txOne networks | Keep the Operation Running

2.0 TXOne StellarOne for StellarProtect

Administrator's Guide

All-terrain protection for mission critical assets

Windows

SC 2022 awards EUROPE

WINNER

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

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

Document Part No.: APEM29594/220907

Release Date: September 2022

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

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

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

Privacy and Personal Data Collection Disclosure

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

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

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

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

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

Table of Contents

Preface

Chapter 1: Introduction

Chapter 2: The Web Console

Chapter 3: Dashboard

Chapter 4: Agent Management

Chapter 5: Policy Setting

Chapter 6: Logs

Chapter 7: Administration

Chapter 8: Technical Support

Appendix A: Log Descriptions

Appendix B: Syslog Content - CEF

Index

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 viii*
- *Audience on page viii*
- *Document Conventions on page viii*
- *Terminology on page ix*

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: http://success.trendmicro.com 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 following table provides the official terminology used throughout the TXOne StellarOne documentation:

TABLE 1. Document Conventions

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

Terminology

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

Terminology	Description
server	The StellarOne console server program
server endpoint	The host where the StellarOne server is installed
agents	The host running the StellarProtect program
NAT agents	The agents that are built under the routers with the Network Address Translation (NAT) function enabled
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 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

Chapter 1

Introduction

This section introduces TXOne StellarOne and how it manages the agents providing Industrial-Grade Next-Generation Antivirus and Application Lockdown protection to your assets. An overview of management functions is provided. This manual will focus on its use for TXOne StellarProtect: an / OTICS-compatible, high performance and zero touch endpoint protection solution.

Topics in this chapter include:

About TXOne Stellar

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

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

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

Key Features and Benefits

The StellarOne management console provides following features and benefits.

TABLE 1-1. Features and Benefits

FEATURE	BENEFIT
Dashboard	The web console dashboard provides summarized information about monitored agents. Administrators can check deployed agent status easily, and can generate security reports (Legacy Mode only) related to specific agent activity for specified periods.

FEATURE	BENEFIT
Centralized Agent Management	TXOne StellarOne allows administrators to perform the following tasks: • Monitor StellarProtect/StellarProtect (Legacy Mode) agent status • Examine connection status • View configurations • Collect agent logs on-demand or by policy - 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
Centralized Event Management	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. TXOne StellarOne provides event management features that let administrators quickly know about and take action on blocked file events.
Server Event Auditing	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.

What's New

TXOne StellarOne 2.0 provides following new features and enhancements.

TABLE 1-2. What's New in TXOne StellarOne 2.0

FEATURE	BENEFIT
Application Lockdown	This feature prevents malware attacks and increases protection level by locking down files defined in an Application List. Three modes are available for selection: • Detect: The applications that are not in the Approved List will be allowed to run, and users will receive a notification. • Enforce: The applications that are not in the Approved List will be blocked from running, and users will receive a notification. • Disable: The Application Lockdown mode can also be disabled in case users may have the needs, but it is recommended to have this function enabled.
Agent Component Update Schedule	In addition to the existing component update schedule function of the StellarOne console, now users can also configure the component update schedule for the agents (StellarProtect). The system can run component update automatically at users' assigned time frequency.
Self-management Group Policy	This newly-added group policy allows the operators on site to configure the agents' policy settings on their own. Once being switched to the self-management status, the local agents are free from the StellarOne console's policy management.
Real-Time Malware Scan in Maintenance Mode	A Real-Time Malware Scan toggle switch is added under the Maintenance Mode option, reminding users to enable Real-Time Malware Scan during the maintenance period for seamless protection.
Open API	Provides open API for users to query data from agents. Users can also generate API keys and set the expiration dates for different user accounts for account management.

Chapter 2

The Web Console

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

Topics in this chapter include:

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. The OVA file supports VMware ESXi and VMware Workstation systems, and the VHDX file supports Windows Hyper-V Manager Windows system.

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. In a web browser, type the address of the StellarOne in the following format: `https://<targetserver IP address>`. The log on screen will appear.
2. Enter your credentials (user name and password).

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

   - User name: `admin`

- Password: `txone`

3. Click **Log On**.

4. If this is the first time the StellarOne console being used, follow below procedures to complete the initial settings.

   a. The **Login Information Setup** window will appear and prompt 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.

   d. Enter your first Activation Code, and then click **Continue**. If you want to enter an activation code for another product, click **Enter Another Code** instead of **Continue**.

   e. The **EULA/OT Intelligent Trust Agreement** screen will appear. 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. Please refer to *OT Intelligent Trust on page 7-30* for more details.

   f. Specify the time settins such as the **Date and Time** as well as the **Time Zone**, and then click **Continue**.

   g. The StellarOne console is ready for use now.

5. 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 righ corner of the screen, and then click **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, and then click **Log Off**.

Note

Users 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

The **Dashboard** provides an overview of monitored agent events and StellarOne console's system status. Click the **Dashboard** tab in the top navigation bar of the StellarOne web console. The **Dashboard** screen with two tabs of **Summary** and **System** appears.

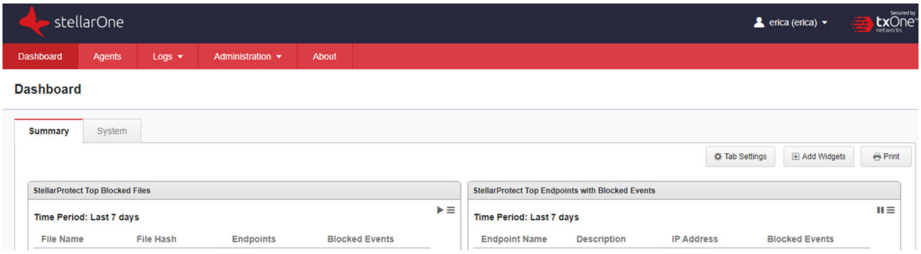


Figure 3-1. The Dashboard Screen

Table 3-1. About the Dashboard Screen

Function	Description
Summary	Under this tab, two widgets for monitoring StellarProtect agent events can be added: • **Top Endpoints with Blocked Events** • **Top Blocked Files** Please refer to *Widgets for Monitoring StellarProtect on page 3-3* and *Add Widgets on page 3-5* for more details. **Note** By default the **Summary** tab page is set as the landing page of the **Dashboard**.

FUNCTION	DESCRIPTION
System	Under this tab, users can check StellarOne console's system status related to: • CPU Usage • Memory Usage • Disk Usage
Tab Settings	This button allows users to customize their own tab names. By simply clicking this button, specifying the desired tab name in the **Tab Name** field, and clicking **OK**, users can easily change the tab name.
Add Widgets	This button allows users to add their desired widgets to the **Dashboard** screen. Please refer to *Add Widgets on page 3-5* for more details.
Print	This button allows users to print the current **Summary** or **System** page.

Widgets for Monitoring StellarProtect

Two widgets for monitoring StellarProtect agent events can be added under the **Summary** tab of the **Dashboard** screen.

- **Top Endpoints with Blocked Events**: This widget displays the endpoints with the most blocked events. By default, the widget is displayed on the **Summary** tab of the **Dashboard**.

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

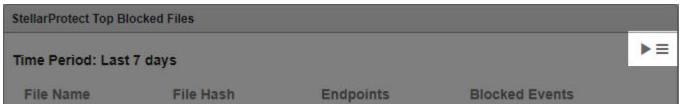
COLUMN	DESCRIPTION
Endpoint Name	Name of the endpoint
Description	Description assigned to the endpoint
IP Address	IP address of the endpoint
Blocked Events	Total number of events blocked on the endpoint

- **Top Blocked Files**: This widget displays a list of files that triggered the most blocked events.

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
Endpoints	Total number of the endpoints that reported the blocked events triggered by the file
Blocked Events	Total number of the blocked events triggerd by the file

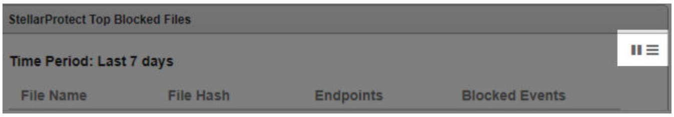
Tip



StellarProtect Top Blocked Files

Time Period: Last 7 days

File Name   File Hash   Endpoints   Blocked Events



StellarProtect Top Blocked Files

Time Period: Last 7 days

File Name   File Hash   Endpoints   Blocked Events

- Click the play button to start auto refresh. Click the pause button to pause auto refresh.
- The dropdown-menu button provides two functions:
  - **Widget Settings**:
    - **Widget Name**: allows users to edit the name for the widget.
    - **Time Period**: allows users to select a specific timeframe, which determines the number of the blocked events or files to display (The default value is **Last 7 days**).
    - **Auto Refresh Settings**: allows users to change the setting to manual refresh or to configure the auto refresh frequency (The default value is **Every 5 minutes**).
  - **Remove Widget**: allows users to remove the widgets from the **Dashboard** screen.
- To move a widget, click and hold on the title bar of the widget and drag it to various locations on the tab page.
- To resize a widget, mouse over the edge of the widget and a diagonal resize pointer appears. Drag it to resize the widget.

Add Widgets

The number of widgets that users can add to a tab depends on the tab page layout. Once the number of widgets exceeds the maximum number the tab page can accomodate, users must remove a widget from the tab page or create a new tab for the widget.

Procedure

1. Go to **Dashboard** in the navigation at the top of the web console.
2. Go to the tab (**Summary** or **System** under the **Dashboard**) that you want to add the widget to.
3. Click the **Add Widgets** button at the right side, and then the screen for widget adding appears.
4. Click the checkbox(es) next to the widget names to add one or more widgets to the current tab.
5. Click the **Add** button to complete the task.

Chapter 4

Agent Management

This chapter introduces how to manage StellarProtect agents via StellarOne web console.

Topics in this chapter include:

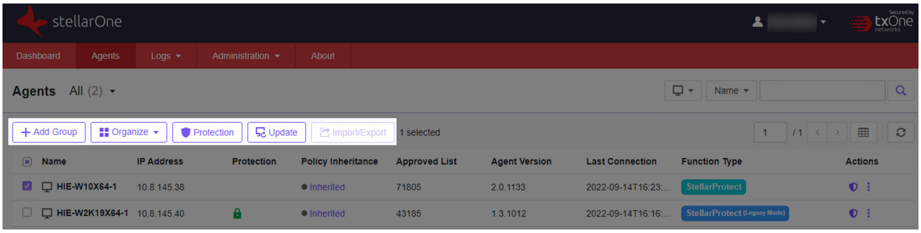
About the Agent Screen

The StellarOne console facilitates agent management by allowing users 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.

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 and enables users to perform configuration tasks, which are one-time commands for triggering immediate actions.

Note

- All agents are under the **All** group by default.
- The screen automatically refreshes every 5 minutes.



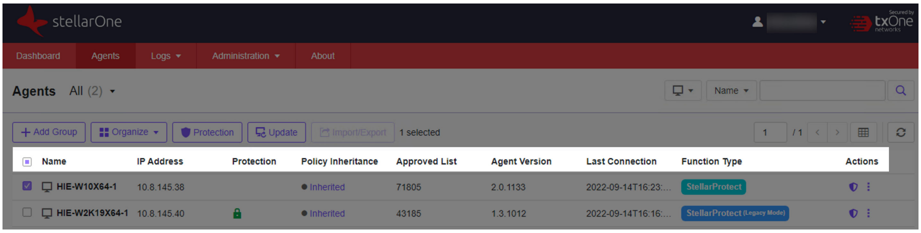
☐	Name	IP Address	Protection	Policy Inheritance	Approved List	Agent Version	Last Connection	Function Type	Actions
☑	HIE-W10X64-1	10.8.145.38		● Inherited	71805	2.0.1133	2022-09-14T16:23:...	StellarProtect	
☐	HIE-W2K19X64-1	10.8.145.40	🔒	● Inherited	43185	1.3.1012	2022-09-14T16:16:...	StellarProtect (Legacy Mode)	

FIGURE 4-1. The Agents Screen - Toolbar

TABLE 4-1. Toolbar

TOOLS	DESCRIPTION
+Add Group	This tool allows users to create groups according to location, type, or purpose for better multi-agent management. Please refer to *Add Groups on page 4-6* for more details.

Tools	Description
Organize	This tool allows users to edit description for agent(s), move agent(s) to another group, and remove agent(s)/group(s). Please refer to *Edit Description for Agents on page 4-6* and *Organize Agents/Groups on page 4-7* for more details.
Protection	This tool allows users to configure Maintenance Mode, update Approved List when the Application Lockdown feature is enabled, and customize file scan settings. Please refer to *Configure Maintenance Mode on page 4-11*, *Update Approved List on page 4-13*, and *Scan Now on page 4-14* for more details.
Update	This tool allows users to update components and deploy patches for agents. Please refer to *Update Agent Components on page 4-16* and *Deploy Agent Patches on page 4-17* for more details.
Import/Export	Currently StellarProtect doesn't support the **Import/Export** tool. This tool is used for StellarProtect (Legacy Mode) agent management.



☐ Name	IP Address	Protection	Policy Inheritance	Approved List	Agent Version	Last Connection	Function Type	Actions
☑ HIE-W10X64-1	10.8.145.38		● Inherited	71805	2.0.1133	2022-09-14T16:23:...	StellarProtect	⋮
☐ HIE-W2K19X64-1	10.8.145.40	🔒	● Inherited	43185	1.3.1012	2022-09-14T16:16:...	StellarProtect (Legacy Mode)	⋮

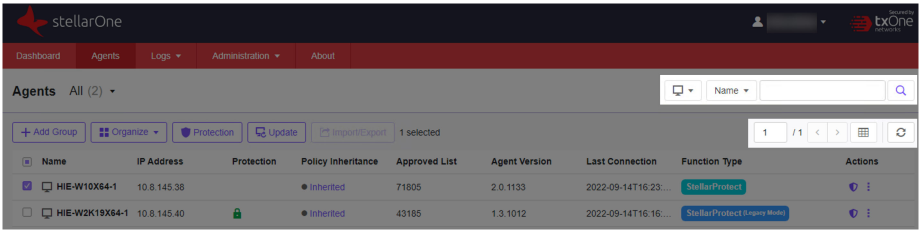
Figure 4-2. The Agents Screen - Table Header

Table 4-2. Table Header

Headers	Description
Name	• 🖵 : This icon indicates an agent. • 📁 : This icon indicates a group. • 🖵: This icon indicates the agent's license is expired and needs to be renewed.

HEADERS	DESCRIPTION
IP Address	Indicates the IP Address of the endpoint (one IP address corresponds to a single agent).
Protection	• 🔒 : This icon indicates the endpoint's Application Lockdown feature is enabled. • 🛡 : This icon indicates the endpoint is under protection. • 🔧 : This icon indicates the endpoint is in maintenance mode. • ⊗ : This icon indicates the endpoint has no protection at all and is exposed to security threat.
Policy Inheritance	• **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 users. • **Self-managed**: Indicates the agent/group is free from the StellarOne console's policy management and can self-manage its own policy settings. • 🟢: The green light indicates the policy settings for the agent synchronizes with the StellarOne console. • ●: The gray light indicates the policy settings for the agent does not synchronize with the StellarOne console. • 🔗: The icon indicates the agent/group is free from the StellarOne console's policy management and is allowed to configure its own policy settings on site.
Approved List	Indicates the total number of applications added in the Approved List. If the endpoint is creating its Approved List, a progress bar instead will appear.
Agent Version	Indicates the firmware version of the agent.
Last Connection	Indicates the last time the agent was connected with the StellarOne console.

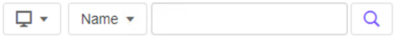
Headers	Description
Function Type	Indicates two function types of StellarProtect: - StellarProtect: for devices with Windows 7 or later versions. - StellarProtect (Legacy Mode): for devices with legacy platforms such as Windows XP/2000.
Actions	Under this header, users can - click 🛡 , the policy icon, for linking to the **General Info** policy page. - click the kebab menu (three dots menu) for organizing agents and renaming/removing groups. Please refer to *Edit Description for Agents on page 4-6* and *Organize Agents/Groups on page 4-7* for more details.

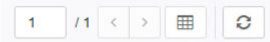


☐	Name	IP Address	Protection	Policy Inheritance	Approved List	Agent Version	Last Connection	Function Type	Actions
☑	HIE-W10X64-1	10.8.145.38		● Inherited	71805	2.0.1133	2022-09-14T16:23:...	StellarProtect	🛡 ⋮
☐	HIE-W2K19X64-1	10.8.145.40	🔒	● Inherited	43185	1.3.1012	2022-09-14T16:16:...	StellarProtect (Legacy Mode)	🛡 ⋮

Figure 4-3. The Agents Screen - Other Tools

Table 4-3. Other Tools

Tools	Description
Filter	 : This tool allows users to quickly find the agents/groups by sorting and searching. Please refer to *Filter Options for Agents/Groups on page 4-9* for more details.

Tools	Description
Table Display Settings	: This tool allows users to customize the table display settings by: • 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. • manually refreshing the table for the latest outputs

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 mainscreen 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 muiltiple agents at the same time, click the checkboxes next to the target agents or groups. Click the **Organize** tool on the toolbar.
    - To edit description for a single agent, click the kebab menu (three dots menu) corresponding to the target agent under the **Actions** header.
4. A drop-down menu appears. Click the first option **Edit Description**, and then a window appears.
5. Specify the description for the agent in the text field.
6. Click **Confirm** to complete this task.

Organize Agents/Groups

Users can organizing agents/groups by:

- renaming groups
- removing groups
- removing (unregistering) 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 kebab menu (three dots menu) of the target group under the **Actions** header. A drop-down menu appears. Select the **Rename** button and then a pop-up window appears. Delete the old group name and replace it wih 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 muiltiple 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 kebab menu (three dots menu) of the target agent/group under the **Actions** header. A drop-down menu appears. Select the **Remove** button 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 remove muiltiple 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 kebab menu (three dots menu) of the target agent under the **Actions** header.

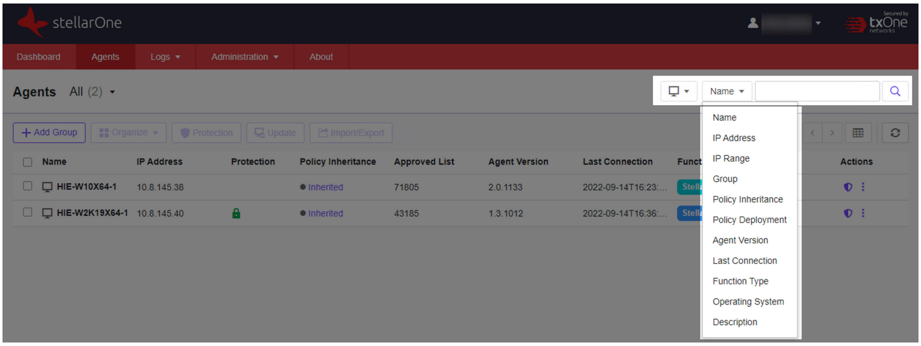
A drop-down menu appears. Select the **Move** button and then a pop-up window appears. Select the group and click **Confirm** to complete this task.

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



□	Name	IP Address	Protection	Policy Inheritance	Approved List	Agent Version	Last Connection	Funct	Actions
□	HIE-W10X64-1	10.8.145.38		● Inherited	71805	2.0.1133	2022-09-14T16:23:...	Stell	⋮
□	HIE-W2K19X64-1	10.8.145.40	🔒	● Inherited	43185	1.3.1012	2022-09-14T16:36:...	Stell	⋮

FIGURE 4-4. Filter Options

TABLE 4-4. Filter Options for Agents/Groups

OPTIONS	DESCRIPTIONS
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. Select the available group.
Policy Inheritance	Three kinds of Policy Inheritance: **Inherited**, **Customized**, and **Self-managed**, are available for selection.
Policy Deployment	The status of policy deployment from StellarOne to Agents. Select **Completed** or **In Progress**.
Agent Version	Type the Agent Version.
Last Connection	The last time the agents were connected with StellarOne. Select the default time period or select **Custom** to specify a time period. Default time period: • Last 1 hour • Last 24 hours • Last 7 days • Last 30 days
Function Type	Select **StellarProtect** or **StellarProtect (Legacy Mode)**
Operating System	Select an operating system of the target endpoints.
Description	Type the full or partial description to query specific endpoints.

Agent Protection

The **Protection** tool sends one-time commands to endpoints for triggering immediate actions, allowing users 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

To perform file updates on endpoints, users can configure Maintenance Mode settings to define a period when StellarProtect allows all file executions and adds all files that are created, executed, or modified to the Approved List. During the maintenance period, all newly-added files can be updated accompanied with real-time virus scan for consistent security. StellarProtect can learn the newly-added applications and ensure the execution of these applications are under protection.

Note

If users change the policy settings of Application Lockdown, OT Application Safeguard, and Real-Time Malware Scan during maintenance period, the policy settings will not be enforced until the maintenance period ends.

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 **Protection** button from the Tool Bar at the top of the **Agents** screen.
5. A pop-up window appears. Click **Configure Maintenace Mode** option.

6. Click **Confirm**.

7. The configuration window appears. Please read the notice and check either **Enable** or **Disable** radio button.

   - Click **Enable** to start the Maintenance Mode settings. Please go to Step 8 for next procedure.

   - 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(s) will start blocking the execution of files that are not recognized by the 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.

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

   - 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 toggle switch for enabling/disabling **Real-Time Malware Scan** is added under the Maintenance Mode option. The default setting is ON.

Note

- If users disable **Real-Time Malware Scan** in the policy setting, it is reommended to enable the **Real-Time Malware Scan** toggle switch here during maintenance period to ensure seamless protection. After maintenance period ends, the system will follow the original policy setting (Real-Time Malware Scan disabled).
- Please refer to *Real-Time Malware Scan on page 5-9* for more details about this function.

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

Update Approved List

This function allows users to update the Approved List on selected agents/ groups by several simple clicks. 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.

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 **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

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

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 **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 three sections: **Files to Scan**, **Scan Action**, and **Scan Exclusions**.

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 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 9999 MB. Files exceeding the specified file size will not be scanned.
- (Optional) Check **Aggressive scan (include all OT applications and CA files)** to allow scanning files in existing trusted list.

b. In the **Scan Action** section, users pre-define the action once threats are detected during the scanning process. Select **Quarantine** to place the suspcious or infected files detected in an isolated folder for futher checking. Select **No action** to produce only a readout of results with no actions taken on the suspicious files.

c. (Optional) The **Scan Exclusions** section provides users an option 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 **OK** to deploy the settings to the selected endpoints.
10. The **Command Deployment** window appears showing the deployment status. Click the **Close** button to close the window.

Agent Update

This section introduces how to update scan components and deploy patches for StellarProtect agents via StellarOne web console.

Topics in this section include:

- *Update Agent Components on page 4-16*
- *Deploy Agent Patches on page 4-17*

Update Agent Components

Users can update StellarProtect agent components on selected endpoints via StellarOne web console. It is recommended to update agent components regularly to protect the endpoints from 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

Users can deploy patch files for StellarProtect agents on selected endpoints via StellarOne web console. It is recommended to update agent patches regularly to protect the endpoints from 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.

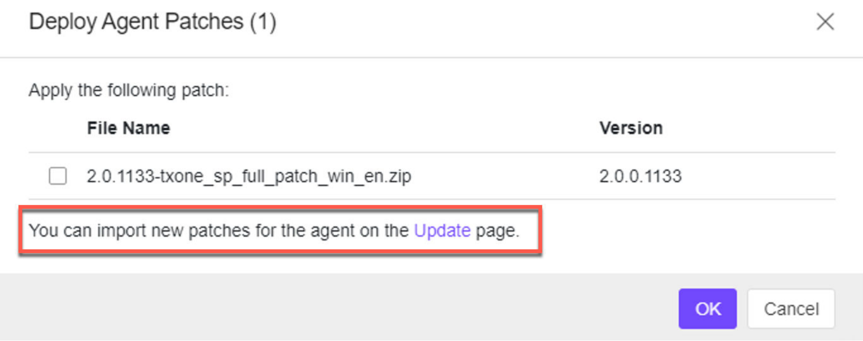
3. Select one or more endpoints (agents or groups) by clicking the checkboxes next to them.

4. Click the **Protection** 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.



Deploy Agent Patches (1)

Apply the following patch:

	File Name	Version
□	2.0.1133-txone_sp_full_patch_win_en.zip	2.0.0.1133

You can import new patches for the agent on the Update page.

FIGURE 4-5. Select the Patch Version

Note

By clicking the **Update** link, users will be directed to the *Downloads/ Updates on page 7-19* 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.

Chapter 5

Policy Setting

Unlike the settings offered on the **Agents** screen (which are one-time commands for triggering immediate actions), users configure the **Policy** settings for long-term pattern deployment on the agents.

After users organize agents into various groups and build up multi-level hierarchy among the groups (parent groups above child groups), they can configure the **Policy** settings for the top-level groups and apply the policy settings to each level by:

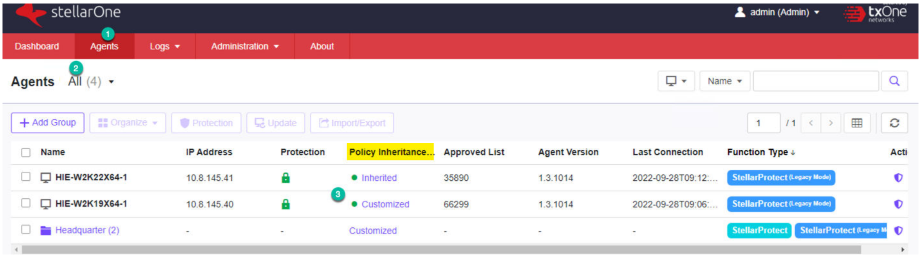
- Policy **Inherited**: The group policy is inherited from the parent group
- Policy **Customized**: The group policy is customized for specific agents/ groups via StellarOne console
- Policy **Self-managed**: The group policy is self-managed by local agents/ groups. The local agents/groups are free from the StellarOne console's policy management and the operators at local side can configure policy settings on their own.

Topics in this chapter include:

- *Agent Component Update Schedule on page 5-15*
- *Operations Behavior Anomaly Detection on page 5-16*
- *OT Application Safeguard on page 5-20*
- *DLL Injection Prevention on page 5-22*
- *Device Control on page 5-23*
- *User-Defined Suspicious Objects on page 5-24*
- *Agent Password on page 5-25*
- *Patch on page 5-25*
- *Trusted Certificates on page 5-27*

About the Policy Screen

Click the **Agents** tab in the top navigation bar of the StellarOne web console. Click the **All** group, and then a screen displays the second level of groups/ agents managed by StellarOne. Navigate to the target agent or group, and then click its corresponding **Policy Inheritance** (**Inherited**, **Customized**, or **Self-managed**). Then the **Policy** screen appears.

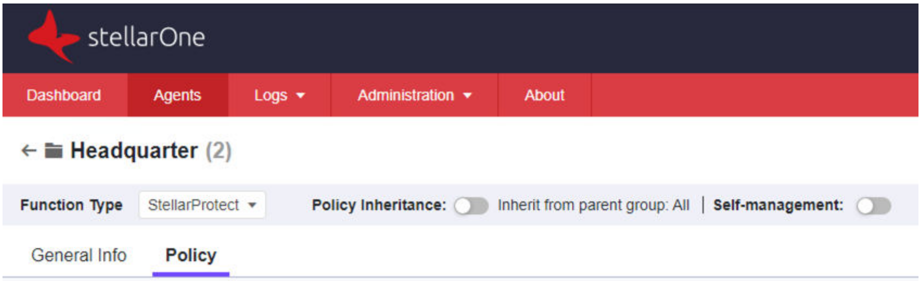


	Name	IP Address	Protection	Policy Inheritance...	Approved List	Agent Version	Last Connection	Function Type ↓	Acti
□	HIE-W2K22X64-1	10.8.145.41	🔒	● Inherited	35890	1.3.1014	2022-09-28T09:12:...	StellarProtect (Legacy Mode)	
□	HIE-W2K19X64-1	10.8.145.40	🔒	● Customized	66299	1.3.1014	2022-09-28T09:06:...	StellarProtect (Legacy Mode)	
□	Headquarter (2)	-	-	Customized	-	-	-	StellarProtect StellarProtect (Legacy M	

FIGURE 5-1. Go to the Policy Screen

Note

You can also click the the corresponding **Policy Inheritance** link of the **All** group to check it's policy settings.



← Headquarter (2)

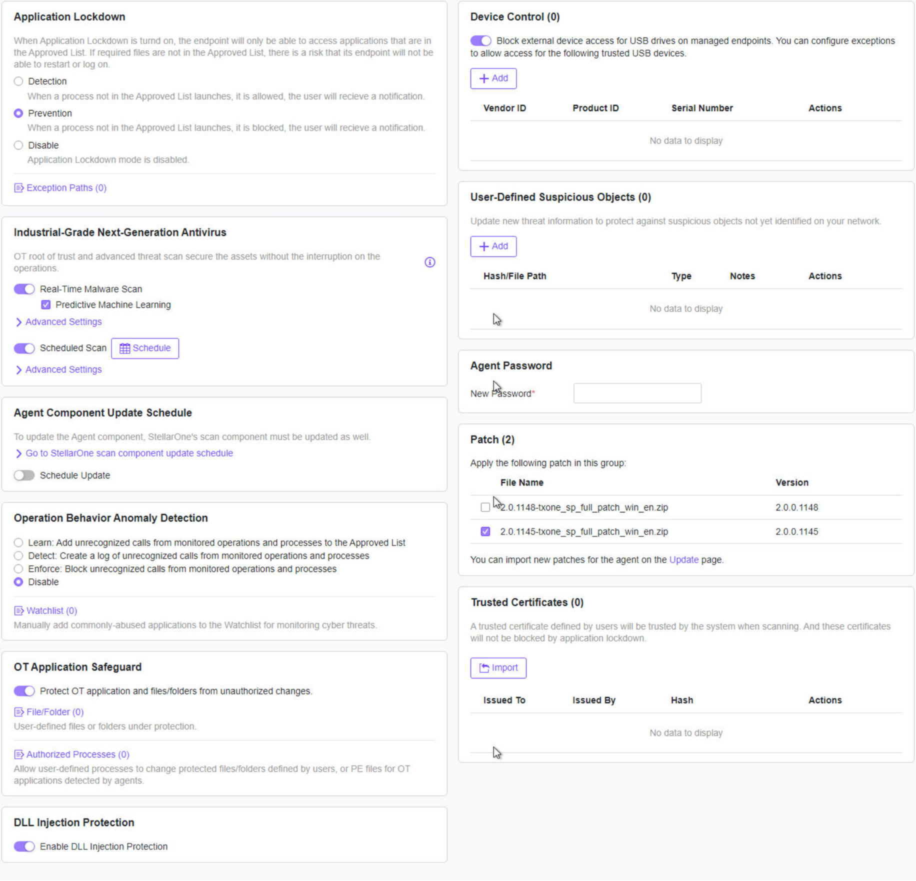
Function Type: StellarProtect

Policy Inheritance: Inherit from parent group: All | Self-management:

FIGURE 5-2. Switch Options of the Policy Screen

TABLE 5-1. Switch Options of the Policy Screen

OPTIONS	DESCRIPTION
Funtion Type	The dropdown button next to the **Function Type** allows users to switch between **StellarProtect** and **StellarProtect (Legacy Mode)**.
Policy Inheritance	The toggle button allows users to enable or disable the group policy inheritance from the parent group.
Self-management	The toggle button allows users to enable or disable the agent's self-management, which, when enabled, will set the agent free from StellarOne console's policy management.
General Info/**Policy**	The tabs allow users to switch between the displays of General Information or Policy settings.



Application Lockdown

When Application Lockdown is turnd on, the endpoint will only be able to access applications that are in the Approved List. If required files are not in the Approved List, there is a risk that its endpoint will not be able to restart or log on.

○ Detection

When a process not in the Approved List launches, it is allowed, the user will recieve a notification.

● Prevention

When a process not in the Approved List launches, it is blocked, the user will recieve a notification.

○ Disable

Application Lockdown mode is disabled.

Exception Paths (0)

Industrial-Grade Next-Generation Antivirus

OT root of trust and advanced threat scan secure the assets without the interruption on the operations.

Real-Time Malware Scan

☑ Predictive Machine Learning

Advanced Settings

Scheduled Scan Schedule

Advanced Settings

Agent Component Update Schedule

To update the Agent component, StellarOne's scan component must be updated as well.

Go to StellarOne scan component update schedule

Schedule Update

Operation Behavior Anomaly Detection

○ Learn: Add unrecognized calls from monitored operations and processes to the Approved List

○ Detect: Create a log of unrecognized calls from monitored operations and processes

○ Enforce: Block unrecognized calls from monitored operations and processes

● Disable

Watchlist (0)

Manually add commonly-abused applications to the Watchlist for monitoring cyber threats.

OT Application Safeguard

Protect OT application and files/folders from unauthorized changes.

File/Folder (0)

User-defined files or folders under protection.

Authorized Processes (0)

Allow user-defined processes to change protected files/folders defined by users, or PE files for OT applications detected by agents.

DLL Injection Protection

Enable DLL Injection Protection

Device Control (0)

Block external device access for USB drives on managed endpoints. You can configure exceptions to allow access for the following trusted USB devices.

+ Add

Vendor ID	Product ID	Serial Number	Actions
No data to display			

User-Defined Suspicious Objects (0)

Update new threat information to protect against suspicious objects not yet identified on your network.

+ Add

Hash/File Path	Type	Notes	Actions
No data to display			

Agent Password

New Password*

Patch (2)

Apply the following patch in this group:

	File Name	Version
□	2.0.1148-txone_sp_full_patch_win_en.zip	2.0.0.1148
☑	2.0.1145-txone_sp_full_patch_win_en.zip	2.0.0.1145

You can import new patches for the agent on the Update page.

Trusted Certificates (0)

A trusted certificate defined by users will be trusted by the system when scanning. And these certificates will not be blocked by application lockdown.

Import

Issued To	Issued By	Hash	Actions
No data to display			

FIGURE 5-3. Functions of the Policy Screen

TABLE 5-2. Functions of the Policy Screen

FUNCTION	DESCRIPTION
Application Lockdown	This function provides protection by only allowing the access of the applications that are in the Approved List. Please refer to *Configure Application Lockdown on page 5-7* for more details.

Function	Description
Industrial-Grade Next-Generation Antivirus	The industrial-grade next-generation antivirus provides real-time and scheduled scan settings. Please refer to *Industrial-Grade Next-Generation Antivirus on page 5-9* for more details.
Agent Component Update Schedule	Users can schedule the component update for agents. Please refer to *Agent Component Update Schedule on page 5-15* for more details.
Operations Behavior Anomaly Detection	This function provides protection against fileless attacks. Please refer to *Operations Behavior Anomaly Detection on page 5-16* for more details.
OT Application Safeguard	This function ensures continuous operations by allowing the OT applications recognized by StellarProtect to be updated without being blocked or restricted. Please refer to *OT Application Safeguard on page 5-20* for more details.
DLL Injection Protection	This function provides protection against DLL hijacking attacks. Please refer to *DLL Injection Prevention on page 5-22* for more details.
Device Control	This function provides protection against unauthorized access of USB devices. Please refer to *Device Control on page 5-23* for more details.
User-Defined Suspicious Objects	This function allows users to manually add suspicious file hashes or paths to prevent the endpoints from be infected by these files. Please refer to *User-Defined Suspicious Objects on page 5-24* for more details.
Agent Password	This function allows the administrators to change the StellarProtect admin password for all connected endpoints via StellarOne console. Please refer to *Agent Password on page 5-25* for more details.
Patch	This function allows the administrator to deploy patch files to all agents under the same group policy. Please refer to *Patch on page 5-25* for more details.
Trusted Certificates	This function allows the administrator to add new trusted certificates in the policy settings. Please refer to *Trusted Certificates on page 5-27* for more details.

Configure 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. 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. Navigate to the target agent or group and click the **Policy Inheritance** link.
4. Go to the **Application Lockdown** section.
5. Three modes are avaible 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, please refer to the *Lockdown Exclusions on page 5-7*.

Configure Exception Paths

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

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. Navigate to the target agent or agent group.

4. Go to the Policy page by either way listed below.

    - Click the **Policy Inheritance** link.

    - Click the Policy icon under the **Actions** header, and then click the **Policy** tab.

5. Click the **Exception Paths** under the **Application Lockdown** feature.

    - For adding exception paths:

        a. Click the **+Add** button, and then a pop-up window appears.

        b. Select among **Folder**, **File**, or **Regular Expression** and input the required information in the corresponding text field.

        Note

        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 under the **Actions** header.

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

Industrial-Grade Next-Generation Antivirus

The Industrial-Grade Next-Generation Antivirus provides ICS root of trust and advanced threat scan to secure the endpoints without interrupting the endpoints's operations. Related settings include:

- *Real-Time Malware Scan on page 5-9*
- *Scheduled Scan on page 5-11*

Real-Time Malware Scan

Real-time Malware Scan provides persistent and ongoing file scan for the endpoints. Each time a file is received, opened, downloaded, copied, or modified, **Real-time Malware Scan** always scans the file for security assessment. After performing the **Real-time Malware 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, a notification message appears indicating the name of the infected file and the specific security risk.

Moreover, a persistent scan cache is maintained and reloaded each time the **Real-time Malware Scan** is executed. The **Real-time Malware 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. 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. Navigate to the target agent or agent group and click the **Policy Inheritance** link.
4. Go to the **Real-time Malware Scan** in the **Industrial-Grade Next-Generation Antivirus** section.
5. Enable the **Real-Time Malware Scan** by simply clicking the toggle to switch it on.

Note

You can refer to the *Advanced Settings on page 5-12* for more configurations for the types of the files to be scanned, the action 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.

Turn on the **Predictive Machine Learning** function by simply checking it after you enable the **Real-Time Malware Scan**.

Scheduled Scan

Users 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. 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. Navigate to the target agent or agent group and click the **Policy Inheritance** link.
4. Go to the **Scheduled Scan** in the **Industrial-Grade Next-Generation Antivirus** section.
5. Enable the **Scheduled Scan** function by simply clicking the toggle to switch it on.
6. Click the calendar icon. A **Schedule** window appears.
7. 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., Feburary only has 28 days (29 days on a leap year), 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.

8. Specify the scan start time in the **Start Time** field (by default it's set as **00:00**).

9. Click **Confirm** to complete the setting.

Note

You can refer to the *Advanced Settings on page 5-12* for more configurations for the types of the files to be scanned, the action after possible security risk is detected, and the scan exclusion list.

Advanced Settings

The **Advanced Settings** for the **Real-Time Malware Scan** and **Scheduled Scan** provides more configurations for the types of the files to be scanned, the action after possible security risk is detected, and the scan exclusion list.

Advanced Settings for Real-Time Malware Scan

Procedure

1. Go to **Agents** > **Policy** > **Industrial-Grade Next-Generation Antivirus**.
2. Click the **Advanced Settings** in the **Real-Time Malware 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 9999 MB. Files exceeding the specified file size will not be scanned.

6. In the **Scan Action** section, users pre-define the action once threats are detected during the scanning process. Select **Quarantine** to place the suspicious files detected in an isolated folder for futher checking. Select **No action** to produce only a readout of results with no actions taken on the suspicious files.

7. The **Scan Exclusions** section provides users an option 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 the folder/file paths or file extensions.

8. Click **Confirm** to complete the advanced settings for Real-Time Malware Scan.

Advanced Settings for Scheduled Scan

Procedure

1. Go to **Agents** > **Policy** > **Industrial-Grade Next-Generation Antivirus**.

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**, **Scan Action**, and **Scan Exclusions**.

5. 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 compressed files** and select the **Maximum layers** between 1 and 20 for the compressed files.

   - (Optional) To skip scanning files over a certain size, check **Skip files larger than** and specify the file size between 1 and 9999 MB. Files exceeding the specified file size will not be scanned.

6. In the **Scan Action** section, users pre-define the action once threats are detected during the scanning process. Select **Quarantine** to place the suspicious files detected in an isolated folder for futher checking. Select **No action** to produce only a readout of results with no actions taken on the suspicious files.

7. (Optional) The **Scan Exclusions** section provides users an option 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 .

8. Click **Confirm** to complete the advanced settings for Scheduled Scan.

Agent Component Update Schedule

Users can configure the component update schedule for the StellarProtect agents via StellarOne webconsole; thus the system can run component update automatically at users' assigned time frequency.

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. Navigate to the target agent or group and click its corresponding **Policy Inheritance** link.

4. On the **Policy** tab page, toggle on the **Schedule Update** in the **Agent Component Update Schedule** section.

   Tip

   It is suggested to determine the agent's component update schedule by referring to the StellarOne console's component update schedule setting first.

5. (Optional) Click **StellarOne scan component update shcdule** and view the current settings for StellarOne's component update schedule.

   Note

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

6. After the **Schedule Update** is toggled on, radio buttons for setting the **Frequency** and **Start Time** appear, enabling users to schedule component update for the agent(s.)

   - The default setting for **Weekly** update is **every Sunday**.
   - The default setting for **Monthly** update is **on day 01**
   - The default setting for **Start Time** is **20:00**.

   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), it is recommended to select **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.

Operations Behavior Anomaly Detection

StellarProtect provides the **Operations Behavior Anomaly Detection** to protect the endpoints from fileless attacks.

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. Navigate to the target agent or group and click the **Policy Inheritance** link.

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

Basically, the **Operations Behavior Anomaly Detection** has four modes:

- **Learn**: Under this mode, StellarProtect will monitor unrecognized program calls and add them to the trusted-operation list. In this way, the agent will continuously learn more and more OT-related program call behaviors.
- **Detect**: Under this mode, StellarProtect wil monitor unrecognized program calls and log them for future analysis.
- **Enforce**: Under this mode, StellarProtect will monitor unrecognized program calls and block them to secure the endpoint.
- **Disable**: Under this mode, the **Operations Behavior Anomaly Detection** is disabled and protection for fileless attacks is turned off.

Note

- In either **Detect** or **Enforce** mode, users have one more option, **Aggressive Mode,** for stronger antivirus protection. Please refer to *Aggressive Mode on page 5-17* for more details.
- Users can manually add commonly-abused applications used in operations and processes to the **Watchlist** for strengthening security monitoring. Please refer to *Watchlist on page 5-19* for more details.

Aggressive Mode

In either **Detect** or **Enforce** mode, users have one more option, **Aggressive Mode,** for stronger antivirus protection. This feature helps enhance protection by adding parameter identification in the monitoring task, allowing users to check the operation process and its accompanied changes in parameters under monitoring.

Note

The **Aggressive Mode** executes strict rules for ensuring the utmost security by allowing only the recognized calls with identified parameters from monitored operation processes.

Below is an example of how the **Aggressive Mode** works.

1. When users select the **Learn** mode under the **Operations Behavior Anomaly Detection**, the following process is learned:

    - `explorer.exe → cmd.exe → powershell.exe → script.ps1 argument1`

2. When users switch to the **Detect** or **Enforce** mode and disable the **Aggressive Mode**, StellarProtect will not block recognized program calls with unidentified parameters, thus the following process is allowed:

    - `explorer.exe → cmd.exe → powershell.exe → script.ps1 argument2`

    Note

    The `argument2` is the new data that's passed into the process and thus changes the process' parameter, which does not count as an unrecognized application in the process when **Aggressive Mode** is disabled.

3. When the **Aggressive Mode** is enabled, no matter it's under the **Detect** or **Enforce** mode, the following process is not allowed:

    - `explorer.exe → cmd.exe → powershell.exe → script.ps1 argument2`

    Note

    The `argument2` is detected as an unrecognized parameter that must be blocked when **Aggressive Mode** is enabled.

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

- `explorer.exe` → `cmd.exe` → `powershell.exe` → `script.ps1 argument1`

Watchlist

Users can manually add commonly-abused applications used in operations and processes to the **Watchlist** for strengthening security monitoring. By default, StellarProtect monitors `Powershell.exe`, `wscript.exe`, `cscript.exe`, `mshta.exe`, `psexec.exe` when the **Operations Behavior Anomaly Detection** is enabled.

Procedure

1. Go to **Agents** > **Policy Inheritance**, scroll down and find the **Operations Behavior Anomaly Detection**. Enable **Operations Behavior Anomaly Detection** by selecting **Learn**, **Detect**, or **Enforce**.

   Note

   The default setting for **Operations Behavior Anomaly Detection** is **Disable**. If users don't enable **Operations Behavior Anomaly Detection**, the process monitoring will not be activated.

2. In addition to the default applications that will be monitored by StellarProtect, if users need to add other applications for monitoring, please click the **Watchlist** link.

3. The **Watchlist** window appears. Click **+Add** and then specify the application to be monitored.

4. Click **Add** and the added application appears in the **Monitored Application** list.

5. Click **Close** to close the window.

   Note

   Users can delete the added application(s) by clicking the trash-can icon under the **Actions**.

6. Users can check the Agent event logs to see if there's any anomalous operation or process detected. Please refer to *Agent Events on page 6-2* for more details.

OT Application Safeguard

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

Note

Upon launch, StellarProtect will auto-detect currently-installed OT applications and put them under protection. The recognized OT applications will be shown on the **General Info** tab page.

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. Navigate to the target agent or agent group and click the Policy icon under the **Actions** header.
4. The **General Info** screen appears. Check the OT Applications automatically recognized by the StellarProtect agent.

Note

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. Please refer to *Configure Maintenance Mode on page 4-11* for how to enable this function.

5. Users can also manually add the installation path for the application into the Safeguard's protection list.

   a. Click the **Policy** tab 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 a pop-up 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 users want to protect all files inside the selected folder, please uncheck the **Executable files only** radio button.

   Tip

   By unchecking the **Executable files only** option, 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. Users can also add user-defined processes.

   a. Go to **Policy** > **OT Application Safeguard**, and then click the **Authorized Processes** option.

b. A pop-up window appears. Click the **+Add** button, and then specify the authorized processes in the corresponding text fields.

Important

By adding the authorized process, users may set other applications to be trusted and change the protected files/folders previousely 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. Click the **Agents** tab in the top navigation bar of the StellarOne web console.
2. Click the **All** group on the **Agents** screen.
3. The **Agents** screen displays a list of agents managed by StellarOne. Navigate to the target agent or group and click its corresponding **Policy Inheritance** link.
4. Scroll down and find the **DLL Injection Prevention** at the left side of the screen.

5. Click the toggle **Enable DLL Injection Prevention** to enable it.

Device Control

StellarProtect agent supports one-time USB access permission on site; while StellarOne console offers permanent USB access permission via remote configuration. For the local agent, when USB device control has been enabled, every time users plug in USB devices, the agent will prompt a message for users to confirm if the USB device access is allowed. On top of that, StellarOne users with administrator or operator role can add trusted USB devices into the **Device Control** list, allowing the specified devices to access directly without further check, thus facilitating the trusted USB access for good.

Procedure

1. Go to **Agents**.
2. Click the **All** group on the **Agents** screen. The **Agents** screen displays a list of agents managed by StellarOne.
3. Navigate to the target agent or group and click its corresponding link under the **Policy Inheritance** header.
4. Make sure the **Device Control** toggle is switched on.
5. Click **Add**. The **Add Trusted USB Device** window appears.
6. Specify at least one of the following information for the trusted USB device.
   - **Vendor ID**
   - **Product ID**
   - **Serial number**
7. Click **OK** to complete the setting.

8. Check if the USB device is successfully added in the device control list.

9. (Optional) To edit the USB device information, select the USB device and click the edit icon under the **Actions** header. A pop-up window appears. Edit the USB device information in the related text fields and then click **OK**.

10. (Optional) To remove a USB device from trusted list, choose either way listed below.

    - For removing mutiple 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 devices, click the edit icon under the **Actions** header.

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

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.

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. Navigate to the target agent or group and click its corresponding **Policy Inheritance** link.

4. Scroll down and find the **User-Defined Suspicious Object** at the right side of the screen.

5. Click **Add**. The **Add Item to User-Defined Suspicious Objects** window appears.
6. Select **Hash** or **File Patch** as the suspicious file type.
7. Specify the file hash or path in the corresponding text field.
8. (Optional) Specify notes in the **Notes** text field.
9. Click **OK** to complete this task.

Agent Password

This function allows OT administrators to change the StellarProtect admin password for all connected endpoints via the StellarOne console.

Procedure

1. Click the **Agents** tab in the top navigation bar of the StellarOne web console. The **Agents** screen displays a list of agents managed by StellarOne. Navigate to the target agent or group and click the corresponding **Policy Inheritance** link.
2. Scroll down and find the **Agent Password** at the right side of the screen.
3. 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

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 every time under each group policy.

Procedure

1. Click the **Agents** tab in the top navigation bar of the StellarOne web console. The **Agents** screen displays a list of agents managed by StellarOne. Navigate to the target agent or group and click the corresponding **Policy Inheritance** link.

2. Scroll down and find the **Patch** at the bottom right corner of the screen.

3. Click the checkbox next to the version of the patch file for deployment.

   Note

   Users can import new patches for the agent on the *Downloads/Updates on page 7-19* page.

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

   Note

   Since StellarProtect is able to use global policies for all agents as well as group policy for group-owned machines to conduct the patching process on multiple devices, before you select agent version please note the following:

   - Global policy is the default agent landing policy, so every agent will apply this policy first before moving to other groups. We suggest that the global policy should use lower agent version as its base policy.

   - If you don't want to set any agent version for patch deployment, please unclick all checkboxes next to the agent version patch files in the **Patch** section.

Important

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

Trusted Certificates

Trusted Certificates provides an import function allowing the administrator to add new trusted certificates.

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. Navigate to the target agent or group and click the corresponding link under the **Policy Inheritance** header.
4. Go to **Policy** > **Trusted Certificates**.
5. Click **Import** to import the selected trusted certificate file.
6. To remove the trusted certificate(s), choose either way listed below.
   - For removing mutiple 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 edit icon under the **Actions** header.

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

Chapter 6

Logs

This chapter describes how to access StellarOne-generated logs and the logs related to StellarProtect 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 6-4*
- *System Logs on page 6-8*
- *Audit Logs on page 6-10*

Agent Events

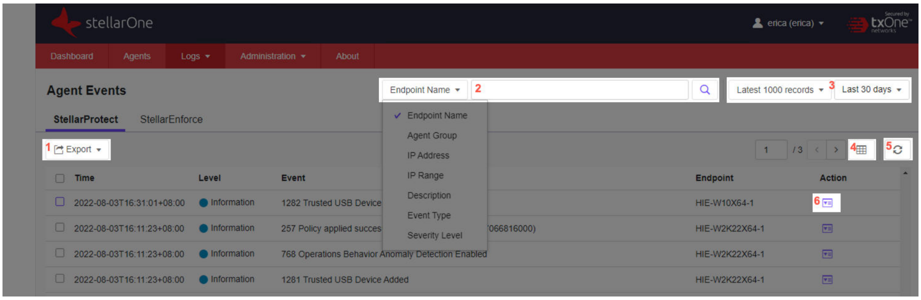
The StellarOne collects activities on agents and log them in the **Agent Events**.

Procedure

1. Mouse over the **Logs** tab in the top navigation bar of the StellarOne web console. Click the **Agent Events** option.
2. Click the **StellarProtect** tab, the StellarProtect agent event logs appear.
3. Regarding how to search for the relevant log messages for troubleshooting or analysis. Please refer to *Agent Events Log Filtering on page 6-3* for detailed procedures.

> **Note**
>
> Please refer to *StellarProtect Agent Event Log Descriptions on page A-2* in the Appendices for more details about event IDs and corresponding log information.

About Agent Events Screen



□	Time	Level	Event	Endpoint	Action
□	2022-08-03T16:31:01+08:00	● Information	1282 Trusted USB Device	HIE-W10X64-1	
□	2022-08-03T16:11:23+08:00	● Information	257 Policy applied succes 066816000)	HIE-W2K22X64-1	
□	2022-08-03T16:11:23+08:00	● Information	768 Operations Behavior Anomaly Detection Enabled	HIE-W2K22X64-1	
□	2022-08-03T16:11:23+08:00	● Information	1281 Trusted USB Device Added	HIE-W2K22X64-1	

FIGURE 6-1. StellarProtect Agent Events Logs

Table 6-1. About Agent Events Screen

Item	Description
(1) Export	Users can export log list as an `.csv` file by clicking the **Export** button. It provides a drop-down menu consisting of: • **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	This tool allows users to search for the relevant log messages for troubleshooting or analysis. Please refer to *Agent Events Log Filtering on page 6-3* for detailed procedures.
(3) Log display setting	Users can customize how many logs to be displayed either by: • the number of the latest log records • the logs generated within a particular period
(4) Screen display setting	By clicking this button, users can customize the screen display by: • selecting how many logs to be displayed per page • hiding certain contents by unchecking **Time**, **Severity**, **User ID**, **Client IP**, or **Message** in the **Cusomize Table Display** window.
(5) Refresh	The button allows users to manually refresh the screen for the latest log outputs.
(6) Action	

Agent Events Log 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** > **StellarProtect**. Click the **Endpoint Name** 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 **Endpoint Name**, **IP Address**, **IP Range**, or **Description**, and then type the search strings in the search field.

    - Select the **Agent Group**, **Event Type**, or **Severity Level**, a search box with an arrow pointing downwards appears. Tap on it to see the options under different categories.

        - **Agent Group**: 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 *StellarProtect Agent Event Log Descriptions on page A-2* for more details about different event types.

        - **Severity Level**: A drop-down menu with options of **Warning**, **Critical**, and **Information** appears. Select one of them for viewing the log records by different levels.

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.

Server Events

Activities on StellarOne Servers and configuration deployed on StellarProtect Agents by StellarOne are logged and shown in the **Server Events** screen.

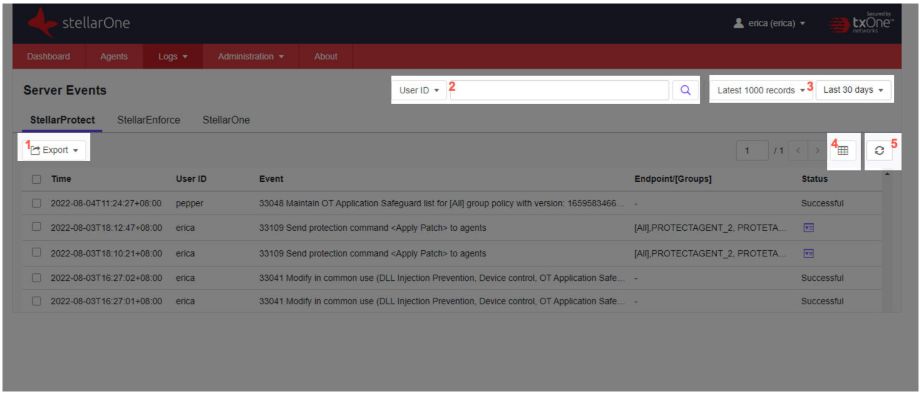
Procedure

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** tab, the configuration events deployed on StellarProtect Agents by StellarOne appear.

3. Click the **StellarOne** tab, the StellarOne server event logs appear.

About Server Events Screen



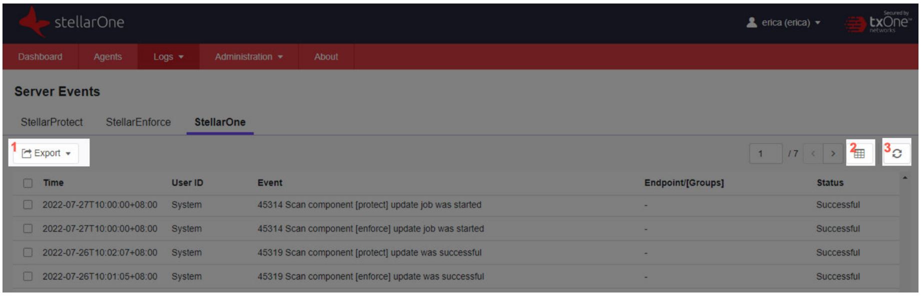
□	Time	User ID	Event	Endpoint/[Groups]	Status
□	2022-08-04T11:24:27+08:00	pepper	33048 Maintain OT Application Safeguard list for [All] group policy with version: 1659583466...	-	Successful
□	2022-08-03T18:12:47+08:00	erica	33109 Send protection command <Apply Patch> to agents	[All],PROTECTAGENT_2, PROTETA...	
□	2022-08-03T18:10:21+08:00	erica	33109 Send protection command <Apply Patch> to agents	[All],PROTECTAGENT_2, PROTETA...	
□	2022-08-03T16:27:02+08:00	erica	33041 Modify in common use (DLL Injection Prevention, Device control, OT Application Safe...	-	Successful
□	2022-08-03T16:27:01+08:00	erica	33041 Modify in common use (DLL Injection Prevention, Device control, OT Application Safe...	-	Successful

FIGURE 6-2. Server Events Logs for SterllarProtect

TABLE 6-2. About StellarProtect Server Events Screen

ITEM	DESCRIPTION
(1) Export	Users can export log list as an `.csv` file by clicking the **Export** button. It provides a drop-down menu consisting of: • **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
(2) Filter	This tool allows users to search for the relevant log messages for troubleshooting or analysis. Please refer to *Server Events Log Filtering on page 6-7* for procedures.
(3) Log display setting	Users can customize how many logs to be displayed either by: • the number of the latest log records • the logs generated within a particular period
(4) Screen display setting	By clicking this button, users can customize the screen display by: • selecting how many logs to be displayed on one page • hiding certain contents by unchecking **Time**, **Severity**, **User ID**, **Client IP**, or **Message** in the **Cusomize Table Display** window.
(5) Refresh	The button allows users to manually refresh the screen for the latest log outputs.



Server Events

Time	User ID	Event	Endpoint/[Groups]	Status
2022-07-27T10:00:00+08:00	System	45314 Scan component [protect] update job was started	-	Successful
2022-07-27T10:00:00+08:00	System	45314 Scan component [enforce] update job was started	-	Successful
2022-07-26T10:02:07+08:00	System	45319 Scan component [protect] update was successful	-	Successful
2022-07-26T10:01:05+08:00	System	45319 Scan component [enforce] update was successful	-	Successful

Figure 6-3. Server Events Logs for SterllarOne

TABLE 6-3. About StellarOne Server Events Screen

ITEM	DESCRIPTION
(1) Export	Users can export log list as an `.csv` file by clicking the **Export** button. It provides a drop-down menu consisting of: • **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	By clicking this button, users can customize the screen display by: • selecting how many logs to be displayed per page • hiding certain contents by unchecking **Time**, **Severity**, **User ID**, **Client IP**, or **Message** in the **Cusomize Table Display** window.
(3) Refresh	The button allows users to manually refresh the screen for the latest log outputs.

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 *StellarProtect Server Event Log Descriptions on page A-18* 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 *StellarProtect Server Event Log Descriptions on page A-18* and *StellarOne Server Event Log Descriptions on page A-20* in the Appendices for more details about event IDs and corresponding log information..

System Logs

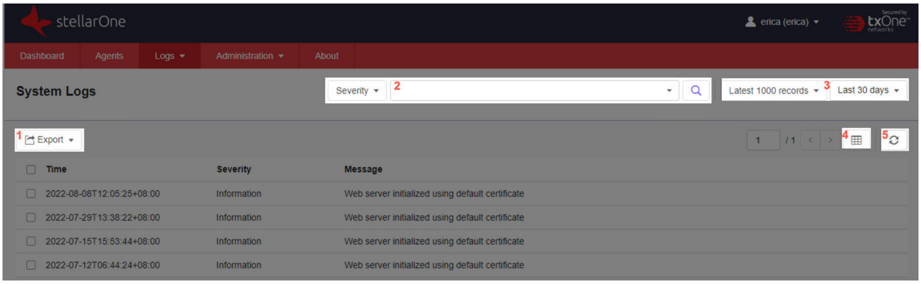
Internal system processes generated by StellarOne Servers are logged and shown in the **System Logs**.

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



□	Time	Severity	Message
□	2022-08-08T12:05:25+08:00	Information	Web server initialized using default certificate
□	2022-07-29T13:38:22+08:00	Information	Web server initialized using default certificate
□	2022-07-15T15:53:44+08:00	Information	Web server initialized using default certificate
□	2022-07-12T06:44:24+08:00	Information	Web server initialized using default certificate

Figure 6-4. System Logs Screen

Table 6-4. About System Logs Screen

Item	Description
Export	Users can export log list as an `.csv` file by clicking the **Export** button. It provides a drop-down menu consisting of: • **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	Users can filter logs by selecting or specifying certain severity level directly in the search bar. The severity levels are listed as below: • Warning • Notice • Information • Debug • Emergency • Alert • Critical • Error 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.
Log display setting	Users can customize how many logs to be displayed either by: • the number of the latest logs records • the logs generated within a particular period
Screen display setting	By clicking this button, users can customize the screen display by: • 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	The button allows users to manually refresh the screen for the latest log outputs.

Audit Logs

The **Audit Logs** screen displays the user activities such as login, logout, or account creation/deletion.

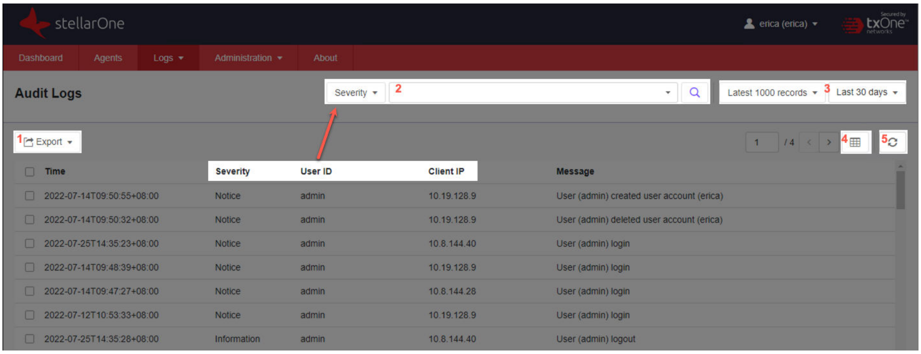
Procedure

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



	Time	Severity	User ID	Client IP	Message
□	2022-07-14T09:50:55+08:00	Notice	admin	10.19.128.9	User (admin) created user account (erica)
□	2022-07-14T09:50:32+08:00	Notice	admin	10.19.128.9	User (admin) deleted user account (erica)
□	2022-07-25T14:35:23+08:00	Notice	admin	10.8.144.40	User (admin) login
□	2022-07-14T09:48:39+08:00	Notice	admin	10.19.128.9	User (admin) login
□	2022-07-14T09:47:27+08:00	Notice	admin	10.8.144.28	User (admin) login
□	2022-07-12T10:53:33+08:00	Notice	admin	10.19.128.9	User (admin) login
□	2022-07-25T14:35:28+08:00	Information	admin	10.8.144.40	User (admin) logout

FIGURE 6-5. Audit Logs Screen

TABLE 6-5. About Audit Logs Screen

ITEM	DESCRIPTION
(1) Export	Users can export log list as an `.csv` file by clicking the **Export** button. It provides a drop-down menu consisting of: • **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	This tool allows users to search for the relevant log messages for troubleshooting or analysis. Please refer to *Audit Log Filtering on page 6-12* for procedures.

Item	Description
(3) Log display setting	Users can customize how many logs to be displayed either by: • 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: • selecting how many logs to be displayed per page • hiding certain contents by unchecking **Time**, **Severity**, **User ID**, **Client IP**, or **Message** in the **Cusomize 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.
        - Warning
        - Notice

- Information
- Debug
- Emergency
- Alert
- Critical
- Error

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

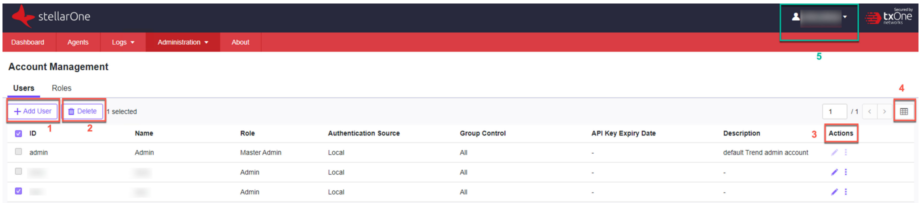
This chapter introduce the StellarOne web console's administration settings.

Topics in this chapter includes:

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**. The former one allows users to manage accounts; the latter one provides information about different privileges for different accounts.



Account Management

Users Roles

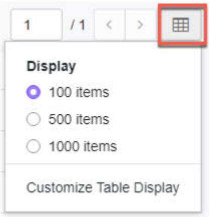
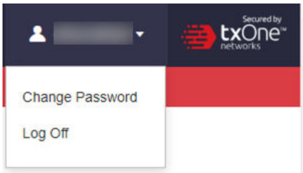
1 selected

☑ ID	Name	Role	Authentication Source	Group Control	API Key Expiry Date	Description	Actions
□ admin	Admin	Master Admin	Local	All	-	default Trend admin account	
□ [redacted]	[redacted]	Admin	Local	All	-	-	
☑ [redacted]	[redacted]	Admin	Local	All	-	-	

Figure 7-1. Account Management Screen

Table 7-1. About Account Management Screen - Users

Item	Description
(1) **+Add User**	This button allows users to add account(s) for accessing StellarOne web console. Please refer to *Add Accounts on page 7-7* for procedures.
(2) **Delete**	This button allows users to delete account(s). Please refer to *Delete Accounts on page 7-9* for procedures.
(3) **Actions**	This button allows users to edit or delete account(s). Please refer to *Edit Accounts on page 7-8* for procedures.

Item	Description
(4) **Screen display setting**	 1 / 1 Display ● 100 items ○ 500 items ○ 1000 items Customize Table Display By clicking this button, users can customize the screen display by: • 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**	 [redacted] Secured by txOne networks Change Password Log Off Click the account icon at the top-right corner of the screen to change your password or log off.

For more information about the **Roles** tab page, please visit *Account Types on page 7-3*.

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	• Manage StellarOne: The privilege of configuring system settings • Account Management: The privilege of managing StellarOne accounts • 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
Operator	Asset control	• 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	• Read only for the Dashboard, Agent Events logs, as well as the configurations of the Agent's Policy, Scheduled Report, Notification, and StellarOne's Scan Component information. • Allowed to download the Agent's installer package and `Group.ini` file • 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	√	√	
Scan now	√	√	
Update Approved List	√	√	
Update agent components	√	√	
Deploy agent patch	√	√	
Check connection	√	√	
Collect event logs	√	√	
Import / Export (Approved List / agent configuration)	√	√	
Organize (edit description / move / delete)	√	√	

Task	Account Privilege Allowed		
	Admin	Operator	Viewer
Configure group policy	√	√	
Configure global policy	√	√	
Monitor agent event logs	√	√	√
Monitor server event logs	√	√	
Monitor system logs	√	√	
Monitor audit logs	√	√	
Account management	√		
Single Sign-On	√		
System time settings	√	√	
Syslog forwarding	√	√	
Log purge	√	√	
Schedule report	√	√	√
Notification settings	√	√	√
SMTP settings	√	√	
Proxy settings	√	√	
Downloads / Updates	√	√	√
Firmware update	√		

Task	Account Privilege Allowed		
	Admin	Operator	Viewer
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 7-3* 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.

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).

Delete Accounts

This section describes how to delet 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 wan 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).

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 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. Upload the StellarOne metadata XML file to your IdP, and then download the IdP metadata XML file.
5. Click the **Upload** button to upload the IdP metadata XML file to StellarOne web console to complete the SAML 2.0 single sign-on configuration.

   Important

   The IdP metadata XML file must be re-uploaded if there is a configuration change on the IdP.

6. After the IdP metadata XML file is uploaded, the **Test Connection** button will appear.

7. Click the **Test Connection** button to test the IdP connection with StellarOne.

> **Note**
>
> Invalid logon error message may appear after the SAML configuration is completed. Please refer to *Resolving the SSO Issue on page 7-12* to check email setting in IdP server, and system time synchronization in IdP and StellarOne servers.

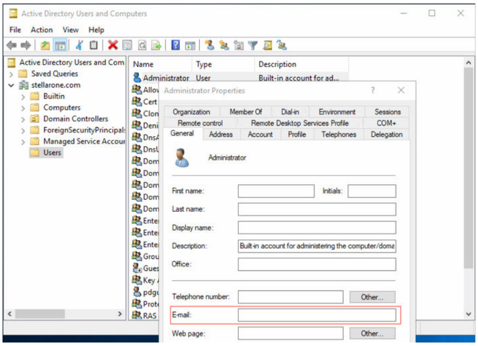
Resolving the SSO Issue

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.



Administrator | User | Built-in account for ad...

Administrator

First name:

Initials:

Last name:

Display name:

Description: Built-in account for administering the computer/doma

Office:

Telephone number:

E-mail:

Web page:

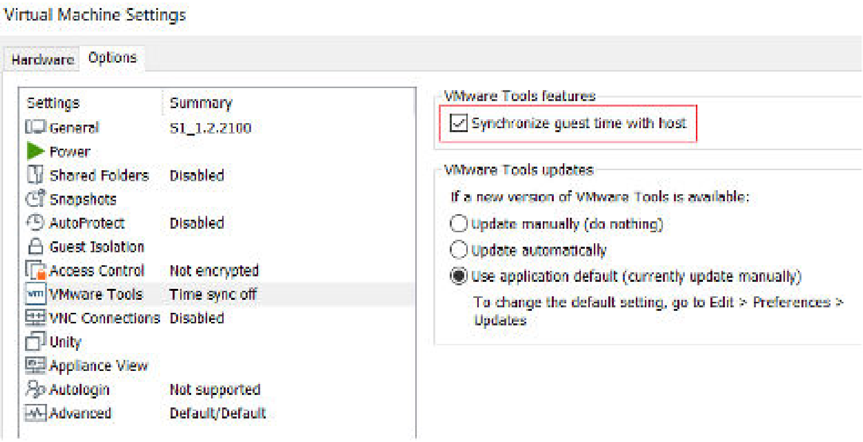
FIGURE 7-2. Resolving SSO Issue - Email Check

4. Make sure the system time in IdP and StellarOne servers are synchronized. Below are suggested procedures for time synchronization setting.

   a. Ensure the time in the IdP server synchronizes with the host PC that runs the StellarOne Virtual Machine (VM).

   b. Open the VM settings of StellarOne. Go to **Options** > **VMware Tools**.

   c. Click the checkbox of **Synchronize guest time with host**, and then click **OK**.



Virtual Machine Settings

Settings	Summary
General	S1_1.2.2100
Power	
Shared Folders	Disabled
Snapshots	
AutoProtect	Disabled
Guest Isolation	
Access Control	Not encrypted
VMware Tools	Time sync off
VNC Connections	Disabled
Unity	
Appliance View	
Autologin	Not supported
Advanced	Default/Default

VMware Tools features

☑ Synchronize guest time with host

VMware Tools updates

If a new version of VMware Tools is available:

○ Update manually (do nothing)

○ Update automatically

● Use application default (currently update manually)

To change the default setting, go to Edit > Preferences > Updates

FIGURE 7-3. Virtual Machine Settings - Time Synchronization

System Time

Users can configure the system time settings for the StellarOne web console.

Procedure

1. Go to **Administration** > **System Time**.

2. In the **Date and Time** section, click the edit icon to select the date and time.

3. Click **Apply**.

4. In the **Time Zone** section, click the arrow downwards in the blank bar. A drop-down menu with global time zone appears.

5. Select the appropriate time zone for the sytem, and then click **Save** to complete 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.

   Please refer to *Agent Event Format on page B-2*, *StellarProtect Server Event Format on page B-5*, or *StellarOne Server Event Format on page B-6* in the Appendices for details about the logs forwarded in the Common Event Format (CEF).

Log Purge

This feature allows users to manage the volume of log files for optimizing StellarOne's disk space usage.

Procedure

1. Go to **Administration** > **Log Purge**.
2. There are two ways for log purge settings. Users can choose from either one listed below:

    - **Purge Now**:

        Use this setting to purge logs immediately.

        a. Click the drop-down menu next to the **Purge** title, and then select the log types to be purged.

            - All Logs
            - System Log, Audit Log, Server Events, or Agent Events

        b. Click the drop-down menu next to the **older than** title, and then select a specified time frame. The files older than 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)

        c. Click the drop-down menu next to the **Keep at most** title, and then select the maximum 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 the **Purge** button, 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 wan to purge: **System Log**, **Audit Log**, **Server Events**, or **Agent Events**.

  b. Click the drop-down menu next to the **older than** title, and then select a specified time frame. The files older than 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)

  c. Click the drop-down menu next to the **Keep at most** title, and then select the maximum 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 the **Save** button, and the event logs will be automatically purged once per day.

Notification and SMTP Settings

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. (Optional) If the SMTP server requires authentication, click the checkbox next to **SMTP server requires authentication**. Specify the **User name** and **Password** as the SMTP server authentication credential.
4. Click the **Send Test Email** button to send a test email from StellarOne (This step is essential for Step 12).
5. Click **Save** to complete the SMTP setting.
6. Go to **Administration** > **Notification** for notification criteria and email setting.
7. Under the **Warning Level Agent Events**, click the **Send warning level agent events** toggle to enable it.

   Note

   When the switch under **Warning Level Agent Events** is enabled, StellarOne console will send a notification to your email when an incident that triggers a "**Warning**" happens.

8. Under the **Outbreak**, click the **Send outbreak notifications** toggle to enable it.

   Note

   When the switch under **Outbreak** is enabled, StellarOne console will send a notification to your email when more than a specified number of open warning messages have appeared in a specified time period.

9. 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).

10. Under **Email Notifications**, specify the email address for receiving the notifications in the **Send to** field.

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

12. Go to the specified email box to check if you receive the test email sent from StellarOne (refer to Step 4).

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 `opcmd.exe` Command Line Interface tool on the local StellarProtect Agent.

Downloads/Updates

The **Downloads/Updates** page allows users to configure scan component settings for StellarOne, to download the Agent Installer Package and import or delete the patch files for StellarProtect, as well as to download the `Group.ini` file for registering StellarProtect agents to a specific group via StellarOne.

Procedure

1. Go to **Administration** > **Downloads/Updates**.
2. Under the **StellarOne** tab:
   - To start the component update for StellarOne immediately, click the **Update Now** button under **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.
- Users can refer to the **Last Updated:** next to the **Update Now** button for the last time the scan component was updated.

- To schedule for the component update, click the toggle **Schedule Update** under the **Scan Component Update Schedule** to enable the function.
  - Click the radio buttons under **Frequency** to set the frequency by **Daily**, **Weekly**, or **Monthly**.

    Important

    Since not every month contains the date 29th, 30th, or 31st, e.g., Feburary only has 28 days (29 days on a leap year), it is recommended to select **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.

  - Click the **Start Time** to determine when to start the scheduled scan component update.
- To specify the download source for StellarOne, click either of the radio buttons under **Scan Component Update Source (StellarOne)**. If users select **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, please select **Other update source** and specify the address in the text field.
- To specify the download source for StellarProtect agents, click either of the radio buttons under **Scan Component Update Source (Agents)**. Users can download the component update source directly from the StellarOne server, or select **Other update source** and specify the address in the text field.

3. Under the **StellarProtect** tab:

   - To download the latest Agent Installer Package for StellarProtect. Click the **Download** button.

     Note

     If the StellarOne and StellarProtect uses proxy for communication, 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 7-18* for detailed procedures.

   - To directly register the StellarProtect agent to a specific group via StellarOne console, click the **download a Group.ini** link and add it into the installer package. Please refer to *Group Mapping on page 7-21* for detailed procedures.

   - To import the patch files for StellarProtect, click the **Import** button to import a patch manually.

   - To remove StellarProtect patch file(s), click the checkbox(es) next to the patch file name(s), and then the **Delete** button appears next to the **Import** button. Click the **Delete** button to remove the selected entries.

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 **StellarProtect** or **StellarProtect (Legacy Mode)** tab according to your target agent type.

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 Firmware and SSL Certificate

This section describes how to import fimware and SSL certificate to the StellarOne web console.

Importing Firmware

Procedure

1. Go to **Administration** > **Firmware**.

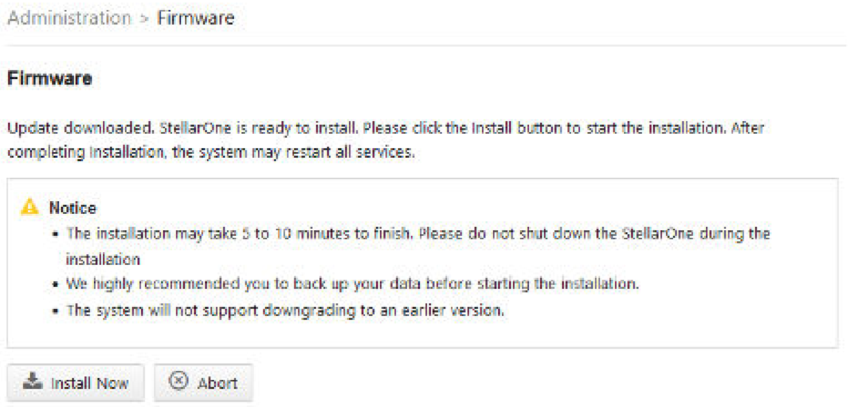
2. Click the **Import** button to import the firmware patch file (e.g. acus.fw_2.0.xxxx.acf) to StellarOne.

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.



Administration > Firmware

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.

FIGURE 7-4. Firmware Update Notice

Importing SSL Certificate

Procedure

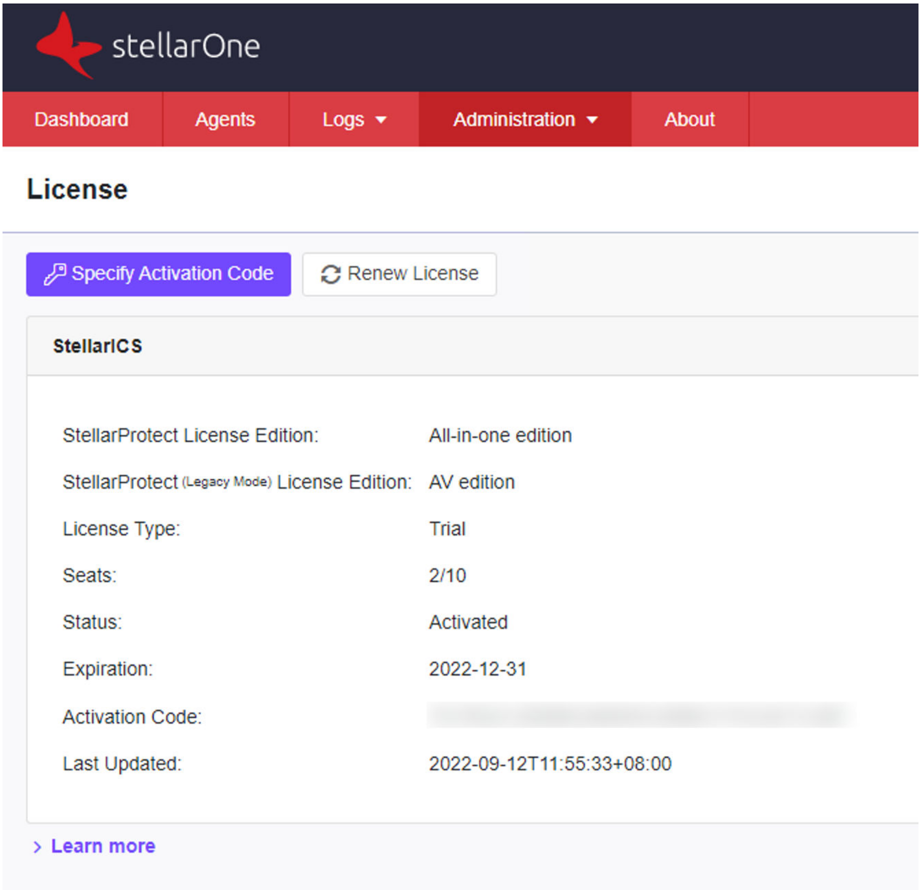
1. Go to **Administration** > **SSL Certificate**.
2. Click **Import Certificate**, and then the **Import Certificate** window appears.
   - Click the **Select file...** next to the **Certificate** option to select the target certificate.
   - Click the **Select file...** next to the **Private Key** option to select the target private key.
   - (Optional) Specify the passphrase in the **Passphrase** text field.
3. Click **Import and Restart** to start importing the target certificate.

Note

Importing the certificate requires restarting the StellarOne console.

License Management

Go to **Administration** > **License** to add or renew licenses for Stellar products. Below table lists details about the **License** page.



StellarProtect License Edition: All-in-one edition

StellarProtect (Legacy Mode) License Edition: AV edition

License Type: Trial

Seats: 2/10

Status: Activated

Expiration: 2022-12-31

Activation Code: [redacted]

Last Updated: 2022-09-12T11:55:33+08:00

FIGURE 7-5. License Page

TABLE 7-4. License Information

ITEM	DESCRIPTION
Specify Activation Code	The button for users to add new activation code.
Renew License	The button for users to renew license after adding new activation code.
License Edition	Displays current license edition for StellarProtect and/or StellarProtect (Legacy Mode). Please refer to *License Editions on page 7-28* for more details.
License Type	• 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	Specifies current number of agents registered to StellarOne and the total number of agents that can be registered to StellarOne. For example, **Seats: 2/10** means: • 2 agents have been registered • Up to 10 agents can be registered
Status	• Activated: The existing license is effective. • Expired: The existing license is out of date. **Note** It is recommended to renew license promptly in order to protect your devices from virus threat. Please refer to *License Activation and Renewal on page 7-27* for license renewal.
Expiration	Displays the effective date of existing license.
Activation Code	The code that is required for activating StellarOne.
Last Updated	Displays the last time the Activation Code is updated.
Learn More	Click the link to go to the online help web page for more license details.

License Activation and Renewal

For users who installs the StellarOne for the first time, please refer to StellarOne Installation Guide for initial license activation. For users who want to renew license, please follow below procedures.

Procedure

1. Go to **Administration** > **License**.
2. If users want to enter a new Activation Code, click the **Specify Activation Code** button.
   a. The **Specify Activation Code** window appears. Input the new Activation Code to renew license for StellarOne console.
   b. Click **Save**.
   c. A message of succesful update will appear.

   Note

   If the update fails, please check if the StellarOne server can connect externally to the TXOne Product License server.
3. If users want to renew license for the existing Activation Code, click the **Renew License** button.
4. The StellarOne will connect to the TXOne Product License server for license renewal.

Change Activation Code

If users need to change the Activation Code, please follow below steps.

Procedure

1. Contact your TXOne sales representative for changing Activation Code.

2. After you receive the new Activation Code, go to **Administration** > **License**, and click **Specify Activation Code** button.

3. Input the new Activation Code and click **Save**.

4. Click **Renew License** to update your product license.

   Note

   It is required to click **Renew License** button for StellarOne console to connect with TXOne Product License Server.

5. A message with **Licenses have been updated successfully** appears. As a result, the **Last Updated** item now shows the date and time the license was updated.

Renew License

If users need to renew license with the same Activation Code, please follow below steps.

Procedure

1. Contact your TXOne sales representative for license renewal request.

2. After the license renewal is confirmed, go to **Administration** > **License**, and click **Renew License** button.

3. A message with **Licenses have been updated successfully** appears. The **Last Updated** item now shows the date and time the license was updated.

License Editions

See below as the three kinds of license editions for the TXOne Stellar version 2.0. 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: • Anti-Virus (Real-Time Malware Scan) • Application Lockdown	Annual
	StellarProtect (Legacy Mode) Agent: • Application Lockdown (with on-demand scanning)	
StellarKiosk	StellarProtect Agent: • Anti-Virus (Real-Time Malware Scan)	Annual **Note** StellarKiosk was named StellarMix before the TXOne Stellar version 2.0.
	StellarProtect (Legacy Mode) Agent: • Application Lockdown (with on-demand scanning)	
StellarOEM	StellarProtect Agent: • Application Lockdown	Perpetual **Note** • StellarOEM provides permanent use and 5-year technical support for the TXOne Stellar. • StellarOEM was named Perpetual before the TXOne Stellar version 2.0.
	StellarProtect (Legacy Mode) Agent: • 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
Next Generation AntiVirus (NGAV)	√	√	-
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	√	√	√

OT Intelligent Trust

When enabled, TXOne OT Intelligent Trust shares anonymous threat information with the Smart Protection Network, allowing TXOne to rapidly indentify and address new threats. You can disable TXOne OT Intelligent Trust anytime through 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, click the **Enable TXOne OT Intelligent Trust (recommended)** toggle to switch it on.

Chapter 8

Technical Support

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

Learn about the following topics:

Troubleshooting Resources

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

Using the Support Portal

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

Procedure

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

Tip

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

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

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

Threat Encyclopedia

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

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

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

Contacting Trend Micro and TXOne

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

TABLE 8-1. Trend Micro Contact Information

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

TABLE 8-2. TXOne Contact Information

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

- Worldwide support offices:

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

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

- Trend Micro product documentation:

  https://docs.trendmicro.com

Speeding Up the Support Call

To improve problem resolution, have the following information available:

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

Sending Suspicious Content to Trend Micro

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

Email Reputation Services

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

https://ers.trendmicro.com/

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

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

File Reputation Services

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

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

Record the case number for tracking purposes.

Web Reputation Services

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

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

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

Other Resources

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

Download Center

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

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

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

Appendix A

Log Descriptions

The following tables provides log descriptions.

Topics in this section include:

StellarProtect Agent Event Log Descriptions

This table details the Windows event log descriptions for StellarProtect.

Event ID	Level	Category	Event Content	Event Details
256	Information	System	Service started	The service has started.
257	Information	System	Policy applied successfully (Version: %version%)	Policy has been applied successfully.
258	Information	System	Patch applied. File Name: %file_name%	Patch has been applied successfully.
259	Information	System	Patching in progress	Patching is in progress. After the earlier-applied patch has been completely updated, the system will automatically try to apply this patch: %deferred_file_name%.
513	Information	intelli_av	ICS Inventory List Update Succeeded	The ICS Inventory List has been updated successfully.
514	Information	intelli_av	Real Time Scan Enabled	The real-time scan is enabled.

Event ID	Level	Category	Event Content	Event Details
515	Information	intelli_av	Scheduled Scan Start	The scheduled scan has started.
516	Information	intelli_av	Scheduled Scan End	The scheduled scan has ended.
517	Information	intelli_av	On-Demand Scan Start	The manually launched scan has started.
518	Information	intelli_av	On-Demand Scan End	The manually launched scan has ended.
519	Information	intelli_av	Scheduled Scan Enabled	The scheduled scan has been enabled. Next scan will be on %NextScan%.
520	Information	intelli_av	Scheduled Scan Disabled	The scheduled scan has been disabled.
768	Information	anomaly_detect	Operations Behavior Anomaly Detection Enabled	Mode: %Mode% Level: %Level%

Event ID	Level	Category	Event Content	Event Details
769	Information	anomaly_detect	Added Operations Behavior Anomaly Detection Approved Operation	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%

Event ID	Level	Category	Event Content	Event Details
770	Information	anomaly_detect	Removed Operations Behavior Anomaly Detection Approved Operation	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%
784	Information	anomaly_detect	DLL Injection Prevention Enabled	The DLL Injection Prevention has been enabled.
1280	Information	device_control	Device Control Enabled	The Device Control has been enabled.
1281	Information	device_control	Trusted USB Device Added	Vendor ID: %HEX % Product ID: %HEX% Serial Number: %STRING% Type: permanent or one time

Event ID	Level	Category	Event Content	Event Details
1282	Information	device_control	Trusted USB Device Removed	Vendor ID: %HEX % Product ID: %HEX% Serial Number: %STRING%
1792	Information	lockdown	File access allowed: %PATH %	Access Image Path: %PATH% Access User: %USERNAME% Mode: %MODE% List: %LIST%
1793	Information	lockdown	Added to Approved List in Maintenance Mode	Path: %PATH% Hash: %SHA256_HEXS TR%
1794	Information	lockdown	Approved List updated in Maintenance Mode	Path: %PATH% Hash: %SHA256_HEXS TR%
1795	Information	lockdown	Approved List initialization started	Approved List initialization started
1796	Information	lockdown	Approved List initialization completed	Approved List initialization completed Count: %COUNT %

Event ID	Level	Category	Event Content	Event Details
1797	Information	lockdown	Application Lockdown enabled	Application Lockdown enabled Mode: %MODE%
1798	Information	lockdown	DLL/Driver Lockdown enabled	DLL/Driver Lockdown enabled
1799	Information	lockdown	Script Lockdown enabled	Script Lockdown enabled
1800	Information	lockdown	Intelligent Runtime Learning enabled	Intelligent Runtime Learning enabled
2048	Information	update	Component update has started.	Component update has started
2049	Information	update	Component update has ended.	Component update has ended.
2050	Information	update	Scheduled component update has been enabled. Next update will be on %NEXT_UPDATE_LOCAL_TIME_STR% (agent's local system time).	Scheduled component update has been enabled. Next update will be on %NEXT_UPDATE_LOCAL_TIME_STR% (agent's local system time).
2051	Information	update	Scheduled component update has been disabled.	Scheduled component update has been disabled.

Event ID	Level	Category	Event Content	Event Details
4352	Warning	system	Service stopped	The service has stopped.
4353	Warning	system	Unable to apply policy (Version: %version%)	The policy can not be applied.
4354	Warning	system	Unable to update file: %dst_path%	Unable to update file. Source Path: %src_path% Destination Path: %dst_path % Error Code: %err_code%
4355	Warning	system	Unable to apply patch. File Name: %file_name%	Unable to apply patch. File Name: %file_name% Error Code: %err_code%

Event ID	Level	Category	Event Content	Event Details
4609	Warning	intelli_av	Incoming Files Scanned, Action Taken by Antivirus: %PATH%	Incoming files were scanned by antivirus. Actions were 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 Content	Event Details
4610	Warning	intelli_av	Incoming Files Scanned, Action Taken by Next-Generation Antivirus: %PATH%	Incoming files were scanned by next-generation antivirus. Actions were 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 Content	Event Details
4611	Warning	intelli_av	Local Files Scanned, Action Taken by Antivirus: %PATH%	Local files were scanned by antivirus. Actions were 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 Content	Event Details
4612	Warning	intelli_av	Local Files Scanned, Action Taken by Next-Generation Antivirus: %PATH%	Local files were scanned by next-generation antivirus. Actions were 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: %PATH %	Suspicious program execution was blocked. File Path: %PATH % File Hash: %STRING%

Event ID	Level	Category	Event Content	Event Details
4614	Warning	intelli_av	Suspicious Program Currently Running: %PATH %	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: %PATH%	Application execution was blocked by antivirus. Target Process: %PATH% File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING%

Event ID	Level	Category	Event Content	Event Details
4617	Warning	intelli_av	Application Execution Blocked By Next-Generation Antivirus: %PATH%	Application execution was blocked by next-generation antivirus. Target Process: %PATH% File Hash: %STRING% Threat Type: %STRING% Threat Name: %STRING%
4864	Warning	anomaly_detect	Operations Behavior Anomaly Detection Disabled	Operations Behavior Anomaly Detection has been disabled.
4865	Warning	anomaly_detect	Process 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%

Event ID	Level	Category	Event Content	Event Details
4866	Warning	anomaly_detect	Process 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%
4880	Warning	anomaly_detect	DLL Injection Prevention Disabled	DLL Injection Prevention has been disabled.
5120	Warning	change_control	ICS File Change Blocked by SafeGuard: %PATH%	ICS files changed to executable files were blocked by SafeGuard. Blocked Process: %PATH% Target File: %PATH%

Event ID	Level	Category	Event Content	Event Details
5121	Warning	change_control	ICS Process Manipulation Blocked by SafeGuard: %PATH%	ICS Process Manipulation was blocked by SafeGuard. Blocked Process: %PATH% Target Process: %PATH%
5376	Warning	device_control	Device Control Disabled	Device Control has been 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%

Event ID	Level	Category	Event Content	Event Details
5888	Warning	lockdown	File access allowed: %PATH %	Access Image Path: %PATH% Access User: %USERNAME% Mode: %MODE% Reason: %ALLOWED_REA SON% File hash allowed: %SHA256_HEXS TR% %THROTTLING_I NFO_MSG%
5889	Warning	lockdown	File access blocked: %PATH %	Access Image Path: %PATH% Access User: %USERNAME% Mode: %MODE% Reason: %BLOCKED_REA SON% File hash blocked: %SHA256_HEXS TR% %THROTTLING_I NFO_MSG%
5890	Warning	lockdown	Unable to add to or update Approved List: %PATH%	Unable to add to or update Approved List: %PATH%

Event ID	Level	Category	Event Content	Event Details
5891	Warning	lockdown	Application Lockdown disabled	Application Lockdown disabled
5892	Warning	lockdown	DLL/Driver Lockdown disabled	DLL/Driver Lockdown disabled
5893	Warning	lockdown	Script Lockdown disabled	Script Lockdown disabled
5894	Warning	lockdown	Intelligent Runtime Learning disabled	Intelligent Runtime Learning disabled
5895	Warning	lockdown	Approved List initialization canceled	Approved List initialization canceled
8706	Critical	intelli_av	Real Time Scan Disabled	The Real-Time Scan has been disabled.
9216	Critical	change_control	Maintenance Mode Start	The Maintenance Mode has started.
9217	Critical	change_control	Maintenance Mode End	The Maintenance Mode has ended.

StellarProtect Server Event Log Descriptions

This table lists the server event log descriptions for StellarProtect.

ID	Content
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 scheduled pattern update Modify schedule update setting**s** 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 Change Window> to agents
33107	Send protection command <Scan Now> to agents

ID	Content
33108	Send protection command <Update Component> to agents
33109	Send protection command <Apply Patch> to agents
33110	Send protection command <Initialize Lockdown Approved List> 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

StellarOne Server Event Log Descriptions

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

ID	Content
45322	Scan component [%s] update failed due to unable to connect to the network
45323	Customize policy
45324	Inherit policy from [%s]

Appendix B

Syslog Content - CEF

The following tables map syslog content between StellarOne log output and CEF syslog types.

Topics in this section includes:

- *Agent Event Format on page B-2*
- *StellarProtect Server Event Format on page B-5*
- *StellarOne Server Event Format on page B-6*

Agent Event Format

Please refer to below table as StellarProtect's agent events in the Common Event Format.

Table B-1. 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
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	Jan 02 2006 15:04:05 GMT +00:00
msg	<string>	

CEF Field Name	Description	Possible Values
category	OPTION: 0 SYSTEM: 1 INTELLI_AV: 2 ANOMALY_DETECT: 3 CHANGE_CONTROL: 4 DEVICE_CONTROL: 5 MISC: 15	
agentEndpoint	<string>	
agentIp	<string>	
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>	

CEF Field Name	Description	Possible Values
obadLevel	<string>	
accessUser	e	
processId	<string>	
parentProcess1	<string>	
parentProcess2	<string>	
parentProcess3	<string>	
parentProcess4	<string>	
targetArguments	<string>	
parentArguments1	<string>	
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>	

CEF Field Name	Description	Possible Values
type	<string>	

StellarProtect Server Event Format

Please refer to below table as StellarProtect's server events in the Common Event Format.

Table B-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	2.0
Device Event Class ID	Event ID	{}
Name	Event category	Server Event
Severity	LOG_INFO: 6	{6}
Extension		
eventTime	StellarProtect format	Jan 02 2006 15:04:05 GMT +00:00
msg	<string>	
userName	<string>	
userRole	<string>	
clientIp	<string>	

StellarOne Server Event Format

Please refer to below table as StellarOne's server events in the Common Event Format.

Table B-3. StellarOne 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	StellarOne
Device Version	Device Version	2.0
Device Event Class ID	Event ID	{}
Name	Event category	Console Log
Severity	LOG_INFO: 6	{6}
Extension		
eventTime	StellarOne format	Jan 02 2006 15:04:05 GMT +00:00
msg	<string>	
userName	<string>	
userRole	<string>	
clientIp	<string>	
status	UNSPECIFIED: 0 AU_SUCCESS: 1 AU_FAIL: 2	{0, 1, 2}
product	<string>	{protect}

Index

txOne
networks

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

www.txone.com

Item Code: APEM29594/220907