode%
2021	Warning	Access Approved	File access allowed: %path% An error occurred while checking the Trusted Hash List	Access Image Path: %path% Access User: %username% Mode: %mode%
2022	Warning	Access Approved	Process allowed by Fileless Attack Prevention: %path% %argument%	Access User: %username% Parent Process 1 Image Path: %path% Parent Process 2 Image Path: %path% Parent Process 3 Image Path: %path% Parent Process 4 Image Path: %path% Mode: Unlocked Reason: %reason%
2500	Warning	Access Blocked	File access blocked	
2503	Warning	Access Blocked	Change of File/ Folder blocked: %path%	Access Image Path: %path% Access User: %username% Mode: %mode%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
2505	Warning	Access Blocked	Change of Registry Value blocked. Registry Key: %regkey% Registry Value Name: %regvalue%	Access Image Path: %path% Access User: %username% Mode: %mode%
2506	Warning	Access Blocked	Change of Registry Key blocked. Registry Key: %regkey%	Access Image Path: %path% Access User: %username% Mode: %mode%
2507	Information	Access Blocked	Action completed successfully: %path%	Action: %action% Source: %source%
2508	Warning	Access Blocked	Unable to take specified action: %path%	Action: %action% Source: %source%
2509	Warning	Access Blocked	File access blocked: %path%	Access Image Path: %path% Access User: %username% Mode: %mode% Reason: Not in Approved List File Hash blocked: %hash%
2510	Warning	Access Blocked	File access blocked: %path%	Access Image Path: %path%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
				Access User: %username% Mode: %mode% Reason: Hash does not match expected value File Hash blocked: %hash%
2511	Information	Access Blocked	Change of File/ Folder blocked: %path%	Access Image Path: %path% Access User: %username% Mode: %mode%
2512	Warning	Access Blocked	Change of Registry Value blocked. Registry Key: %regkey% Registry Value Name: %regvalue %	Access Image Path: %path% Access User: %username% <hr/>  Note Enabling the Service Creation Preventio n feature triggers Event ID 2512.
2513	Warning	Access Blocked	Process blocked by Fileless Attack Prevention:	Access User: %username%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
			%path% %argument%	Parent Process 1 Image Path: %path% Parent Process 2 Image Path: %path% Parent Process 3 Image Path: %path% Parent Process 4 Image Path: %path% Mode: locked Reason: %reason %
2514	Warning	Access Blocked	File access blocked: %BLOCKED_FILE _PATH%	Access Image Path: %PARENT_PROCE SS_PATH% Access User: %USER_NAME% Reason: Blocked file is in a folder that has the case sensitive attribute enabled.
3000	Warning	USB Malware Protection	Device access allowed: %path%	Access Image Path: %path% Access User: %username% Device Type: %type%
3001	Warning	USB Malware Protection	Device access blocked: %path%	Access Image Path: %path%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
				Access User: %username% Device Type: %type%
4002	Warning	Process Protection Event	API Hooking allowed: %path%	Threat Image Path: %path% Threat User: %username%
4003	Warning	Process Protection Event	API Hooking blocked: %path%	Threat Image Path: %path% Threat User: %username%
4004	Warning	Process Protection Event	DLL Injection allowed: %path%	Threat Image Path: %path% Threat User: %username%
4005	Warning	Process Protection Event	DLL Injection blocked: %path%	Threat Image Path: %path% Threat User: %username%
4500	Information	Changes in System	File/Folder created: %path%	Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4501	Information	Changes in System	File modified: %path%	Access Image Path: %path% Access Process Id: %pid%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
				Access User: %username%
4502	Information	Changes in System	File/Folder deleted: %path%	Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4503	Information	Changes in System	File/Folder renamed: %path% % New Path: %path% %	Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4504	Information	Changes in System	Registry Value modified. Registry Key: %regkey% Registry Value Name: %regvalue% % Registry Value Type: %regvaluetype%	Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4505	Information	Changes in System	Registry Value deleted. Registry Key: %regkey% Registry Value Name: %regvalue% %	Access Image Path: %path% Access Process Id: %pid% Access User: %username%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
4506	Information	Changes in System	Registry Key created. Registry Key: %regkey%	Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4507	Information	Changes in System	Registry Key deleted. Registry Key: %regkey%	Access Image Path: %path% Access Process Id: %pid% Access User: %username%
4508	Information	Changes in System	Registry Key renamed. Registry Key: %regkey% New Registry Key: %regkey%	Access Image Path: %path% Access Process Id: %pid% Access User: %username%
5000	Warning	Device Control	Storage device access allowed: %PATH%	Access Image path: %PATH% Access User: %USERNAME% Device Type: %TYPE% %DEVICEINFO%
5001	Warning	Device Control	Storage device access blocked: %PATH%	Access Image path: %PATH% Access User: %USERNAME% Device Type: %TYPE% %DEVICEINFO%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
5002	Information	Device Control	Trusted USB device connected	Vendor ID: %HEX % Product ID: %HEX % Serial Number: %STRING% Active User: %STRING%
5003	Information	Device Control	Trusted USB device disconnected	Vendor ID: %HEX % Product ID: %HEX % Serial Number: %STRING% Active User: %STRING%
5004	Warning	Device Control	Untrusted USB device connected	Vendor ID: %HEX % Product ID: %HEX % Serial Number: %STRING% Active User: %STRING%
5005	Warning	Device Control	Untrusted USB device disconnected	Vendor ID: %HEX % Product ID: %HEX % Serial Number: %STRING%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
				Active User: %STRING%
5006	Information	Device Control	USB device added into trusted device list	Device Type: %STRING% Vendor ID: %HEX % Product ID: %HEX % Serial Number: %STRING% Type: %STRING%
5007	Information	Device Control	USB device removed from trusted device list	Device Type: %STRING% Vendor ID: %HEX % Product ID: %HEX % Serial Number: %STRING%
6000	Information	System	%Result%	Update Source: %SERVER% [Original Version] Virus Pattern: %VERSION% Spyware Pattern: %VERSION% Digital Signature Pattern: %VERSION% Program Inspection

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

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

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

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

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

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

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

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

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

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

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

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

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
				Scanner: %VERSION%
8000	Information	System	Real Time Scan is enabled.	
8001	Warning	System	Real Time Scan is disabled.	
8010	Warning	System	Incoming files were scanned by antivirus. Action was taken according to settings.	File Path: %PATH% % File Hash: %HASH% % Threat Type: %TYPE% % Threat Name: %NAME% % Action Result: %INTEGER% % Quarantine Path: %PATH% %
8011	Warning	System	Application execution was blocked by antivirus.	Process Image Path: %PATH% % File Hash: %HASH% % Threat Type: %TYPE% % Threat Name: %NAME% %
8012	Information	System	Incoming file detected malicious and quarantined successfully	File Path: %PATH% % File Hash: %STRING% % Threat Type: %STRING% %

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
				Threat Name: %STRING% Quarantine Path: %PATH% Reboot Required: %NEED_REBOOT %
8013	Warning	System	Failed to quarantine incoming file detected malicious	File Path: %PATH % File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING%
8014	Information	System	Malicious file execution was detected. The infected executable file was quarantined successfully	File Path: %PATH % File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING% Quarantine Path: %PATH% Reboot Required: %NEED_REBOOT %
8015	Warning	System	Malicious file execution detected. Failed to quarantine the	File Path: %PATH % File Hash: %STRING%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
			infected executable file	Threat Type: %STRING% Threat Name: %STRING%
8016	Warning	System	Suspicious program execution blocked	File Path: %PATH% File Hash: %STRING%
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 Login) enabled	Mode: %Mode% Level: %Level% Learning time: %LearningTime% day(s)
8602	Information	anomaly_detect	Operations Behavior Anomaly Detection (User Login) disabled	
8603	Information	anomaly_detect	Operations Behavior Anomaly Detection (Application	Mode: %Mode% Level: %Level%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
			Behavior) enabled	Learning time: %LearningTime% day(s)
8604	Warning	anomaly_detect	Operations Behavior Anomaly Detection (Application Behavior) disabled	
8605	Information	anomaly_detect	Operations Behavior Anomaly Detection (Script Behavior) enabled	Mode: %Mode% Level: %Level% Learning time: %LearningTime% day(s)
8606	Warning	anomaly_detect	Operations Behavior Anomaly Detection (Script Behavior) disabled	
8610	warning	anomaly_detect	An abnormal user login detected by Operations Behavior Anomaly Detection	Domain: %Domain% Account: %Account% Login Type: %LoginType% Source IP: %IP%
8611	warning	anomaly_detect	A user login failure detected by Operations Behavior Anomaly Detection	Domain: %Domain% Account: %Account% Login Type: %LoginType%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
				Source IP: %IP%
8612	warning	anomaly_detect	An unrecognized application detected by Operations Behavior Anomaly Detection	PID: %PID% Program Path: %Path% Program Hash: %SHA256% Program Size: %Size% Certificate: %CertificateSigner% Vendor: %VendorName% Product: %Product%
8613	warning	anomaly_detect	Malicious application behavior detected by Operations Behavior Anomaly Detection	Program Path: %Path% Program Hash: %SHA256% Program Size: %Size% Certificate: %CertificateSigner% Vendor: %VendorName% Product: %Product%
8614	warning	anomaly_detect	Suspicious application behavior detected by Operations	Program Path: %Path% Program Hash: %SHA256%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
			Behavior Anomaly Detection	Program Size: %Size% Certificate: %CertificateSigner% Vendor: %VendorName% Product: %Product%
8615	warning	anomaly_detect	Script Behavior allowed by Operations Behavior Anomaly Detection: %PATH% %ARGUMENT%	Access User: %USERNAME% Parent Process 1: %PATH% %ARGUMENT% Parent Process 2: %PATH% %ARGUMENT% Parent Process 3: %PATH% %ARGUMENT% Parent Process 4: %PATH% %ARGUMENT% Mode: %MODE% Level: %LEVEL% %THROTTLING_INFO_MSG%
8616	warning	anomaly_detect	Script Behavior blocked by Operations Behavior Anomaly Detection: %PATH% %ARGUMENT%	Access User: %USERNAME% Parent Process 1: %PATH% %ARGUMENT%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
				Parent Process 2: %PATH% %ARGUMENT% Parent Process 3: %PATH% %ARGUMENT% Parent Process 4: %PATH% %ARGUMENT% Mode: %MODE% Level: %LEVEL% %THROTTLING_I NFO_MSG%
8620	Information	anomaly_dete ct	Login account added baseline	Domain: %Domain% Account: %Account% Login Type: %LoginType% Source IP: %IP%
8621	Information	anomaly_dete ct	Login account excluded from baseline	Domain: %Domain% Account: %Account% Login Type: %LoginType% Source IP: %IP%
8622	Information	anomaly_dete ct	Application added to baseline	Application Path: %Path%
8623	Information	anomaly_dete ct	Application excluded from baseline	Application Path: %Path%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
8624	Information	anomaly_detect	Script behavior added to baseline	Access User: %USERNAME% ID:%ID% Monitored Process / Script: %PATH% %ARGUMENT% Parent Process 1: %PATH% %ARGUMENT% Parent Process 2: %PATH% %ARGUMENT% Parent Process 3: %PATH% %ARGUMENT% Parent Process 4: %PATH% %ARGUMENT%
8625	Information	anomaly_detect	Script behavior excluded from baseline	ID:%ID% Monitored Process / Script: %PATH% %ARGUMENT% Parent Process 1: %PATH% %ARGUMENT% Parent Process 2: %PATH% %ARGUMENT% Parent Process 3: %PATH% %ARGUMENT%

EVENT ID	LEVEL	CATEGORY	EVENT	DETAILS
				Parent Process 4: %PATH% %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.
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)

CODE	DESCRIPTION
0x0004020d	System Reserved. (Not used)
0x8004020d	System Reserved. (Not used)
0x0004020e	Reboot required.
0x8004020e	Reboot required for unexpected reason.
0x0004020f	Allowed to perform task.
0x8004020f	Permission denied.
0x00040210	System Reserved. (Not used)
0x80040210	Invalid or unexpected service mode.
0x00040211	System Reserved. (Not used)
0x80040211	Requested task not permitted in current status. Check license.
0x00040212	System Reserved. (Not used)
0x00040213	System Reserved. (Not used)
0x80040213	Passwords do not match.
0x00040214	System Reserved. (Not used)
0x80040214	System Reserved. (Not used)
0x00040215	Not found.
0x80040215	"Expected, but not found."
0x80040216	Authentication is locked.
0x80040217	Invalid password length.
0x80040218	Invalid characters in password.
0x00040219	Duplicate password. Administrator and Restricted User passwords cannot match.
0x80040220	System Reserved. (Not used)

CODE	DESCRIPTION
0x80040221	System Reserved. (Not used)
0x80040222	System Reserved. (Not used)
0x80040223	File not found (as expected, and not an error).
0x80040224	System Reserved. (Not used)
0x80040225	System Reserved. (Not used)
0x80040240	Library not found.
0x80040241	Invalid library status or unexpected error in library function.
0x80040260	System Reserved. (Not used)
0x80040261	System Reserved. (Not used)
0x80040262	System Reserved. (Not used)
0x80040263	System Reserved. (Not used)
0x80040264	System Reserved. (Not used)
0x00040265	System Reserved. (Not used)
0x80040265	System Reserved. (Not used)
0x80040270	System Reserved. (Not used)
0x80040271	System Reserved. (Not used)
0x80040272	System Reserved. (Not used)
0x80040273	System Reserved. (Not used)
0x80040274	System Reserved. (Not used)
0x80040275	System Reserved. (Not used)
0x80040280	Invalid Activation Code.
0x80040281	Incorrect Activation Code format.

Server Event Log Descriptions for StellarProtect (Legacy Mode)

This table lists the server event log descriptions for StellarProtect (Legacy Mode).

ID	SERVER EVENT	DESCRIPTION
1011	Unable to send reports	Unable to send scheduled reports to %email_address %.
1012	Unable to send notifications	Unable to send notifications to %email_address%.
3001	Purge agent event logs - automatic	Automatic purge of agent event logs.
3002	Purge agent event logs - manual	Manual purge of agent event logs.
3004	Purge server event logs - automatic	Automatic purge of server event logs.
3005	Purge server event logs - manual	Manual purge of server event logs.

ID	SERVER EVENT	DESCRIPTION
4001	Take action on unapproved blocked file	<p>Request sent to endpoint(s): Add blocked file to Approved List.</p> <p>File name: %file_name%</p> <p>File hash: %file_hash% (SHA-1)</p> <p>Request sent to endpoint(s): Delete the blocked file.</p> <p>File name: %file_name%</p> <p>File hash: %file_hash% (SHA-1)</p> <p>Request sent to endpoint(s): Ignore the blocked file.</p> <p>File name: %file_name%</p> <p>File hash: %file_hash% (SHA-1)</p> <p>Request sent to endpoint(s): Quarantine the file.</p> <p>File name: %file_name%</p> <p>File hash: %file_hash% (SHA-1)</p> <p>Request sent to endpoint(s): Restore the file from quarantine.</p> <p>File name: %file_name%</p> <p>File hash: %file_hash% (SHA-1)</p>
4004	Release the quarantined malicious file	<p>Request sent to endpoint(s): Restore the file from quarantine.</p> <p>File name: %file_name%</p> <p>File hash: %file_hash% (SHA-1)</p>
4005	Delete the quarantined malicious file	<p>Request sent to endpoint(s): Delete the file from quarantine.</p> <p>File name: %file_name%</p> <p>File hash: %file_hash% (SHA-1)</p>

ID	SERVER EVENT	DESCRIPTION
4006	Take action on unapproved fileless attack	<p>Request sent to endpoint(s): Add blocked process chain and command argument.</p> <p>Process chain: %process_name%</p> <p>Command argument: %parameter%</p> <p>Request sent to endpoint(s): Ignore blocked process chain and command argument.</p> <p>Process chain: %process_name%</p> <p>Command argument: %parameter%</p>
4100	Login Account Added to Baseline	<p>A user login account has been added to the Situational Awareness baseline.</p> <p>Domain:%domain%</p> <p>Account:%account%</p> <p>Login type:%logon_type%</p> <p>Source IP:%source_ip%</p>
4101	Application Added to Baseline	<p>An application has been added to the Situational Awareness baseline.</p> <p>Application Path: %app_path%</p>
5001	Turn Application Lockdown on	Turned Application Lockdown on for endpoint(s).
5002	Turn Application Lockdown off	Turned Application Lockdown off for endpoint(s).
5011	Add trusted file hashes	<p>Added 1 trusted file hash to endpoint(s).</p> <p>Added %num% trusted file hashes to endpoint(s).</p>
5013	Delete approved files	Removed specified items from the Approved List on endpoint(s) using SLtasks.exe.
5021	Block access from storage devices	Blocked access from storage devices on endpoint(s).

ID	SERVER EVENT	DESCRIPTION
5023	Allow access from storage devices	Allowed access from storage devices on endpoint(s).
5025	Add trusted USB device on selected endpoint(s)	Add trusted USB device on selected endpoint(s)
5601	Export agent settings	Exported (%file_desc%) from %endpoint_name%.
5602	Import agent settings	Imported (%file_desc%) to endpoint(s).
5700	Scan for malware	Scanned endpoint(s) for malware.
5701	Update agent components	Updated agent components on endpoint(s).
5800	Change agent administrator password	Changed password on endpoint(s).
5900	Update agent Approved List	Updated Approved List on endpoint(s).
6001	Deploy agent patch	Deploy agent patch to endpoint(s). Patch name: %patch_name%
6101	Agent transferred to new StellarOne server	Agent transferred to new StellarOne server
6201	Turn Maintenance Mode on	Turned Maintenance Mode on for endpoint(s).
6202	Turn Maintenance Mode off	Turned Maintenance Mode off for endpoint(s).
6301	Deploy group policy	Deploy group policy. Version: %version%.
6401	Set Intelligent Runtime Learning	Set Intelligent Runtime Learning. Version: %policy_version%

ID	SERVER EVENT	DESCRIPTION
6402	Set Agent Password	Set Agent Password. Version: %policy_version%
6403	Set Schedule Scan Setting	Set Schedule Scan Setting. Version: %policy_version%
6404	Set User-Defined Suspicious Objects	Set User-Defined Suspicious Objects. Version: %policy_version%
6405	Set Agent Patch	Set Agent Patch. Version: %policy_version%

Server Event Log Descriptions for StellarOne

This table lists the server event log descriptions for StellarOne.

ID	CONTENT
45313	Scan component update now
45314	Scan component [%s] update task started
45315	Enable scan component scheduled update
45316	Disable scan component scheduled update
45317	Modify scan component update source for StellarOne
45318	Modify scan component update source for agents
45319	Scan component [%s] update was successful
45320	Scan component [%s] update was successful but no duplicate is needed
45321	Scan component [%s] update failed with internal error
45322	Scan component [%s] update failed due to unable to connect to the network
45323	Customize policy

ID	CONTENT
45324	Inherit policy from [%s]
45325	Scan component [%s] update failed due to <%s>
45569	Modify sync interval: [%s] Minutes
45824	Enable forwarding logs to Trend Micro Vision One
45825	Disable forwarding logs to Trend Micro Vision One

Syslog Content - CEF

The following section maps syslog content between StellarOne log output and CEF syslog types.

Topics in this section includes:

- [StellarProtect/StellarProtect \(Legacy Mode\) Syslog Content - CEF on page A-88](#)
- [StellarOne Syslog Content - CEF on page A-94](#)

StellarProtect/StellarProtect (Legacy Mode) Syslog Content - CEF

The following section describes StellarProtect/StellarProtect (Legacy Mode) agent/server events in the Common Event Format.

Topics in this section includes:

- [StellarProtect Agent Event Format on page A-88](#)
- [StellarProtect Server Event Format on page A-91](#)
- [StellarProtect \(Legacy Mode\) Agent/Server Event Format on page A-92](#)

StellarProtect Agent Event Format

See the following table for StellarProtect agent events in the Common Event Format.

TABLE A-1. StellarProtect Agent Event Format

CEF FIELD NAME	DESCRIPTION	POSSIBLE VALUES
Header		
CEF:Version	CEF format version	CEF:0
Device Vendor	Device Vendor	TXOne Networks
Device Product	Device Product	StellarProtect
Device Version	Device Version	2.0.1145
Device Event Class ID	Event ID	{}
Name	Event category	Agent Event
Severity	LOG_CRIT: 2 LOG_WARNING: 4 LOG_INFO: 6	{2, 4, 6}
Extension		
eventTime	StellarProtect format	Apr 02 2022 13:31:51 GMT +00:00
msg	<string>	
category	OPTION: 0 SYSTEM: 1 INTELLI_AV: 2 ANOMALY_DETECT: 3 CHANGE_CONTROL: 4 DEVICE_CONTROL: 5 MISC: 15	
agentEndpoint	<string>	
agentIp	<string>	

CEF FIELD NAME	DESCRIPTION	POSSIBLE VALUES
agentLocation	<string>	
agentVendor	<string>	
agentModel	<string>	
agentOS	<string>	
policyVersion	<string>	
detailMsg	<string>	
targetProcess	<string>	
fileHash	<string>	
threatType	<string>	
threatName	<string>	
filePath	<string>	
actionResult	<int>	
quarantinePath	<string>	
obadMode	<string>	
obadLevel	<string>	
accessUser	<string>	
processId	<string>	
parentProcess1	<string>	
parentProcess2	<string>	
parentProcess3	<string>	
parentProcess4	<string>	
targetArguments	<string>	
parentArguments1	<string>	

CEF FIELD NAME	DESCRIPTION	POSSIBLE VALUES
parentArguments2	<string>	
parentArguments3	<string>	
parentArguments4	<string>	
blockedProcess	<string>	
targetFile	<string>	
vid	<int>	
pid	<int>	
sn	<string>	
accessImagePath	<string>	
srcPath	<string>	
dstPath	<string>	
errCode	<int>	
patchFileName	<string>	
filePath	<string>	
type	<string>	

```

Time: Nov 22 04:00:07
IP: 10.8.145.45
Host:
Facility: local3
Priority: info
Tag: 2022-11-21T20:00:07Z 864c9868f43d Stellar[1]
Message: CEF:0|TXOne Networks|StellarProtect|2.0.1145|515|Agent Event|6|eventTime=Nov 21 2022 20:00:07 GMT+00:00 msg=Scheduled Scan Start
category=2 agentEndpoint=Z-W7X86T1CPSP1 agentIP=10.8.145.170 agentLocation=vC agentVendor=Zzzz agentModel=W7x86_testCrash agentOS=Windows 7
Ultimate Edition Service Pack 1 (build 7601), 32-bit desc=W7SP_remark serverIP=10.8.145.45
    
```

FIGURE A-1. Example of StellarProtect Syslog Content

StellarProtect Server Event Format

See the following table for StellarProtect server events in the Common Event Format.

TABLE A-2. StellarProtect Server Event Format

CEF FIELD NAME	DESCRIPTION	POSSIBLE VALUES
Header		
CEF:Version	CEF format version	CEF:0
Device Vendor	Device Vendor	TXOne Networks
Device Product	Device Product	StellarProtect
Device Version	Device Version	3.1
Device Event Class ID	Event ID	{}
Name	Event category	Server Event
Severity	LOG_INFO: 6	{6}
Extension		
eventTime	StellarProtect format	Apr 02 2023 13:31:51 GMT +00:00
msg	<string>	
userName	<string>	
userRole	<string>	
clientIp	<string>	

StellarProtect (Legacy Mode) Agent/Server Event Format

See the following table for StellarProtect (Legacy Mode) agent/server events in the Common Event Format.

TABLE A-3. Agent Event Format

CEF KEY	DESCRIPTION	POSSIBLE VALUES / EXAMPLE
Header (logVer)	CEF format version	CEF:0
Header (vendor)	Device Vendor	TXOne Networks

CEF KEY	DESCRIPTION	POSSIBLE VALUES / EXAMPLE
Header (pname)	Device Product	StellarOne, StellarProtect (Legacy Mode)
Header (pver)	Device Version	2.0.1145
Header (eventid)	Device Event Class ID	2509, 6005
Header (eventName)	Name	Agent Event, Server Event, Console Log
Header (severity)	Severity	4
rt	Logged Time	Apr 02 2022 13:31:51 GMT +00:00
msg	Event Id mapped message	File access blocked. File not found in Approved List
dvchost	Computer name	localhost
dvc	IP address	192.168.154.137
cs1Label	Detailed Event Message	Detailed Event Message
cs1	Event ID mapped detailed message	File access blocked: C:\Documents and Settings\Administrator\Local Settings\Temp\isD5V0T.tmp\is-H7K40.tmp Malware detected: Quarantine. File path: C:\\eicar\EICAR_TEST_FILE.exe
cs2Label	Client OS	Client OS
cs2	OS description	Microsoft Windows 7 Enterprise Edition Service Pack 1 build 7601, 64-bit
cs3Label	Client Description	Client Description
cs3	Description	-

CEF KEY	DESCRIPTION	POSSIBLE VALUES / EXAMPLE
suser	Login User	PC1688\\Administrator
act	Action Type	ACTION_TYPE_BLOCKED
fileHash	SHA1	2201589AA3ED709B3665E4FF979E10C6AD5137F C
filePath	File path	C:\\Documents and Settings\\Administrator\\Local Settings\\Temp\\is-D5V0T.tmp\\is-H7K4O.tmp
fileCreateTime	File create time	04 02 2022 14:00:21
fileModificationTime	File modified time	04 02 2022 14:00:21
logGuid	Log GUID	: F43500BB-1F8A-4589-A292-144A9DA343AA, {56B7345A-B6D3-4BBB-A515-4AFFAE04092F}
ServerIP	Server IP	10.8.145.157

```

Time: Nov 23 20:16:21
IP: 10.8.145.45
Host:
Facility: local3
Priority: warning
Tag: 2022-11-23T12:16:20Z StellarOne [1]
Message: CEF:0|TXOne Networks|StellarProtect (Legacy Mode)|2.0.1145|2510|Agent Events|4|rt=Nov 23 2022 12:16:15 GMT+00:00 msg=File access blocked. File hash does not match the expected value of the file with that path in Approved List dvchost=Z-W10IOT-2 dvc=10.8.145.10 logGuid={631219FB-E2C9-4CA2-8643-38BADD044847} cs1Label=Detailed Event Message cs1=File access blocked: C:\\windows\\system32\\WINHTTP.dll cs2Label=Client OS cs2=Windows 10 build 19044, 64-bit cs3Label=Client Description cs3= suser=NT AUTHORITY\\NETWORK SERVICE act=ACTION_TYPE_BLOCKED
fileHash=091963d9538af4b2b94477180f95edae481f267e filePath=C:\\windows\\system32\\WINHTTP.dll fileCreateTime=10 12 2022 11:02:52
fileModificationTime=10 12 2022 11:02:52 serverIP=10.8.145.45

```

FIGURE A-2. Example of StellarProtect (Legacy Mode) Syslog Content

StellarOne Syslog Content - CEF

The following section maps syslog content between StellarOne log output and CEF syslog types.

Topics in this section includes:

- [StellarOne System Event Format on page A-95](#)
- [StellarOne Audit Event Format on page A-97](#)

StellarOne System Event Format

See the following table for StellarOne system events in the Common Event Format.

TABLE A-4. StellarOne Server Event Format

CEF FIELD NAME	DESCRIPTION	VALUE TYPE	POSSIBLE VALUES
Header			
CEF:Version	CEF format version	<String>	CEF:0
Device Vendor	Vendor name	<String>	TXOne Networks
Device Product	Product name	<String>	StellarOne
Device Version	Product version	<String>	3.0.4115
Signature ID	System Event Logs	<Integer>	0
Event Name	System Event Logs	<String>	SYSTEM_EVENT
Severity	The severity of the system event	<Integer>	<ul style="list-style-type: none"> • 2: Information • 4: Notice • 6: Warning • 7: Error
Extension			
start	The time when the event log is generated. Format: MMM dd yyyy HH:mm:ss GMT +00:00	<DateTime>	Dec 26 2023 15:04:05 GMT+00:00
cat	Device event category	<Integer>	4: System Event Logs

CEF FIELD NAME	DESCRIPTION	VALUE TYPE	POSSIBLE VALUES
dvchost	(Optional) The hostname of the device generating the event log. It is used to preserve the information of the device generating the event log when it is not the same device sending the syslog.	<String>	stellar1
deviceExternalId	(Optional) The serial number of the device generating the event log	<string>	79070e12-4089-12ee-8435-0050679a1021
eventId	System event ID	<Integer>	8226 See StellarOne System Event IDs and Messages on page A-97 for the defined system event IDs and the corresponding messages.
msg	The message of the system event	<string>	See StellarOne System Event IDs and Messages on page A-97 for the defined system event IDs and the corresponding messages.
serverIP	StellarOne server IP address	<string>	10.8.145.123

```
2023-12-22T20:11:05Z StellarOne [1]: CEF:0|TXOne Networks|
StellarOne|3.0.4115|0|SYSTEM_EVENT|4|start=Dec 22 2023 12:11:04
GMT+00:00 cat=4 dvchost=stellar1 deviceExternalId=79070e12-4089-12ee-
8435-0050679a1021 eventId=8226 msg=System time adjusted (385ms)
serverIP=10.8.151.203
```

```
2023-12-22T21:31:52Z StellarOne [1]: CEF:0|TXOne Networks|
StellarOne|3.0.4115|0|SYSTEM_EVENT|7|start=Dec 22 2023 13:31:51
GMT+00:00 cat=4 dvchost=stellar1 deviceExternalId=79070e12-4089-12ee-
8435-0050679a1021 eventId=6 msg=Sync with NTP server (pool.ntp.org)
failed serverIP=10.8.120.203
```

FIGURE A-3. Examples of StellarOne System Events

StellarOne System Event IDs and Messages

See the following table for StellarOne system event IDs and messages.

TABLE A-5. StellarOne Server Event IDs and Messages

ID	MESSAGE	ARGUMENTS
6	Sync with NTP server (\$0) failed	\$0: NTP server
8224	NTP server (\$0) synchronized	\$0: NTP server
8226	System time adjusted (\$0 ms)	\$0: delta in ms

StellarOne Audit Event Format

See the following table for StellarOne audit events in the Common Event Format.

TABLE A-6. StellarOne Audit Event Format

CEF FIELD NAME	DESCRIPTION	VALUE TYPE	POSSIBLE VALUES
Header			
CEF:Version	CEF format version	<String>	CEF:0
Device Vendor	Vendor name	<String>	TXOne Networks
Device Product	Product name	<String>	StellarOne

CEF FIELD NAME	DESCRIPTION	VALUE TYPE	POSSIBLE VALUES
Device Version	Product version	<String>	3.0.4115
Signature ID	Audit Event Logs	<Integer>	0
Event Name	Audit Event Logs	<String>	AUDIT_EVENT
Severity	The severity of the audit event	<Integer>	<ul style="list-style-type: none"> • 2: Information • 4: Notice • 6: Warning • 7: Error
Extension			
start	The time when the event log is generated. Format: MMM dd yyyy HH:mm:ss GMT +00:00	<DateTime>	Dec 26 2023 15:04:05 GMT+00:00
cat	Device event category	<Integer>	5: Audit Event Logs
dvchost	(Optional) The hostname of the device generating the event log. It is used to preserve the information of the device generating the event log when it is not the same device sending the syslog.	<String>	stellar1
deviceExternalId	(Optional) The serial number of the device generating the event log	<String>	79070e12-4089-12ee-8435-0050679a1021

CEF FIELD NAME	DESCRIPTION	VALUE TYPE	POSSIBLE VALUES
eventId	Audit event ID	<Long>	8193 See xxx for the defined audit event IDs and the corresponding messages.
suser	The username of the user who triggers the audit event.	<String>	admin
cs1Label	For example, the key for client IP address is labelled as "clientIpAddress"	<String>	clientIpAddress
cs1	The client IP address from which the user logs in and executes commands.	<String>	10.8.144.27
msg	The message of the audit event.	<String>	User (admin) login See xxx for the defined audit event IDs and the corresponding messages.
serverIP	StellarOne server IP address	<String>	10.8.151.99

```
2023-12-22T19:51:05Z StellarOne [1]: CEF:0|TXOne
Networks|StellarOne|3.0.4115|0|AUDIT_EVENT|4|start=Dec 22 2023
11:51:04 GMT+00:00 cat=5 dvchost=stellar1 deviceExternalId=79070e12-
4089-12ee-8435-0050679a1021 eventId=8193 suser=admin
cs1Label=clientIpAddress cs1=10.8.144.27 msg=User (admin) login
serverIP=10.8.151.99
```

```
2023-12-22T19:59:15Z StellarOne [1]: CEF:0|TXOne
Networks|StellarOne|3.0.4115|0|AUDIT_EVENT|4|start=Dec 22 2023
11:59:14 GMT+00:00 cat=5 dvchost=stellar1 deviceExternalId=79070e12-
4089-12ee-8435-0050679a1021 eventId=8193 suser=admin
cs1Label=clientIpAddress cs1=10.8.144.27 msg=User (admin) logout
serverIP=10.8.151.99
```

FIGURE A-4. Examples of StellarOne Audit Events

StellarOne Audit Event IDs and Messages

See the following table for StellarOne audit events IDs and messages.

TABLE A-7. StellarOne Audit Event IDs and Messages

ID	MESSAGE	ARGUMENTS
8193	User (\$) login	\$0: Account ID
8194	User (\$) login failed	\$0: Account ID
8195	User (\$) logout	\$0: Account ID
8196	User (\$) timeout, force logout	\$0: Account ID
8197	User (\$) changed password	\$0: Account ID
8208	Reset admin account from vshell	None
8209	User (\$) created user account (\$1)	\$0: Account ID \$1: User account ID being created

ID	MESSAGE	ARGUMENTS
8211	User (\$0) deleted user account (\$1)	\$0: Account ID \$1: User account ID being deleted
8214	User (\$0) changed user account (\$1) password	\$0: Account ID \$1: User account ID being changed
8225	User (\$0) changed system time (\$1)	\$0: Account ID \$1: new system time in ISO 8601, e.g., "2023-12-11T18:12:14+08:00"
8226	User (\$0) enabled NTP synchronization (\$1)	\$0: Account ID \$1: NTP server
8227	User (\$0) disabled NTP synchronization	\$0: Account ID
8228	User (\$0) synchronized system time with NTP server (\$1)	\$0: Account ID \$1: NTP server
8229	User (\$0) changed time zone to (\$1)	\$0: Account ID \$1: new time zone ID, e.g., "Asia/Taipei"
8243	User (\$0) changed the syslog setting (\$1)	\$0: Account ID \$1: Setting Name
8273	User (\$0) changed SSL certificate	\$0: Account ID
8289	User (\$0) executed "Purge Now"	\$0: Account ID
8290	User (\$0) changed auto-purge settings	\$0: Account ID

ID	MESSAGE	ARGUMENTS
10241	User (\$0) created (\$1)'s API Key expired on (\$2)	\$0: Account ID \$1: Account ID \$2: time in ISO 8601, e.g., "2023-12-15T16:42:16+08:00"
10242	User (\$0) deleted (\$1)'s API key	\$0: Account ID \$1: Account ID
10243	User (\$0) created (\$1)'s API Key (No expiration)	\$0: Account ID \$1: Account ID

```
2023-12-22T19:51:05Z StellarOne [1]: CEF:0|TXOne
Networks|StellarOne|3.0.4115|0|AUDIT_EVENT|4|start=Dec 22 2023
11:51:04 GMT+00:00 cat=5 dvchost=stellar1 deviceExternalId=79070e12-
4089-12ee-8435-0050679a1021 eventId=8193 suser=admin
cs1Label=clientIpAddress cs1=10.8.144.27 msg=User (admin) login
serverIP=10.8.151.99
```

```
2023-12-22T19:59:15Z StellarOne [1]: CEF:0|TXOne
Networks|StellarOne|3.0.4115|0|AUDIT_EVENT|4|start=Dec 22 2023
11:59:14 GMT+00:00 cat=5 dvchost=stellar1 deviceExternalId=79070e12-
4089-12ee-8435-0050679a1021 eventId=8193 suser=admin
cs1Label=clientIpAddress cs1=10.8.144.27 msg=User (admin) logout
serverIP=10.8.151.99
```

FIGURE A-5. Examples of StellarOne Audit Events

Index

A

- account management, 7-4
 - access rights, 7-4, 7-5
 - account types, 7-4, 7-5
 - privileges, 7-4, 7-5
- administration, 7-1
 - account, 7-3
 - account management, 7-3
 - notification, 7-16
 - Single Sign-On, 7-11
 - syslog forwarding, 7-19
 - system, 7-36
 - system time, 7-37
 - update, 7-19
- Administration
 - log purge, 7-37
- Agent policy settings, 5-27
- agents, 4-1
 - export/import settings, 4-35
 - protection, 4-20
 - update, 4-28
- Agent status settings, 4-8
- Agent view and policy settings, 5-23
- appendices, A-1
 - agent syslog content - CEF, A-88
 - log descriptions, A-2
 - syslog content - CEF, A-88, A-94

D

- Dashboard, 3-2

G

- group policy screen, 5-107
- Group policy settings, 5-106, 5-108

L

- legacy mode
 - collect event logs, 4-32
 - export agent settings, 4-35
 - import agent settings, 4-36
- license, 7-28
 - New License Key/File, 7-29
 - Renew License Key, 7-29
- license editions, 7-34
 - StellarICS, 7-34
 - StellarKiosk, 7-35
 - StellarOEM, 7-35
- license features, 7-36
- logs, 6-1
 - agent events, 6-2
 - audit logs, 6-15
 - server events, 6-10
 - system logs, 6-13

O

- Operations Behavior Anomaly Detection, 5-27
 - migration, 5-45
 - Policy-based approved applications, 5-38
 - Policy-based Approved Login Accounts, 5-37
 - Policy-based watchlist, 5-36
 - Strict Mode, 5-41

P

- Policy configuration, 5-1

S

- scheduled report, 7-17

- server accounts, 7-5
 - account privilege allowed, 7-5-7-7
 - task, 7-5-7-7
- situational awareness
 - StellarProtect (Legacy Mode), 5-101
- Situational awareness, 5-95
 - StellarProtect, 5-95
- support
 - resolve issues faster, 8-5

T

- technical support, 8-1
 - contact, 8-5
 - troubleshooting resources, 8-2

U

- update
 - apply policies, 4-31
 - check connections, 4-31